الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جـــامعة عبد الحميد إبن باديس - مستغانم
كليــة الحقوق والعلوم السياسية
قسم القانون العام

أطروحة مقدمة ضمن متطلبات نيـل شهـادة الدكتوراه علوم في الحقوق

تـــخصص: قانون جنائي

تـحـت عـــنوان:

الـمسؤولية الجنائية للمجرم الـمعلوماتي

دراسة تأصيلية موضوعية في التشريع الجزائري والمقارن

مـن إعداد الطالب:
– بن أحمد محمد

إشـــراف الأستاذ الدكتور:
– عـــباسة طـــاهـر

وقد نوقشت هذه الأطروحة في جلسة علنية بتاريخ 2022/03/22

أعضاء لجنة المناقشة				
الرقم	الإسم واللقب	الرتبة	المؤسسة الجامعية	الصفة
1	حيتالة معمر	أستاذ	جامعة مستغانم	رئيسًا
2	عباسة طاهر	أستاذ	جامعة مستغانم	مشرفًا ومقررًا
3	محمد كريم نور الدين	أستاذ محاضر "أ"	جامعة مستغانم	عضوًا
4	فرعون محمد	أستاذ محاضر "أ"	جامعة سيدي بلعباس	عضوًا
5	مبطوش الحاج	أستاذ	جامعة تيارت	عضوًا
6	منقور قويدر	أستاذ محاضر "أ"	جامعة غليزان	عضوًا

السنة الـــجامعية: 2021-2022

بسم الله الرحمن الرحيم

أعوذ بالله من الشيطان الرجيم

بسم الله الرحمن الرحيم

﴿ يَا مَعْشَرَ الْجِنِّ وَالْإِنْسِ إِنِ اسْتَطَعْتُمْ أَنْ تَنْفُذُوا مِنْ أَقْطَارِ

السَّمَاوَاتِ وَالْأَرْضِ فَانْفُذُوا لَا تَنْفُذُونَ إِلَّا بِسُلْطَانٍ ﴾

سورة الرحمن الآية (33)

شكر وعرفان

أعوذ بالله من الشيطان الرجيم

بسم الله الرحمن الرحيم

﴿ . . . رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ ﴾ صدق الله العظيم

فالحمد لله والشكر لله إبتداءً وإنتهاءً . . . أحمد الله وأسجد له شاكرًا على حسن توفيقه وكريم عونه على إنجاز هذا العمل بفضله وجوده وكرمه، . . . والصلاة والسلام على أشرف المرسلين سيدنا ومولانا محمد الأمين صلى الله عليه وسلم وعلى آله وصحبه أجمعين .

فالشكر هو الظل الظليل، والكلمة الطيبة التي يتفيء تحتها الإنسان حينما يثقل كاهل واجب المعروف وعظيم الإحسان . . . وإذا كان الإعتراف بالحق فضيلة . . . فإن إسداء الشكر لمن يستحقه فريضة . . . لذا أجده لزامًا علي أن أسطر بقلمي وأتلو بلساني أسمى عبارات الشكر والعرفان إلى كل أعضاء هيئة المناقشة الموقرة .

- فأتوجه بخالص آيات الشكر والتقدير والعرفان لفضيلة الأستاذ الدكتور "**عباسة طاهر**"، الذي شرفني بقبول سيادته الإشراف على هذه الأطروحة، ومنحني من علمه ووقته، وعلى ما قدَّمه لي من نصح صادق، فكانت جلساتي معه ثرية وغنية من فيض ثقافته القانونية الغزيرة، فجزاه الله عني وعن كل طلاب العلم أعظم الجزاء .

- ومن يمن الطالع ومن دواعي الغبطة والسرور، أتقدم بعاطر الشكر والثناء إلى فضيلة الأستاذ الدكتور "**حيتالة معمر**" بتفضل سيادته رئاسة لجنة المناقشة، فهو شرف للبحث وللباحث، فجزاه الله عن العلم وأهله خير الجزاء .

- كما أتوجه بالشكر الجزيل وخالص تقديري وإمتناني إلى فضيلة الأستاذ الدكتور "**محمد كريم نور الدين**" لتفضل سيادته بقبول الإشتراك في عضوية لجنة المناقشة، فله مني جزيل الشكر وعظيم التقدير .

- وأيضاً لا يسعني في هذا المقام إلاّ أن أتوجه بأسمى عبارات الشكر والتقدير إلى فضيلة الأستاذ الدكتور "**فرعون محمد**"، وإنه لفخر كبير وشرف عظيم بقبول سيادته المشاركة في عضوية لجنة المناقشة، فجزاه الله عني خير الجزاء .

- وبالحب المخلص الذي لا حدّ له، وبالعرفان والشكر العظيم أتقدم إلى فضيلة الأستاذ الدكتور "**مبطوش الحاج**" على قبول سيادته الجلوس في عضوية لجنة المناقشة، فجزاه الله عنا وعن العلم خير الجزاء .

- كما يطيب لي في هذا المقام، أن أسدي عميق شكري وتقديري وعظيم المودة والإمتنان لفضيلة الأستاذ الدكتور "**منقور قويدر**" لتفضل سيادته قبول المشاركة في عضوية لجنة المناقشة، فله مني جزيل الشكر وعظيم التقدير .

كما لا يفوتني في هذا المقام أن أتقدم بالشكر والثناء العميقين، إلى وطني العزيز الجزائر سائلاً الله عز وجل أن يحفظ بلادي ويمنّ عليها بنعمة الأمن والأمان.

ومن هذا المنبر أقف أيضاً وقفة إجلال وإحترام لجامعة عبد الحميد إبن باديس هذا الصّرح العلمي المتميز، وأخصُّ بالذكر كلية الحقوق والعلوم السياسية عِمادةً وإدارةً على ما قدمته وتقدمه لأبنائها الطلبة من علمٍ ومعرفةٍ . . .

وفي الأخير أتوجه بالشكر والتقدير إلى مصلحة ما بعد التدرج بهذه الكلية عمالاً وموظفين على كل ما بذلوه لأجلنا فبارك الله لهم جميعاً في عمرهم وولدهم، ومتعتهم بدوام الصحة والعافية . . . **اللهم آمين**

إهداء

أحمد الله عز وجلّ أن وفقني لإتمام أطروحة الدكتوراه بغير حول مني ولا قوة فللّه وحده الحمد والمشيئة.

إلى أمي الحبيبة . . .إلى أبي الغالي . . . حفظهما الله ورعاهما بلطفه وكرمه وأطال في عمرهما وأرضاهما عني في الدنيا والآخرة.

إلى كل إخوتي الأكارم وأخواتي الكريمات

وكل أبنائهم

أخص بالذكر أخي عابد رشيد

إلى كل من ساعدني أهدي عملي هذا

بن أحمد محمد

لائـــحة الـــــمختصرات

المختصرات العربية

(ص)	صفحة
(ط)	طبعة
(ع)	عدد
(ج)	جزء
(ج)	جلسة
(س)	سنة
(ق)	قانون
(ف)	فقرة
(م)	مادة
(مج)	مجموعة
(س. ق)	سنة قضائية
(ج. ر)	جريدة رسمية
(م. ق. ق)	مجموعة القواعد القانونية
(ق. ع. ج)	قانون العقوبات الجزائري
(ق.ع. ف)	قانون العقوبات الفرنسي
(ق. ع. م)	قانون العقوبات المصري
(ق. إ. ج. ج)	قانون الإجراءات الجزائية الجزائري
(ق.م. ج)	القانون المدني الجزائري
(د. د. ن)	دون دار نشر
(د. ت. ن)	دون تاريخ نشر
(ق. م. ن. م)	قرار محكمة النقض المصرية
(ق. م. ع. ج)	قرار المحكمة العليا الجزائرية
(ق. م. د. ف)	قرار مجلس الدولة الفرنسي
(مج.أ.ن)	مجموعة أحكام النقض
(إ.أ.م.إ.م)	الإتفاقية الأروبية لمكافحة الإجرام المعلوماتي
(إ.ع.م.ج.ت.م)	الإتفاقية العربية لمكافحة جرائم تقنية المعلومات
(ق.م.د)	قرار المجلس الدستوري

المختصرات الفرنسية

(P)	***Page***
(S)	***Sirey***
(V)	***Voir***
(N°)	***Numéro***
(D)	***Dalloz***
(VOL)	***Volume***
(ART)	***Article***
(Ed)	***Edition***
(Cass)	***Cassation***
(Crim)	***Criminel***
(Obs)	***Observation***
(Op. Cit)	***Ouvrage précité***
(P.U.F)	***Presses universitaires France***
(Chron)	***Chronique***
(C.P.F)	***Code pénal français***
(Ord)	***Ordonnance***
(D.C.E.E.N)	***Droit du commerce électronique et de l'économie numérique***
(J.O.R.F)	***Journal officiel république française***
(Cass. Crim)	***Cassation criminelle***
(Bull)	***Bulletin***
(J.C.P)	***Juje des contentieux de la protection***
(C.A)	***Cour d'Appel***
(C.C.C.C)	***Cour de cassation, chambre criminelle***
(S.J.G)	***La semaine juridique générale***
(ISO)	***Organisation internationale de normalisation***
(ISP)	***Internet service provider***
(ASTD)	***Des atteintes aux systèmes de traitement automatisé de données***
(D.C.E.E.N)	***Droit du commerce électronique et de l'économie numérique***

المختصرات الإنجليزية:

Net	***Network***
Inter	***International***
W.S	***Work Station***
H.W	***Hard Ware***
S.W	***Soft War***
P.C	***Portable computer***
I.P	***Internet Protocol***
L.A.N	***Local Area Network***
W.A.N	***Wide Area Network***
P.D.N	***Public data Network***
T.C.P	***Transmission control protocol***
I.S.O	***International Organization for Standardization***
I.S.O.C	***Internet Society***
ITU	***International telecommunication union***
CPU	***Units processing central***
RAM	***Memory Access Armdom***
NCP	***Network Control Protocol***
ICT	***Information and Communications Technology***

مُقَدِّمَة

الجريمة مرتبطة بالإنسان وجودًا وعدمًا، تطورًا وتخلفًا، والإنسان مرتبط بالمجتمع فاعلاً ومنفعلاً، وكما أن الصلة وطيدة بين الجريمة والمجتمع فإن الصلة أيضًا وطيدة بين تطور المجتمع الحضاري والعلمي والتكنولوجي من ناحية وتطور الجريمة من ناحية أخرى، وقد تكون تلك الصلة مثيرة للدهشة، ولكن سرعان ما تكشف هذه الدهشة ستارها عندما نعلم أن تطور المجتمع وما يصاحبه من تطور علمي وتكنولوجي ينعكس أثره على تطور الجريمة والمجرمين، فالجريمة بإعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تقدم وتطور، بمعنى أن أقصى ما يصل إليه المجرم من براعة ودراية نتيجة لهذه الثقافات والتعاليم يحاول جاهدًا إستخدامها في جريمته، فالجريمة هي محصلة كل ذلك.

والإنسان بما حباه الله تعالى من علم ليفجر به الثورة التكنولوجية الحالية، فإنه لم يقف عند جني الثمار الإيجابية لهذه الثورة وإنعكاساتها المختلفة في مناحي الحياة، وإنما إستغلها بمكره السيء في إكتشاف العديد من الأساليب الإجرامية العديدة والجديدة التي سهلت له إرتكاب هذا النوع من الإجرام.

ولا يخفى على أحد أن العصر الحديث وما أحدثته العولمة من كينونة العالم قرية صغيرة كانت دون شك عوامل شديدة التأثير على القانون والسياسة التشريعية في الدول المختلفة، بل كان لها الأثر الكبير على السياسة الجنائية التي يتبعها المشرع الجنائي في العالم ككل، ولذلك كله كان ولابد من مجاراة هذه العولمة وخلق سياسة تشريعية سريعة وحديثة ومتطورة حسب هذا التطور الهائل الذي يشهده الإنسان من ناحية، وللحفاظ على المجتمع من الإنهيار من ناحية أخرى.

ومع مجيئ ثورة المعلومات فُرِضَ على العالم تحديات كثيرة ولَّدها التطور الهائل العلمي والتكنولوجي، وحيث ترتب على هذه الثورة الهائلة في مجال تكنولوجيا المعلومات والإتصالات لاسيما الحديثة منها، أن أصبح العالم يعيش حياة زاخرة بالإتصالات السريعة ونقل المعلومات عبر المسافات البعيدة، والتحاور مع قواعد البيانات المحلية والعالمية، والتعامل مع نظم إلكترونية تقوم على الخبرة والذكاء الإصطناعي، كل هذا ما كان يمكن له أن يتحقق إلاَّ بوجود هذا الشيء الرائع المتمثل في جهاز الحاسب الآلي، والذي تزيد أهميته وتتجلى قدرته الفائقة عند إرتباطه بشبكات التواصل كالإنترنت فأصبحت فيه المعلومات معيار تقدم الشعوب وتخلفها، ومع تطور الحاسبات الآلية وربطها بشبكات التواصل الإجتماعية المختلفة، كل هذا أدى إلى ظهور ما يسمى "بنظم

المعلوماتية" وما لها من قيمة مادية ومعنوية، وإزداد شغف الحصول على المعلومات أيًا كان نوعها إلى بروز مشاكل جديدة ومختلفة تمامًا عما كان يعيشه الإنسان من قبل.

من هنا تأثرت الجريمة تأثرًا كبيرًا بالتطور الهائل الذي عرفه الإنسان وما يصاحبه يوميًا من تكنولوجيا جد متطورة، فتزايدت معها أصناف الجرائم وأعداد المجرمين المستخدمين لهذه التكنولوجيا لاسيما خلال السنوات العشر الأخيرة، الأمر الذي أدى إلى الإهتمام التشريعي بهذه الجرائم ومرتكبيها.

أهمية موضوع الدراسة:

تنبع أهمية هذه الدراسة من حداثة الموضوع، فهو معاصر وحيوي بالنسبة للباحثين، حيث تعد الجرائم المعلوماتية من أكبر التحديات التي نواجهها في وقتنا الحاضر، وهذه الجرائم تثير العديد من المشكلات القانونية والعملية، والتي يسميها البعض بالمشكلات الموضوعية لقانون العقوبات وكذا النصوص القانونية الخاصة والمكملة له في مواجهة هذا النوع من الإجرام.

وتعد الجرائم المعلوماتية – الإلكترونية – نوعًا مستحدثًا من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب، لذا فإن هذا النوع من الجرائم يثير مشكلات قانونية هامة لاسيما من الناحية الموضوعية، وهذه المشكلات ترتبط بدورها بصور عديدة من الإجرام المعلوماتي التي وضح المشرع الجزائري وكذا المقارن البنيان القانوني لها وتحديد أهم معالمها وهذا من خلال تعديل قانون العقوبات.

وترجع أهمية دراسة موضوع الجرائم الإلكترونية أو المعلوماتية إلى الإنتشار الواسع لوسائل التقنية من جهة وإلى إزدياد هذا النوع من الجرائم من جهة أخرى، والذي أصبح يتماشى جنب إلى جنب مع الإستخدام الواسع للتعاملات والخدمات الإلكترونية، وكذا عصرنة جميع القطاعات الحكومية وغير الحكومية على مختلف الأصعدة الدولية والإقليمية والوطنية، فأصبحت الجريمة المعلوماتية متلازمة مع التطور السريع والهائل في مجال تكنولوجيا الإتصالات والمعلومات، وهذا كل نتيجة للتقدم الكبير في إستخدامات الشبكة العالمية للإتصالات والمعلومات، الأمر الذي جعل من هذه الجرائم بصورها المختلفة تهدد الأمن المعلوماتي للأفراد والمؤسسات والحكومات.

وغنيٌ عن البيان أن العديد من دول العالم قد تنبهت لخطورة هذا الأمر، فوضعت تشريعات جنائية التي كفلت الحفاظ على المصالح الخاصة والعامة وتقريرها وحمايتها، حيث لم تكتفي بالقواعد العامة في قانون العقوبات لتنظيم هذه المسألة بل أفردت لها قوانين مستقلة ومتكاملة مما يؤدي إلى تحقيق الأهداف التي تسعى إليها الدول بما يتفق وإطار السياسات الجنائية الحديثة.

ولا يخفى على أحد أن نمو جرائم الحاسوب والإنترنت أصبح يزداد يومًا بعد يوم حتى وصلت إلى الحد الذي يمكن معه القول بأن إيقافها أو حتى الحد منها غَدَا أمرًا صعبًا، وأمام هذا النمو الهائل لِكَم الجرائم المعلوماتية وأنواعها وأساليب إرتكابها، فقد وجد المهتمون بالقانون الجنائي أنفسهم في مأزق أمام عدم جدوى كثير النصوص بالتصدي لهذه الجريمة ومجابهتها. ولأهمية موضوع هذه الجريمة محل الدراسة أدى ذلك إلى حدوث ثورة في العلوم الجنائية ككل؛ حيث وقف كل من الفقه والقانون في هذا المجال حائرين أمام التطور الهائل لعدد الجرائم المعلوماتية وجسامتها وخطورتها.

كما تكمن أهمية هذه الدراسة في محاولة إيجاد الحلول التشريعية لمكافحة الجرائم المعلوماتية بوصفها جرائم إرتبطت بالتقنية الحديثة، فالحاسب الآلي وشبكة الإنترنت يجتاحان عالمنا المعاصر بسرعة لامتناهية، وهذا بسبب التطور الهائل في ثورة المعرفة المعلوماتية، حيث صاحب هذا التطور تدخل عديد الدراسات والقوانين والإجتهادات الفقهية في إعادة النظر في جميع المسائل السلبية المترتبة عن هذا التطور، لذا كان على المشرع التدخل بقوة لإحتوائها.

لذا فإن أهمية القيام بهذه الدراسة تدور حول الدور الذي تلعبه التشريعات الجنائية الدولية والوطنية المقارنة في مكافحة هذه الجريمة، ومدى قدرتها في منع إنتشار هذه الظاهرة التي تفشت بقوة في الآونة الأخيرة وتسارع نموها.

أهداف موضوع الدراسة:

تهدف هذه الدراسة بشكل مخصص إلى معالجة جملة من الأهداف أهمها:

- التعريف بالجريمة المعلوماتية وتحديد أهم خصائصها المميزة لها ودراسة أنواعها وطبيعتها القانونية، مع الإشارة إلى المخاطر المترتبة عليها.

– كما تهدف هذه الدراسة إلى التعرف على مصطلح الجريمة المعلوماتية ومفارقتها ببعض المصطلحات المشابهة لها والتي توضح مدى خطورة هذه الظاهرة الإجرامية على الفرد والمجتمع على سواء.

– البحث عن أهم التوجهات الجنائية الحديثة في مجال مكافحة الإجرام المعلوماتي، ومدى كفاية القوانين الحالية في مواجهة هذا النوع المستجد من الجرائم.

– تسليط الضوء على أبعاد ظاهرة الإجرام المعلوماتي، ودور القوانين العقابية الوطنية والمقارنة في إحتواء كل من الجريمة والمجرم.

ولتحقيق الأهداف المرجوة من هذه الدراسة إرتأينا ما يلي:

– وضع الإطار المفاهيمي العام لكل من الجريمة المعلوماتية وطبيعتها القانونية، وكذا المجرم المعلوماتي ودوافعه الإجرامية.

– تسليط الضوء على الجانب الموضوعي في قيام وتحديد المسؤولية الجنائية للمجرم المعلوماتي.

– التعرف على أهم المعاملات الإلكترونية والإطلاع على حجم التطور الذي وصلت إليه.

– التعرف على أهم الجرائم المعلوماتية التي تصاحب هذه المعاملات الإلكترونية، وعلى أهم مسببات تفشيها وعلى حجم الخسائر التي قد تحدثها.

– إبراز دور قانون العقوبات والقوانين المكملة له في التدخل للتصدي لهذا النوع من الجرائم في كل من التشريع الوطني والمقارن.

– الإطلاع على أهم ما كتب حول الجريمة المستحدثة بصفة عامة والجريمة المعلوماتية بصفة خاصة.

– تحديد أهم أنواع الجرائم المعلوماتية التي ترتكب باستخدام التقنية الحديثة.

– تبيان خطورة الجريمة المعلوماتية وضرورة التصدي لها.

أسباب إختيار موضوع الدراسة:

يأتي وراء إختيار هذا الموضوع عدة أسباب أهمها:

– ندرة الدراسات القانونية في هذا الموضوع لاسيما في المكتبات الجزائرية، فنكاد لا نجد دراسة قانونية متكاملة في الكتابات الأكاديمية حول موضوع الجرائم المعلوماتية ومن ضمنها عنوان هذه الأطروحة "المسؤولية الجنائية للمجرم المعلوماتي" والتي ما زالت في بداياتها، والمكتبات الجامعية

بحاجة إلى كتب وبحوث تتناول مثل هذه المواضيع المعاصرة والمهمة. إضافة إلى ميول الباحث إلى مثل هذه الدراسات وبتشجيع من المشرف على هذه الأطروحة، أن نكتب سويًا في موضوع جنائي فقهي معاصر لم يأخذ حظه من البحث والدراسة، فتم الإتفاق على القدم في الخوض في غمار هذا الموضوع.

– من أهم أسباب إختيار هذا الموضوع أيضًا هو التعرف عن قرب في هذه الظاهرة الإجرامية المستحدثة وفي كل ما تحتويه من ظواهر إجارمية مختلفة، ومعرفة أهم الوسائل التشريعية التي أقرتها الدول لمواجهتها، ومدى فاعلية تلك الوسائل في تحقيق الحماية الجنائية المطلوبة للحاسبات الآلية وما تحتويه من برامج ومعلومات، ضف إلى ذلك حداثة الجريمة المعلوماتية في المجتمع وتأثيرها بشكل كبير على فئة معينة من الأفراد، الأمر الذي يمثل تهديدًا جديدًا للأمن القومي داخل المجتمع.

– رغبة الباحث في دراسة خبايا هذا الموضوع وذلك من خلال الوقوف على أحكام المسؤولية الجنائية للمجرم المعلوماتي بالتفصيل وبيان نجاعتها، على الرغم من أن المشرع الجزائري لم يقر بوضوح عن قانون خاص لمواجهة الإجرام المعلوماتي، مع وجود قانون العقوبات الذي تحدث في ذلك دون توسع.

حدود الدراسة:

إن التعامل مع هذه الدراسة في مثل هكذا مواضيع ليس بالأمر الهين، لذلك كان لابد علينا التركيز على مجموعة من المحددات حتى لا نخرج عن حدود هذه الدراسة والتي تتمثل في الآتي:

– حُددت هذه الدراسة في الإعتماد على الجانب الموضوعي لتقرير المسؤولية الجنائية للمجرم المعلوماتي، وذلك من خلال مسايرة قانون العقوبات لمثل هذه الجرائم وكذا بعض القوانين المكملة له سواء على مستوى التشريع الوطني أو المقارن.

– بما أن هذه الدراسة تدخل في حدود ومجال القانون الجنائي لذلك فلن نتناول بالتفصيل الجانب التقني والفني للحواسيب والإنترنت، وسوف نقتصر فقط على ما يصلح لموضوعنا من الدراسات الإلكترونية والمعلوماتية.

– أيضًا من محددات هذه الدراسة سوف يكون التشريع الجنائي الجزائري الأساس الذي نعتمد عليه في دراستنا هذه إلى جانب كل من التشريع الفرنسي والتشريع المصري، كما يمكن الإستعانة ببعض

التشريعات الجنائية المقارنة في المجال المعلوماتي عربية كانت أم غربية، خاصة التي تميزت قوانينها ببعض المفاهيم وتفردت في مواضيع معينة.

– كما سوف نتناول أهم الآراء الفقهية والأحكام القضائية المتعلقة بالجرائم المعلوماتية ومدى قبولها أو رفضها لموضوع المسؤولية الجنائية للمجرم المعلوماتي سواء في الجزائر أو دول أخرى.

فرضيات الدراسة:

سوف تقوم هذه الدراسة على مجموعة من الفرضيات الرئيسية وذلك على النحو التالي:

– إن الطبيعة القانونية الخاصة للمسؤولية الجنائية في مثل هذه الجرائم تتطلب الخروج على الأحكام العامة لقانون العقوبات، وأن أحكام المسؤولية فيها وعناصرها تختلف عن المسؤولية في باقي الجرائم التقليدية، وأن هذا الخروج على الأحكام العامة يحمل معه العديد من النقاط الضرورية والمستجدة وهذا حتى يجاري قانون العقوبات التطور الحاصل والتسارع الموجود في مناحي الحياة المختلفة، وإحتوائه على جميع الأفعال والسلوكيات التي يستنكرها المجتمع حتى وإن كانت حديثة وغير مألوفة.

– إن مصلحة المجتمع في الحفاظ على كيانه من أي عبث أو تخريب تقتضي بالضرورة وضع أحكام خاصة لهذا النوع من المسؤولية، لاسيما تحديد مسؤولية الشخص المعنوي الجزائية عند إرتكابه مثل هذه الجرائم موضوع الدراسة، بل يجب أن يكون تحديد هذه المسؤولية أكثر إنضباطًا ووفق مجموعة من الأسس التي تحددها وتنظمها، وهذا حتى تتوافق مع التفكير الإنساني المتطور دائمًا.

– فهذه الدراسة سوف تقوم ببيان صحة هذه الفرضيات أو عدم صحتها دون أن نحمل في طيات نفوسنا أي قرار مسبق أو متسرع، وذلك كله سعيًا وراء أن تكون دراستنا موضوعية محققة لأفضل الأهداف الممكنة، وقدر جهدنا البشري الذي لا يخلو من النقص والخطأ، فقد نصيب وقد نخطئ.

صعوبات الدراسة:

لقد واجه الباحث العديد من الصعوبات في مراحل إعداد هذه الدراسة، وفي الواقع أن الصعوبات التي يمكن أن يقابلها أي باحث في مثل هذه المواضيع لا تحصى فهو موضوع جديد لاسيما في الدراسات المتعلقة بالقانون الجنائي، ولعل أهم الصعوبات التي واجهت الباحث نجد ما يلي:

– حداثة هذا الموضوع نسبيًا وأيضًا الإشكاليات الكثيرة التي تكتسيه، لذا كان لابد علينا من الوقوف على أهم التشريعات التي تم إصدارها مؤخرًا في مكافحة الإجرام المعلوماتي ودراستها دراسة تحليلية ومقارنتها ببعض الكتب الفقهية الحديثة، ناهيك عن الصعوبة أيضًا في التواصل ببعض الأساتذة المتخصصين في المجال المعلوماتي.

– صعوبة المصطلحات العلمية الخاصة بتكنولوجيا الحواسيب الآلية والتقنية الحديثة، ويرجع ذلك لجدة تلك المصطلحات على اللغة العربية من جهة، وعلى النصوص القانونية من جهة أخرى، ناهيك على قلة المراجع القانونية المتخصصة في هذا الشأن لاسيما في الكتابات الأكاديمية الجزائرية، وكذا ندرة الدراسات الإحصائية الدقيقة وإن وجدت فصعوبة الوصول إليها، بالإضافة إلى أنه مجال تكنولوجي بإمتياز وجديد بالنسبة للدراسات المتعلقة بالقانون الجنائي.

إشكالية الدراسة:

تتلخص مشكلة أو إشكالية الدراسة في أن القانون الجزائري لم ينص على كافة أشكال الإجرام المعلوماتي، فإذا ما جئنا على قانون العقوبات نجده لم يعالج هذا النوع من الجرائم بشكل دقيق وموسع.

وعليه نطرح الإشكاليات التالية:

- **هل أن قانون العقوبات يمثل فعلاً الشريعة العامة في الحقل الجنائي لكل القوانين الخاصة والمكملة له؟ أم أنَّ هذا القانون يبقى قاصرًا في بعض الأحيان على إحتواء بعض الأفعال الإجرامية المستحدثة؟ وما مدى كفاية النصوص الموضوعية الحالية في قانون العقوبات الجزائري والقوانين المكملة له لمواجهة الجريمة المعلوماتية؟**
- **هل فعلاً أدركت التشريعات الوطنية سواءً في الجزائر وكذا التشريعات المقارنة على السواء حقيقة الجريمة المعلوماتية؟ وهل أفردت لها نصوص عامة وخاصة لضبط كل التعاملات الإلكترونية بما يضمن حماية كافية للنظام المعلوماتي ككل؟**
- **ما مدى وفرة الأحكام والقواعد الجنائية العامة والخاصة في تقرير المسؤولية الجنائية للمجرم المعلوماتي؟ وهل يحتاج الأمر إلى رؤية جديدة وقانون جديد؟ أم أن الأمر يبدو عسيرًا في ظل التقنيات المتطورة في الوقت الراهن؟**

منهجية الدراسة:

إن كل باحث ومن أجل الوصول لإجابة شافية ووافية ولا ربما متكاملة الأركان وهذا من خلال الأسئلة التي دارت حولها الدراسة والتي كونت في الأساس مشكلة البحث، من هذا كله كان ولابد من إتباع منهجًا علميًا أكاديميًا، يتبعه الباحث خطوة تلو الأخرى للوصول إلى نهاية طريقه في هذا البحث الطويل، وكذا الوصول إلى أفضل النتائج المتحصل عليها.

ومنهجنا في هذه الدراسة سوف يجمع أكثر من أسلوب من أساليب المنهج العلمي الأكاديمي حيث إعتمدنا في دراستنا هذه على المنهج الوصفي وكذا المنهج التحليلي كأساس في البحث، بالإضافة إلى الإستعانة بالمنهج المقارن كمنهج مساعد كلما إقتضت الضرورة ذلك، كما لا يُغْنينا الحال عن الإستعانة بأي منهج علمي آخر نراه ضروري في هذه الدراسة كالمنهج التاريخي والمنهج الإستقرائي.

فمنهجنا في هذه الدراسة يجمع بين أكثر من أسلوب منهجي وهم على النحو التالي:

- أسلوب المنهج الوصفي: حيث أننا سوف نبدأ هذه الدراسة بالوصف الدقيق نوعًا ما لما هو عليه الوضع في مفهوم الإجرام المعلوماتي والمراحل المختلفة التي مر بها، حتى نكون كالمصدر الذي يعطي صورة صحيحة الملامح عن حقيقة هذا الموضوع الأكاديمي والإجتماعي.
- أسلوب المنهج التحليلي: فبعد أن نوصف ونوضح هذا الموضوع، نعمد مجددًا إلى تحليل أهم النصوص القانونية والوقوف على المراد منها نصًا وروحًا، مسترشدين برأي كل من الفقه والقضاء المقارنين.
- أسلوب المنهج المقارن: وبعد الوصف والتحليل سوف نعتمد على أهم القوانين المقارنة التي تناولت هذا الموضوع، بما فيها الدراسات الفقهية المقارنة التي سبقتنا زماناً ومكاناً إلى مثل هذا الموضوع، لاسيما فيما يخص القواعد الموضوعية الخاصة بالجريمة المعلوماتية والمجرم المعلوماتي.
- أسلوب المنهج التاريخي: وهو تتبع السنوات والتواريخ التي مرت بها هذه الجريمة المعلوماتية وذلك بالإستناد على العديد من المراجع والمصادر العامة منها والخاصة الفقهية والقانونية، وحتى المقالات المنشورة في المجلات والمواقع الإلكترونية، وهذا من أجل تأصيل موضوع الدراسة.

ولعل الهدف الذي يرمي إليه الباحث من خلال إتباع هذه المناهج العلمية المختلفة هو وجود تشريع جنائي عقابيي عصري يضاهي التشريعات العالمية في مجال الإجرام المعلوماتي، وكذا الخروج منها برؤية قانونية مفادها تحديد المسؤولية الجنائية للمجرم المعلوماتي كدراسة تأصيلية موضوعية في كل من التشريع الجزائري والمقارن.

نطاق هيكلة الدراسة:

تعتمد هذه الدراسة من حيث هيكلها العام على الشكل التالي:

الباب التمهيدي: ماهية الجريمة المعلوماتية وتحديد طبيعتها القانونية.

الباب الأول: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي.

الباب الثاني: جرائم المساس بالمعطيات المعالجة آليًا والموجودة داخل وخارج النظام المعلوماتي.

البَاب التّمهِيدي

ماهية الجريمة المعلوماتية
وتحديد طبيعتها القانونية

الباب التمهيدي: ماهية الجريمة المعلوماتية وتحديد طبيعتها القانونية

تمهيد وتقسيم:

تعد الجرائم المعلوماتية من أكبر التحديات التي نواجهها في وقتنا الحاضر، وهذه الجرائم المستحدثة تثير العديد من المشكلات القانونية والعملية، والتي يسميها البعض بالمشكلات الموضوعية لقانون العقوبات في مواجهة هذا النوع من الإجرام، وذلك بإعتبارها نوعاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب والتي تتطلب ضرورة تحقق أركان الجريمة لقيامها.

وبما أن الجريمة المعلوماتية من الجرائم الحديثة لذلك لن نجد بسهولة ماهيتها وطبيعتها الخاصة لا في شروحات الفقه الجنائي أو إجتهادات القضاء المختص أو حتى في النصوص القانونية ذات الصلة، وهذا بحكم أنها ظاهرة إجرامية مستحدثة لها طبيعة قانونية خاصة تختلف بها عن باقي الجرائم الأخرى، لأن الجريمة كفكرة أو كموضوع لا تقف عند أي تحليل لها، فإدراك ماهية أية جريمة يقتضي التعرف بها لاسيما في ظل نظام العولمة.

وذلك ما سوف نتطرق إليه بالدراسة والتحليل في هذا الباب التمهيدي، وهذا من خلال التطرق إلى فصلين إثنين على التوالي وهما:

الفصل الأول: مفهوم الجريمة المعلوماتية والمجرم المعلوماتي

الفصل الثاني: تحديد الطبيعة القانونية للجريمة المعلوماتية

الفَصل الأَوّل

مفهوم الجريمة المعلوماتية
والمجرم المعلوماتي

الفصل الأول: مفهوم الجريمة المعلوماتية والمجرم المعلوماتي

تمهيد وتقسيم:

في ظل مفهوم الجريمة المعلوماتية والمجرم المعلوماتي، وما صاحب ذلك من عولمة الجريمة بشكل عام، وحيث الحالة غير المستقرة التي إنتقل إليها العالم اليوم لاسيما بعد تطور أساليب إرتكاب الجرائم وذلك بإستخدام وسائل وتقنيات علمية حديثة وجد متطورة، ناهيك عن العوامل المساعدة لنمو الجريمة المتعولمة وتعدد أشكالها وتغير سمات مرتكبيها.

كل هذا يقودنا من خلال هذا الفصل إلى الحديث عن الإطار المفاهيمي العام لكل من الجريمة المعلوماتية وكذا المجرم المعلوماتي، وذلك وفق مبحثين إثنين على التوالي:

المبحث الأول: تعريف الجريمة المعلوماتية وسماتها الخاصة

المبحث الثاني: تعريف المجرم المعلوماتي ودوافعه الإجرامية

المبحث الأول: تعريف الجريمة المعلوماتية وسماتها الخاصة

تمهيد وتقسيم:

مع تنامي فكرة الجريمة المتعولمة وما صاحبها من ظهور للجرائم المستحدثة، وجد في الحقل الجنائي نوع جديد من هذه الجرائم أطلق عليها في كثير من الدراسات القانونية مصطلح "الجريمة المعلوماتية"، لذا يكون من الأهمية لدراستها والوقوف على فكرتها ومظاهرها من حيث هي، وتقصي سماتها الخاصة والمختلفة في التعرف عليها من قرب، وذلك بإستخلاص المصطلحات المكونة لها وإستظهار السمات والخصائص المميزة لها، والتي تميزها عما قد يختلط بها أو يتشابه معها من جرائم تقليدية أخرى، لأن ذلك يعد أمراً ضرورياً.

وهذا ما نريد الحديث عنه من خلال هذا المبحث، والذي بدوره سوف نقسمه إلى مطلبين إثنين على الشكل التالي:

المطلب الأول: تعريف الجريمة المعلوماتية

المطلب الثاني: السمات الخاصة بالجريمة المعلوماتية

المطلب الأول: تعريف الجريمة المعلوماتية

تعد الجريمة المعلوماتية من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث، والسبب في ذلك يعود حتماً إلى إرتباط هذه الجرائم بوسائل التقنيات التكنولوجية الحديثة من أجهزة كمبيوتر وشبكات ومواقع إلكترونية، وبما أننا نبحث في تعريف الجريمة المعلوماتية فإنه في الحقيقة لا يوجد في الوقت الحالي تعريف جامع مانع لهذا النوع من الجرائم، فقد إختلف الفقه القانوني في تعريفها، أما التشريعات الجنائية المقارنة فنجد بعضها عرفت الجريمة المعلوماتية بطريقة غير مباشرة، وبعضها الآخر لم يتعرض لتعريفها أصلاً، والسبب في ذلك أن مهمة المشرع الجنائي هي تجريم الأفعال ووضع الجزاء المناسب لها، أما تعريف الجرائم وشرح المصطلحات القانونية المتعلقة بها، هي من عمل الفقه والقضاء.

لذا في هذا المطلب نريد أن نشير إلى أن مسألة تعريف الجريمة المعلوماتية سواء من الناحية الإصطلاحية أو الفقهية وكذا من الناحية القانونية، هي في الحقيقة مسألة خلاف في تحديد المعنى الدقيق لها، وهذه المسألة هي في الواقع من أكثر المشاكل التي ترتبط بهذه الظاهرة الإجرامية، والسبب الحقيقي في ذلك يعود إلى حداثة هذا النوع من الجرائم من جهة، ومن جهة أيضاً إلى جانبها التقني والفني الذي يجهله الكثير ممن تناولونها بالبحث والدراسة، كما أن قصور كثير التشريعات في النص عليها أدى إلى عدم وضع تعريف شافي ينهي الإختلافات بين الفقهاء والمشرعين.

ومن وجهة النظر الواسعة لدى غالبية الفقه القانوني فإن تحديد التعريف بالمشكلة ومصطلحاتها يكون في الحقيقة نقطة بداية مهمة، علاوة على ذلك فإن فهم نطاق المصطلح سوف يسهل عملية المواءمة الوطنية والدولية لهذه المشكلة محل البحث والدراسة، لاسيما من الناحية القانونية، وهذا لأن الجريمة المعلوماتية هي ظاهرة إجتماعية وسلوكات إنسانية تجمع بين أمور فنية وأخرى تقنية وجدت بوجود التطور البشري ومعرفته للتكنولوجيا.

من هذا المنطلق كله فإن هذا المطلب سيتناول بالدراسة ثلاثة فروع على التوالي تقودنا إلى تعريف الجريمة المعلوماتية عموماً، سواء من الناحية الإصطلاحية (فرع أول) ثم من الناحية الفقهية (فرع ثاني)، وأخيراً من الناحية القانونية (فرع ثالث).

الفرع الأول: التعريف الإصطلاحي للجريمة المعلوماتية

تعتبر الجريمة المعلوماتية والمرتكبة عبر إستخدام تكنولوجيا الإتصال كالإنترنت مثلاً من الأثار السلبية التي خلفتها هذه التقنية العالية، حيث أخذت هذه الظاهرة الإجرامية حيزًا كبيرًا من الدراسات والأبحاث من أجل تحديد مصطلح دقيق يعبر عنها، مما إنجرّ عنه وضع عدد لا بأس به من المصطلحات للدلالة عليها[1]، والتي من بينها جرائم الحاسوب وجرائم الإنترنت وجرائم تقنية المعلومات... وغيرها كثير. لكن المشكلة الأساسية لا تكمن في الإختلاف حول التعبير الإصطلاحي الدال على هذه الظاهرة الإجرامية المستحدثة، وإنما في عدم الإتفاق على تعريف إصطلاحي جامع لها[2]، إذ أنّ وضع تعريف إصطلاحي لها يعد أمرًا بالغ الصعوبة وهذا بحكم أنها جريمة لا تعرف الخمول وفي تطور مستمر، فهي في الحقيقة ظاهرة متجددة ولديها سرعة الإستجابة للمتغيرات والتطورات التكنولوجية مقارنة بالإستجابة البطيئة للتشريعات الجنائية[3].

ونظرًا لحداثة الجريمة المعلوماتية، والإختلاف الفقهي والقانوني بشأنها؛ جعلها تكتسب العديد من التسميات والمصطلحات وفق مرجعيات مختلفة، إلاّ أنّ جلها تصب في معنى واحد تقريبًا، حيث أظهرت هذه الدراسة أنّ العديد من الأبحاث التي أجريت بصدد تعريف هذه الجريمة، هو عدم الإتفاق على وضع مصطلح معين، والذي يكون أكثر دقة للدلالة على مفهوم هذه الجريمة المستحدثة، حيث وجدت العديد من المصطلحات التي شاع إستخدامها، سواء على مستوى الفقه أو القانون، لكن كل واحد منها يتطابق فقط مع النظرة الخاصة بالموضوع محل البحث.[4]

ومع إختلاف التسميات والمصطلحات الدالة على جرائم عصر التكنولوجيا، ومع إعتبار هذا الأخير أحد أهم ركائز هذه الجرائم بصفة عامة؛ فإنه يمكن الوصول إلى جملة من التسميات

---

[1]– ***ELAZZOUZI Ali :*** *La cyber criminalité au Maroc, Ed. bishops solution, Casablanca, maroc,2010, P17.*

[2]– **مشتاق طالب وهيب النعيمي:** تزوير المعلومات كأحد صور الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2018، ص36. – **أحمد كيلان عبد الله صكر:** الجرائم الناشئة عن إساءة إستخدام الحاسوب، ماجستير، جامعة بغداد، العراق، 2002، ص28.

[3]– **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017، ص27. – **فتيحة رصاع:** الحماية الجنائية للمعلومات على شبكة الإنترنت، ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2012، ص39.

[4]– يتفق معظم الفقه الحديث أنّ هذه الجريمة ناشئة أساسًا من التقدم التكنولوجي، ومدى التطور الذي يطرأ على نظام الحواسيب، فهو متجدد بصفة دائمة ومستمرة خاصة في مجال تكنولوجيا المعلومات، حيث هناك من يفضل أن يطلق عليها مصطلح (جرائم التكنولوجيا الحديثة) وهذا بسبب أن الحواسيب بمختلف أشكالها وأحجامها من الأجهزة التقنية الحديثة التي أفرزتها التكنولوجيا الحديثة، والتي قد تظهر في المستقبل القريب بأشكال أكثر تعقيدا، تكون ذات طاقة تخزينية كبيرة وسرعة فائقة ومرونة في التشغيل، (أنظر في ذلك: – **عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار النهضة العربية، القاهرة، مصر، 2000، ص20).

والمصطلحات التي أطلقت على هذا النوع من الجرائم، فمنها ما هو شائع ومتداول في كثير من الدول والقوانين، وذلك نظرًا لحداثتها وإتساعها الرهيب الذي مسّ بجميع مجالات الحياة الانسانية العامة والخاصة، لاسيما الحساسة منها (أولاً)، ومنها ما هو غير شائع وإنما مألوف لدى البعض دون الآخر (ثانياً). وعليه سوف نقوم بدراسة هذه التسميات والمصطلحات المختلفة والمعتمدة قانوناً وفقهًا.

أولاً: بالنسبة للتسميات والمصطلحات الشائعة

يمكن تسمية هذا النوع من الجرائم محل الدراسة بالعديد من التسميات والمصطلحات الشائعة والمتداولة وحتى المعروفة لدى الكثير من الناس، والتي تقريبًا إعتمدها المشرع الجنائي في الكثير من النصوص القانونية.

ولعل من أبرز هذه التسميات والمصطلحات نجد على سبيل المثال ما يلي:

أ- **الجريمة المعلوماتية *L'infraction d'informatique*:** والمقصود بها أيضًا جرائم المعلومات "*Crime d'information*" وهي من أكثر التسميات المتداولة فقهًا وأقلها تشريعًا، حيث أنّ أغلب الكتب والأبحاث العلمية والأكاديمية المتعلقة بالجريمة محل الدراسة تسميها بذلك،[1] وبتحليل مصطلح "معلوماتية *Informatique*" يتضح أنه عبارة عن مجموعة من العمليات الآلية التي يخضع لها موضوع المعلوماتية بما يشتمل عليه من بيانات ومعلومات معالجة ومخزنة آليًا داخل النظام المعلوماتي، ناهيك عن عمليات الجمع والتحليل والمعالجة والصياغة والنقل والإسترجاع والتداول وغيرها، والتي تتم جميعها من خلال البرامج الموجودة على الحاسبات الآلية أو ما يقوم مقامها من النظم المتطورة.[2]

وهناك إتجاه حديث للفقه الجنائي يراهن على إستعمال مصطلح "الجرائم المتصلة بالمعلوماتية *Le délit criminalité*"، وهذا ما أكده غالبية الفقه الفرنسي، كما تأثر بذلك الفقه العربي قاطبة فيما بعد والذي إستقر على إستخدام مصطلح الجريمة المعلوماتية أو ما يطلق عليها أيضًا

[1]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص41.

[2]- **عبد الله أحمد هلالي:** المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مجلة الحقوق، جامعة البحرين، المجلد السادس، العدد13، 2009، ص462.

"بالجريمة الإلكترونية*L'infraction électronique* "،[1] أو كما يصطلح عليه في كثير القوانين العربية المقارنة "بجرائم تقنية المعلومات *Crime liés aux technologies de l'information*".[2]

ب- الجريمة الإلكترونية *L'infraction électronique*: هناك بعض الفقه من يعتمد هذا المصطلح على أساس أن هذه الجريمة تقوم من خلال الأفعال والسلوكيات التي يعاقب عليها القانون ولها صلة وطيدة بالحاسب الآلي وكل ما يرتبط به من أنظمة إلكترونية،[3] وهذا المصطلح يشيد هو الآخر بدور تكنولوجيا المعلومات في إرتكاب عدد كبير من الجرائم المستحدثة، لكن يرى معظم الفقه الحديث أن مصطلح "الجريمة المعلوماتية" هو الأكثر دقة من مصطلح "الجريمة الإلكترونية" وإنّ كانت هذه الأخيرة في بعض الجوانب صحيحة لأنها في ذات الوقت تمثل إنعكاسًا لفهم طبيعة العلاقة بين عناصر الجريمة وهذا المصطلح.[4]

وعلى العموم فمصطلح الإلكترونية يشمل جميع المعدات ذات النبضات الإلكترونية، مما يجعلها تسمية منتقدة، فحتى الأدوات المنزلية اليوم أصبحت ذات نبضات إلكترونية.[5]

ج- جرائم الكمبيوتر أو الحاسوب *Crimes computer*: يقصد بها كل عمل إجرامي وغير قانوني يرتكب بإستخدام جهاز الكمبيوتر "الحاسوب" كأداة أساسية له، والذي يكون الدور له في تلك الجرائم إما هدفًا أو أداةً لها،[6] وتسمية جرائم الكمبيوتر شاعت قبل ظهور وتعميم شبكة الإنترنت وإستمرت حتى وقتنا الحالي، والتي تطورت فيما بعد وأصبحت تسمى "جرائم الحاسوب" أو "جرائم المحمول" أو "جرائم الهاتف النقال" وغيرها من التسميات ذات الصلة، وذلك بإعتبارها أنظمة تقنية بمفهومها الواسع والشامل والمتطور، التي تزاوج بين تقنيات الحوسبة وكل فنيات الإتصال الحديثة وشبكات المعلومات[7].

---

[1]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص42.

[2]- ومنه مثلاً: القانون السوداني رقم (13 لعام 2007) والقانون العماني رقم (12 لسنة 2011) والقانون الإماراتي (رقم 5 لسنة 2012) والقانون الكويتي رقم (63 لسنة 2015) والقانون القطري رقم (14 لسنة 2014) والقانون المصري رقم (175 لسنة 2018).

[3]- **محمد سامي الشوا:** ثورة المعلومات وإنعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة، مصر، 2003، ص20.

[4]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص43.

[5]- **ذياب البداينة:** الجرائم الإلكترونية، المفهوم والأساليب، ورقة علمية مقدمة إلى الملتقى الدولي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، جامعة عمان، الأردن، من (02 إلى 2014/09/04)، مجلة الجامعة لعام 2015، ص5.

[6]- **شرين دبابنة:** الجرائم الإلكترونية والقرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، القاهرة، مصر، 2015، ص19.

[7]- **سيناء عبد الله محسن:** المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، ورقة عمل مقدمة إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المغرب، من (19 إلى 2007/06/20)، مجلة الندوة، ص50.

ويرى جانب من الفقه أنّ إستخدام مصطلح "جرائم الكمبيوتر" أعم وأشمل من إستخدام مصطلح "الجرائم المعلوماتية"، وحجتهم في ذلك أن جرائم الكمبيوتر تشمل كافة الجرائم التي تقع على أجهزة الحاسبات الآلية بشكل عام أو بواسطة الحاسوب، والذي يستخدم فيها هذا الأخير كأداة رئيسية لإرتكاب هذا النوع من الجرائم، حيث يشمل ذلك كل أنواع الاعتداء على المعلومات الموجودة داخل الحاسوب.[1]

لذلك نجد البعض يفضل التعبير عن هذه الظاهرة الإجرامية بإستخدام مصطلح "جرائم الكمبيوتر أو الحاسوب" والذي يشير إلى تحديد أية أنشطة إجرامية ترتكب فيها الحواسيب بمختلف أشكالها، وكذا كل الاعتداءات الواقعة على البيانات والبرامج الموجودة داخلها، أي أنّ الكمبيوتر كجهاز يكون فيها الهدف والمضمون وراء النشاط الإجرامي.[2]

ففي بدايات إنتشار هذا النوع من الجرائم في فترات سابقة أُطلق على هذه الجريمة مصطلح "الغش أو إحتيال الحاسوب *Computer fraud*" وهذا على أساس أن هذه الجريمة هي الأكثر شيوعًا عند ظهور مثل هذه السلوكيات[3]، والحقيقة أنّ هذا المصطلح أصبح الآن لا يلائم مثل هذه الجرائم، ذلك أنّ الغش أو الإحتيال المعلوماتي هو الآن أحد أنواع الجرائم المعلوماتية وليس مصطلحًا يطلق على هذه الظاهرة الإجرامية الحديثة ككل.[4]

كما نجد جانب آخر من الفقهاء وحتى بعض الدراسات القانونية من يستخدم مصطلح "إساءة إستخدام الحاسب *Computer mésuse or abuse*" على إعتبار أنه مصطلح يشمل تشكيلة واسعة من الجرائم المتعلقة بالحاسبات، فهذه الجرائم لا تتحقق إلاّ عن طريق الإستخدام السيء للحواسيب، وهذا المصطلح أيضًا معيب إذ أنه في مثل هذا المنظور قد نرى حالات تنطوي على إساءة استخدام الحاسب ومع ذلك لا تصل إلى درجة السلوك الإجرامي، مع العلم أنّ هناك حالات كثيرة تتم بإستخدام الحاسب بصورة مشروعة وسليمة وترتكب من ورائها جرائم.[5]

رغم أنّ هناك من يتفق مع هذا الرأي من حيث شمولية مصطلح جرائم الكمبيوتر عن مصطلح الجرائم المعلوماتية، إلاّ أنّ هذه التسمية أصبحت اليوم منتقدة وذلك لقصورها فقط على

---

[1]– **أمير فرج يوسف:** الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008، ص105.

[2]– **لينا محمد الأسدي:** مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار الحامد، عمان، الأردن، 2015، ص20.

[3]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص27.

[4]– **أحمد كيلان عبد الله صكر:** الجرائم الناشئة عن إساءة استخدام الحاسوب، المرجع السابق، ص29.

[5]– **أحمد كيلان عبد الله صكر:** نفس المرجع، ص31.

الجرائم التي ترتكب بواسطة جهاز الكمبيوتر أو عليه، دون وجود إتصال بالشبكة العالمية للمعلوماتية[1] بينما مصطلح الجرائم المعلوماتية تشمل من حيث المفهوم والمضمون كل الجرائم التي ترتكب على جهاز الحاسوب أو بواسطته وكل أشكال الإعتداء على المعلومات والبرامج الموجودة بداخله.[2]

وعليه يجد الكثير من الفقه الحديث أنّ مصطلح جرائم الكمبيوتر غير دقيق، كونه يركز على عنصر أساسي في إرتكاب هذا النوع من الإجرام وهو جهاز الكمبيوتر أو ما يطلق عليه أيضا بالحاسوب، فهذا المصطلح يهمل الجوانب الأخرى التي يستند عليها في قيام هذه الجريمة، كما أنه مصطلح عام يشمل الجرائم المرتكبة ضد المكونات المادية والمعنوية للحاسوب، ومن جهة أخرى نجده يستبعد الجرائم التي يكون فيها الحاسب وسيلة لتنفيذ العمل الإجرامي كالتزوير والإحتيال وغيرها من الأعمال المرتبطة بإستخدام الحاسوب أو الكمبيوتر[3].

د- جرائم الإنترنت *Crimes sur Internet*: إذا كانت الإنترنت كوسيلة إتصال جديدة تسهل أمور كثيرة في المجتمع، ولها العديد من الفوائد العلمية والعملية، إلاّ أنّ البعض أساء إستخدام تلك الإمكانيات التي تقدمها شبكة الإنترنت، وذلك من خلال إرتكاب أفعال غير مشروعة تنطوي تحت طائلة العقوبات.[4]

لذلك نجد من الفقه من يفضل تسمية هذا النوع من الجرائم "بجرائم الإنترنت"، أي تلك الناشئة عن الإستعمال غير المشروع في التواصل بين الشبكات، وهذا بسبب أن الإنترنت هي تلك الوسيلة والأداة التوصيلية بين الشبكات دون إعتبار للحدود[5]، حتى وإنّ ذهب الكثير منهم على إعتبار الجريمة المعلوماتية التي يرتكبها المجرم تكون من خلال شبكة الإنترنت.[6]

---

[1]- **سيناء عبد الله محسن:** المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، المرجع السابق، ص51.

[2]- **لورنس سعيد الحوامدة:** الجرائم المعلوماتية، أركانها وآلية مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، العدد الثالث، 2016، ص10.

[3]- **محمد علي قطب:** الجرائم المستحدثة وطرق مواجهتها، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2009، ص131.

[4]- **رامي عمر غريب أبو ركبة:** جرائم المساس بأنظمة الكمبيوتر والإنترنت، مجلة كلية الشريعة والقانون، جامعة الأزهر، القاهرة، مصر، العدد 14 لعام 2012، ص851.

[5]- **عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن إستخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص71.

[6]- **حسن طاهر داوود:** جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، السعودية، 2000، ص24.

ولقد نمت الإنترنت بشكل مذهل خلال السنوات العشر الأخيرة، فبعد أن كانت مجرد شبكة أكاديمية صغيرة أصبحت تضم ملايين المستخدمين في كافة أنحاء العالم، وتحولت من مجرد شبكة أكاديمية إلى بيئة متكاملة للإستثمار والعمل والإنتاج والحصول على المعلومات، ولكن اليوم هذه النظرة بدأت تتغير بشكل جذري لاسيما بعد أن أصبحت هذه الشبكة حقلاً لإرتكاب عديد الجرائم التي تمس كل المناحي الحياتية للفرد والمجتمع وهو ما يطلق عليه بجرائم الإنترنت.

هـ- جرائم مواقع التواصل الإجتماعي *Crimes sur les réseaux sociaux*: يطلق على مواقع التواصل الإجتماعي باللغة الإنجليزية "*Social media*" لكن هذا المصطلح ليس هو الوحيد المتعارف عليه، إذ يوجد مصطلح "*Social net work*" أي الترابط الشبكي الإجتماعي، أما عن المصطلح العربي فإنّ مواقع التواصل الإجتماعي نجده أدق من ناحية الوصف[1].

ولقد عرَّف إتجاه في الفقه الجنائي مواقع التواصل الإجتماعي بأنها: "منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثم ربطه عن طريق نظام إجتماعي إلكتروني مع أعضاء آخرين لديهم الإهتمامات والهوايات نفسها"[2]، أو هي عبارة عن: "مجموعة من مواقع الإتصال عبر شبكة الإنترنت، وهذه المواقع تكون مخصصة للتفاعل والتبادل الإجتماعي، وبحيث تكون مفتوحة لجميع الناس لتبادل الحوار والآراء وكتابة ما يرغبون بمشاركته أو نشره مع الآخرين من جميع أنحاء العالم، وللاشتراك بهذه المواقع ليس عليك إلاّ التسجيل من خلال الإيميل بكل سهولة لتصبح أحد المشتركين بهذه الوسائل المختلفة، التي تفتح أمامك العالم"[3].

كما عرَّف المشرع الفرنسي مواقع التواصل الإجتماعي عبر شبكة الإنترنت بموجب المادة الرابعة من القانون رقم (575-2004) بأنها: "بروتوكول إتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية"[4].

---

[1]- **دينا عبد العزيز فهمي:** الحماية الجنائية من إساءة إستخدام مواقع التواصل الإجتماعي، دار النهضة العربية، مصر، 2018، ص15.

[2]- **زاهر رامي:** إستخدام مواقع التواصل الإجتماعي في العالم العربي، مجلة التربية، العدد 15، جامعة عمان الأهلية، عمان، الأردن، 2003، ص23.

[3]- **عبد الرزاق محمد الدليمي:** الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر والتوزيع، عمان، الأردن، 2011، ص183.

[4]- ***JORF N° 0143 :*** *du 22 Juin 2004 (P11168, texte N° 2) loi N° 2004- 575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

*- **Article N° 04:** « On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout formant de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre ».*

ولقد ساعدت التطورات في تكنولوجيا الإتصال والإعلام على زيادة التواصل بين الناس على مستوى كافة المجتمعات، متخطية كافة الحدود السياسية والثقافية، ومن ثم فقد أحدثت شبكة الإنترنت بتقنياتها وتطبيقاتها المتقدمة والمتطورة سواء على الحاسب الآلي والموبايلات والهواتف الذكية درجة عالية من التأثير فاق كل ما أحدثته وسائل الإتصال والإعلام التقليدية، يجرى خلالها أشكال متنوعة من التواصل الاجتماعي، منها "فيسبوك *Facebook*" و"تويتر *Twitter*" و"ماي سبيس *My space*" وغيرها كثير جدًا من مواقع التواصل الإجتماعي وكذا التطبيقات الداعمة للإتصالات السريعة مثل "الواتس آب *Whatsapp*" و"فايبر *Viber*" و"سكايب *Skype*" و"إيمو *Imo*" وغيرها كثير من أدوات التواصل الإجتماعي.[1]

ولكن للأسف الشديد تحولت مواقع التواصل الإجتماعي من نعمة إلى نقمة بسبب سوء الإستخدام من قبل بعض الأفراد الذين خلقوا نوع من الإجرام أطلق عليه الجرائم عبر مواقع التواصل الإجتماعي والتي ذهب ضحيتها كثير من الأبرياء.

و- جرائم تقنية المعلومات *Crimes liés aux technologies de l'information*: من بين المشرعين الذين إعتمدوا هذه التسمية، نجد على سبيل المثال كل من المشرع المصري ونظيره المشرع الأردني، حيث كانت في السابق يطلق عليها "بجرائم أنظمة المعلومات" ولكن سرعان ما أستبدلت بمصطلح "جرائم تقنية المعلومات"، ولعلها أشمل وأوسع من الأولى، حيث بهذه التسمية حاول كل منهما حصر جملة الأفعال والسلوكيات غير المشروعة والمتصلة بالنظام المعلوماتي، والتي قد تقع على المعلومة الرقمية أو حتى بواسطتها[2].

وفعلاً قد تم إعتماد هذه التسمية – تقنية المعلومات- في كثير القوانين العربية والغربية وذلك نظرًا لإمكانية حصر جميع عناصر النظام المعلوماتي في هذا المصطلح، وأيضًا لشموليته جميع الجرائم ذات الصلة.

ثانيًا- بالنسبة للتسميات والمصطلحات غير الشائعة

كما أنّ هناك تسميات ومصطلحات يمكن أن تنطبق على هذا النوع من الجرائم، إلاّ أنها مصطلحات غير شائعة عند الجميع، ومن أهمها نجد على سبيل المثال:

[1]- **فخري محمود خليل:** جرائم البلطجة الإلكترونية، د.د.ن، 2019، ص32. - **دينا عبد العزيز فهمي:** المرجع السابق، ص25.

[2]- **محمود رجب فتح الله:** الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2019، ص62.

أ-جرائم تكنولوجيات الإعلام والإتصال *Crimes liés aux technologies de l'information et de la communication*: نظرًا لعدم شيوع التسمية كثيرًا، إلاّ أنها تعد أحد أهم أنواع جرائم العصر التكنولوجي، وهذا ما ذكره المشرع الجزائري من خلال القانون رقم (04/09) والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،[1] لكن هذه التسمية تحتمل التأويل؛ فتكنولوجيات الإعلام والإتصال تدل في عادتها على مجال الصحافة المكتوبة والمرئية والاعلام.

وهناك من يستخدم مصطلح جريمة تكنولوجيا المعلومات والإتصالات "*ICT crime*"[2] وذلك للإشارة إلى جميع الأفعال التي لها علاقة بوسائل الاتصال السلكية واللاسلكية بما فيها وسائل التواصل الإجتماعي عبر شبكة الإنترنت، ومع ذلك فإنه يبقى هذا المصطلح يقيد من نطاق السلوك الإجرامي، إذ أنه يشير فقط إلى الجرائم المتعلقة بمجال وسائل الإتصالات، ويستثني الجرائم الأخرى التي قد يكون الحاسوب الشخصي يلعب دورًا أساسي فيها كتزوير الوثائق الإلكترونية وغيرها من الجرائم المعلوماتية.[3]

وبعدها جاء مصطلح "التكنولوجيا العالية *High-Tech*" والذي تم إستخدامه نتيجة التطورات التكنولوجية في العقود الأخيرة، لكن في الواقع أنّ هذا المصطلح يتجاوز تكنولوجيا شبكات المعلومات بما فيها الإعلام والإتصال، ليشمل كافة التطورات التكنولوجية الأخرى، حيث أنّ هذه التسمية واسعة ومطلقة ولا تخص فقط هذا النوع من السلوكيات.[4]

ب- جرائم المساس بأنظمة المعالجة الآلية للمعطيات *Des atteintes aux systèmes de traitement automatisé de données*: لقد تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" معتبراً أن النظام المعلوماتي وما يحتويه من كيانات

---

[1]- راجع في ذلك نص المادة الثانية من القانون رقم (04/09) والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها والمؤرخ في 05 غشت 2009، الجريدة الرسمية العدد (47) لعام 2009.

[2]- يمكن تعريف تكنولوجيات المعلومات والإتصالات *Information and communications technology*، وإختصارها (*ICT*) بأنها: "جميع التقنيات التي تستخدم في الإتصالات ووسائط البث، وأنظمة إدارة المباني الذكية، وأنظمة المعالجة الآلية والإرسال، السمعية والبصرية وغيرها"، كما أستخدمت مؤخرا للتعبير عن توظيف خطوط الإتصال لنقل أنواع وصيغ متنوعة من البيانات، حيث يتم دمج الشبكات السمعية والبصرية وشبكات الحاسوب من خلال نظام مشترك للكابلات ووسائل الإرسال السلكية واللاسلكية، ما يمكن إعتبار مصطلح (*ICT*) الذي ظهر الثمانينيات من القرن الماضي، وازدادت خدماته في عام 1997م، بأنه المرادف الأوسع لمصطلح "تقنية المعلومات *Informatique*" – متاح على الموقع التالي: **https://ar.m.wikipédia.org**، تاريخ التصفح للموقع في: 2018/04/12.

[3]- **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، المرجع السابق، ص28.

[4]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص37.

مادية ومنطقية هو محلاً للجريمة المعلوماتية، بحيث يمثل نظام المعالجة الآلية للمعطيات الركن المفترض الذي يلزم تحقيقه حتى يمكن البحث في مدى توافر أو عدم توافر أي جريمة من جرائم الإعتداء على هذا النظام، ولعل من بين المشرعين الذين إعتمدوا هذه التسمية أيضًا إلى جانب المشرع الجزائري نجد المشرع الفرنسي،[1] ولكن سرعان ما تراجع المشرع الجزائري عن مصطلح أنظمة المعالجة الآلية للمعطيات وحتى تسمية جرائم تكنولوجيا الإعلام والإتصال، وإستبدالهما بإسم الوسائل الإلكترونية والمعلوماتية.[2]

وربما هذه رؤية جديدة من المشرع الجزائري في أن مصطلح "المعلوماتية" يجمع بين جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأية جريمة تقليدية أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو أي نظام للإتصالات الإلكترونية.

ج- الجريمة السيبرانية *Cyber crime*: كما يحلو للبعض بتسميتها "بالجرائم السيبرانية"، ومن أبرز الفقهاء الذين إعتمدوا هذه التسمية نجد الفقيه "أوبريش سيبر *Ubrich Sieber*"[3] كما شاع أيضًا إلى جانب هذه التسمية إستخدام مصطلح "الإجرام الكوني" والذي أستخدم للإشارة إلى بعض الأنشطة الإجرامية التي يكون فيها الحاسب الآلي أداة لتسهيل وتنفيذ الجرائم التقليدية في أية منطقة من العالم الواسع.[4]

ومع ذلك فإن هذا المصطلح أيضا غير دقيق وغير واضح، لأنه ينافي المدلول الحقيقي في تكييف الجرائم، بل ينبغي أن يكون مصطلح يترجم فعلاً الأعمال الإجرامية التي تتم ضد الحاسوب وأنظمته المعلوماتية على حد سواء، وليس فقط مجرد تسمية تنسب إلى شخص معين حتى ولو كان هو مخترع الحاسوب الآلي بعينه.

---

[1]- جاءت هذه التسمية "المساس بأنظمة المعاجلة الآلية للمعطيات" بموجب القسم السابع مكرر المستحدث بالقانون رقم (04-15) المعدل والمتمم لقانون العقوبات الجزائري، ونفسها التي ذكرها المشرع الفرنسي، يراجع المواد: (394 مكرر إلى 394 مكرر8) من قانون العقوبات الجزائري. **الملحق رقم (05)**، وكذا المواد (323-1 إلى 323-7) من قانون العقوبات الفرنسي. **الملحق رقم (03)**

[2]- وهذا ما جاء في سياق نص المادة (144 مكرر) من قانون العقوبات الجزائري، المعدل والمتمم بالقانون رقم (11-14) المؤرخ في 02 غشت 2011، بقولها: "يعاقب بغرامة من 100000 دج إلى 500000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانةً أو سبًا أو قذفًا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى ...".

[3]- **الفقيه "أوبريش سيبر *Ubrich Sieber*"**: ألماني الجنسية، وكان مدير في معهد ماكس بلانك للشؤون الخارجية، وهو أستاذ مختص في القانون الجنائي وعلم الاجرام، كما يعد أستاذ فخري وعضو هيئة التدريس بكلية الحقوق في جامعة (فرايبورغ) وكذا جامعة (لودفيغ ماكسيميليان في ميونخ) وللمزيد حول الموضوع طالع موقع معهد (ماكس بلانك) للقانون الجنائي الأجنبي والدولي، فرايبورغ، ألمانيا، متاح على الموقع التالي: ***https://www.mpicc.de/en/home/sieber.html*** تاريخ التصفح للموقع في 2017/07/08.

[4]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص40.

د- جرائم الوسط الرقمي أو البيئة الرقمية *Environnement numérique*: عمد بعض فقهاء القانون الجنائي على تسمية هذا النوع من الإجرام "بجرائم الوسط الرقمي"[1] أو "بجرائم البيئة الرقمية"، فعرفوها وفق أسس علمية من منطلق حداثتها من جهة، وإرتباطها بمفهوم الرقمنة والأرقام من جهة أخرى، وإعتبروا كل جريمة تتصل بعناصر الوسط الرقمي هي جريمة رقمية بحكم أنّ هذا الوسط أصبح أخطر الأوساط الإجرامية على الإطلاق.

ورغم كونه واحد من بين أهم التسميات في عالم الجريمة المستحدثة، إلا أنه مصطلح يمتاز بكونه إفتراضي محسوس وغير ملموس، وكذا أنه مصطلح مبني على لغة رقمية[2] لا يمكن أن يفهمها الكثير من الناس.

كما يمكن القول هنا بأنّ الثورة التكنولوجية التي قادتنا إلى ما يسمى بجرائم الوسط الرقمي؛ قد أوجدت جرائم وسط حديث وغير معروف، أو على الأقل يصعب على العامة فهمه والتعامل مع خباياه، ألا وهو الوسط الإفتراضي، أو ما يطلق عليه بجرائم الوسط الإفتراضي "الإنترنت" وذلك نظرًا لما يمتاز به هذاالأخيرمن أنظمة معلوماتية مسهلة لإرتكاب الجريمة، وكذا لكونه دخيل على مجال التجريم والعقاب.

---

[1]- **مصطلح الوسط الرقمي:** هو في الحقيقة مصطلح مستحدث من حيث المضمون والدلالة معًا، أما الوسط المقصود هنا فهو المرادف لمصطلحات "البيئة، المحيط، المجال، الفضاء ..." بمعناها المعنوي والإفتراضي المحض وليس المادي، وذلك حين نقول الوسط العلمي معناه "البيئة العلمية" وليس بالضرورة البيئة الطبيعية والمحيط بمفهومه المعتاد اللذان يدلان على الحفاظ على البيئة من التلوث وما إلى ذلك، فالمقصود هنا هو مكونات الوسط التي تفرض نظام خاص. "من أصحاب هذا الرأي نجد الفقيه المصري الأستاذ الدكتور **هشام محمد فريد رستم**، أستاذ القانون الجنائي، ورئيس قسم القانون الجنائي سابقًا بجامعة أسيوط، مصر".

[2]- **مصطلح الرقمية:** تعني لغة "الأرقام" أي أننا نتحدث ونتكلم بالأرقام، هذه الأخيرة هي تلك الرموز والأشكال التي تعارف عليها الإنسان منذ القديم للتعبير عن تسلسل منطقي يساعد الناس في عمليات الحساب. والأرقام هي من (0 إلى9) أما ما يفوق عن رقم (9) فهي كلها أعداد مركبة من أرقام، إذ الأعداد غير محددة أما الأرقام فهي تدور بين الصفر(0) والتسعة (9)، فيفهم من هذا أنّ كل عدد هو مجموعة أرقام، لكن ليس بالضرورة أنّ كل رقم هو عدد. أما علاقة ذلك بالوسط الرقمي فإن كل من الأرقام والأعداد تقوم وفق مجموعة أنظمة تختلف على حسب الأرقام أو الأعداد المعتمد عليها؛ فعندما نتحدث عن النظام الرقمي الثنائي *Le système numérique binaire*، والذي يقوم على أساس الرقمين (0 و 9)، نكون أمام نظام أرقام، بالإضافة إلى أنظمة أخرى كالنظام الرقمي الثماني *Le système numérique octal* والمؤسس على الرقم (8)، بالإضافة إلى نظام أعداد وإنّ كان يستعمل الأرقام بدرجة أقل مثل النظام الرقمي العشري*Le système numérique décimal* فنكون أمام نظام أعداد يقوم على أساس العدد (10)، وكذا النظام الرقمي السادس عشر *Le système numérique hexadécimal* والقائم على العدد (16)، بالإضافة إلى أنظمة رقمية أخرى عديدة ومتنوعة.

- أنظر أكثر: (- **مروة أديب محمد الجوهري:** الحاسوب والإعجاز العددي في القرآن الكريم، مجلة كلية العلوم الإسلامية، جامعة القاهرة، مصر، مج08، عدد15، 2014، ص08 وما بعدها).

رأي الباحث:

بناءًا على ما سبق ذكره، فإنه قد يتبادر إلى الأذهان للوهلة الأولى أنّ مسألة تعريف هذه الظاهرة الإجرامية المستحدثة من حيث التسمية أو المصطلح أمر متفق عليه من طرف كل من تناولوها بالبحث والدراسة، لكن في الحقيقة فإن مسألة تحديد مفهوم إصطلاحي واحد تعد من أكثر المشاكل التي ترتبط بهذه الظاهرة الإجرامية، ولا ربما السبب في ذلك يعود حتمًا إلى حداثة هذه الجرائم، وكذا جانبها التقني الذي لازال يجهله الكثير ممن تناولها بالدراسة والبحث، كما أنّ قصور بعض التشريعات المقارنة في رصد هذه الظاهرة بشكل جدي أدى إلى عدم وضع مصطلح شافي ينهي كل الإختلافات بين الفقهاء، كما يمكننا أن نشير إلى أنه بغياب مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن إساءة إستغلال تقنية المعلومات وإستخدامها، فقد ألقى مسؤولية كبيرة على عاتق القضاء المختص في مواجهة المجرم المعلوماتي حين إساءة إستخدام الأنظمة المعلوماتية، لاسيما في مسألة التكييف القانوني ومساءلة الجناة.

وعلى العموم فإنّ كل المصطلحات المستعملة للدلالة على هذا النوع من الإجرام وما يرتبط به من تكنولوجيا المعلومات قد تستخدم أحياناً على نحو متبادل ومتنوع، الأمر الذي يجعل من هذه الجريمة معضلة قانونية متنوعة، وذلك لأنّ هناك تنوع واضح في الآراء، الأمر الذي يسبب خلاف مفاهيمي بين كثير الدول والقوانين بشان المبادئ الأساسية حول هذه الجرائم.

وبعد أنّ قصدنا التوسيع في مفهوم ونطاق مصطلح هذه الجريمة، وتطرقنا إلى عديد التسميات والمصطلحات، سواء منها ما تتسم بالماديات الملموسة أو المعنويات المحسوسة، ووضحنا أنها تسمى بعدة تسميات؛ يمكن أن نصل إلى دلالتها العامة التي قادتنا إلى وسط حديث وغير معروف، أو على الأقل عالم يصعب على العامة فهمه والتعامل مع خباياه يسمى "بالإجرام المعلوماتي".

وعليه يرى الباحث أنّ إستخدام مصطلح "الجريمة المعلوماتية" أو "جرائم تقنية المعلومات" فهاتين التسميتين تعدان حسب تقديرنا المتواضع الأكثر شيوعًا وملائمةً لهذه الظاهرة الإجرامية، وأنها تدل بحد ذاتها على مفهوم دقيق ومدلول واسع وواضح، بحيث ينصرف إلى كل سلوك مجرم له علاقة بالبيانات والمعلومات المخزنة داخل النظام المعلوماتي، كما أنه مصطلح شامل لجميع المصطلحات التي يستخدمها الفقه والقانون في هذا المجال للدلالة على السلوكيات المجرمة والتي

تتم بواسطة الأنظمة المعلوماتية والحواسيب الآلية وكل التكنولوجيات المتصلة بها، لذلك نحن بدورنا سوف نستخدم في هذه الدراسة كثيرًا مصطلح "الجريمة المعلوماتية" وهذا للدلالة على مختلف الظواهر موضوع بحثنا.

الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية

لابد من الإشارة هنا إلى أن الفقه الجنائي الحديث يذهب في تعريفه لهذه الجريمة إلى إتجاهات ثلاثة، فالأول يقوم على الوسيلة المعتمدة في إرتكاب هذه الجرائم وهو ما يطلق عليه "بالإتجاه الفني" وبالتالي ينظر إلى المعيار الشخصي لدى فاعل الجريمة وهو ما يسمى "بالإتجاه الشخصي"، أما الثالث والأخير فمؤسس على موضوع الجريمة ومحلها، والذي يعرف "بالإتجاه الموضوعي".

حيث ذهب جانب كبير من الفقه إلى القول بأن الجريمة المعلوماتية هي جريمة تقاوم التعريف وأنها الجريمة المانعة[1]، الأمر الذي ذهب معه عدد لا بأس به من الفقه إلى القول بأن وضع تعريف لظاهرة إجرامية مستحدثة مثل الجريمة المعلوماتية يخشى معه حصرها في مجال ضيق يمكن أن يفقدها خصوصيتها.

وعلى الرغم من وجاهة هذا الرأي إلا أن الأخذ به وعدم الإتفاق على تعريف للجريمة المعلوماتية من شأنه أن يؤدي إلى إثارة العديد من المشكلات العملية والتي من بينها صعوبة تقدير حجم وخطورة هذه الظاهرة، وتعذر إيجاد الحلول المناسبة لمواجهتها، وكذلك صعوبة التعاون الدولي بشأنها، وأيضًا كيف يمكننا القول أننا أمام جريمة تعد إلكترونية ما لم يكن لها تعريف واضح ومحدد.[2]

وبالرغم من كثرة المصطلحات المستعملة في تعريف هذا النوع من الإجرام، فإن حقيقتها العلمية لم تحدد حجم هذه الظاهرة بصورة دقيقة، بل وضعت مفاهيم جمة ترتب عنها مشاكل كثيرة[3]، من بينها إختلاف الفقه الحديث بشأن تحديد تعريف جامع للجريمة المعلوماتية، حيث لا يوجد تعريف واحد لها، مما جعل المهتمون بهذا المجال يبذلون ما في وسعهم من أجل وضع تعريف دقيق لهذه الجريمة.

---

[1]– **أيمن عبد الله فكري:** جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص29.

[2]– **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017، ص29.

[3]– **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص43.

ومع ذلك فإن الجريمة المعلوماتية وإن كانت تختلف عن الجريمة التقليدية، خاصة وأنها تتسم بطابع خاص هو أنها جرائم في جميع الأحوال يكون الحاسب الآلي وشبكة الإنترنت الأداة الأساسية في إرتكابها، وأن مرتكبها ليس كالأشخاص العاديين وإنما ذو خبرة فائقة في مجال الحواسيب، وأن محل هذه الجريمة هو دائمًا المعطيات إما بذاتها أو بما تمثله[1]، فهي لا تخرج جميعها عن ثلاثة إتجاهات حديثة يعتمد كل واحد منها على معيار معين في تعريفه للجريمة المعلوماتية.

لذلك فقد صاغ الفقه الحديث وكثير من المنظمات المحلية والدولية المتخصصة مجموعة من التعاريف الفقهية المختلفة، والتي كانت متباينة ضيقًا واتساعًا في معناها ومفهومها، وهذا تبعًا للمعيار الذي أعتمد في تعريف هذه الجريمة المستحدثة[2]، وهذا كله من خلال الدور الذي يمكن أن يلعبه الحاسب الآلي والنظام المعلوماتي في إرتكاب هذه الجريمة.

وعليه سوف نتطرق في هذه الجزئية إلى مجموعة من التعاريف الفقهية، والتي تختلف بإختلاف المعيار المعتمد في تعريفها للجريمة المعلوماتية، وهذا كالآتي:

أولاً- التعريف على أساس الوسيلة المستعملة لإرتكاب الجريمة (الإتجاه الفني)

لقد إعتمد أصحاب هذا الرأي في تعريفهم للجريمة المعلوماتية على أساس الوسيلة المستعملة[3] في إرتكاب الجريمة، وطالما أن وسيلة إرتكاب هذه الجريمة هو الحاسوب أو إحدى الوسائل التقنية الحديثة المرتبطة به، فتعتبر حسب رأيهم من قبيل الجرائم المعلوماتية.

وهذا ما تبناه أصحاب هذا الإتجاه الفني، ومن جهة نظرهم أنه لا تقوم الجريمة المعلوماتية ما لم يكن الحاسوب الآلي وسيلة رئيسية لإرتكابها[4]، لذا إعتمد أنصار هذا الإتجاه في تعريفه لها

---

[1]- **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص182.

[2]- وسوف نرى مستقبلاً تعدد المعايير والمواقف التي قيلت في تعريف هذه الجريمة ما بين موسع ومضيق لها، وما بين تعريف موضوعي ينظر إلى السلوك الإجرامي ذاته من الناحية القانونية، وآخر تعريف شكلي يرتكز فقط على المفردات العلمية والتقنية الخاصة بها والمستحدثة في مجال تقنيات الحاسب الآلي وشبكة الإنترنت.

[3]- تعرف الوسيلة المستعملة عموما بأنها: "الطريقة التي يتم إستخدامها من قبل مرتكب الجريمة لمباشرة السلوك الإجرامي أو النشاط المادي للجريمة"، وأحيانًا يقرر القانون لزومًا لوجودها لكي يمكن إحداث تطابق بين النموذج الإجرامي وبين الواقعة المادية، ومن ثم تحديد المسؤولية الجنائية وإستحقاق العقاب، ولكي يعترف القانون بالوسيلة المستعملة يجب لزومًا توافرها بعينها حتى نكون أمام جريمة تستوجب العقوبة أو إتخاذ تدابير معينة حيال مرتكبها، أو أنها تصبح ظرفًا مشددًا يجعل من العقوبة مشددة، (لمزيد من التفصيل حول الموضوع أنـظر فـي ذلك: - **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، الأردن، 2009، ص36).

[4]- كما قد تكون الوسيلة المستعملة في إرتكاب الجريمة، هي شبكة الإتصالات الدولية، فتعرف الجريمة على أساسها أنها: "كل فعل غير مشروع يقوم بواسطة الشبكة الدولية للإتصالات - الإنترنت" إلا أنه يبقى معيار منتقد. (أنظر: - **يونس عرب:** موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، منشورات إتحاد المصارف العربية، ج1، ط1، القاهرة، مصر، 2002، ص7).

على أساس الوسيلة المستعملة في إرتكاب الجريمة، ولعل من بين أهم ما جاء به أنصار هذا التوجه من تعاريف نجد ما يلي:

- عرفها الفقيه الألماني "تيدمان– *Tiedemann*" بأنها: "جريمة تشمل كل أشكال السلوكيات غير المشروعة والتي ترتكب بإستخدام الحاسب الآلي"[1].
- وعرفها آخرون أنها: "أي عمل غير قانوني يستخدم فيه الحاسب الآلي كأداة رئيسية للجريمة"[2].
- وذكرت بأنها: "الإعتداءات غير القانونية التي ترتكب بواسطة تقنية المعلومات بإستخدام أجهزة المعالجة الآلية للمعطيات بغرض تحقيق مصلحة"[3].
- وقيل فيها بأنها: "كل فعل جنائي يستخدم الكمبيوتر في إرتكابه أداة رئيسية"[4].
- وعرفها الفقيه هشام محمد فريد رستم بأنها: "كل سلوك غير مشروع يمس المجتمع، والذي يرتكب بإستخدام الحاسب الآلي"[5].
- وجاء في ذكرها أيضًا أنها: "كل نشاط إجرامي تستخدم فيه تقنية الحاسوب بطريقة مباشرة أو غير مباشرة أو كهدف لتنفيذ العمل الإجرامي المقصود"[6].
- كما عرفت أنها: "كل الأفعال والإعتداءات غير القانونية التي تتصل بالمعلوماتية وترتكب بواسطة الحاسوب بغرض تحقيق ربح أو مصلحة"[7].
- وعرفها البعض بأنها: "كل المخالفات التي تتم بإستخدام شبكات الإتصالات الرقمية سواء أرتكبت ضد فرد أو مجموعة من الأفراد بدافع الجريمة وبقصد إيذاء الضحية ماديًا أو معنويًا بطريقة مباشرة أو غير مباشرة"[8].

---

[1]– **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2007، ص27.

[2]– **ذياب البداينة:** الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، عمان، الأردن، 2002، ص102.

[3]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص48.

[4]– **محمد محمود مكاوي:** الجوانب الأخلاقية والإجتماعية للجرائم المعلوماتية، المكتبة العصرية، المنصورة، مصر، 2010، ص29.

[5]– **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1992، ص 29.

[6]– **محمد الأمين البشري:** التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنت، من (1–2000/5/3)، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ط 03، مج 03– 2004، ص 1036. – **طه السيد أحمد الرشيدي:** مدى المواجهة التشريعية لجرائم المعلومات، دار الكتب والدراسات العربية، الاسكندرية، مصر، 2016، ص18.

[7]– **أمين طعباش:** الحماية الجنائية للمعاملات الإلكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، مصر، 2015، ص17.

– **محمد نصر محمد:** الوسيط في الجرائم المعلوماتية، ط1، مركز الدراسات العربية للنشر والتوزيع، القاهرة، مصر، 2015، ص33.

[8]– **ذياب موسى البداينة:** الجرائم الإلكترونية المفهوم والأساليب، الملتقى العلمي الدولي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، جامعة عمان، الأردن، 2014، مجلة الكلية، ص77.

– كما عرَّفها "توم فوستر *Tom–Fsoter*"" على أنها: "فعل إجرامي يتم بإستخدام الحاسوب كأداة رئيسية"[1].

– وذكرت بأنها: "أي نوع من أنواع الجرائم التي ترتكب بإستخدام الحاسوب أو تسهل بإستخدامه".[2]

– وعرفها "مارتان واسيك *Martin Wasik*" بأنها: "كل سلوك غير أخلاقي تستخدم فيه الحاسبات أو بياناتها أو برامجها بطريقة غير مشروعة لإرتكاب جريمة تنطوي بطريقة أو بأخرى على إستعمال تكنولوجيا المعلومات".[3]

– وعرفت كذلك بأنها: "أي سلوك غير مشروع يرتكب بواسطة حواسيب أو أي نظام حاسوبي أو شبكة حاسوبية، من أجل الوصول إلى المعلومات وعرضها أو توزيعها بصورة غير مشروعة".[4]

– أما مؤتمر الأمم المتحدة العاشر المتعلق بمنع الجريمة ومعاقبة المجرمين، فقد تبنى هو الآخر تعريفاً للجريمة المعلوماتية ضمن أحد توصياته مفاده أنها: "أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وهذه الجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية".[5]

– كذلك عرفت بأنها: "الفعل غير المشروع الذي يتورط في إرتكابه الحاسب الآلي، أو يستخدم في إقترافه الحاسوب بإعتباره الأداة الرئيسية".[6]

نقد الإتجاه: إن التنوع في الجرائم المعلوماتية والناشئة عن إستخدام الحاسوب أو الإنترنت، يجعل التمييز قائمًا بينها وبين الجرائم الحديثة الأخرى، ولكن ليست بالضرورة كل جريمة ناشئة عن إستخدام الحاسوب أو الإنترنت هي من الجرائم المعلوماتية، بل أن هناك عديد الأفعال ما يمكن وصفه بالجرائم التي كانت وسيلتها الإنترنت، كجرائم الإرهاب والإجرام المنظم وغيرها، ويقضي مثل هذا الطرح أو المعيار هو تجريم الوسيلة المستعملة، وإن كانت في طبيعتها مشروعة.[7]

---

[1]– **محمود أمحمد عبابنة:** جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص15.

[2]– **عبد الرحمن عبد العزيز الشنيعي:** أمن المعلومات وجرائم الحاسب الآلي، (د.د.ن)، 1995، ص28.

[3]– ***MARTIN Wasik:*** *Crime and the computer, Oxford university, 1991, P4.*

[4]– **تركي بن عبد الرحمن المويشير:** بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2009، ص11.

[5]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص50.

[6]– **عبد الله أحمد هلالي:** إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، ص13.

[7]– **عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن إستخدام الإنترنت، دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص224.

والإنترنت لا يمكن أن تكون وسيلة إلى إرتكاب جرائم كونها بالأصل من الأنشطة المشروعة ذلك أن الإنترنت لا يمكن حيازتها وإستخدامها بشكل ذاتي، فهي ليست شيء ملموس وإنما سلوك تقني يحتاج إلى وسائل أخرى للقول بتوافرها، حيث تحتاج إلى الحاسوب وملحقاته على أن تكون متصلة فيما بينها بشبكة أو عدة شبكات مما يخلق في النهاية بيئة رقمية –نظم معلوماتية– كاملة حتى يمكن القول بتوافر الإنترنت.

فالإنترنت والحواسيب ليست بيئة غير مشروعة أصلاً إنما يمكن إرتكاب أعمال إجرامية على هذه البيئة أو من خلالها أو عبرها[1]، وعليه فإن وجدت علاقة بين الحاسب الآلي وإرتكاب بعض الجرائم، فهو نتيجة طبيعة للتطور التكنولوجي في الوقت الحاضر.

وعليه فإن الإعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في إرتكابها هو أمر غير منطقي تمامًا، لأن تعريف الجريمة يستوجب الرجوع إلى الفعل المجرم والأساس المكون له وليس إلى الوسائل المستخدمة لتحقيقه فحسب، أو لمجرد أن الحاسب الآلي أتستخدم في جريمة ما يتعين أن نعتبرها من الجرائم المعلوماتية. على أساس أننا لكي نكون أمام جرائم معلوماتية؛ يجب الرجوع إلى السلوك الأساسي المكون لها وليس إلى الوسائل المستخدمة لتحقيقه فحسب، كما يرى الأستاذ والفقيه القانوني "*R F. Anderson*" أنه: "ليس مجرد أن الحاسب قد أستخدم في جريمة ما، أن نعتبرها من الجرائم المعلوماتية...".[2]

ثانيًا– التعريف على أساس معرفة الفاعل بتقنية المعلومات (الإتجاه الشخصي)

بعد الإنتقادات الشديدة التي وجهت للإتجاه السابق، تم إعتماد إتجاه ومعيار جديد يهتم بصفة الجاني من حيث معرفته التقنية والفنية بأمور التكنولوجيا والحواسيب، لذا جاءت تعريفات الإتجاه الشخصي للجريمة المعلوماتية تستند إلى مدى المعرفة التقنية لدى مرتكب الجريمة، إذ أن هذا النوع من الإجرام يتطلب لتنفيذه توافر قدر من المعرفة الفنية لدى الفاعل، وأن يكون ملمًا بتقنية المعلومات من أجل القيام بجريمته، ومن أهم التعاريف القائمة على هذا المعيار نجد على سبيل المثال:

[1]– **محمد أحمد فكيرين:** أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، لبنان، 1993، ص51.

[2]– **يونس عرب:** موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، المرجع السابق، ص8.

– تعريف لوزارة العدل الأمريكية الذي جاء فيه أن جرائم تقنية المعلومات هي: "جرائم لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من إرتكابها".[1]

– كما عرفتها موسوعة "بريتانيكا *Britanika*" بأنها: "أي جريمة ترتكب عن طريق معرفة خاصة ومن له خبرة بتكنولوجيا الحاسوب".[2]

– ومن أهم تعاريف هذا الإتجاه نجد أيضًا تعريف الفقيه "أوبريش سيبر *Ubrich Sieber*" بأنها:

«*Est considéré comme crime informatique tout comportement illégal ou non autorisé qui concerne un traitement automatique de données ou de transmission de données*».[3]

– ومن تعريفات هذا الإتجاه نجد تعريف الفقيه "ديفيد تومبسون" "*David thompson*" والذي قال عنها: "أية جريمة يكون متطلبًا لإقترافها أن تتوافر لدى فاعلها معرفة تقنية وفنية للحاسب".[4]

– وعرفها آخرون بأنها: "ذلك النوع من الجرائم التي تتطلب إلمامًا خاصًا بتقنيات الحاسب الآلي ونظم المعلومات لإرتكابها أو التحقيق فيها ومقاضاة فاعلها".[5]

– كما عرفت أيضًا بأنها: "جريمة أو مجموعة الجرائم التي تتضمن أفعال غير مشروعة تكون لدى فاعلها معرفة بتقنيات وتكنولوجيات الحاسوب تمكنه من إرتكابها".[6]

– وقيل فيها أيضًا: "الجرائم التي يتم إرتكابها إذا قام الشخص بإستخدام معرفته بالحاسوب لإنجاز عمل غير قانوني".[7]

---

[1]– ويبدو أن هذا الإتجاه هو ما أخذ به معهد "ستانفورد أكاديمي للأبحاث الأمريكية" بالقول: "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من إرتكابها"، وهو نفس التعريف الذي تبنته وزارة العدل الأمريكية في دليلها لعام 1979، والمشار إليه أعلاه. – **عمار عباس الحسيني:** جريمة الإتلاف المعلومات، دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2019، ص12. – **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2005، ص34–35.

[2] **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص47.

[3]– ***ROSE (Ph) :*** *La criminalité informatique, édition (p. u. f) Paris, France, 1995, P33.*

[4]– ***DAVID (Th) :*** *Current trends in computer crime, computer control quarterly, Vol (09 N°(01), Ed, 1991, P8.*

- مشار إليه عند كل من:(– **عمار عباس الحسيني:** جريمة الإتلاف المعلومات، دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2019، ص12.– **محمود أحمد عبابنة:** جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر ، عمان، الأردن، 2005، ص17).

[5]– **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص13.

[6]– **محمد نصر محمد:** الوسيط في الجرائم المعلوماتية، المرجع السابق، ص35.

[7]– **عبد الله اليوسف:** التقنية والجرائم المستحدثة، مؤتمر الظواهر الإجرامية المستحدثة وسبل مواجهتها، تونس، في: (28–1999/6/30) مجلة المؤتمر، ص26.

– وذكرت بأنها: "الجريمة التي تنجز من خلال معرفة خاصة بتكنولوجيا الحواسيب".[1]

– كما يعرف أنصار هذا الإتجاه الجريمة المعلوماتية بأنها: "كل فعل غير مشروع يكون فيه العلم الكافي بتكنولوجيا الحاسبات الآلية لازمًا لإرتكابها".[2]

– كما قيل فيها أيضًا: "الجريمة التي يتم إرتكابها إذا قام شخص ما بإستخدام معرفته بالحاسب الآلي بعمل غير قانوني".[3]

نقد الإتجاه: هذا الإتجاه لم يسلم من النقد أيضًا، فقد ذهب البعض إلى القول أن هذا الإتجاه يضيق كثيرًا من مفهوم الجريمة المعلوماتية، حيث أن مشاركة المعرفة التقنية بالحاسب الآلي في النشاط الإجرامي سيضفي على هذا النشاط وصف الجريمة، فهذا القول ينطوي على مغالطة كبيرة حسب رأيهم، حيث أن كثيرة هي الجرائم المعلوماتية التي تحدث من طرف أناس محدودي المعرفة بتكنولوجيات الحواسيب[4]، وأيضًا نظرًا لكون أغلبها جرائم إشتراك ومساهمة جنائية؛ يرتكبها العديد من أشخاص مبتدئون في المجال الإلكتروني ولا يتقنون التعامل مع عناصر الوسط الرقمي.[5]

كما يتضح أيضًا من بعض التعريفات السابقة والتي تؤكد على ضرورة أن يكون لدى الجاني الدراية الكافية بتقنية المعلومات وتكنولوجية الحواسيب، فإنه يجب بالمقابل أيضًا أن يتوافر لدى أجهزة العدالة الجنائية الإلمام الكافي بهذه التقنيات والتكنولوجيات، بمعنى أن الجريمة الإلكترونية التي لم يكن لدى فاعلها أو لدى أجهزة العدالة الدراية الكاملة بهذه التقنيات من أجل ملاحقة الجاني وإقامة الدعوى ضده وتقديمه للمحاكمة، وإلاَّ فلا تعد هذه الجريمة إلكترونية، ومثالها الدول النامية التي تفتقر إلى هذه الدراية الكافية بالتكنولوجيات الحديثة والتي لا يتوافر لديها هذه التقنية العالية[6].

---

[1]– **أسامة أحمد المناعسة وجلال محمد الزغبي:** جرائم تقنية المعلومات الإلكترونية، ط2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2014، ص39.

[2]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص28.

[3]– **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2001، ص23.

[4]– **محمد عبد الله سلامة:** جرائم الكمبيوتر والإنترنت، ط1، منشأة المعارف، الاسكندرية، مصر، 2006، ص13–14.

[5]– **يونس عرب:** موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، المرجع السابق، ص11.

[6]– **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص14.

بل ذهب أنصار الإتجاه الشخصي إلى أبعد من ذلك وهو أن الجرائم التي يفتقر مرتكبيها وحتى أجهزة العدالة الجنائية فيها إلى هذه الدرجة من المعرفة بالتقنية، فإنها تعد جرائم تقليدية وعادية تتكفل بها النصوص التقليدية للقوانين الجنائية[1]، فحسب هذه التعاريف أنه يجب أن تتوافر معرفة كبيرة بتقنيات الحواسيب وكل الوسائط الإلكترونية الأخرى، وهذا ليس فقط لإرتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا الإتجاه بدوره يضيّق بدرجة كبيرة من مفهوم الجريمة المعلوماتية.

وهكذا يظهر قصور هذه التعاريف واضحًا، إذ أن مجرد توافر المعرفة التقنية بعلمٍ ما لا يكفي في ضوء عدم توافر العناصر القانونية الأخرى لتصنيف الجريمة ضمن الجرائم المتعلقة بذلك العلم.

ثالثًا- التعريف على أساس محل وموضوع الجريمة (الإتجاه الموضوعي)

إن محل الجرائم المعلوماتية هو دائمًا المعطيات الحاسوبية بدلالتها الواسعة[2]، إما بذاتها كالبيانات والمعطيات المدخلة والمخرجة أو المخزنة[3] أو بما تمثله كالبرامج على مختلف أنواعها[4]، وقد تكون هذه المعطيات والبرامج موجودة داخل النظام أو على أحد الوسائط التقنية المعدة للتخزين، أو أنها تكون في طور النقل والتبادل ضمن وسائل الإتصال المدمجة مع نظام الحوسبة.

حيث يذهب أنصار هذا الإتجاه إلى الإستناد على محل الجريمة المعلوماتية، فلكي تتحقق هذه الجريمة _عندهم_ يجب أن يكون الحاسب أو أنظمته محلاً وموضوعًا لهذه الجريمة، وعليه في ظل هذا الإتجاه فإن تعريف هذه الجريمة يرتكز على الأفعال غير المشروعة التي تقع ضد الحاسب أو النظام المعلوماتي، ليس بإعتبارهما الوسيلة في إرتكاب الجريمة أو من له خبرة تقنية بهما، بل كونهما موضوعًا ومحلاً لإرتكابها[5].

---

[1]- **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، المرجع السابق، ص30.

[2]- من أهم الدلالات الواسعة لمعطيات الحاسوب نجد على سبيل المثال: (البرامج بأنواعها، البيانات المدخلة، بيانات ومعلومات معالجة آليًا ومخزنة، المعلومات المستخرجة والمتبادلة ما بين النظم ... وغيرها كثير).

[3]- **البيانات والمعطيات هي:** كل ما يمكن إلتقاطه ومعالجته سواء عن طريق تسجيله وتصنيفه وتنظيمه، مع إمكانية إرساله بواسطة إشارة أو مجموعة إشارات تحمل المفاهيم المتمثلة بواسطة المعطيات، حيث تتم بواسطة ناقل فيزيائي أو إلكتروني أو حتى ضوئي.
(أنظر: - **عبد الفتاح مراد:** موسوعة مصطلحات الكمبيوتر والإنترنت، د. د. ت، القاهرة، مصر، د. ت. ن، ص1047).

[4]- **البرامج:** تعد من أهم المصنفات المعلوماتية من حيث وجوب الإعتراف بها وتوفير الحماية القانونية لها، والبرامج أو البرمجيات هي الكيان المعنوي للحاسوب والنظام ككل، فمن دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط الحاسوباتية، وهي بوجه عام تنقسم إلى (برمجيات التشغيل) وأخرى (برمجيات التطبيق)، أنظر في ذلك: (- **أمير فرج يوسف:** الجرائم المعلوماتية على شبكة الإنترنت، المرجع السابق، ص55).

[5]- ***ROSE (Ph) :*** *La criminalité informatique, Op.Cit, P58.*

ومن أبرز التعاريف التي قال بها أصحاب هذا الإتجاه نجد على سبيل المثال:

– تعريف الأستاذ "توماس سميدينقوف *Thomas (J) Semdinghoff*" الذي ذهب إلى القول: "أن ما يسمى جريمة حاسوب يجب أن تتضمن تقريبًا أي ضرب من ضروب النشاط المعلوماتي الموجه ضد الحاسب أو المنطوي على إستخدام نظام الحاسب".[1]

– وعرفها الأستاذ "روسنبلاط *Rosenblatt*" بقوله هي: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".[2]

– كما عرفها الأستاذ "أولريش سيبر *Ulrich siber*" بأنها: "كل تصرف غير مشروع يتعلق بالمعالجة الآلية للمعطيات أو نقلها".[3]

– وجاء ذكرها أيضًا بأنها: "سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة جريمة محله معطيات الحاسوب".[4]

– ويرى آخرون من ذات الإتجاه بأنها: "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان محلها مرتبطًا بتقنية المعلومات".[5]

– وعرفت أنها: كل سلوك غير أخلاقي أو غير مصرح به يتعلق بموضوع المعالجة الآلية للبيانات أو المساس بها".[6]

– وقيل فيها أيضًا: "الجريمة الجنائية التي تنطوي على الحاسب كموضوع للجريمة أو محل لإرتكاب العنصر المادي لها".[7]

---

[1]– ***THOMAS (J) SMEDINGHOFF :*** *The legal guide to developing and marketing software, john wille & sons, 1986, P310.*

- مشار إليه عند: (– **عمار عباس الحسيني:** جريمة الإتلاف المعلوماتي، المرجع السابق، ص13).

[2]– **يونس عرب:** دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والأنترنت، ط1، إتحاد المصارف العربية، بيروت، لبنان، 2002، ص213.

[3]– **عبد اللطيف معتوق:** الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري، ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2012، ص10.

[4]– **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الإجرام والمجرم المعلوماتي، ط1، دار النهضة العربية، القاهرة، مصر، 2009، ص14. – **محمود محمد المرزوقي:** جرائم الحاسب الآلي، مقال منشور في المجلة العربية للفقه والقضاء، الصادرة عن منظمة الدول العربية، القاهرة، مصر، العدد 28، 2003، ص53.

[5]– **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، مصر، 1992، ص31.

[6]– **عادل يحي:** السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2014، ص45.

[7]– **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2005، ص179.

– كما عرفتها منظمة التنمية والتعاون الإقتصادي "*OCDE*" عام 1986 والتابعة لمنظمة الأمم المتحدة على أنها: "كل سلوك غير مشروع ومنافي للأخلاق أو غير مسموح به يرتبط إرتباط وثيق بموضوع المعالجة الآلية للبيانات من حيث المساس بها أو الإعتداء عليها عن طريق تدخل تقنية المعلوماتية"[1].

– وعرفها مركز شكاوى الإنترنت "*IC3*"[2] بأنها: "النشاط غير القانوني على واحد أو أكثر من مكونات الحاسوب أو شبكة الإنترنت وكذا المواقع المتاحة عبر الشبكة وغرف الدردشة والبريد الإلكتروني وغيرها من وسائل التواصل الإجتماعي".[3]

– وهناك تعريف لمكتب تقييم التقنية في الولايات المتحدة الأمريكية جاء فيه: "تلك الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية موضوعا رئيسيا".[4]

– كما عرفت بأنها: "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".[5]

– وزاد البعض في تعريفها بقولهم: "ليست هي التي يكون الحاسب الآلي أداة لإرتكابها، بل هي التي تقع على الحاسب أو داخل نظامه المعلوماتي".[6]

– وذكرها بعض الفقه الفرنسي أنها: "كل الأفعال غير المشروعة التي يكون الغرض منها موجه ضد الأموال والقيم المعلوماتية الموجودة داخل نظام المعالجة الآلية للمعطيات".[7]

---

[1]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2008، ص49. – **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص49.

[2]– **مركز شكاوى الإنترنت (*IC3*) هو:** إختصار لعبارة (*Internet crime complaint center*) والذي تأسس بالشراكة مع مكتب التحقيقات الفيدرالية الأمريكية (*FBI*)، والمركز الوطني لجرائم ذوي الياقات البيضاء (*Nationnal white collar crime center*)، وكذا مكتب مساعدة العدالة (*Bureau of justice assistance*) وهو وسيلة لتلقي الشكاوى الجنائية لضحايا جرائم الإنترنت، ولمزيد من التفصيل حول جرائم الإنترنت وكيفية عمل هذا المركز يرجى زيارة هذا الموقع الإلكتروني *www.ic3.gov* (تاريخ تصفح الموقع في 2017/02/28).

[3]– **طه السيد أحمد الرشيدي:** المرجع السابق، ص19. – **محمد عبد الله العوا:** جرائم الأموال عبر الإنترنت، المرجع السابق، ص18.

[4]– **هشام محمد فريد رستم:** الجرائم المعلوماتية، بحث مقدم إلى المؤتمر العلمي الدولي حول القانون والكمبيوتر والإنترنت، كلية الحقوق، جامعة العين، الإمارات العربية المتحدة، مجلة الكلية لعام 2001، ص111.

[5]– **فتيحة رصاع:** الحماية الجنائية للمعلومات على شبكة الإنترنت، ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2012، ص32.

[6]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص30.

[7]– **أمين طعباش:** الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2015، ص17.

– وعرفت كذلك بأنها: "كل تلاعب بمحتوى الحاسب الآلي ونظامه المعلوماتي من أجل الحصول على مكسب أو إلحاق خسارة بالمجني عليهم".[1]

– وتم تعريفها كذلك أنها: "كل سلوك إجرامي سلبي أو إيجابي يتم بموجبه الإعتداء على البرامج أو المعلومات المخزنة للإستفادة منها بأية صورة كانت".[2]

نقد الإتجاه: هذا المعيار هو الآخر منتقد، وذلك لتعقيده وصعوبة تحديد السلوكيات الواجب تجريمها، أن الإعتداءات على الكيانات المادية للحاسوب يخرج عن نطاق الجرائم الإلكترونية، لأن هذه الكيانات ما هي إلا قيم مالية، مما يجعلها محل صالح لتطبيق نصوص التجريم التقليدية المنظمة للجرائم الواقعة على الأموال[3]، إلا أنه يعد هنا الإتجاه من أهم المعايير التي تناولت .... الجريمة المعلوماتية بشكل صائب نوعًا ما، ففي منطق أصحاب هذا الإتجاه أن الجريمة المعلوماتية ليست هي التي يكون الحاسب الآلي أداة إرتكابها، بل هي الجريمة التي تقع على الحاسب أو داخل نظامه[4]، إذ أنهم يعتمدون في تعريفها على موضوعها بغض النظر عن الوسيلة المعتمدة أو صفات الجاني والمجني عليهم.

رأينا الخاص:

بعد هذا العرض المطوّل لبعض التعاريف التي حاولت تحديد مفهوم هذه الظاهرة الإجرامية، لابد لنا من وقفة نبين من خلالها ما هو التعريف المناسب من منظور المعيار الملائم لذلك.

فبالنسبة للإتجاه الذي أُعتمد على معيار الوسيلة المستعملة في إرتكاب الجريمة فهو غير دقيق، لأن تعريف الجريمة المعلوماتية يقوم في الأساس على الفعل الرئيسي المكوِّن لها وليس فقط الوسيلة المستخدمة في إرتكاب هذا الفعل، إذ لا يمكن أن يطلق على جريمةٍ ما أنها جريمةٌ معلوماتية لمجرد أن الحاسب أو النظام قد أُستخدم في تنفيذها، بل لابد من الرجوع إلى نوع السلوك المكون للجريمة وكذا محل الإعتداء وليس فقط التركيز حول الوسيلة المستخدمة لإرتكابها.

أما عن الإتجاه الذي يعتمد على معيار الخبرة والمعرفة في الأمور التقنية في إرتكاب الجريمة فهو الآخر غير سديد، والسبب في ذلك أنه يربط مفهوم هذا النوع من الجرائم بمعيار

---

[1]– **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، المرجع السابق، ص36.

[2]– **محمد حامد الهيتي:** التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص152.

[3]– **يونس عرب:** موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص11.

[4]– **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، المرجع السابق، ص34.

شخصي يتصل بالفاعل يصعب إكتشافه أو تحديده بسهولة، فكثيرة هي هذه الجرائم المرتكبة من طرف أشخاص يفتقرون إلى المعرفة والخبرة التقنية والفنية للحاسبات الآلية وملحقاتها.

أما عن الإتجاه القائل بتعريف هذه الجريمة على أساس موضوعها ومحلها كمعيار لتعريف الجريمة المعلوماتية، فإنه تعريف مقبول نوعًا ما وذلك لأنه يتناسب مع كافة أنواع الإجرام المعلوماتي فنعتقد أن هذا الإتجاه الأخير كان موفقًا بعض الشيء في تعريف هذه الجريمة، لكنه لم يكن في ذات الدرجة من حيث التكييف والتحديد لعناصر الجريمة.

وهذا إذا ما دلَّ فإنه يدلُّ على عدم وجود توافق الفقه الجنائي الحديث على تعريف جامع مانع لجرائم الحاسوب والإنترنت بمفهومها الصحيح، فهناك العديد من التعريفات الموسعة والضيقة والتي يمكن ردها إلى ضوابط ومعايير مختلفة، وكلها تظل عاجزة عن الإحاطة بمفهوم دقيق للجريمة المعلوماتية، إذ أنها كما قيل عنها أنها جريمة تقاوم التعريف، ولا يوجد لديها تعريف متفق عليه للدلالة عليها، مما يصعب معه التقدير بإمكانية إيجاد تعريف موحد، والسبب في ذلك راجع إلى حداثة هذه الجريمة نسبيًا وأنها مُتَحَوِّرةٌ مستقبلاً، وهو ما يخشى معه حصرها في نطاق واحد وضيق مما قد يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

ونحن من جانبنا نتفق مع هذه التعاريف جميعها، إذ أنها تعاريف حاولت الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية، سواء التي قد تقع بواسطة النظام المعلوماتي أو أنها تقع داخل هذا النظام على المعطيات والبرامج والمعلومات، أو تلك التي إهتمت بالتركيز على فاعل الجريمة ومقدرته التقنية في البيئة الإلكترونية، أو التي تهتم بالغاية والنتيجة التي يسعى إليها المجرم المعلوماتي.

وعليه فإنه بالنظر إلى كل التعاريف واسعة الإتجاهات والمفاهيم الفقهية والقانونية المطروحة سلفًا؛ يمكن من خلالها أن نتصور أن كل سلوك تقليدي مجرم يتصل بعناصر الوسط الرقمي هو بمثابة جريمة معلوماتية، إلا أن بعض الفقه يرى عكس ذلك تمامًا، فهم يفرِّقون بين تقنية المعلومات والمعلومات في حد ذاتها، حيث كل من إعتمد على تقنية المعلومات دون المساس بالمعلومات المعالجة آليًا فهنا نكون أمام جريمة تقليدية يعاقب عليها وفق الأحكام الجنائية التقليدية، أما من قصد المعلومات المعالجة والمخزنة بالإعتداء والمساس بها فهنا نكون أمام جريمة

معلوماتية، وهذا ما يتفق مع الإتجاه الأخير المعتمد على موضوع الجريمة في تعريفها إذ يكاد يكون هو أقرب أنواع التعريفات والتي يمكن أن تطبق على معظم جرائم الحاسوب إن لم يكن كلها.

وفي الأخير وتأسيسًا على ما تقدم فإن التعريف الذي يمكن أن يقترحه الباحث بناءً على ما تقدم ذكره، هو أن الجريمة المعلوماتية هي عبارة عن: "كل سلوك إيجابي أو سلبي غير مشروع ومخالف للقواعد القانونية أُرتكب عمدًا أو بالخطأ بإستخدام تكنولوجيا الحاسوب أو النظام المعلوماتي وما في حكمهما من شأنه المساس بالمواقع الإلكترونية أو البيانات والمعلومات المعالجة آليًا أو بأي مصلحة معلوماتية محمية قانوناً يترتب عنه ضرر بالغير".

ونحن من هذا التعريف نميل أكثر إلى الإتجاهين الأول والثالث فقط دون الإتجاه الثاني، وهذا بسبب أن الجريمة المعلوماتية تعتمد على معيارين إثنين – حسب رأينا المتواضع – وهما المعيار الفني والمعيار الموضوعي، لأن هاذين المعيارين يصلحان تقريبًا لكل الجرائم المعلوماتية.

مع العلم أن هذا التعريف الذي يضعه الباحث قد يكون هو الآخر محل الإنتقاد، وهذا أمر ممكن جدًا، وهذا بحكم أن هذه الجريمة ظاهرة حديثة ومتغيرة بإستمرار، ناهيك عن التكنولوجيا المعقدة والتي تلعب دورًا كبيرًا في حدوثها.

الفرع الثالث: التعريف القانوني للجريمة المعلوماتية

معظم القوانين سواء الأوروبية أو العربية إعتمدت في تعريفها للجريمة المعلوماتية على معيارين إثنين وهما المعيار الفني والمعيار الموضوعي، وذلك على النحو التالي:

أولاً: في القوانين الغربية

في هذا الإطار آثر المشرع الإنجليزي في قانون إساءة إستخدام الحاسوب لعام 1990، على عدم وضع تعريف محدد لجرائم الحاسوب، وكذا الجرائم المشابهة لها، وهذا بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسبًا للتطورات العلمية في المستقبل، لاسيما في المجالات الفنية والتقنية في عالم الحواسيب والإنترنت[1].

ولعل من بين أهم التعاريف التي وردت عن بعض الدول الغربية وبالخصوص الأوروبية، في تعريفها للجريمة المعلوماتية نجد على سبيل المثال:

[1]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص46-47.

أ- تعريف القانون الأمريكي: ولقد عرفها القانون الأمريكي رقم (1213) لعام 1986 المتعلق بمواجهة جرائم الكمبيوتر بأنها: "الإستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الإستخدام الضار بأجهزة الكمبيوتر، على أن تتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة".[1]

ب- تعريف إتفاقية الأمم المتحدة: فقد عرفتها منظمة التعاون الإقتصادي والتنمية (*OCDE*) التابعة للأمم المتحدة بأنها: "كل فعل أو إمتناع عن فعل من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية".[2]

ج- تعريف القانون البلجيكي: من خلال الإجابة البلجيكية على الإستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية (*OCDE*) حول الغش المعلوماتي عام 1982 ورد للجريمة المعلوماتية تعريف قانوني مقتضاه أنها عبارة عن: "كل فعل أو إمتناع عن فعل من شأنه الإعتداء على الحقوق المادية أو المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[3]

ثانيًا- في القوانين العربية

لقد عرفت كل الدولة العربية الجريمة المعلوماتية، في قوانينها الخاصة والداخلية وإن إختلفت نوعًا ما هذه التعاريف من قانون لآخر، ولعل السبب في ذلك، يرجع إلى رغبة المشرع الجنائي العربي في تحديد السلوك الإجرامي المستحدث على الوجه الدقيق، فراح كل قانون عربي محاولاً أن يضبط نموذج السلوك[4]، الذي يعد جريمة معلوماتية، وهذا حفاظًا على حقوق وحريات الأفراد من جهة، وإحترامًا لمبدأ المشروعية من جهة أخرى.

أ- تعريف جامعة الدول العربية: لم يرد في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[5]، أي تعريف لمصطلح الجريمة المعلوماتية، وإنما تركت المجال مفتوح أمام كل دولة عربية في تعريف

---

[1]- **جميل عبد الباقي الصغير:** القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، مصر، 1992، ص10.

[2]- **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2011، ص15.

[3]- **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، المرجع السابق، ص37.

[4]- أي سلوك إجرامي يشمل فعل الإتيان أو الإمتناع عن الفعل، لذلك يطلق عليه الفقه الجنائي (بالسلوك الإيجابي والسلوك السلبي) بشرط أن يكون هذا السلوك بنوعيه غير مشروع، وهذا بإعتبار أن المشروعية تنفي عن الفعل الصفة الجرمية، وإسباغ الصفة الإجرامية لا تتحقق في ميدان القانون الجنائي إلا إذا كان الفعل منصوص ومعاقب عليه قانوناً، معنى أن إرادة المشرع تجاه الفعل غير المشروع تكمن في تجريمه بنص القانون، ومن غير ذلك لا نستطيع الكلام عن الجريمة حتى ولو كان السلوك مخالفًا للأخلاق، لمزيد من التفصيل حول الموضوع، ينظر في ذلك: (- **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، المرجع السابق، ص32).

[5]- حررت هذه الإتفاقية باللغة العربية بمدينة القاهرة في جمهورية مصر العربية في 2010/12/21.

الجريمة المعلوماتية، وذلك رغبة منها في تعزيز روح التعاون العربي لمكافحة جرائم تقنية المعلومات التي أصبحت تهدد أمنها ومصالحها وسلامة مجتمعاتها، وإقتناعًا أيضًا منها بضرورة الحاجة إلى تبني سياسة جنائية حديثة ومشتركة تهدف إلى المجتمع العربي ضد جرائم تقنية المعلومات ونبذ كل أشكال الإجرام الحديث مع مراعاة النظام العام لكل دولة، وهذا ما نصت عليه المادة الأولى من هذه الإتفاقية بقولها: "تهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها".[1]

ب- تعريف القانون السوري: عرفها قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم (17) لسنة 2012، فجاء في نص المادة الأولى منه: "الجريمة المعلوماتية، جريمة ترتكب بإستخدام أجهزة الحاسوب أو الشبكة، أو تقع على المنظومات المعلوماتية".[2]

ج- تعريف القانون السعودي: عرفها قانون نظام مكافحة الجرائم المعلوماتية السعودي رقم (79) لسنة 2007 بموجب المادة (8/1) منه بالقول: "الجريمة المعلوماتية، أي فعل يرتكب متضمناً الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[3]

د- تعريف القانون القطري: عرفها قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014 بموجب المادة الأولى منه بالقول: "الجريمة الإلكترونية، أي فعل ينطوي على إستخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام هذا القانون".[4]

هـ- تعريف القانون الكويتي: حيث عرفت المادة الأولى من القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، للجريمة المعلوماتية بأنها: "كل فعل يرتكب من خلال إستخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"[5].

---

[1]- أنظر المادة الأولى من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والمشار إليها سلفاً.

[2]- أنظر المادة الأولى من القانون السوري رقم (17) لعام 2012 والمتعلق بقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

[3]- أنظر في ذلك المادة (8/1) من القانون السعودي رقم (79) لسنة 2007. والمتعلق بقانون نظام مكافحة الجرائم المعلوماتية.

[4]- أنظر في ذلك المادة الأولى من القانون القطري رقم (14) لسنة 2014 والمتعلق بقانون مكافحة الجريمة الإلكترونية.

[5]- أنظر في ذلك المادة الأولى من القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

و- تعريف القانون الجزائري: أما في الجزائر فقد تبنى المشرع تعريفًا للجريمة المعلوماتية، وذلك بموجب المادة الثانية من القانون رقم (04/09) والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، بأنها: "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة أو نظام الإتصالات الإلكترونية".[1]

ويتفق كثير من المهتمين والباحثين في هذا المجال مع هذا التعريف القانوني للمشرع الجزائري، كونه يشمل عديد الإعتداءات الواقعة على النظام المعلوماتي بما في ذلك شبكة المعلومات العالمية الإنترنت، فضلاً عن الجرائم التي من الممكن أن ترتكب أو يسهل إرتكابها بواسطة نظم الحوسبة كالكمبيوتر وغيرها، وكذا نظم الإتصالات الإلكترونية وأيضًا وسائل التواصل الإجتماعي الحديثة.[2]

المطلب الثاني: السمات الخاصة بالجريمة المعلوماتية

على الرغم مما أضافته نظم المعالجة الآلية من الجوانب الإيجابية، إلا أنها في المقابل جلبت معها طائفة جديدة من الجرائم أطلق عليها "بالإجرام المعلوماتي *Délit de l'information*"، فجعلتها تتميز بسمات وطابع خاص يميزها عن غيرها من الجرائم التقليدية الأخرى. وخصوصية هذه الجريمة تتعدد من حيث مميزاتها (فرع أول) كما أن لها خصوصية من حيث وسائل إرتكابها والأخطار الناجمة عنها (فرع ثاني) وهذا ما سوف نقوم بدراسته في هذا المطلب.

الفرع الأول: خصوصية الجريمة المعلوماتية من حيث مميزاتها

تتميز هذه الجريمة عن الجرائم التقليدية بمجموعة من الخصائص الفريدة والمتميزة، بحيث تكمن أهمية تبيان وتحديد تلك الخصائص في تحديد طبيعتها الخاصة، ولعل من بين أهم هذه المميزات نجد ما يلي:

أولاً: أنها من الجرائم المنظمة والعابرة للحدود الوطنية

تتميز الجريمة المعلوماتية بعدم وجود حدود جغرافية لها، وهذا راجع إلى الإنتشار الواسع لأجهزة الحواسيب عبر أرجاء العالم هذا من جهة، ومن جهة أخرى نجد أن شبكة الإنترنت قد ألغت

[1]- أنظر في ذلك المادة الثانية من القانون الجزائري رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الصادر بتاريخ 05 أوت 2009.

[2]- **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2019، ص59.

أي حدود جغرافية بين الدول جاعلة من العالم قرية صغيرة، فإتصفت معها هذه الجريمة بالعالمية[1]، وأنها عابرة للحدود الدولية *Transnational*، ذلك أن ربط العالم بشبكة من الإتصالات من خلال الأقمار الصناعية والفضائيات وشبكة الإنترنت كل ذلك ساعد على الإنتشار الثقافي والمعلوماتي، وساعد أيضا في إنتشار الجريمة، وهو ما أصطلح عليه "بعولمة الثقافة وعولمة الجريمة" ومنه أصبحت ثقافة الجريمة أمراً ممكناً وشائعاً لا يعترف بالحدود الإقليمية للدول ولا يعترف لا بالمكان ولا بالزمان، وإنما أصبحت ساحتها العالم أجمع[2].

وذلك أن شبكة الإنترنت وكما يشاهد الجميع نجدها ربطت العالم بشبكة إتصالات جد متميزة وفعالة، فقربت جميع شعوب العالم على الرغم من إختلاف جنسهم وعقائدهم وثقافاتهم ولغاتهم من بعضهم البعض بصورة لم تكن موجودة من قبل حتى كادت أن تلغي الحدود الجغرافية بين الدول، وعلى الرغم من هذه الإيجابيات إلا أن إستخدام هذه الشبكة أدى إلى حدوث سلبيات عديدة تمثلت في ظهور نوع جديد من الإجرام المنظم، والذي أصبح منتشر في كل المعمورة بواسطة الاستخدام الواسع والمجاني للإنترنت[3]، وما صاحبه من خلق مشكلة عالمية أصبحت تعرف بالجريمة المعلوماتية التي لا تعترف بالحدود الإقليمية للدول والعابرة لها، فلا تراعي في ذلك لا الزمان ولا المكان، ومن دون أن تخضع في ذلك للحراسة ونقاط التفتيش، وهذه الخاصية مكنت مجرمي المعلوماتية من إرتكاب جرائمهم عن بعد من دون حاجة إلى الحركة والتنقل ما بين الدول، حتى أصبح العالم بأجمعه ساحة واسعة لتلك الجرائم[4].

وبالتالي يمكن لمرتكب هذه الجرائم والذي يكون موجود في دولة ما من إرتكاب جريمته عبر حاسبه الآلي بإستخدام الشبكة العالمية "الإنترنت" ليوقع أضرَارًا بشخص آخر يوجد في دولة أخرى دون أن يغادر المجرم مقعده الذي جالساً عليه أمام الحاسب الآلي، وهكذا هو مجتمع التقنية

---

[1]– **خالد ممدوح ابراهيم:** حوكمة الإنترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2011، ص360. – **عمرو عيسى الفقي:** الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، مصر، 2006، ص86. – **جميل عبد الباقي الصغير:** الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص75.

[2]– **محمود رجب فتح الله:** المرجع السابق، ص266.

[3]– **فيروز لطرش:** الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، ع1، جامعة زيان عاشور، الجلفة، الجزائر، 2016، ص325.

[4]– **عزيزة رابحي:** الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018، ص96. – **عبد الوهاب ملياني:** المرجع السابق، ص56. – **نسرين عبد الحميد نبيه:** المرجع السابق، ص133.
– **محمود أحمد عبابنة:** المرجع السابق، ص34. – **نهلا عبد القادر المومني:** المرجع السابق، ص50.

الحديثة[1] لذلك هذا النوع من الإجرام هو صورة صادقة من صور العولمة *La Mondialisation*، وهذا لإمكانية إرتكابها عن بعد، وهو الأمر الذي أثار العديد من التساؤلات حول مسألة القانون الواجب التطبيق في مثل هذه الحالات من الجرائم، والسبب يعود في ذلك إلى تعدد الأماكن التي يمكن من خلالها للجاني إرتكاب جريمته والتي يمكن أن تكون بين أكثر من دولة، هذا بالإضافة إلى خضوع القانون الجنائي لمبدأين في غاية الأهمية وهما إقليمية القانون الجنائي وعالمية القانون الجنائي من حيث المكان، أما من حيث الزمان فإن التوقيت الزمني يختلف بين الدول أيضًا[2].

وكل ما سبق ذكره، وما سوف يأتي معنا في هذه الدراسة يعطي من الدلالة على أن الأمر تخطى كل الحدود المعتادة ووصل الأمر إلى أن عرف العالم جماعات متخصصة في القرصنة الإلكترونية والإرهاب الإلكتروني، بحيث لم يعد الأمر يختص به أفراد عاديين، بل أنها أصبحت جريمة منظمة بإمتياز عابرة للحدود الوطنية تستهدف أماكن متعددة في دول مختلفة تتأثر بها في آن واحد[3]، فتتم عادة بأسلوب منظم أي بتعاون أكثر من شخص واحد في إرتكابها من خلال الإتفاق المسبق في تسهيل إتمامها، ويظهر ذلك بوضوح في إستئجار القراصنة المحترفين للقيام بالأعمال غير المشروعة مقابل مبالغ مالية أو فوائد أخرى[4]، حيث نجد أن مستخدم الإنترنت من دولة ومورد المعلومات أو مقدم خدمة الإشتراك من دولة أخرى، ومن يقوم بمعالجة البيانات وإدخالها ونشرها عبر الشبكة من دولة ثالثة، وهذا الطابع الدولي والمنظم لهذه الجريمة يثير العديد من الإشكاليات والصعوبات لا سيما مشكلة تحديد القضاء أو المحكمة المختصة دوليًا بنظرها، وكذا القانون الواجب التطبيق عليها، ولهذا فمكافحة هذا النوع من الإجرام المنظم يتطلب تعاونًا دوليًا وتوافقًا كبيرًا بين كل التشريعات الوطنية[5] وضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي للحد منها أو مواجهتها[6].

---

[1]– **مجتمع التقنية الحديثة:** هو مجتمع لا يعترف بالحدود الطبيعية أو الحدود السياسية، فهو مجتمع منفتح النظير عبر شبكات تخترق الزمان والمكان دون أن تخضع لضوابط المراقبة الحدودية، فتسمح لمستخدميها بالتنقل المعنوي والافتراضي بين مختلف الدول والقارات بدون تعقيدات أو صعوبات أو عوائق. (أنظر: – **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص33).

[2]– **أحمد كيلان عبد الله صكر:** الجرائم الناشئة عن إساءة استخدام الحاسوب، ماجستير، كلية الحقوق، جامعة بغداد، 2002، ص35.

[3]– **رشاد خالد عمر:** المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الإسكندرية، مصر، 2013، ص36.

[4]– **بن عقون حمزة:** السلوك الإجرامي للمجرم المعلوماتي، ماجستير، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2011، ص25. – **منير محمد الجهيني وممدوح محمد الجهيني:** المرجع السابق، ص15.

[5]– **محمد خليفة:** الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر، 2007، ص37.

[6]– **أحمد محمود مصطفى:** جرائم الحاسبات الآلية في التشريع المصري، المرجع السابق، ص19.

ثانيًا: أنها جريمة يصعب إكتشافها وإثباتها بسهولة

تتسم الجرائم الناشئة عن إستخدام تكنولوجيا المعلومات بصعوبة إكتشافها بدرجة أولى، ويرجع ذلك في أن أغلبها لا يلاحظها المجني عليه مع أنها قد تقع أثناء وجوده على الشبكة، ولكنه لا يكون عالمًا بها ولا ينتبه إليها إلا بعد فترة من وقوعها، وذلك لأن الجاني يتعامل مع نبضات إلكترونية غير مرئية لا يمكن قراءتها بسهولة[1]، إلاّ بواسطة الحاسب الآلي وذلك من خلال إتباع طرق وأساليب لا يفطن إليها المستخدم العادي للشبكة، ومن أمثلتها إرسال فيروسات أو دس بعض البرامج الخاصة وتغذيتها ببعض البيانات التي تؤدي إلى عدم شعور المجني عليه بوقوع هذه الجريمة، ضف إلى ذلك أن الذين يرتكبون مثل هذه الجرائم الإلكترونية أنفسهم يستعملون تدابير أمنية واقية تخفيهم وتحجبهم عن الرؤية وتزيد من صعوبة الوصول إليهم أو حتى إكتشافهم[2].

فأغلب المجرمين في الجرائم التقليدية يتركون أثرًا يؤدي إلى إكتشافهم والعثور عليهم ولو بعد حين من الزمن، أما في الجرائم المعلوماتية فلا تترك في الأغلب آثارًا خارجية أو مادية تدل عليهم ففي نطاق الجرائم التقليدية نادراً ما تجد السلطات المختصة بالتحقيق والتحري صعوبة في كشف الآثار التي تدل على الجاني أو الكيفية التي تم إرتكاب الجريمة بها أو الخطوات التي تتبعها لإرتكاب جريمته، أما في نطاق الجريمة المعلوماتية فإنه يصعب أحياناً، بل وفي كثير منها من إكتشاف هذه الجريمة أو معرفة مرتكبيها، والسبب في ذلك هو أنها لا تترك آثارًا لها، كما يرجع السبب الرئيسي في ذلك أيضاً إلى التطور التكنولوجي الحاصل والمتلاحق الذي وصل إليه المجرم المعلوماتي اليوم[3]، ويطلق الفقه الحديث على هذه الآثار مصطلح "الآثار المعلوماتية الرقمية *Artefacts informationnels numériques*"، والتي تتيح لأصحاب الضبط القضائي في حال وجود مثل هذه الآثار القدرة على رؤية أو الكشف عن مسرح الجريمة والتي يمكن من خلالها حل القضية والوصول إلى الفاعل بسهولة[4].

---

[1]– **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017، ص 74.

[2]– **عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار النهضة العربية، القاهرة، مصر، 2000، ص40.

[3]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص49.

[4]– **جميل عبد الباقي الصغير:** الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص17.

ومع ذلك لا زالت الأجهزة المستخدمة في سبيل الكشف في مثل هذه الأنواع من الجرائم والتعرف على مرتكبيها تعاني الكثير أمام التطورات الحاصلة[1]، ضف إلى ذلك أن ما يصعب من إكتشاف هذه الجرائم هو قدرة المجرم على محو آثار جريمته في زمن قياسي قد لا يستغرق أكثر من ثوانٍ معدودةٍ.

كما تتصف الجرائم المعلوماتية من جهة ثانية أنها صعبة الإثبات، ولكن ليست مستحيلة الإثبات، حيث أنها جرائم لا تترك في الغالب أثرًا ماديًا ظاهرًا يمكن ضبطه ويشير إلى فاعله، وإنما هي كيانات منطقية تكون ضمن بيئة إلكترونية يمكن بسهولة إخفائها والتخلص منها[2]، ومن جانب آخر أن الجاني ينفذ جريمته عن بعد، فهو لا يكون متواجد في مسرح الجريمة خاصة إذا تم ذلك عن طريق إستخدام شبكة الإنترنت[3].

كما أن نقص الخبرات الفنية لدى سلطات البحث والتحري وجمع الإستدلالات أو حتى عند سلطات التحقيق، يكون أيضًا من الأسباب المهمة في صعوبة الحصول على الدليل، إذ يتطلب التحقيق في هذه الجرائم قدرًا كبيرًا من المهارات والمعلومات الفنية والدراية الواسعة بالوسائل التقنية، ولعل قلة خبرات سلطات التحقيق هو أحد أسباب الإخفاق في إكتشاف هذه الجرائم والحصول على الدليل بشأنها بل والأكثر من هذا أحياناً المحقق يتلف الدليل عن خطأ ودون قصد منه، وهذا لقلة الدراية في كيفية التعامل مع هذه التقنية العالية[4].

ومن جانب آخر تكمن صعوبة الحصول على الدليل المادي لإثباتها، وهذا يرجع إلى إفتقاد وجود الآثار المادية التقليدية للجريمة وغياب الدليل البيولوجي أو الفيزيقي كالبصمات وغيرها من الشواهد المادية الأخرى[5]، بينما تغلب الصفة الإلكترونية على الدليل المتوفر في الجريمة المعلوماتية، فأغلب البيانات والمعطيات الإلكترونية تكون على شكل رموز مما لا يمكن للإنسان العادي قراءتها بسهولة، ناهيك على أنها معطيات قابلة للتغيير أو أنها تمحى تمامًا من السجلات المخزونة في ذاكرة الحاسبات الآلية، وهذا ما يصعب من التعرف على مرتكب الجريمة وذلك

---

[1]– **عزيزة رابحي:** المرجع السابق، ص97.

[2]– **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص58.

[3]– **أحمد كيلان عبد الله صكر:** المرجع السابق، ص41.

[4]– **محمود رجب فتح الله:** المرجع السابق، ص206. – **محمد علي سويلم:** شرح قانون جرائم تقنية المعلومات المصري، دار المطبوعات الجامعية، الإسكندرية، مصر، 2019، ص111.

[5]– **محمود رجب فتح الله:** المرجع نفسه، ص266.

بسبب غموض الدليل[1]، كما أن الجاني من الممكن أن يستخدم اسمًا مستعارًا، أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت *Cybercafés*[2].

ثالثًا: أنها جريمة لا يتم الإبلاغ عنها في أغلب الأحيان

ومن الخصائص التي تمتاز بها الجريمة المعلوماتية أيضًا أنها جرائم لا يتم الإبلاغ عند وقوعها في أغلب الأحيان، وذلك بسبب الثقة في عدم إكتشاف الفاعل أو الخوف من التشهير، خاصة إذا كان الأمر يتعلق بإحدى الشركات أو المؤسسات المالية أو التجارية، وذلك لتجنب الإساءة لسمعتها ورغبة منها في عدم زعزعة ثقة العملاء بها، وكذلك الأمر يحدث مع بعض الفئات من المواطنين العاديين وحتى رجال الأعمال[3]، وهو إحجام وإمتناع هؤلاء عن الإبلاغ عن مثل هذه الجرائم، والتي قد تهز من مراكزهم المالية في مجتمع المال والأعمال الذي ينتمون إليه، وكذا الخوف من فقدان ثقة المتعاملين معهم، ولربما أيضًا الخوف من الفضيحة والتشهير[4].

وهذا بدوره يقودنا إلى أنه لا توجد إحصائيات دقيقة لهذا النوع من الجرائم، والسبب في ذلك هو عدم تعاون المجني عليهم مع الأجهزة الأمنية، حيث أنهم لا يقومون بالتبليغ عن هذه الجرائم التي وقعت في حقهم[5]، فالرقم المظلم *Nombre sombre*[6] بين حقيقة عدد الجرائم التي تم إكتشافها رسميًا وعدد الجرائم التي لم يتم التبليغ عنها هو رقم شاسع وكبير، ومن هنا يمكننا القول أن الفجوة بين عدد هذه الجرائم الحقيقي وما تم إكتشافه فرق شاسع وكبير حقًا، لذا نجد أن معظم الجرائم المعلوماتية تم إكتشافها بالمصادفة أو التبليغ عنها بتحفظ، بل وبعد وقت طويل من إرتكابها[7].

---

[1]– **حسين بن سعيد الغافري:** بحث مقدم بعنوان "الجوانب القانونية للمعلوماتية بين النظرية والتطبيق" مقدم إلى المؤتمر العلمي الأول، والمنعقد في الفترة الممتدة من 13-2011/03/14، كلية الحقوق، جامعة السلطان قابوس، سلطنة عمان، مجلة الكلية، 2011، ص10. – **خالد ممدوح إبراهيم:** المرجع السابق، ص79.

[2]– **سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، 2013، ص21.

[3]– **حسين بن سعيد الغافري:** نفس المرجع، ص9 وما بعدها.

[4]– **فريد منعم جبور:** حماية المستهلك عبر الإنترنت ومكافحة الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص183.

[5]– **لينا محمد الأسدي:** المرجع السابق، ص26.

[6]– الرقم المظلم أو المبهم يعني وجود فارق كبير بين حجم الإجرام الحقيقي والإجرام المثبت رسميًا في محاضر رسمية، وهو عدد معرض للزيادة أو النقصان، ويرجع ذلك لعدة إعتبارات منها أن الجرائم الخطيرة غالبا ما يتم الإبلاغ عنها وتصل إلى علم الجهات الأمنية القضائية، ولكن بالمقابل فإن هناك جرائم لا تصل إلى علم السلطات المختصة كالجرائم البسيطة أو الجرائم الأخلاقية.
(أنظر أكثر: – **محمد شلال حبيب:** أصول علم الإجرام، العاتك لصناعة الكتاب، توزيع المكتبة القانونية، بغداد، العراق، 2007، ص42).

[7]– **خالد حسن أحمد لطفي:** المرجع السابق، ص22.

رابعًا: أنها جريمة قليلة المخاطرة وسهلة التنفيذ

لا تتطلب الجريمة المعلوماتية عنفًا للقيام بها أو مخاطرة وجهدًا كبيرًا في تنفيذها، فهي تنفذ بأقل جهد ممكن، وهذا مقارنة بالجرائم التقليدية الأخرى التي تتطلب نوعًا من المجهود العضلي، والذي يكون في صورة المخاطرة وممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف[1] فنسبة مخاطرة الجاني في الجرائم المعلوماتية قليلة نسبيًا بالمقارنة مع المخاطرة في الجرائم التقليدية فهو غير معرض لخطر المواجهة المباشرة مع المجني عليه أو غيره ولا لخطر المواجهة المسلحة مع الشرطة[2]، وهو ما يصطلح عليه "بالجرائم الناعمة *Crime doux*"، فعملية نقل بيانات من كمبيوتر إلى آخر أو السطو الإلكتروني على أرصدة بنك لا تتطلب أي عنف أو تبادل إطلاق النار مع رجال الأمن[3].

كما أنها جرائم سهلة وسريعة التنفيذ؛ إذ أنه وفي أغلب الأحيان لا يكون الركن المادي سوى القيام بالضغط على مفتاح أو زر معين في الجهاز، فهي لا تتطلب الإعداد قبل التنفيذ أو إستحضار معدات كبيرة، فقد يتم أحياناً التنفيذ عبر الهاتف المحمول[4]، ولهذا نشأت الحاجة الملحة لوجود طرق حماية قوية للمعلومات المخزنة في أجهزة الحواسيب أو وسائط النقل الإلكترونية التي تمنع الإختراق أو الدخول غير المصرح به[5].

وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو إستخدام معدات وبرامج معينة، على الرغم من تنفيذها عن بعد، حيث لا تتطلب الجرائم المعلوماتية إلا جرائم سرقة معدات الحاسب، ولا تستلزم وجود الجاني في مكان وقوع الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في مكان بعيد كل البعد عن مكان وقوع الجريمة، سواء كان ذلك من خلال الدخول للشبكة والنظام المعني أو من خلال إعتراض عملية تحويل المعلومات والقيام بسرقتها أو المساس بها[6].

---

[1] **أحمد عبد الله المراغي:** المرجع السابق، ص71.

[2]– **عبد الوهاب مليانى:** أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقياد، تلمسان، الجزائر، 2017، ص61.

[3]– **خالد حسن أحمد لطفي: :** جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الإبتزاز الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، مصر، 2018، ص21.

[4]– **خالد حسن أحمد لطفي:** المرجع نفسه، ص20.

[5]– وهذا ما سوف نأتي على شرحه في حينه أثناء دراستنا لجرائم الدخول أو البقاء غير المشروع في النظام المعلوماتي.

[6]– **محمود رجب فتح الله:** المرجع السابق، ص265.

خامسًا: أنها جريمة ذات جاذبية ومغرية لمرتكبيها

نظرًا لما تمثله أسواق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين في الإجرام المعلوماتي أو الإجرام المنظم، فقد غدت أكثر جاذبية لإستثمار الأموال وغسلها، وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن من الدخول إلى الشبكات المعلوماتية وسرقة البنوك أو إعتراض العمليات المالية وتحويل مسارها[1] وهذا ما جعلها ذات جاذبية ومغرية لمرتكبها بسبب وجود ضخامة في الفوائد والمكاسب، لذا فإن الخسارة الاقتصادية التي تسببها هذه الجرائم عادة ما تكون باهضة في غالبية الجرائم التي تستهدف الربح السريع[2].

سادسًا: أنها جريمة غير أخلاقية

قد لا يتوقف تأثير الجرائم المتصلة بالتكنولوجيات الحديثة عند الأثر المادي الناجم عنها، وإنما يتعدى ذلك ليهدد نظام القيم والأخلاق خاصة في المجتمعات المحافظة والمغلقة بحكم العرف أو الدين وذلك ما أصطلح عليه عند البعض "بالتلوث الثقافي *Pollution culturelle*"[3]، حيث ظهرت على شبكة الإنترنت وما تتضمنه من مواقع وصفحات للتواصل الإجتماعي الرسمية منها والمشبوهة، عدد هائل من الجرائم غير الأخلاقية كجرائم القدح والقذف والتحقير، والشائعات والأخبار الكاذبة، وتشويه السمعة للآخرين سواء أكانوا رموزًا سياسية أو فكرية أو دينية أو أشخاصًا عاديين[4]، كما قد يكون الهدف من هذه الجرائم هو إبتزاز بعض الأشخاص بنشر بعض الشائعات عنهم، وكلها جرائم غير أخلاقية يساء إستخدامها للنيل من سمعة وشرف الغير وكرامتهم[5]، وذلك كله من أجل البحث عن الشهرة أو بقصد التأثير على الرأي العام بأفكار مشوهة وبعيدة كل البعد عن الواقع والحقيقة.

---

[1]– **أسامة المناعسة:** جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، عمان، الأردن، 2001، ص21.

[2]– **مفيد الزيدي:** قضايا العولمة المعلوماتية، دار أسامة للنشر والتوزيع، عمان، الأردن، 2003، ص96.

[3]– **خالد حسن أحمد لطفي:** المرجع السابق، ص22.

[4]– **شرين دبابنة:** الجرائم الإلكترونية والقرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، عمان، الأردن، 2015، ص19.

[5]– **منير الجهيني وممدوح الجهيني:** المرجع السابق، ص 46. – **محمد الشوابكة:** المرجع السابق، ص52.

ناهيك عن عديد الجرائم غير الأخلاقية الأخرى كجرائم إستغلال الأطفال والنساء جنسيًا والجرائم الإباحية والخليعة ... وغيرها كثير، مما أثَّر بشكل رهيب على أخلاق وعادات مجتمعاتنا وقيمنا وتقاليدنا التي باتت اليوم أمام تحدي حقيقي[1].

سابعًا: أنها جريمة تقع أثناء المعالجة الآلية للبيانات

من خصائص الجريمة المعلوماتية أيضاً، أنها جريمة تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالنظام المعلوماتي، بحيث يمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية أصلاً، والخاصة بالتعدي على نظام معالجة المعطيات[2].

ذلك أنه في حالة تخلف هذا الشرط المفترض تنتفي معه الجريمة المعلوماتية، وأن هذه الأخيرة قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل النظام، سواء عند البدء في إدخال البيانات أو أثناء مرحلة معالجة البيانات ذاتها، أو حتى في مرحلة إسترجاع أو إخراج هذه البيانات في شكل معلومات[3].

وكذلك الأمر بالنسبة للمعلومات فقد تكون في حالة إنتقال أو موجودة في ذاكرة النظام المعلوماتي نفسه، أي أنها في حالة غير مادية، والشكل الآخر أن تكون هذه المعلومات متجسدة في صورة مادية بتخزينها على دعامة إلكترونية[4].

الفرع الثاني: خصوصية الجرائم المعلوماتية من حيث وسائل إرتكابها وخطورة وقوعها

تتسم أيضًا الجريمة المعلوماتية بخصائص فريدة من نوعها سواء من حيث وسائل إرتكابها أو من حيث خطورة وقوعها والأضرار الناجمة عنها، وهذا فيما يلي:

أولاً: من حيث وسائل إرتكابها

هذا النوع من الجرائم يقع في بيئة إلكترونية، لأنها تعتمد بالأساس على وسائل الإتصالات التكنولوجية الحديثة[5]، فهي لم تظهر إلا مع بروز عصر الحواسيب ونظام الإنترنت، وكون هذه

---

[1]– **شرين دبابنة:** المرجع السابق، ص21.

[2]– **خالد حسن أحمد لطفي:** المرجع السابق، ص24.

[3]– **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، المرجع السابق، ص86.

[4]– **خالد حسن أحمد لطفي:** المرجع السابق، ص25.

[5]– **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، المرجع السابق، ص32. – **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي، المرجع السابق، ص14.

الجريمة حديثة ومتطورة نسبيًا فإنه لا يتصور وقوعها إلا بإستخدام الحاسوب ومعطياته عن طريق الربط بشبكة الإنترنت، حيث يعتبران الأداة الرئيسية والوسيلة التي يقوم من خلالها المجرم المعلوماتي من إرتكاب جريمته[1]، بالإضافة إلى إستعانته بوسائل وأجهزة تقنية أخرى مثل آلة الطبع والماسح الضوئي والسكانر وأجهزة الربط بالشبكات وغيرها، ولكن مع ذلك كله يمكن للمجرم إرتكاب جريمته بوسائل إلكترونية أخرى كجهاز الهاتف المحمول المتطور، وغيرها كثير من الأجهزة والتقنيات الحديثة التي يمكن أن تظهر إلى الوجود في أي لحظة[2].

فلقد لعب كل من الحاسب الآلي وشبكة الإنترنت دورًا بالغ الأهمية في العالم المعاصر، حيث أقدمت العديد من الدول المتقدمة صناعيًا على إنتاج هذه التقنية المتطورة وإبتكار معها البرامج والمصنفات لتحقيق الربح المادي، وبدأت هذه الأجهزة في الإنتشار السريع، فأصبح البشر اليوم لا يمكنهم الإستغناء عنها في حياتهم اليومية، ولقد أشارت بعض الإحصائيات التي تناولت موضوع التطور الحاصل في مجال الحواسيب والبرمجة الإلكترونية أن هذا التطور له من الأثر البالغ لإزدياد هذا النوع من الجرائم[3].

هذا ولابد من الإشارة هنا إلى أن جهاز الحاسب الآلي وكل ما يتعلق به من ملحقات مادية، إذا كان موضوعًا للإعتداء عليه بالإتلاف أو سرقة الجهاز نفسه أو شتاته أو تكسيره مثلاً، فلا تثور هنا أية مشكلة معلوماتية، وذلك لأن نصوص قانون العقوبات التقليدية كفيلة بردع الجاني وضمان حقوق الضحية، لأن الحاسب الآلي في هذا المقام يعتبر من الأموال المادية المنقولة، إنما تثور المشكلة المعلوماتية عندما يطال الإعتداء على محتويات الحاسب الآلي من بيانات ومعلومات وبرامج منطقية مخزنة بداخله[4].

كما يتطلب إرتكاب الجريمة المعلوماتية الإلمام بالمعرفة التقنية من قبل الفاعل، فهو قد يكون صاحب خبرة فائقة في مجال الحواسيب أو على دراية كبيرة بمجالات إستخدامها، لأنه غالبًا ما يكون من المتخصصين في معالجة البيانات آليًا[5]، وهذه الخبرة والمعرفة بالتقنية قد تتفاوت بين

---

[1]– **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الإجرام والمجرم المعلوماتي، المرجع السابق، ص27.

[2]– **عبد الوهاب ملياني:** أمن المعلومات، المرجع السابق، ص62.

[3]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، المرجع السابق، ص80.

[4]– **زينب أحمد عوين:** عدم كفاية قواعد القانون الجنائي في مكافحة الجريمة المعلوماتية، مقال منشور في مجلة كلية الحقوق، جامعة النهرين، بغداد، العراق، المجلد 13، ع 1، 2011، ص 5 وما بعدها.

[5]– **لينا محمد الأسدي:** المرجع السابق، ص28.

مرتكبي هذا النوع من الجرائم، فمنهم صاحب خبرة واسعة وذكاء، ومنهم متوسطي المعرفة بالإعلام الآلي، وهذا راجع إلى التركيبة المعقدة لأجهزة الحواسيب وكذا برامج الحماية الإلكترونية القوية التي تضعها المؤسسات والشركات والحكومات، فكلما كان الهدف أكبر وأكثر حساسية كلما تطلب ذلك خبرة تقنية وفنية أكبر، لذا فإن هذا النوع من الإجرام ينفذه عادة متخصصون في مجال الإعلام الآلي[1]، أضف إلى ذلك أن إكتشاف هذا النوع من الإجرام ومكافحته يتطلب أيضًا خبرة فنية وتقنية عالية لدى جهاز الشرطة أو السلطة المنوطة بالتحري عن هذه الجرائم ومرتكبيها، وذلك لمجابهتها والحد من آثارها[2].

ثانيًا: من حيث خطورتها والأضرار الناجمة عنها

إن الإعتماد الكلي على الحاسبات الآلية في إدارة مختلف الأعمال اليومية وفي شتى المجالات ضاعف من الأضرار والخسائر التي تخلفها الجريمة المعلوماتية، خاصة عندما ظهرت شبكة الإنترنت وشجعت على عصرنة الإدارة والإستعمالات الشخصية، بدءًا من الإستعمال الحكومي ثم المؤسساتي والفردي كوسيلة ساهمت بشكل كبير في تسهيل حياة الناس اليومية، ورفع الحرج عنهم في أمور كثيرة.

وقد شهدت العقود الأخيرة تطورًا سريعًا في حجم المعلومات وطبيعتها وقيمتها الإنسانية والحضارية والاقتصادية والتجارية، وبعد أن أصبحت المعلومات عاملاً أساسيًا في مجال الخدمات إلى جوار الطاقة ومستوى إنتاج المواد الصناعية وسيرورتها أيضًا إلى طاقة كامنة للمخاطر، أصبحت هذه الحالة موضوعًا وميدانًا للإجرام المستحدث[3].

ولاشك أن هذه الجرائم تشكل تحدي كبير للعالم بأسره، وذلك بالنظر إلى حجم الأضرار والخسائر الناجمة عنها، بإعتبارها تستهدف الإعتداء على البيانات والمعطيات والمعلومات المخزنة داخل النظم المعلوماتية، وما يزيد من خطورة هذه الجرائم هو تهديدها للأمن القومي والاقتصادي، وكذا حقوق الأفراد وحرياتهم[4]، إذ يمكن القول تقريبًا أنه لا توجد جهة أو شخص أو مؤسسة مستثناة من الآثار الخطيرة لهذه الجريمة، وبالفعل فقد تكبدت العديد من الدول والمجتمعات كمًّا هائلاً من

---

[1]– **فيروز لطرش:** الجريمة الإلكترونية في الجزائر، المرجع السابق، ص325.

[2]– **فريحة حسين:** الجرائم الإلكترونية والإنترنت، مجلة المعلوماتية، جامعة الجزائر، ع 36، 2011، ص7 وما بعدها.

[3]– **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص68.

[4]– **إبراهيم شاكر:** جرائم الإنترنت، دار المسرة، عمان، الأردن، 2014، ص59.

الأضرار والخسائر المادية والمعنوية نتيجة هذا الإجرام الذي ليس له حدود[1]، ويُرَدُّ هذا النمو الإجرامي الغريب إلى عوامل عديدة كالنمو التكنولوجي السريع والمتطور والمرتبط بصناعة الحواسب وتكنولوجيا الاتصالات، وكذا التوافر السهل لأدوات الجريمة وتقنيات البرمجة، وسرعة الإتصالات ومجانية إستخدامها، والدرجة العالية في فهم ومعرفة خبايا تكنولوجيا الحواسيب[2].

فأصبحت بذلك تتزايد خطورة الجرائم المعلوماتية يومًا بعد يوم، وهذا تبعًا للتقدم المذهل في مجال التقنية وإستغلالها السلبي في كافة المعاملات لاسيما منها الإقتصادية والمالية الوطنية والدولية[3] مما نتج عنه أضرار بالغة الخطورة وخسائر مالية كبيرة، فقد قدرت لوحدها الأرباح العائدة من وراء تصميم برامج الفيروسات وبيعها بحوالي 275 مليون دولار أمريكي سنويًا، ناهيك عن عائدات الجرائم المعلوماتية الأخرى كسرقة الحسابات البنكية والمصرفية، وترويج الأفلام الإباحية عبر الشبكة، ففي تقرير نشرته المجموعة الإقتصادية الأوروبية حول خسائر الجرائم المرتكبة بواسطة النظم المعلوماتية كالغش والإحتيال والتلاعب بالبيانات وغيرها، بلغت لوحدها حوالي 65 مليون أورو سنويًا، وهذا الرقم في تزايد مستمر، وذلك مقارنة بالخسائر الناجمة عن الجرائم التقليدية[4].

هذا بالإضافة إلى الأضرار النفسية والإجتماعية التي تمس كافة فئات المجتمع سواء كانوا أشخاص بالغين أو مراهقين أو أطفال، مما يجعلهم عرضة لهذه الجرائم التي تقودهم مبكرًا لسلوك الإنحراف كجرائم الإباحية والاستغلال الجنسي، وجرائم فضح الأسرار الشخصية ونشرها، وكذلك القذف والتشهير، وكلها جرائم تؤدي إلى الإضرار بالسمعة الشخصية والمالية، بالإضافة إلى أخطر موضوع وهو الإنتشار الواسع لتجارة الجنس والدعارة وعرض الصور الخليعة، حيث تشكل عائدات هذه التجارة الإلكترونية الغير مشروعة لوحدها ما نسبته 60% من مجمل عائدات الخدمات

---

[1]– فقد قدرت فاتورة الجرائم المعلوماتية في العالم خلال عام 2011 بحوالي 388 مليار دولار أمريكي، وهذه التكاليف هي أعلى من الإنفاق السنوي لمنظمة (اليونيسيف) لوحدها، بحوالي 100 ضعف، كما يقدر المعدل الزمني لوقوع الجرائم المعلوماتية حول العالم بحوالي 50 ألف جريمة في الساعة الواحدة، يتأثر بها ما يقارب 589 مليون شخص عبر العالم. (أنظر أكثر: – **ثامر علي النويران:** الجرائم الإلكترونية وطرق الحد منها، بحث مشاركة في المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، مجلة كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، السعودية، 2015، ص177).

[2]– **أحمد كيلان عبد الله صكر:** الجرائم الناشئة عن إساءة إستخدام الحاسوب، المرجع السابق، ص37. – **ذياب البداينة:** الجرائم الإلكترونية، المرجع السابق، ص95.

[3]– **أحمد محمود مصطفى:** جرائم الحاسبات الآلية، المرجع السابق، ص15.

[4]– ***QUEMENER (M), FERRY (J) :*** *Cybercriminalité défimondial, economica, 2eme édition, Paris, France, 2009, P72.*

المدفوعة على الشبكة العنكبوتية[1]، كما أن هناك خطورة تتعلق بالجماعات المنظمة والمتطرفة، حيث وفر لهم الفضاء الإلكتروني منصة للاتصال والتنسيق والاجتماع مع بعضهم البعض، وذلك كله من شأنه أن يسهل عملية ترويج ثقافة الإجرام والعنف والتطرف والإرهاب[2].

وخلاصة ذلك كله هو أن تدرج خطر الإجرام المعلوماتي يكون بحسب الغاية ونوع الهدف، فقد يكون الهدف أفراد كأن تكون الغاية من وراء قرصنتهم إلكترونيًا هو التسلل والفضول، وقد تزداد خطورة ذلك إذا اُستعملت هذه المعلومات المتحصل عليها لغرض الابتزاز أو التشهير وتشويه السمعة، وقد تزداد خطورة هذه الجرائم أكثر إذا ما طالت مؤسسات الدولة المالية والإقتصادية وغيرها من الشركات، وتزداد خطورتها أكثر وتصبح تدميرية وهذا عندما تطال الأمن القومي وسلامة الدولة وذلك بسبب التجسس والإرهاب وغيرها من التهديدات الأمنية[3].

[1]– **إبراهيم الخضيري:** الجرائم المعلوماتية، دار العلوم، بيروت، لبنان، 2004، ص96.

[2]– **طارق ابراهيم الدسوقي عطية:** الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2009، ص176.

[3]– **فيروز لطرش:** الجريمة الإلكترونية في الجزائر، المرجع السابق، ص326.

المبحث الثاني: تعريف المجرم المعلوماتي ودوافعه الإجرامية

تمهيد وتقسيم:

من المقرر قانوناً أنّ المجرم الذي يقترف الجرائم المعلوماتية يطلق عليه لدى الكثير من الفقه بمصطلح "المجرم المعلوماتي"[1]، والذي بدوره يختلف عن المجرم الذي يقترف الجرائم التقليدية، وهذا الأخير يطلق عليه مصطلح "المجرم التقليدي"[2]، فالمجرم المعلوماتي ليس كغيره من الجناة التقليديين بل يتمتع بمزايا تميزه عن غيره من المجرمين، وإذا كنا في مجال الإجرام المعلوماتي فيجب علينا أن ننظر إلى هذا المجرم من عدة زوايا سواء من حيث الظروف التي دفعته لإرتكاب جريمته وأسبابها، وكذا تحديد أصناف وصفات هؤلاء المجرمين، وذلك حتى يسهل على المهتمين من كيفية إعادة تأهيلهم إجتماعيًا ويعودوا إلى حضيرة المجتمع كمواطنين صالحين ينفعوا المجتمع ولا يضروه.

ونظرًا لإنتشار ثورة المعلومات الرقمية وما تبع ذلك من إزدياد في عدد الجرائم المعلوماتية سواء على الصعيد العالمي أو الوطني، فقد حظيت أبحاث علم الإجرام في هذا المجال بالعديد من الدراسات القانونية والتي تحاول كشف النقاب عن مفهوم المجرم المعلوماتي، سواء من حيث الطوائف التي ينتمي إليها وكذا الأنماط الخاصة به، دون أن ننسى العوامل التي تدفعه لإرتكاب هذا النوع من الجرائم.

وعلى ذلك، سوف نقسم هذا المبحث إلى مطلبين إثنين على التوالي:

- **المطلب الأول: تصنيفات المجرم المعلوماتي وأهم صفاته.**
- **المطلب الثاني: دوافع المجرم المعلوماتي على المستوى الفردي والمجتمعي.**

[1]– قد تتعدد التسميات التي تستخدم للإشارة إلى هؤلاء الأشخاص الذين يرتكبون هذا النوع من الجرائم، فقد يستخدم مصطلح "مجرمي الحواسيب" أو "مجرمي الإنترنت" أو "مجرمي تكنولوجيا المعلومات" أو "مجرمي السيبر " ... وغيرها كثير، لذا فإنّ الإختلاف في هذه التسميات بطبيعة الحال نابع في الأصل من الإختلاف الموجود في المصطلح ذاته الذي يستخدمه الباحث للإشارة إلى هذه الجرائم، ويمكننا القول هنا، أنّ جميع هذه التسميات على الأرجح أنها صحيحة لأنها تعكس فهم كل باحث ودارس في هذا المجال لمعنى وطبيعة المسألة وفقًا للأساس الذي إعتمده لصياغة وجهة نظره من وضع المصطلح المستخدم للإشارة إلى الجريمة والمجرم بالمفهوم المقصود.

[2]– **محمود رجب فتح الله:** المرجع السابق، ص241.

المطلب الأول: تصنيفات المجرم المعلوماتي وأهم صفاته

إنّ إرتباط الجريمة المعلوماتية بالحاسب الآلي وتكنولوجيا الإتصالات، نتج عنه ظهور أنماط وطوائف جديدة من المجرمين (فرع أول)، كما أن لهم مميزات وصفات ينفردون بها وتميزهم عن بقية المجرمين العاديين (فرع ثاني).

الفرع الأول: تصنيفات المجرم المعلوماتي

لقد أنتجت الجرائم المعلوماتية تصنيفات جديدة من المجرمين يمكن تصنيفهم إلى عدة طوائف وأنماط، فلقد أظهرت الكثير من الدراسات والأبحاث المختلفة في هذا المجال عن وجود أنماط عديدة من مجرمي المعلوماتية، وهذا لا يعني بطبيعة الحال أنّ كل مجرم يندرج تحت طائفة محددة فقط، بل يمكن أن يكون المجرم المعلوماتي الواحد له مزيجًا بين أكثر من طائفة، لذا فهو ليس بالتصنيف البسيط كما يعتقد البعض.[1]

ومن جانب آخر، أكدت العديد من الدراسات والأبحاث العلمية والأكاديمية على أنّ تصنيف المجرمين أو جناة المعلوماتية تنحدر حسب فئات وطوائف مختلفة يمكن تقسيمها إلى قسمين إثنين على التوالي، المجرمون الهواة والمبتدؤون (أولا) والمجرمون المتخصصون والمحترفون (ثانيا).

أولاً: المجرمون الهواة والمبتدؤون

يعتبر نمط المجرمون الهواة والمبتدؤون من الأنماط الأقل خطورة مقارنة مع غيرهم من المجرمين الآخرين مرتكبي جرائم التقنية بإحترافية، وهذا نظرًا لقلة خبرتهم في مجال المعلوماتية، وكذا لإنتفاء القصد الجنائي لديهم في كثير من الأحيان حين إرتكابهم بعض صور هذه الجرائم، وهذا بحكم لأن هذا النمط من "هواة المعلوماتية *Passionnés d'informatique*" لا تتوفر لديهم الخبرة الكافية في إستخدام تقنيات الحاسبات الآلية مما يؤدي بهم الأمر أحياناً إلى الوقوع في الكثير من الأخطاء التي قد يترتب عنها إرتكابهم جرائم معلوماتية.

وهذا الصنف من المجرمون الهواة والمبتدؤون يندرج تحته عدد لا بأس به من الطوائف التي ذكرتها كثير من الأبحاث والدراسات الفقهية، ولعل من أهمها نجد:

[1]– يبدو أنّ هناك أيضًا عدم وجود إتفاق حول طوائف المجرمين الذين يرتكبون مثل هذه الجرائم، فنجد كل فقه يقسم هذه الطوائف وفقًا لمعيار معين، سواء من حيث معيار المحل أو معيار السلوك أو معيار الوسيلة ...إلخ. (أنظر: – **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص80).

أ- **طائفة المتحايلون *Pranksters _ Fraudeurs*:** وهم الأشخاص الذين يمتلكون قدرات فنية لا بأس بها في عالم الحواسيب فهم عادةً من أصحاب الكفاءات المعرفية، إذ يقدمون على إرتكاب بعض الأفعال المجرمة من خلال الدخول عن طريق الغش والتحايل على الأنظمة المعلوماتية، وهذا بغرض التسلية والمزاح، وهذا لإحساسهم في كثير من المرات بالفراغ مع عائلاتهم وأقرانهم، دون أن تكون لديهم نية إحداث أي ضرر بالمجني عليهم[1]، فهم يرتكبون أفعالهم الإجرامية بالحيلة ضد الآخرين بدون قصد إحداث ضرر معين.

ويندرج تحت هذه الطائفة صغار مجرمي المعلوماتية *Petits cyber criminels* وهم فئة من صغار السن النوابغ، أي "نوابغ المعلوماتية *Génie de l'informatique*" المولعون بالثورة المعلوماتية وتقنية الحواسيب وإمتلاكهم لها في سن مبكرة، والشغوفين الذين لديهم ميل وفضول لفهم إستعمالات هذه التقنية وبرامجها، والذين يبقون أمام جهاز الحاسوب لفترات متأخرة من الليل.[2]

كما قد يكونون من فئة الشباب البالغ الذين إنبهروا بالثورة المعلوماتية ولهم قدر لا بأس به من الخبرة الحاسوباتية، ويطلق عليهم "شباب المعلوماتية *Informatique jeunesse*"، ومن ثمة فهم يمارسون مواهبهم في إستخدام التقنية من هواتفهم النقالة كاليوتيوب والطابلات والمبايلات وغيرها من الأجهزة، وذلك بغرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية دون أن يكون يعلم بالجهة التي يتبعها هذا النظام، فإنّ هؤلاء الشباب قد يقدمون على إرتكاب بعض الأفعال المجرمة عن طريق الإستخدام الطائش للحاسبات الآلية الخاصة بهم، وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب إلى معرفة عمليات البرمجة الآلية وإكتشاف ممرات الدخول، ومع ذلك فهؤلاء تكون غايتهم في الغالب مجرد التسلية والملاحظة وليس لديهم النية الإجرامية الكامنة لإرتكاب أفعال في وصف الجريمة المعلوماتية، كما ليس حدود جغرافية لأفعالهم التي قد تصل إلى أنظمة ومراكز بعيدة عن أماكن تواجدهم.[3]

ومع ذلك لا يجب أن نستخف بهذه الفئات من صغار السن أو الشباب المراهق، لأنّ خطر إنزلاق هؤلاء إلى إحتراف الإجرام المعلوماتي هو إحتمال وارد وقائم[4]، لاسيما في غياب الأسرة

---

[1]- **محمود رجب فتح الله:** المرجع السابق، ص248. - **بلال أمين زين الدين:** المرجع السابق، ص42. - **عبد الوهاب مليايني:** المرجع السابق، ص69.

[2]- **غنية باطلي:** المرجع السابق، ص37.

[3]- **محمد سامي الشوا:** المرجع السابق، ص53. - نائلة عادل محمد فريد قورة، المرجع السابق، ص61.

[4]- **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، المرجع السابق، ص104.

والمدرسة، وعندئذ قد يتحول هذا الشباب أو الطفل من مجرد هاوي صغير للأفعال المعلوماتية غير المشروعة إلى محترف لها.

وكمثال على الجرائم التي تقترفها هذه الطائفة الإجرامية ما حدث في الولايات المتحدة الأمريكية أين قام بعض طلاب إحدى الثانويات في مدينة "مانهاتن *Manhattan*" عام 1980 بإختراق شبكة إتصالات البيانات لإحدى الشركات وتدمير ملفات زبائنها[1]، وكمثال كذلك المراهق الكندي الذي تسبب في إحداث حالة من الفوضى الشديدة على أحد المواقع الإلكترونية التابعة لإحدى الشركات التجارية بإستخدام شبكة الإنترنت، عندما إنهال على هذا الموقع بعديد الرسائل المزعجة فأدى إلى تضخم قائمة المعلومات فيه، حيث تسبب بفعله هذا بخسائر مادية معتبرة[2]، وفي ألمانيا تمكن طالب جامعي عمره تسعة عشرة عامًا من الدخول إلى نظام معلوماتي على نحو غير مصرح به وقام بإفشاء بيانات هذا النظام مما أدى إلى خسارة الشركة التي تتعامل مع هذا النظام بمبلغ قدّر وقتها بـــ 23 ألف مارك ألماني[3].

ب- طائفة الدخلاء أو المتسللون *Malicious Harckers*: ويطلق عليهم أيضا "بالغرباء *Etrangers*" أي "غرباء المعلوماتية *Des inconnus en informatique*"، وهم أشخاص دخلاء أو أجانب عن تلك الأنظمة المعلوماتية ولا تربطهم بها أية صلة، ويندرج تحت هذه الطائفة المستخدمون للنظام أو الموقع الإلكتروني الذين ليس لهم تصريح مسبق بالدخول والعمل على هذا النظام والذي قد يكون خاص بإحدى المؤسسات أو الشركات أو التابع لأحد الأفراد، ويندرج تحت هذه التسمية الكثيرين من مخترعي الفيروسات ومستعمليها.[4]

والدخلاء هم أشخاص أذكياء ومبدعون، عملهم الدخول الغير المشروع إلى النظم المعلوماتية بقصد المتعة أو العبث أو الإجرام[5]، وفي الغالب يكون التخريب هو هدف هؤلاء الدخلاء والمتسللون أي أنهم يقومون بالدخول على نظام غريب عنهم بغرض إرتكاب أفعال غير مشروعة[6]،

---

[1]- **محمود أحمد عبابنة:** المرجع السابق، ص41. - **محمد علي العريان:** المرجع السابق، ص79.

[2]- **مصطفى محمد موسى:** أساليب إجرامية بالتقنية الرقمية، ماهيتها ومكافحتها، دراسة مقارنة، دار الكتب القانونية، القاهرة، مصر، 2005، ص25.

[3]- **عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، المرجع السابق، ص308.

[4]- **مصطفى محمد موسى:** المرجع نفسه، ص26.

[5]- **ذياب البداينة:** الأمن وحرب المعلومات، دار الشروق، عمان، الأردن، 2002، ص133.

[6]- **محمد سامي الشوا:** ثورة المعلومات، المرجع السابق، ص45.

ولا شك أنّ عملية الدخول هذه من هؤلاء الغرباء يكون لها تأثير بالغ الضرر قد تكلف صاحب النظام مبالغ ضخمة لإعادة إصلاح نظم الحماية التي أفسدتها العمليات التخريبية[1]، كما قد يكون الدافع من وراء دخول هؤلاء الغرباء إلى النظم المعلوماتية بقصد التسلية والمزاح مع الآخرين أو بقصد الإستطلاع كهواية لا غير، وهزم والتغلب على النظام في إظهار الذكاء، وبدون إن يكون في نيتهم إحداث خسائر أو ضرر بالمجني عليهم.[2]

ج- طائفة القراصنة – الهاكرز *Hackers* –: طائفة الهاكرز أو القراصنة[3]، تقترب إلى حد بعيد مع فئة صغار نوابغ المعلوماتية ولكنها تتفوق عليها علمًا ومعرفة ودراية واسعة بعمليات البرمجة والتسلل والملاحظة والتطفل على الأنظمة.[4]

فالهاكرز أو القراصنة هم أشخاص متطفلون غايتهم الإعتداء على إجراءات الحماية الأمنية للنظم والشبكات المعلوماتية، فهم لا تتوافر لديهم في الغالب دوافع إجرامية حادقة أو تخريبية وإنما ينطلقون من دافع التحدي وإثبات الذات، فهم يهدفون من وراء دخولهم الأنظمة غير المصرح لهم بدخولها من خلال كسر الحواجز الأمنية الموضوعة لهذا الغرض بهدف التعلم وإكتساب الخبرة أو بدافع الفضول أو لمجرد التأكيد على قدرتهم في إختراق هذه الحواجز والتغلب عليها[5]، وأحياناً يكون الدافع هو الكسب المادي غير المشروع أو التسبب بالإرباك والخسائر للآخرين، وغالبًا ما يعودون هؤلاء القراصنة إلى إختراق نفس النظم المعلوماتية التي تم الإعتداء عليها وذلك بعد

---

[1]- **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، المرجع السابق، ص147.

[2]- **بلال أمين زين الدين:** المرجع السابق، ص41. - **سعيدي سليمة وحجاز بلال:** المرجع السابق، ص30.

[3]- **الهاكرز *Hackers*:** كلمة تخيف الكثيرين خصوصًا مرتادي شبكة الإنترنت، وهي كلمة مشتقة من الإنجليزية "*To Hack*" ومعناه بالفرنسية "*Pirater*" أي المخترق أو المتسلل الذي يبحث عن التفاصيل الخاصة بالتكنولوجيا وأنظمة المعلومات، فعالم الهاكرز عالم واسع وغامض، وبداياتهم كانت قبل ظهور الإنترنت بل وحتى قبل وجود الكمبيوتر نفسه، بحيث تعود بداياتهم الأولى إلى عالم 1878 في الولايات المتحدة الأمريكية، حيث كان أغلب العاملين في شركات الهاتف المحلية من الشباب المتحمسين لمعرفة المزيد عن هذه التقنية الجديدة التي حولت مجرى التاريخ الإنساني، فقد كانوا يسترقون السمع فيستمعون إلى المكالمات الهاتفية الشخصية من خلال تجميع إتصالات خطوط الهاتف والتنصت عليها وكان ذلك بغرض التسلية والفضول في التعلم، حتى إضطرت الشركة وقتها بتغيير بعض الفئات الرجالية بفئات أخرى نسائية لإنهاء هذه المشكلة، فالهاكر يحمل معنى المتخصص في نظم المعلومات والبرمجيات وهي عبارة عن تسمية إختارها لأنفسهم مجموعة من المجرمين الأكفاء والمهرة القادرين على إبتكار البرامج وحل مشكلات تأمين الأنظمة والشبكات، ولعل أول هاكر هو "تيو فالدس ليونكس" أحد أهم مطوري نظام التشغيل المعروف بـــ "*UNIX*" وهو أيضا مبتكر للنظام الأكثر أماناً وشهرة في العالم "*LINUX*". (أنظر أكثر: - **سعيدي سليمة وحجاز بلال:** المرجع السابق، ص22-23).

[4]- **خليفة أحمد الملط:** الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ط2، 2006، ص117.

[5]- **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص81. - **نائلة عادل محمد فريد قورة:** المرجع السابق، ص62.

إصلاحها من أصحابها أو تطوير نظام الحماية الفنية فيها، مما يعيد فيهم روح التحدي للإختراق مجددا[1]. وهناك تقسيم آخر للهاكرز[2] ولقراصنة المعلومات وهم على التوالي:

1- **أصحاب القبعة البيضاء *White hats***: ويعتبرون مستشارون في أمن المعلومات وخبراء ومبرمجين ومسيري بعض الشبكات، ويطلق عليهم "شرطة مقاهي الإنترنت *Cyber policiers*" وهم يحافظون على القيم السامية للهاكر الأوائل، فهم يعملون في ظل القانون على تقديم الإستشارة والمساعدة.

2- **أصحاب القبعة الرمادية *Grey hats***: وهم ممن يقومون بإقتحام النظم والشبكات المعلوماتية دون تصريح مسبق ولكن ليس بغرض التدمير أو التخريب لها ولكن بغرض إكتشاف أغوار هذه النظم والشبكات وإثبات قدراتهم على القرصنة والإختراق.

3- **أصحاب القبعة السوداء *Black hats***: وهم مصنعو الفيروسات والبرامج التدميرية، ويطلق عليهم أيضًا "جواسيس المقاهي *Cyber espions*" أو "إرهاب المقاهي *Cyber terroristes*" وهم من يتسللون إلى النظم والشبكات المعلوماتية بغرض التخريب والعبث بها، وقد إبتعدوا كل البعد عن القيم السامية للهاكرز.

ثانيًا: المجرمون المحترفون

المجرمون المحترفون *Criminels professionnels*، وهم ممن يحملون درجات عالية في تخصصات الحواسيب والمعلوماتية، ويعملون محللي نظم ومبرمجين[3] ويكونون على دراية واسعة ببرامج التشغيل ومعرفة عميقة بالخبايا والثغرات الأمنية الموجودة داخل الأنظمة المعلوماتية، ولعل من جملة المجرمون المحترفون في مجال الإجرام المعلوماتي نجد مثلاً:

---

[1]- **مصطفى محمد موسى:** المرجع السابق، ص26. - **نائلة عادل محمد فريد قورة:** المرجع السابق، ص62.

[2]- **سعيدي سليمة وحجاز بلال:** المرجع السابق، ص33.

[3]- لقد قام معهد *Standford research* بإجراء دراسة على حوالي سبعمائة حالة إجرامية تتعلق بالمعالجة الآلية للبيانات في الولايات المتحدة الأمريكية وكذا أوروبا، توصل فيها إلى أنّ غالبية مرتكبي هذه الجرائم هم من الشباب أصحاب التحدي والجدارة الذين تتراوح أعمارهم ما بين (25 و45) عامًا وهي المرحلة التي تتناسب مع الإحتراف في تقنية المعلومات، وقد إستنتج المعهد من الإحصاءات التي قام بها لمحترفي الإجرام المعلوماتي أن (المحلل) يأتي في المرتبة الأولى من حيث الكفاءة ثم يلي ذلك (المبرمج) ثم (المستخدم) للنظام، بحيث تختلف الأهداف التي يبغي المجرم المعلوماتي تحقيقها جراء سلوكه الإجرامي. (- **بلال أمين زين الدين:** المرجع السابق، ص43).

أ- طائفة الكراكرز *Crackers*: عادة ما يطلق على المجرمون المحترفون في الإجرام المعلوماتي مصطلح "الكراكرز *Crackers*"[1] وهو كل شخص متخصص أو خبير في مجال الحواسيب والمعلوماتية، يقوم بأنشطة غير قانونية تتمثل في إعتداءات تعكس مدى خطورة هؤلاء وميولاتهم الإجرامية بحيث تبنى عليها رغباتهم في إحداث الأضرار بالغير وتدمير الأنظمة المعلوماتية[2]، ناهيك عن الأهداف الأخرى والتي تذهب في الأساس إلى تحقيق الكسب المادي لهم أو تلبية رغبة الجهة التي كلفتهم لإرتكاب جرائم التقنية الحديثة، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية أو التعبير عن موقف فكري أو ديني[3].

وأفراد هذه الطائفة يتم تصنيفهم في الغالب إلى أنماط ومجموعات فرعية متعددة إما تبعًا لتخصصهم في نوع معين من الجرائم أو تبعًا للوسيلة المتبعة من قبلهم في إرتكاب الجرائم، فمثلاً عن ذلك نجد نمط محترفي التجسس بكافة أنواعه الإقتصادي والسياسي والأمني والعسكري والصناعي، كما نجد مثلاً نمط مجرمي الإحتيال والتزوير المعلوماتي وهؤلاء هم من تكون أغراضهم متجهة إلى تحقيق كسب مادي مربح بالإستلاء على أموال الآخرين من خلال سرقة الأموال من الحسابات الإلكترونية المصرفية.[4]

فالكراكر هو شخص يكون لديه هواية قوية في تعلم البرمجة ونظم التشغيل فيستخدم هذه البرامج الجاهزة لكنه يطورها بمعرفته حسب ما تقتضيه الضرورة ولربما يتمكن من كسر شفرتها البرمجية ليتم نسخها وتوزيعها بالمجان، وهذا الصنف ظهر في الأعوام الأخيرة بشدة، وقد ساهم في إنتشاره عاملين أساسيين الأول هو إنتشار الحواسيب والبرامج وكثرتها وسهولة التعامل معها، والأمر الثاني إرتفاع أسعار البرامج وتطبيقاتها الأصلية على الحواسيب التي تبيعها الشركات مما حفز ذلك هؤلاء على إيجاد سبل أخرى من نسخ هذه البرامج الأصلية وبيعها من جديد بأسعار تقل كثيرًا عما وضع لها من أثمان، وأخطر الكراكر هو المبتدئ لأنه يحب أن يجرب برامج الهجوم

---

[1]- **كلمة الكراكرز *Crackers***: هي كلمة إنجليزية معناها "*Cracker*" وتقابلها بالفرنسية "*Craquelins*" ومعناها الكسر أو التكسير ومنها التخريب والتحطيم والعبث، وهي عبارة عن تسمية إختارها لأنفسهم مجموعة من المخربين المهرة القادرين على إختراق أي نظام أو شبكة معلوماتية أو حاسوباتية، فهم أشخاص لديهم الكفاءة الخاصة والمعرفة الواسعة في مجال المعلوماتية، وكثيرًا ما نجد الكتابات المعاصرة قد جعلت من مصطلحي (الهاكر والكراكر) وجهين لعملة واحدة وهي الدمار والخراب داخل الأنظمة المعلوماتية، (أنظر أكثر: - **محمود عبد الله حسين علي:** سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2002، ص54).

[2]- **خالد عياد الحلبي:** إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، عمان، الأردن، 2011، ص33.

[3]- **مصطفى محمد موسى:** المرجع السابق، ص31.

[4]- **عبد الوهاب ملياني:** المرجع السابق، ص72.

دون أن يفقه تطبيقاتها فيستخدمها بعشوائية لذلك فهو يقوم أحياناً بدمار واسع دون أن يدري بما يفعل.[1]

ب- طائفة أصحاب المشكلات الخاصة *Personal problem solvers*: وهم الطائفة الأكثر شيوعًا وإنتشارًا من بقية مجرمي المعلوماتية، فهم يقومون بإرتكاب جرائمهم والتي يترتب عليها في أغلب الأحوال خسائر كبيرة تلحق بالمجني عليهم، ويكون الباعث من وراء هذه الجرائم هو إيجاد حلول لمشكلات أو لمشاكلهم المادية والتي لا يستطيع الجاني حلها بالطرق العادية والتقليدية.[2] فهم يهدفون من إرتكاب نشاطهم الإجرامي إلى تحقيق ربح مادي بطريق غير مشروع، وإن كان هنا إتحاد في تلك الصفة ما بين المجرم التقليدي والمجرم المعلوماتي من هذه الطائفة.

ومن جانب آخر أكدت بعض الدراسات والأبحاث الأكاديمية على أن طائفة أصحاب المشكلات الخاصة لا يسعوْن دائمًا إلى تحقيق مكاسب مادية أو غيرها من المكاسب المربحة، وإنما يرتكبون أنشطتهم الإجرامية بدافع الرغبة في الإنتقام والثأر والحقد، فهو ذلك الحاقد -*Spiteful malveillant*، ولهذا فإنهم ينقسمون إلى موظفين لهذا النظام بوصفهم على علاقة ما بالنظام محل الجريمة، أو غرباء عن النظام، تتوفر لديهم نفس أسباب الإنتقام من الشخص المستهدف في نشاطاتهم وأقرب مثال على ذلك عندما قام أحد الشباب بدافع الثأر من صديقته التي هجرته، فراح ووضع على موقعها الشخصي بشبكة الإنترنت والمفتوح على عدد كبير من أصدقائها، وبدون علمها قام بعرض بعضًا من صورها ذات الطابع الإباحي مصحوبة بتعليقات كلامية سيئة عن أخلاقها وسلوكها.[3]

لذلك فإنّ هذه الطائفة تعد من بين الفئات التي تهدف إعتداءات أفرادها في الأساس إلى تحقيق الكسب المادي لهم أو للجهة التي كلفتهم لإرتكاب جرائم التقنية[4]، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية أو التعبير عن مواقف فكرية أو عقائدية تبعًا لتخصصهم في نوع معين من الجرائم أو تبعًا للوسيلة المتبعة من قبلهم في إرتكاب الجريمة[5]، وعادةً ما يكونوا

---

[1]- **سعيدي سليمة وحجاز بلال:** المرجع السابق، ص27.

[2]- **محمود رجب فتح الله:** المرجع السابق، ص248.

[3]- **ملياني عبد الوهاب:** المرجع السابق، ص73.

[4]- **خالد عياد الحلبي:** المرجع السابق، ص35.

[5]- **علي عبود جعفر:** جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2013، ص116.

مستخدمين في المنشأة أو المؤسسة فتساعدهم صفتهم في إرتكاب جرائمهم ضد تلك المنشأة، وقد يكون دافع الثأر والحقد والغضب من هيئة معينة أو من صاحب العمل يبعث بهم لإرتكاب أفعالهم غير المشروعة[1] سواء بأنفسهم أو بمشاركة وبمساعدة أشخاص آخرين فنيين كانوا أو مجرد وسطاء[2].

وغالبًا ما يتم إرتكاب الجرائم المعلوماتية من قبل هؤلاء الأشخاص وهم يعملون بصفة قيادية داخل المنشأة أو المؤسسة، أي أنهم مسؤولون عن أنظمة معلوماتية يديرونها، فهم يملكون بحكم وظيفتهم المعرفة اللازمة والتقنية الكافية للتلاعب والعبث بالمعلومات الموجودة على الحاسبات الآلية، وهنا يكمن الخطر الحقيقي من طرف هؤلاء، إذ أنهم كثيرًا ما ينظر إليهم بوصفهم مستخدمين مثاليون، والغالبية العظمى منهم يشغلون مراكز قيادية هامة ومسؤولة داخل المؤسسة، ويتمتعون تبعًا لذلك بثقة كبيرة في مجال عملهم ومن قبل العامة، أي أنّ الجرائم المرتكبة بواسطتهم تشبه إلى حد كبير تلك الجرائم المرتكبة بواسطة الموظفين ذوي الياقات البيضاء *les cols blancs* من حيث كونهم من أصحاب التخصصات الوظيفية العالية، ولهم الهيمنة على التقنيات الحديثة وعلى قدر من الذكاء الاجتماعي.[3]

إنّ فئة أصحاب المشكلات الخاصة لا يرتكبون الجرائم المعلوماتية للإثارة العقلية وإختبار الذكاء كما في حالة الدخلاء والمتسللين أو الكسر المادي أو مجرد العبث المعلوماتي؛ فغالبية هذه الفئة غاضبة وناقمة على مكان عملها وعلى الحياة بشكل عام.[4]

ج- طائفة المخربون *Vandales*: ومنهم لصوص نظم المعلومات *Les voleurs de système d'information* والذين يستعملون كل الطرق والوسائل من أجل الدخول بطريقة غير مشروعة إلى النظم المعلوماتية، ويطلق عليهم أيضا مصطلح "متعصبي المعلوماتية *Fanatiques de l'informatique*"، فهم ليسوا متطرفين إلى حد الإرهاب الدولي، وإنما هدفهم تخريب المنظومة المعلوماتية وهي طريقتهم في إرضاء رغباتهم[5]، وهذا على عكس الهاكرز والكراكرز الذين يقومون بأفعالهم لأغراض أقل خطورة.

---

[1]- **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، المرجع السابق، ص148. - **محمد سامي الشوا:** المرجع السابق، ص46.

[2]- **محمد علي العريان:** المرجع السابق، ص80.

[3]- **محمد سامي الشوا:** المرجع نفسه، ص48. - **محمد علي العريان:** المرجع السابق، ص81.

[4]- **سعيدي سليمة وحجاز بلال:** المرجع السابق، ص32.

[5]- **غنية باطلي:** المرجع السابق، ص41.

وقد يكون الهدف من وراء هذا التخريب هو شن حرب عبر وسائط تكنولوجيا المعلومات الحديثة، بحيث يقوم بها فرد أو دولة أو جماعة إرهابية ضد دولة أخرى معادية لها، تسعى من خلاله إلى تدمير المواقع المعلوماتية الخدماتية التي تقدم خدمات إلكترونية للمواطنين في ظل ما يعرف "بإفشال الحكومات الإلكترونية *E-gouvernement*"[1]، وتتميز هذه الطائفة بالخطورة حيث تميل إلى أفعال القرصنة والإرهاب المعلوماتي بإستخدام وسائل على قدر كبير من البراعة في صناعتها وتصميمها كزرع البرامج الفيروسية، واللجوء إلى السلب بالقوة الإلكترونية، والسطو المعلوماتي، وكل ذلك من أجل تحقيق غاياتهم الإجرامية.[2]

ناهيك عن المتطرفون الذين يدافعون عن قضية معينة أو غاية معينة ليس لها علاقة بمصالحهم الشخصية المباشرة، فقد يكون السبب سياسي أو إيديولوجي أو ديني، وبالتالي ليس لهم نوايا إجرامية محددة[3]، وإنما يقومون بتوظيف المعارف التي إكتسبوها في مجال المعلوماتية لتمرير طروحات تخدم توجههم، وهذا ما يقودهم إلى إختراق المواقع الإلكترونية الفردية أو الجماعية لتغيير المعلومات التي تحتوي عليها وهذا للفت الأنظار إلى أفكارهم ومعتقداتهم.[4]

وكذلك من أخطر أصحاب هذه الطائفة نجد العاملون في الجريمة المنظمة *Crime organisé*، حيث أصبح الجهاز الإجرامي المنظم من أخطر الوسائل لإرتكاب الإجرام المعلوماتي، وذلك بحكم إمتلاكهم قاعدة تكنولوجية خاصة بهم بحجم وقوة الشبكة الإجرامية[5]، وفي الغالب تعمل هذه الطائفة ضمن عصابات منظمة هدفها تحقيق الربح المادي مثل عصابات سرقة السيارات، وعصابات تهريب الكوكايين وغيرها من الجرائم المنظمة[6]، وإنّ نسبة هذا النمط من الإجرام قليلة مقارنة ببقية الفئات الأخرى كون أنّ العمل الإجرامي في هذا المجال يتطلب نوعًا من المهارة الفنية في وسائل التقنية الحديثة والتي قد لا تتوافر عادةً في أغلب مجرمي هذه الفئة.[7]

---

[1]– **مصطفى محمد موسى:** المرجع السابق، ص36.

[2]– *Voir plus :* ***QUEMENER (M), FERRY (J),*** *Op. Cit, P83.*

[3]– **عبد الله حسين علي محمود:** المرجع السابق، ص67.

[4]– **عبد الرحمن جلهم حمزة:** المرجع السابق، ص28. – **مصطفى محمد موسى:** المرجع السابق، ص29.

[5]– **غنية باطلي:** المرجع السابق، ص40

[6]– **عبد الرحمن جلهم حمزة:** المرجع نفسه، ص29.

[7]– **نائلة عادل محمد فريد قورة:** المرجع السابق، ص63.

رأي الباحث:

مهما كانت درجة الدقة في رسم حدود كل طائفة من الطوائف التي ينتمي إليها المجرم المعلوماتي، فإننا نرى أنّ أهم الدوافع الرئيسية في إرتكاب الجريمة المعلوماتية والتي تحدد الطائفة التي ينتمي إليها مجرمو المعلوماتية لا تخرج عن ثلاثة دوافع تحركه، الدافع الأول تشترك فيه جريمة معلوماتية مع غيرها من الجرائم التقليدية الأخرى، كتحقيق الربح المادي في جرائم الإعتداء على الأموال وإلحاق الأذى المادي أو المعنوي بالشخص المستهدف في جرائم الإعتداء على الأشخاص، أو دافع ثاني تتميز به عن غيرها من الجرائم التي تتمثل بالرغبة في الدخول إلى أنظمة الحاسب والشبكة بهدف التسلية أو إثبات الذات والقدرة التي يتمتع بها الجاني دون السعي إلى تحقيق مكاسب من أي نوع، أما الدافع الثالث يتمثل في رغبة الإضرار بهذه الأنظمة التابعة للمؤسسة أو المنشأة التي ينتمي إليها الجاني وهذا بدافع الإنتقام بعد فشل أدوات حل مشاكلهم، لأنهم قد يرون الجريمة طريق سهل لحل هذه المشاكل.

كما أنه ينبغي الإشارة هنا، إلى أنّ هذه الطوائف غير مستقرة وليست الوحيدة الثابتة في بيئة الوسط الرقمي والتكنولوجي، إذ بالإمكان القول أنّ هذه الفئات والأصناف من المجرمين المعلوماتيين قابلة للتجدد والتنوع بقدر أي تطور يتم في مجال التقنيات الحديثة وهذا بالتأكيد ناتج عن الصلة بين مجرمي هذا النمط من الإجرام وبين التكنولوجيا الحديثة وكذا البيئة الإجتماعية التي ينشأ فيها هؤلاء.

الفرع الثاني: صفات وسمات المجرم المعلوماتي

يقتضي الإلمام أكثر بجرائم تقنية المعلومات بيان صفات وسمات مرتكبيها، فبعد أن بيَّنا أهم تصنيفات المجرم المعلوماتي لاسيما من حيث الأنماط والفئات العديدة والمختلفة التي يظهرون فيها هؤلاء، سنحاول أن نوضح هنا في هذا الفرع أهم الصفات والسمات المختلفة والتي يتميز بها المجرم المعلوماتي عن المجرم العادي.

والدراسات التي تحدد صفات هذا المجرم وشخصيته التي يتميز بها، كلها تنطلق من تفرد هذا النوع من الجرائم بخصائص عديدة كما سبق وأن بيناه، فينسحب ذلك على المجرم المعلوماتي الذي بدوره تتوفر فيه جملة من الصفات والمميزات كالطابع الإجتماعي والتخصص والإحترافية، إضافة إلى الذكاء والمعرفة وعدم إستعمال العنف وغيرها من الصفات، ويمكن إجمال تلك الصفات والسمات في الآتي:

أولاً: المجرم المعلوماتي إنسان إجتماعي بطبعه

المجرم المعلوماتي كإنسان إجتماعي بطبعه معناه أنه متوافق مع مجتمعه ولا يعيش في إنطوائية عنه، وغالبًا ما تكون له مكانة إجتماعية معتبرة داخل الوسط الذي يعيش فيه، كما قد يكون يحظى بالإحترام فيه.

لذا يختلف مرتكب الجرائم المعلوماتية عن المجرم التقليدي من حيث أنه يعيش وسط المجتمع بشكل طبيعي جداً، فهو يمارس عمله المعتاد في المجال المعلوماتي أو حتى في غيره من المجالات الأخرى، أي أنه إنسان إجتماعي بطبعه[1]، وتطبيقًا لذلك فكثير من جرائم المعلوماتية ترتكب بدافع اللهو أو بدافع الإنتقام أو بدافع إظهار القدرة على التفوق في مواجهة أمن الأنظمة الإجتماعية.[2]

وبالتالي فشخصية المجرم المعلوماتي دائمًا ما نجدها تكتفي بالتفاخر بين أقرانه أو لمجرد الحصول على منفعة شخصية من وراء جرائمه، فالهاكر على سبيل المثال لا يضع نفسه في حالة عداء أمام مجتمعه الذي يعيش فيه، بل إنه إنسان متوافق معه.

كما تشير بعض الأبحاث التي أجريت على هؤلاء أن النتائج المتحصلة تؤكد على أنَّ قراصنة النظم المعلوماتية هم أشخاص متعلمون يرغبون في المساعدة أكثر من كونهم أعداء يحبون التسبب في إلحاق الضرر، وذلك ما يساعدهم في عملية التكيف مع المجتمع[3]، كما أنَّ مرتكبي هذا النوع من جرائم المعالجة الآلية للمعلومات يتميزون في غالب الأحيان بأنهم أفراد ذوي مكانة في المجتمع[4]، فغالبًا ما يكون هؤلاء من أصحاب الوظائف الحيوية في أماكن عملهم سواء في بيئة القطاع الخاص كالشركات والمؤسسات والمنشآت الإقتصادية والمصارف المالية الخاصة، أو في القطاع العام وأجهزته وهيئاته الحكومية[5]، وأبرز مثال على ذلك الموظف الذي يتم فصله من وظيفته ويلجأ إلى أسلوب الإنتقام ممن تسببوا له في ذلك.[6]

---

[1]– **سليمة سعيدي، حجاز بلال:** المرجع السابق، ص34. – **أحمد عبد الله المراغي:** المرجع السابق، ص40.

[2]– **محمد علي العريان:** المرجع السابق، ص77.

[3]– **محمود عبد الله حسين علي:** المرجع السابق، ص54.

[4]– **جميل عبد الباقي الصغير:** الجرائم الناشئة عن إستخدام الحاسب الآلي، المرجع السابق، ص15.

[5]– **خالد حسن أحمد لطفي:** المرجع السابق، ص 23.

[6]– **محمد علي سويلم:** المرجع السابق، ص119

ثانيًا: المجرم المعلوماتي يتميز بالذكاء والمعرفة والمهارة

المجرم المعلوماتي ليس بشخصية عادية فهو يتصف أولاً بالذكاء، أي أنه على قدر كبير من سرعة الفهم وسعة الإطلاع والملاحظة القوية والنشاط الذهني المتقدم[1]، لذلك يقال عادةً عن الإجرام المعلوماتي أنه "إجرام الأذكياء *Criminels intelligents*" أو كما قيل "جرائم الذكاء *Crimes intelligence*" وهذا بالمقارنة مع الإجرام التقليدي الذي يفتقر إلى إستخدام هذا الذكاء في كثير من الأحيان.[2]

كما يمتاز المجرم المعلوماتي بقدرته على التعامل مع جميع النظم والشبكات وكذا القدرة على التعامل مع كل ما يصدر في مجال الحوسبة وبرامجها[3]، فهو شخص يمتلك من المهارات ما يؤهله بالتعديل والتطوير في الأنظمة الأمنية المعلوماتية حتى لا تلاحق أو تتبع أعماله الإجرامية، وهذا الذكاء هو مفتاح الإجرام المعلوماتي لإكتشاف أسرار الثغرات في إختراق البرامج والمواقع الإلكترونية المحصنة[4]، وهذا ما أثبتته عديد الدراسات والإحصائيات أنّ هؤلاء المتورطون في مثل هذه الجرائم لديهم قدر كبير من الذكاء والتفوق يجعلهم يباشرون إجرامهم بدقة متناهية خشية إفتضاح أمرهم أو ضبطهم أثناء قيامهم بالمخاطرة والمغامرة، فهذه الثقة الزائدة بالنفس والإحساس بإمكانية إرتكابهم لجرائمهم دون كشف أمرهم.[5]

بالإضافة إلى إتقانهم عدد لا بأس به من لغات العالم العديدة، لا سيما لغات البرمجة المعروفة بإسم "لغة تقنية المعلومات *Langage informatique*" وهذا ما يجعلهم يستطيعون إكتشاف الأخطاء والثغرات الموجودة في الأنظمة المعلوماتية، فمن خلال دراسة أجراها معهد *Stand Ford Research* أثبتت النتائج أنَّ أغلب مرتكبي هذه الجرائم هم من الأشخاص الأذكياء وغير العاديين، فهممنلهمعلاقاتوطيدة بعالمالكمبيوترو الإنترنت،وهؤلاءلديهم فعلاً قدرات مذهلةعلىحل المشاكل الإلكترونية التي تحمل على الدهشة حتى أنَّ بعضهم يطلق عليهم "بالسحرة*Les Magiciens*"[6]، كما

---

[1]– **يزيد بوحليط:** المرجع السابق، ص87.

[2]– **محمد علي العريان:** المرجع السابق، ص63.

[3]– **يوسف أبو الحجاج:** أشهر جرائم الكمبيوتر والإنترنت، دار الكتاب العربي، القاهرة، مصر، 2010، ص20.

[4]– ***ROSE Philipe :*** *La criminalité informatique 2ème édition (ED.p.u.f), Paris, France, 1995, P59.*

[5]– **غنية باطلي:** المرجع السابق، ص 35.

[6]– **سليمة سعيدي، بلال حجاز:** المرجع السابق، ص35.

أجريت أيضًا مجموعة من الأبحاث من قبل باحثين أمريكيين تبين من خلالها أنَّ مرتكبي هذه الجرائم هم من يشغلون مناصب إدارية تعتمد بشكل كبير على إستخدام التقنية الحديثة.[1]

وعليه فإنه من المقرر أنَّ المجرم الذي يقترف الجريمة المعلوماتية يتسم بخاصية الذكاء والمهارة التي تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت هذه الأخيرة لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية إرتكابها، فإنَّ الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية وتقنية في الغالب، ومن يرتكبها عادةً يكون من ذوي الإختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على الإستعمال الصحيح لجهاز الحاسب الآلي والمعرفة أيضًا في التعامل مع شبكة الإنترنت[2]، فعلى سبيل المثال فإنَّ الجرائم المعلوماتية ذات الطابع الإقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب حتمًا مهارة ومعرفة فنية وتقنية عالية جدًا من قبل مرتكبها.

ومن ناحية ثانية قد يمتلك المجرم المعلوماتي المعرفة والمهارة في كل ما له علاقة بالوسائل الخاصة في هذا المجال، والتي قد يكتسبها عن طريق الخبرة والممارسة والإحتكاك بالآخرين، وهذا ما جعل بعض الفقه يصنف المجرم المعلوماتي ضمن طائفة الأذكياء الذين يستغلون ذكاءهم في تنفيذ أغراضهم الإجرامية، ولا يلجؤون في الإستعانة بالقوة الجسدية في ذلك إلاَّ بالقدر اليسير جدًا[3]، وهذا ما يؤكد على أنّ الجريمة المعلوماتية من الجرائم الناعمة التي لا عنف فيها على عكس الجرائم التقليدية التي يحتاج معظم مرتكبيها إلى إستعمال القوة العضلية لتنفيذها، فنعومة هذه الجريمة وما تدره من أرباح ومن إشباع الفضول عند الكثيرين جعلها من الجرائم المغرية للمجرمين بحكم أنها تحتاج معرفة علمية وقدر من الذكاء والمهارة في توظيف ذلك، والجاني في سبيل هذا كله لا يحتاج من الوقت إلاَّ ثواني أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل من على وسائل الإدخال الحاسوباتية، وهذا ما قد يتسبب في حصول خسائر فادحة رغم أنّ جريمته لا ترى بالعين المجردة.[4]

---

[1]– ***SARGOS (P), MASSE (M) :*** *Le droit pénal spécial né de l'informatique, Ed cujas, Paris, France, 1980, P23.*

[2]– **محمود رجب فتح الله:** المرجع السابق، ص241.

[3]– ***ROSE Philipe :*** *Op. Cit, P63.*

[4]– **عزيزة رابحي:** المرجع السابق، ص94.

ثالثًا: المجرم المعلوماتي شخص محترف ومتخصص

إنَّ خاصية الإحتراف والتخصص في خبايا الحواسيب وما في حكمها من أهم الخصائص أيضًا التي تميز مجرمي المعلوماتية، إذ يستطيع هؤلاء أن يكون لهم تصورًا كاملاً لجرائمهم حتى قبل القيام بها وتنفيذها، ويرجع ذلك أيضًا إلى طبيعة المسرح الذي تحدث فيه الجريمة المعلوماتية وهو نظام الحاسب الآلي وبيئته الإلكترونية، فالجاني يستطيع أن يطبق جريمته على أنظمة مماثلة في تنفيذ الجريمة بكل سهولة وبإحترافية[1].

والجامع بين محترفي الجرائم المعلوماتية هو تمتعهم بقدرة عالية من الإلمام الجيد بالتقنية الحديثة، وإكتسابهم معارف عملية وإنتمائهم إلى التخصصات المتصلة بالحواسيب لاسيما من الناحية الوظيفية، وهذه السمات تتشابه إلى حَدٍ قريب مع سمات المجرمي ذوي الياقات البيضاء[2]، فمجرمي تلك الفئة ينتمون إلى طبقة المتعلمين والمثقفين ومن لديهم تخصصية التعامل مع أجهزة الحاسب الآلي[3].

فالمجرم المعلوماتي له قدرة فائقة في المهارات التقنية التي يستغلها في إختراق التحصينات الدفاعية التي تعدها شركات البرمجة[4]، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجيات الحديثة، وهذه ليست قاعدة ثابتة في أن يكون المجرم المعلوماتي على قدر من العلم والمعرفة الإحترافية والمتخصصة، وهذا ما أثبته الواقع العملي القضائي، أن جانب لا بأس به من مجرمي المعلوماتية لم يتلقوا الدراسة اللازمة، وإنما يستعملون مداركهم ومهاراتهم لإرتكاب هذا النوع من الإجرام.[5]

---

[1]– من الأمور اللافتة للإنتباه أنَّ بعض مجرمي الإنترنت المحترفين والمتخصصين في مجال الحواسيب، قد بلغ مستوى التحدي لديهم بأن نظموا ملتقيات ومعارض سنوية علنية لإستعراض خبراتهم وإنجازاتهم في مجال جرائم الإنترنت وإختراق المواقع الإلكترونية وغيرها، ومن هذه الملتقيات نجد على سبيل المثال "ملتقى *Defon*" الذي يقام سنويًا في مدينة لاس فيجاس الأمريكية، وكذا "ملتقى *Hope*" الذي كانت أولى بداياته عام 1994 وهو الآن يقام كل ثلاثة سنوات في مدينة نيويورك الأمريكية، وأيضًا ملتقى *Sammercon*" الذي تشرف عليه مجلة « *Root and phrack*» بأمريكا، والغريب في الأمر أنه وبالرغم من خطورة مجرمي الإنترنت فإنَّ بعض الشركات العالمية الكبرى العاملة في مجال صناعة وتطوير تقنية المعلومات قد تنبهت لأهمية هؤلاء الأشخاص ومدى إحترافيتهم وتخصصهم في مجال الأمن المعلوماتي، فبدأت في البحث عنهم ومنحهم فرص عمل حقيقية لتسخير قدراتهم المعلوماتية للعمل بأسلوب مشروع وقانوني، والإستفادة منهم في كشف الثغرات الأمنية في البرامج والنظم المعلوماتية التي تنتجها هذه الشركات. (أنظر أكثر: – **عبد الفتاح بيومي حجازي:** الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2004، ص218).

[2]– **خالد حسن أحمد لطفي:** المرجع السابق، ص22.

[3]– **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، المرجع السابق، ص98.

[4]– **فتيحة رصاع:** المرجع السابق، ص54.

[5]– **محمد علي سويلم:** المرجع السابق، ص116.

ولقد تبين في العديد من القضايا أنَّ عددًا كبيرًا من المجرمين لا يرتكبون سوى الجرائم المعلوماتية، أي أنهم يحترفون ويتخصصون في هذا النوع من الجرائم فقط، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس بصورة واضحة أنَّ المجرم الذي يرتكب ويمتهن الإجرام المعلوماتي هو مجرم في الغالب متخصص في إرتكاب جريمته، فهو يتمتع بإحترافية كبيرة في إستخدام الحاسب الآلي لتنفيذ جرائمه، الأمر الذي يقتضي منه الكثير من الدقة والحذر في التوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمتهم كما في حالة البنوك والمؤسسات المالية الكبرى.[1]

رابعًا: المجرم المعلوماتي شخص طبيعي

قد يكون المجرم في الجريمة المعلوماتية شخصًا طبيعيًا يعمل لحسابه الخاص، ويهدف إلى تحقيق مصلحة شخصية له وهذا في الغالب، ولكن يمكن للشخص الطبيعي أن يقوم بهذا الفعل لحساب أحد الأشخاص المعنوية كالشركات أو المؤسسات التي تعمل في مجال المعلوماتية أو أنها تستند في عملها على تكنولوجيا المعلومات، بغية السطو على أحد الأنظمة المعلوماتية أو إحداث أضرار بالغير،[2] وتفيد الإحصائيات أن الأشخاص المعنوية مرتكبي هذه الجرائم لا يحاولون دائمًا الإضرار بالأفراد وإنما المساس بالمؤسسات والشركات لأنها تستطيع تحمل الأضرار والأعباء لما لها من رصيد مالي إحتياطي.[3]

خامسًا: المجرم المعلوماتي شخص لا يستعمل العنف

المجرم المعلوماتي من المجرمين الذين لا يلجؤون إلى إستعمال العنف إطلاقًا في إرتكاب جرائمهم، وذلك بحكم أنه ينتمي إلى طائفة "إجرام الحيلة أو التحايل أو الغش *Délit de fraude*"، فهو لا يلجأ إلى إستعمال العنف في تنفيذ جرائمه، والسبب في ذلك هو أنَّ هذا النوع من الجرائم لا يستلزم أي قدر من العناء أو بذل الجهد للقيام به[4]، فالجرائم المعلوماتية هي "جرائم هادئة بطبيعتها *Soft crimes*" لا تحتاج للعنف والمقاومة.[5]

---

[1]– **محمود رجب فتح الله:** المرجع السابق، ص243.

[2]– **محمد عبد الله أو بكر:** موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، مصر، 2007، ص94.

[3]– **محمد محمد شتا:** فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، 2001، ص99.

[4]– **محمود رجب فتح الله:** المرجع السابق، ص244.

[5]– **نهلا عبد القادر المومني:** المرجع السابق، ص58.

كما يرجع السبب في ذلك أنَّ المجرم المعلوماتي يتمتع بشيء من السلطة، ويراد بالسلطة هنا تلك الحقوق والمزايا التي تؤهل المجرم وتمكنه من إتمام جريمته على أكمل وجه، فكثير من مجرمي المعلوماتية لديهم إما سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة[1]، إضافة إلى إلمامه التام بمسرح الجريمة وبأدواتها، بما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وإفتضاح أمره.[2]

ومنه أيضًا بساطة الوسيلة المستعملة، ويراد بها الإمكانيات التي قد يحتاجها المجرم المعلوماتي لإتمام جريمته، وهذه الوسائل قد تكون في غالب الأحيان وسائل بسيطة وسهلة الحصول عليها، خاصةً إذا كان النظام الذي يعمل به الحاسب الآلي من الأنظمة المشهورة والمتداولة في السوق أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر كبير من الصعوبة مما تحتاج معه شيء من العناء الفكري.

سادسًا: المجرم المعلوماتي شخص يعود للإجرام

يتميز أيضًا المجرم المعلوماتي أنه شخص يعود للجريمة دائمًا كلما سنحت له الفرصة بذلك، إما بهدف التلذذ في إيذاء الآخرين، أو نتيجة شعوره بقدرته ومهارته في الإختراق[3]، وذلك من خلال الدخول غير المصرح به إلى أنظمة الشبكات مرات ومرات، فهو قد لا يحقق غايته في الجريمة الأولى، فيسعى جاهدًا إلى تحقيقها في الجرائم المتتالية.

ويرجع أيضًا عودة مجرمي المعلوماتية إلى إرتكاب جرائمهم مرات عديدة ومتتالية من الرغبة في سد الثغرات والأخطاء السابقة التي أدت إلى التعرف عليهم ومحاكمتهم، وهذا سبب قوي يؤدي بكثيرين منهم بالعودة – العود –[4] إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة الثانية من العودة إلى تقديمهم إلى المحاكمة.[5]

---

[1]– تكون السلطة مشروعة عندما يكون للجاني حق الدخول إلى الحاسب الآلي أو النظام المعلوماتي وإجراء المعاملات الإلكترونية، كما أنه من الممكن أن تكون هذه السلطة غير مشروعة كما في حالة سرقة كود أو شفرة الدخول الخاصة بحاسب أو نظام شخص آخر.

[2]– **محمد علي سويلم:** المرجع السابق، ص118

[3]– **محمد علي سويلم:** المرجع السابق، ص117.

[4]– **العود في القانون معناه:** هو تكرار الجاني لجريمة أو عدة جرائم بعد صدور حكم بات ضده ومعاقبته من أجل الجريمة السابقة، ويشمل العود كافة الجرائم دون إستثناء، لذلك القانون يعاقب على حالة خطورة إجرامية تستخلص من إرتكاب الجريمة العائد فيها الجاني، فهي حالة عود تستأهل العقوبة أو تشديدها. (أنظر كل من: – **سليمان عبد المنعم:** النظرية العامة لقانون العقوبات، المرجع السابق، ص158.
– **محمود نجيب حسني:** المرجع السابق، ص105).

[5]– **محمود رجب فتح الله:** المرجع السابق، ص244.

رأي الباحث:

نتفق بشكل كامل هنا مع الفقه الذي يرى بأنَّ هذه الخصائص لا تكون مطلقة، بمعنى أنّ المجرم المعلوماتي لا يمتلك دائمًا ذكاء عالي المستوى أو خبرة ودراية ومعرفة واسعة بتكنولوجيا المعلومات وبالطرق الفنية والتقنية للحواسيب، أو أنه مجرم غير عنيف، وأنه مجرم متكيف دائمًا مع مجتمعه الذي يعيش فيه، أو أنه من فئة المراهقين الهواة، بل على العكس من ذلك، حيث أثبت الواقع العملي لتاريخ الإجرام والمجرمين قاطبةً أن خصائصهم التي يتميزون بها ليست ثابتة على الدوام، والدليل على ذلك حصول نماذج إجرامية عديدة نتيجة الجريمة المعلوماتية والتي قد تقع من مختلف الأشخاص متفاوتي الأعمار من الكبار أو الأحداث أو الصغار، كما يستطيع الشخص إرتكاب الجريمة المعلوماتية بمفرده أو من خلال تجنيده في مجموعات إجرامية ضمن عصابات الجريمة المنظمة عن طريق شبكة الإنترنت، وهذه أيضًا بحد ذاتها مشكلة أخرى تستلزم منا البحث والدراسة.

المطلب الثاني: دوافع المجرم المعلوماتي على المستويين الفردي والمجتمعي

إنّ الأسباب المؤدية لإرتكاب هذا النوع من الجرائم تختلف عن تلك المعروفة في الجريمة التقليدية وإن كانت تتشابه في البعض منها، فالدوافع والبواعث التي تدفع بالمجرم المعلوماتي لإرتكاب هذا النوع من الإجرام قد تكون مختلفة عن بواعث ودوافع إرتكاب الجرائم من قبل المجرم التقليدي، والسبب في ذلك أنّ الفرق بين سلوكيات الإجرام في العالم المادي والحقيقي تختلف بدورها عن تلك التي تقع في العالم الإفتراضي، والتي تقوم أساسًا على خصوصية بيئة الحواسيب والشبكات الرقمية.

ومن المقرر أنَّ هناك عدد لا بأس به من الأسباب والدوافع التي يمكن أن تكون وراء إرتكاب الجرائم المعلوماتية، سواء منها ما يقع على المستوى الفردي والشخصي (فرع أول) ومنها ما يقع على المستوى المجتمعي (فرع ثاني).

الفرع الأول: الأسباب والدوافع الفردية (الشخصية)

تتعدد الدوافع والأسباب الفردية والشخصية التي تدفع الفرد إلى إحتراف مثل هذا السلوك الإجرامي، سواء كان ذلك بدافع الحقد أو الإنتقام، وإنَّ كان إشتراك هؤلاء المجرمين عند إرتكابهم الجريمة المعلوماتية يكمن في عرض واحد هو مجرد الهواية واللهو في بداية الأمر وذلك نتيجة إنبهارهم بالثورة التكنولوجية والمعلوماتية وما صاحبها من تطور في الحاسبات الآلية.[1]

[1]– **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص81.

ومن المُسلَّم به، أنّ طائفة جناة الجريمة المعلوماتية تختلف عن طوائف ومرتكبي الجريمة التقليدية، لذا من المنطقي والبديهي أنَّ نجد ذات الإختلاف في الأسباب والدوافع وحتى العوامل التي تدفع هؤلاء إلى إرتكاب الإجرام المعلوماتي، ولعل من جملة هذه الأسباب والدوافع الفردية والشخصية نجد على سبيل المثال ما يلي:

أولاً: البحث عن التعلم والإثارة والمتعة والتحدي

أثبتت كثير من الدراسات أنَّ قراصنة الأنظمة المعلوماتية لديهم إهتمام شديد بأجهزة الكمبيوتر وولع بالتعلم عن كيفية عملها، حتى قيل أنّ الدخول إلى أنظمة الكمبيوتر وشبكاته يمكن أن يعلمك كيف يسير العالم[1]، وبناءً على هذا فإنّ أجهزة الكمبيوتر وما تحتويه من نظم معلوماتية ما هي إلاَّ فضاء للتعلم والبحث، وأنَّ قيام الشخص بإكتشاف أساليب جديدة لتطوير معلوماته الذاتية وإستغلالها في كيفية الحصول على المعلومات هو أمر في غاية الإثارة.[2]

ضف إلى ذلك أنَّ هناك بعض الجرائم المعلوماتية التي يرتكبها شباب طائش وصغار السن، وذلك من باب المتعة والتحدي ولا ربما من باب الظهور في الإعلام، وغالبًا ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق خاصة بعد سن العشرينيات وإحساسهم بالمسؤولية[3]، وعلى الرغم من ميْل مرتكبي هذه الأفعال لإثبات تفوقهم ومستوى إرتقائهم وإبداعهم، الأمر الذي دفع ببعض الفقهاء إلى المناداة بعدم تقرير مسؤولية مرتكبي هذه الجرائم خاصة إذا كان الدافع وراء ذلك هو البحث عن التعلم والإثارة والمتعة والتحدي، لأنّ أعمالهم تتمثل في إظهار تفوقهم دون أن تكون نواياهم سيئة وإنما إنبهارهم بالتقنية الحديثة، ولذلك فإنّ هؤلاء ليسوا على قدر كبير من الخطورة الإجرامية، وإنما هو في الغالب أنهم يفضلون تحقيق إنتصارات تقنية دون أن تتوفر لديه أية نوايا سيئة، وإعتبار أعمالهم غير منطوية على نوايا آثمة[4].

ونضرب مثالاً على ذلك ما نشرته مجلة "*L'express*" الفرنسية في سبتمبر 1983 من أحداث قصة بعنوان "ميلاد نزعة" وتدور أحداث هذه القصة في أنَّ عامل طلاء مباني بسيط الحال

---

[1]– **سليمة سعيدي، بلال حجاز**: المرجع السابق، ص36.

[2]– ***SHERIDAN Mouris :*** *L'ordinateur comme cible de la criminalité, (vol d'ordinateurs et piratage), périodique, problèmes politiques et siciaux, N° 953, éd, les documentations françaises, Paris, France, 2008, P41.*

[3]– **محمود رجب فتح الله:** المرجع السابق، ص252.

[4]– ***SHERIDAN Mouris :*** *Op. Cit, P42.*

قد توجه إلى أحد البنوك الفرنسية لإيداع شيك خاص به، وقد تعاصر ذلك مع لحظة تعطل الموزع الآلي للنقود، حيث راح يشاهد مستخدم صيانة الأجهزة الآلية وهو يقوم بإصلاح الآلة وإستخراج نقود البنك من الآلة عند عملية الطلب عن طريق إستخدام بطاقة إلكترونية خاصة، وقد أحدث هذا المشهد وهذا الإبتكار للآلة تصدعًا في حياة عامل الطلاء والذي كان يدعى "*Rotand lava*" وقد حرص هذا الأخير على التعلم والتدرب على تقنية الحاسب الآلي الموزع للنقود، حيث عكف على ذلك لمدة عامين من خلال سرقته مجسم لأحد الموزعات الآلية، وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب جديد في مطالعة عمليات بطاقات السحب "*Cartes de retrait*"، وقد ألقي عليه القبض من قبل الشرطة الفرنسية قبل أن يستفيد من براعته المستحدثة، ومنذ ذلك الحين فقد نسبت إليه تسمية "جريمة سرقة الآلة *Crime de vol de machine*"[1].

ودائمًا ما يلجأ مرتكبي هذه الأفعال إلى التركيز على دقة الأسلوب أكثر من التركيز على الفعل ذاته، فيميلون إلى إظهار تفوقهم ومستوى براعتهم لدرجة أنه إزاء ظهور أي تقنية جديدة ومستحدثة فإنه يكون لديهم شغف كبير في فهم خبايا هذه التقنية وهذه الآلة ويحاولون إيجاد الوسيلة الناجعة إلى تخطيها.[2]

ويزداد هذا الدافع لدى فئات صغار السن من الهواة لهذا المجال الذين يمضون وقتًا طويلاً أمام حواسيبهم الشخصية في محاولة منهم لكسر حواجز الحماية والأمن لأنظمة الحواسيب وشبكات المعلومات، ولإظهار تفوقهم على وسائل التقنية الحديثة، ويمكن القول هنا أنَّ هذا الدافع هو أكثر الدوافع التي يجري إستغلالها من قبل المنظمات الإجرامية، وهي إستدراج هذه الفئات من هواة المعلوماتية إلى قبول المشاركة معهم في أنشطة إعتداء معقدة أو إستئجارهم للقيام بالجريمة المعلوماتية.[3]

ثانيًا: الدافع النفسي والمؤثرات الشخصية

تتعدد البواعث والدوافع النفسية والمؤثرات الشخصية، ومن جملة تلك الدوافع ما نجده مع الأشخاص الذين يعانون من إدمان أو جنون الكمبيوتر *La dépendance à l'ordinateur*، فقد ذكر

---

[1]– نقــلاً عن كل من: (– **محمد سامي الشوا:** المرجع السابق، ص48. – **محمد علي العريان:** المرجع السابق، ص82. – **سليمة سعيدي، حجاز بلال:** المرجع السابق، ص39).

[2]– **محمد سامي الشوا:** ثورة المعلومات، المرجع نفسه، ص48.

[3]– **غنية باطلي:** الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016، ص30.

أحد الأطباء النفسانيين المتخصصين في هذا المجال أنَّ أحد المرضى جاءه يشتكي ويخبره أنَّ عائلته في خطر، وتبين فيما بعد أنّ السبب في مشكلته يكمن في طبيعة عمله كمبرمج على الكمبيوتر في أحد المؤسسات حيث إتضح أنه كان يقضي معظم وقته مع الكمبيوتر وترك عائلته مهملة[1]، ويقول الدكتور "باركي بلاك *Perky black*" أستاذ علم النفس بجامعة نيويورك الأمريكية أنّ قراصنة الأنظمة المعلوماتية جميعًا يتملكهم إحساس وشعور بالقوة تجاه التقنية الحديثة مما يؤدي بهم في كثير من المرات إلى إرتكابهم للجرائم.[2]

نَاهيك عن تأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة ولعه وإدمانه بيئة المعالجة الآلية للمعلومات ونظمها، ومع توافر هذه المؤثرات الخارجية فإن الأمر حتمًا يؤول في النهاية إلى إرتكابه للجريمة المعلوماتية، وهذا جراء آفة نفسية يصاب بها بعض هؤلاء فيلجؤون إلى الأفعال الغير المشروعة ضد الأنظمة المعلوماتية، كأن يقوم بتدمير البرامج المعلوماتية بالفيروسات أو القنابل المنطقية عن طريق زرعها والتي ينشأ عنها أضرار جسيمة بالمجني عليهم.[3]

كما أظهرت بعض الدراسات أنَّ الجوانب السيكولوجية للمجرمين المعلوماتيين تؤكد على شيوع عدم الشعور باللامشروعية الطبيعة الإجرامية وباللامشروعية الأفعال التي يقترفونها، كذلك الشعور بعدم إستحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة من المجرمين، وكذا تغيب في داخلهم مشاعر الإحساس بالذنب وتأنيب الضمير، وإنْ كان ينتاب هذا النوع من المجرمين عمومًا وفي كثير من الأحيان الشعور بالخشية من إكتشافهم وإفتضاح أمرهم، ولكن هذه الرهبة والخشية يفسرها إنتماؤهم في الأعم الأغلب إلى فئة إجتماعية متعلمة ومثقفة، وهذه المشاعر في الحقيقة تبدو متعارضة[4].

ثالثًا: دافع الحقد والإنتقام

كما قد يكون وراء الأسباب التي قد تدفع بالمجرم إلى إقتراف مثل هذا السلوك بدافع الحقد أو الإنتقام، ويتمثل هذا الحقد على شخص أو عدة أشخاص أو على مؤسسة ما، أو على مكانة

---

[1]– **أحمد عبد الله المراغي:** الجريمة الإلكترونية، المرجع السابق، ص41.

[2]– **حسام شوقي:** حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية، القاهرة، مصر، 2003، ص58.

[3]– **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص83.

[4]– **خالد حسن أحمد لطفي:** جرائم الإنترنت، المرجع السابق، ص23.

وظيفية معينة أو حقدًا ماليًا لعدم تمكنهم من القيام بإلتزاماتهم المالية على أكمل وجه فيلجؤون إلى أفعال غير مشروعة ضد الأنظمة المعلوماتية، كما قد يكون الدافع وراء إرتكاب الجريمة المعلوماتية هو عامل الإنتقام من المؤسسة مثلاً التي ينتمي إليها هذا المجرم، خاصةً عندما يتم فصله من عمله فإنّ ذلك من شأنه أن يهيئ له المناخ المناسب والدافع القوي لإرتكاب جريمته.[1]

حيث دفع الحقد والكراهية والإنتقام بمحاسب إلكتروني شاب إلى التلاعب في برامج النظام المعلوماتي الخاص بالشركة التي كان يعمل بها قبل فصله منها، بأن قام بتصميم برنامج يقوم بإختراق أجهزة نظام هذه الشركة على أنّ تختفي كل البيانات الخاصة بالمتعاملين معها وذلك بعض مضي ستة أشهر من تاريخ تركه للعمل، وحدث ما أراد بعد إنتهاء هذه المدة.[2]

وكمثال على ذلك أيضًا حينما قام شخص آخر يعمل في إحدى الشركات الكبيرة لنقل البضائع، وذلك عندما علم أنه تم تغييره من منصبه الإداري الذي كان يشغله، وقبل ما يغادر قام بإرسال فيروس من شأنه أن يمسح محتوى كل ملفات التسيير والخدمات، وأن ما حصل لهذه الشركة هو تكبدها خسائر فادحة لم تكن متوقعة.[3]

وقد أمكن الكشف في بعض الأحوال عن أنّ مجرد إظهار شعور "جنون العظمة *Paranoïa*" هو الدافع لإرتكاب فعل الإجرام المعلوماتي، وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي دائمًا هو مفتاح سرٌّ كل نظام معلوماتي قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها، فقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة مما يؤدي به الأمر إلى إرتكاب جريمة معلوماتية، ومن ثمة يجد فرصته من خلال الإفصاح عن شخصيته أمام العامة وعمال المنشأة.[4]

ومن بين التهديدات العظمى التي تؤثر على سلامة الأنظمة المعلوماتية، هو أن يعهد بمسؤولية المركز أو النظام المعلوماتي لشخص واحد فقط، فقد تدفع هذه الثقة العمياء بهذا المسؤول أو المبرمج لإستخدام موقعه على النظام لمصالحه الخاصة، ونذكر في هذا الشأن واقعة مشابهة للأولى، حيث كان شخص يدعى "ستانلي ريفكين *Stanley Rifkin*" والذي كان يشتغل مستشار في

---

[1]– **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص84.

[2]– **محمد أمين الرومي:** جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004، ص25.

[3]– ***QUEMENER (M), FERRY (J) :*** *Op. Cit, P69.*

[4]– **محمود رجب فتح الله:** المرجع السابق، ص256.

مجال المعلوماتية لدى أحد البنوك الكبرى في أوروبا، وكان يتمتع بثقة مطلقة من جانب هذا البنك، حيث سمحت له إختصاصاته بالولوج على النظام المركزي للمعلومات الخاصة بهذا البنك وذلك بإستخدام مفاتيح إلكترونية جد معقدة، فقام بجملة من التحويلات الإلكترونية المالية من بنك لآخر، وتمكن فعلاً بفضل قدراته أن ينقل في وقت وجيز جدًا ما قدره عشرة مليون دولار أمريكي إلى حساب بنكي فتح بإسمه في إحدى البنوك السويسرية، وسرعان ما ألقي عليه القبض وصدر ضده حكم بالسجن لمدة ستة سنوات.[1]

رابعًا: دافع كسب المال وتحقيق أرباح

أحيانًا يكون الدافع من وراء التسلل وإختراق المواقع الإلكترونية والنظم المعلوماتية هو الحصول على ربح مالي عن طريق المساومة على البرامج أو المعلومات المتحصل عليها بطريقة الإختلاس من جهاز الكمبيوتر، أو عن طريق إستعمال بطاقة سحب آلي مزورة أو منهية الصلاحية، حيث أشارت في هذا المقام إحدى الجمعيات التي تعنى بالأمن المعلوماتي *Sécurité informatique* إلى أنّ معظم جرائم المعلوماتية يكون لمرتكبيها الرغبة في تحقيق الثراء وكسب أرباح مالية، وهو من العوامل الأساسية لإرتكاب هذا النوع من الإجرام، كإختلاس الأموال أو سرقة المعلومات وإبتزاز أصحابها وغيرها من الجرائم المعلوماتية المنصبة ضد الأموال.[2]

كما قد تدفع الحاجة بالبعض إلى دافع تحقيق الثراء السريع وذلك عن طريق إتاحة الإطلاع على معلومات معينة وذات أهمية بالغة خاصةً لمن يطلبها[3]، حيث قد تسعى بعض الشركات التجارية والصناعية للحصول على البرامج والمعلومات عن طريق سرقتها بواسطة الأشخاص القائمين على أجهزة الحواسيب والنظم وذلك مقابل رشوة هذا الموظف أو إغرائه بالمال وإستغلاله[4]، وكمثال على ذلك هو قيام أحد الموظفين الذي كان يعمل كمبرمج كمبيوتر لدى إحدى الشركات التجارية الألمانية، والذي قام بالإستيلاء على إثنين وعشرين شريطًا ممغنطًا تحتوي جميعها على معلومات هامة لها علاقة خاصة بالعملاء وأسرار إنتاج هذه الشركة، وقد هدد السارق ببيعها للشركات المنافسة إذا لم تدفع له فدية مقدارها 200.000 دولار أمريكي، وقد قامت الشركة

---

[1]– **محمد سامي الشوا:** ثورة المعلومات، المرجع السابق، ص55. – **غنية باطلي:** المرجع السابق، ص32.

[2]– **محمد أمين الرومي:** المرجع السابق، ص29.

[3]– **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص82.

[4]– **غنية باطلي:** الجريمة الإلكترونية، المرجع السابق، ص31.

بتحليل هذا الموقف وتقييم الخسائر الناتجة عن بيع هذه المعلومات ووجدت بأنها تفوق بكثير المبلغ المطوب، ففضلت الشركة دفع المبلغ من أجل إسترداد الشرائط الممغنطة المسروقة.[1]

وهكذا تتعدد الأسباب التي تدفع إلى إنتشار الإجرام المعلوماتي حينما تبرز الحاجة إلى تحقيق الكسب السريع نتيجة لوقوع البعض تحت ضغوط معينة مثل وجود مشاكل عائلية لعدم كفاية المال أو لإنعدامه لذلك نجد أحيانًا أنَّ الدافع لإرتكاب الجريمة المعلوماتية يمكن أن يقف وراءه مشكل سداد الديون أو الإدمان على المخدرات أو الخسائر الضخمة لألعاب القمار، ولذلك تتعدد الأسباب اللازمة للوصول إلى هذا الهدف المنشود، ولذا فإن هذا السبب يعد من أكثر الأسباب التي تدفع إلى إنتشار الإجرام المعلوماتي.[2]

فأحيانًا يحاول المجرم المعلوماتي من خلال إرتكابه هذا النوع من الجرائم السعي وراء حل مشكلة شخصية مستعصية وشديدة، فهذه الإنعكاسات وغيرها تشير إلى أنَّ حاجات قوية تدفع هؤلاء لإرتكاب الجريمة المعلوماتية، لذلك فدافع المجرم في بعض المرات ليس هو الجشع فقط كما تصوره بعض فقهاء القانون الجنائي، فالمجرم المعلوماتي لا يضع نفسه في حالة عدائية مع المجتمع الذي يعيش فيه[3] فهو إنسان متكيف ومرتفع الذكاء بما يساعده على فهم الواقع الذي يحيط به، وإنما خطورة الإجرام تزيد لديه كلما زادت مشاكله الإجتماعية التي من المؤكد أنها تطور شخصيته الجنائية.[4]

وأخيرًا، يجب أن لا نستخلص من ذلك إنعدام خطر الإجرام المعلوماتي بحجة عدم توافر النوايا الإجرامية، ولكن أيضًا عندما يكون السلوك غير الواعي يمكن أن يسبب أضرارًا جسيمةً حتى ولو لم يكتشف أي عداء للمجتمع.[5]

---

[1]– مشار إليه لدى كل من: (**محمد سامي الشوا:** ثورة المعلومات، المرجع السابق، ص50. – **سليمة سعيدي، بلال حجاز:** المرجع السابق، ص38. – **محمود عبد الله حسين علي:** المرجع السابق، ص71. – **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص83).

[2]– ففي دراسة قام بها بعض المهتمين حول الأمن المعلوماتي، أشارت إلى أنَّ المحرك الرئيسي لأنشطة إحتيال الكمبيوتر وفيما بعد إحتيال الإنترنت هو بدافع تحقيق الكسب المالي، وأضافت نفس الدراسة أنَّ نسبة 43% من حالات الغش المعلوماتي المعلن عنها قد أُرتكبت من أجل إختلاس الأموال، وأنَّ نسبة 23% من أجل سرقة المعلومات، وأنَّ نسبة 19% هي أفعال عبث وإتلاف للمعلومات، وأنّ نسبة 15% مجرد إستعمالات غير مشروعة للحاسب الآلي كسرقة وقت الحاسوب لأجل تحقيق أغراض شخصية (أنظر كل من: – **محمود عبد الله حسين علي:** المرجع نفسه، ص70. – **محمد أمين الرومي:** المرجع السابق، ص24. – **غنية باطلي:** المرجع نفسه، ص27. – **محمود رجب فتح الله:** المرجع السابق، ص259).

[3]– **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص78.

[4]– **سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية "الإنترنت"، دار النهضة العربية، القاهرة، مصر، 2007، ص22.

[5]– **محمد سامي الشوا:** المرجع السابق، ص51.

الفرع الثاني: الأسباب والدوافع المجتمعية (الإجتماعية)

يوجد أيضًا دوافع وبواعث تكمن وراء إرتكاب الجرائم المعلوماتية، كتلك التي تظهر على المستوى المجتمعي أي تلك التي يكون سببها الرئيسي هو المجتمع، والتي قد تتسبب فيها بعض الظروف الإجتماعية، ومن بينها نجد ما يلي:

أولاً: التحضر والعولمة

يعد التحضر *Urbanisation* أحد أهم أسباب الإجرام المعلوماتي عامة، وذلك بحكم الإختلاف الكامن وراء سكان المناطق الحضرية والمدن الكبيرة وبين سكان مناطق البادية والريف، وهذا الجانب الحضري على الرغم من إيجابياته الكثيرة بالنسبة لهؤلاء السكان إلاَّ أنه توجد معه بعض السلبيات، والتي من أهمها مثلاً عدم القدرة على تلبية متطلبات الحياة الحضرية، وكنتيجة لذلك يجد بعض الناس أنفسهم في تنافس وغير قادرين على مجاراتها مما يجعلهم يتجهون إلى الإنغماس في خبايا التكنولوجيات والتقنيات الحديثة والإستثمار فيها، والتي قد لا تتطلب رأس مال كبير بالنسبة إليهم[1]، ويمكن كذلك تفسير علاقة التحضر بالإجرام المعلوماتي من خلال التغييرات في أنشطة الناس الروتينية في حياتهم اليومية والتأثر ببعض الثقافات الغربية، فمع ظهور شبكة الإنترنت وما تحتويه من وسائل التواصل الإجتماعي العديدة والمختلفة، فقد تغيرت معها طريقة الناس في التواصل والتفاعل مع الآخرين لاسيما في علاقاتهم الشخصية والعائلية والترفيهية والتجارية ... وغيرها، كل ذلك قد خلقت معه فرصًا للجناة من قرصنة أهداف قيمة وسهلة في الحيز الفضائي والمعلوماتي مع غياب الحراسة والحماية الأمنية.

كما أنَّ ظهور العولمة *Mondialisation* وما صاحبها من ظهور للفضاء الإلكتروني خلق معه ظواهر إجتماعية جديدة ومتميزة فرضتها أنظمة الحاسب أنفسها من فرص مباشرة لإرتكاب الجريمة، فأصبح الأشخاص يرتكبون جرائم في البيئة الإلكترونية قد لا يرتكبونها في الواقع المادي وهذا بسبب مكانتهم وموقعهم، بالإضافة إلى ذلك ضعف عوامل الردع وما إنجرَّ معه من تحفز للسلوك الإجرامي في العالم الإفتراضي[2]، ومع ذلك تبقى التكنولوجيا تستلهم من الدراما المليئة بالمغامرات.[3]

---

[1]– **محمود رجب فتح الله:** المرجع السابق، ص257.

[2]– **عمر محمد خير الحاج:** العولمة وآثارها في تطور الجريمة، مجلة الأمن والقانون، كلية شرطة دبي، الإمارات العربية المتحدة، س10، ع1، 2002، ص29.

[3]– **غنية باطلي:** المرجع السابق، ص29.

ثانيًا: الحرمان والفقر والبطالة

تعد الضغوط العامة التي يتعرض لها المجتمع من الحرمان والفقر *Privation et pauvreté* والظروف الإقتصادية الصعبة، من أهم العوامل الضاغطة على المجتمع عامة، وخاصةً على فئة الشباب، مما قد يولد لديهم مشاعر سلبية وناقمة على شرائح من الناس، مما يدفعهم إلى اللجوء لإرتكاب أعمال غير مشروعة يواجهون بها هذه الظروف، ومن ذلك الإتجار الإلكتروني بالبشر والجنس والإباحية وغيرها من الجرائم المعلوماتية.[1]

كما قد ترتبط الجرائم المعلوماتية، شأنها في ذلك شأن سائر الجرائم التقليدية بشبح البطالة *Le chômage* الذي ينتشر بقوة بين فئات عمرية مختلفة من الشباب، لذا نجد كثير من الشباب الذين يمتلكون المعرفة الحاسوباتية يستثمرون ذلك في بعض نشاطات الإجرام المعلوماتي.[2]

ثالثًا: ضعف القانون وتطبيقاته في الجريمة المعلوماتية

توجد الكثير من الدول التي لم تطور تشريعاتها الجنائية حتى تتمكن من مجاراة التقدم التقني في مجال الإجرام المعلوماتي والأساليب الإلكترونية في إرتكابه، وهذا لا يتوقف عن النصوص التشريعية فقط وإنما يشمل أجهزة العدالة من شرطة قضائية وهيئات قضائية، وكيفية تعاملها مع الجريمة المعلوماتية والأدلة الرقمية، وإن كان ذلك يختلف من قانون إلى آخر ومن دولة إلى أخرى.[3]

وبالتالي فإن ضعف إنفاذ القانون وتطبيقاته في الجرائم المعلوماتية قد يؤثر سلبًا على الممارسات العدلية والشرطية في متابعة ورصد وملاحقة مثل هذه الجرائم ومرتكبيها سواءً داخل الوطن أو تلك العابرة منها للحدود الوطنية.[4]

---

[1]– **محمود رجب فتح الله:** المرجع السابق، ص258.

[2]– **علي عدنان الفيل:** المسؤولية الجزائية عن إساءة إستخدام بطاقة الإئتمان الإلكترونية، ط1، المؤسسة الحديثة للكتاب، لبنان، 2011، ص22.

[3]– **محمود رجب فتح الله:** المرجع نفسه، ص260. – **علي عدنان الفيل:** المرجع نفسه، ص19.

[4]– **إبراهيم بن عوض العتيبي:** إستخدام التقنية في التحقيقات الأمنية، مجلة التقنية والأمن، كلية الملك خالد، السعودية، العدد 80، 2005، ص10.

خلاصة القول:

إنّ كل الأسباب السالف ذكرها وغيرها كثير والتي تدفع إلى إرتكاب مثل هذه الأعمال والأفعال غير المشروعة، وسواء كان ذلك بدافع المال أو الإنتقام أو حب المغامرة أو اللهو والفضول، فإنَّ هذه الظاهرة الإجرامية المستحدثة أصبحت اليوم فعلاً تهدد سلامة البيئة الإلكترونية، لذا يجب العمل وبقوة على مجابهتها والحد من إنتشارها والقضاء عليها.

وجدير بالملاحظة، أنَّ أسباب الجرائم المعلوماتية تتفاوت وفق أنواعها، ونوعية الحق المستهدف وكذا صفة الجاني ومستوى تنفيذه وطبيعة الدافع وراءه سواء أكان فردي أو مجتمعي، فجرائم الشباب الهواة تختلف عن أسباب جرائم المحترفين، فتختلف وفق هدفها إذا ما كانت مجرد سرقة للمعلومات أو الرغبة في المتاجرة بها في تحقيق الربح المادي بطريقة غير مشروعة ويبقى هذا الأخير هو الباعث الأول وراء إرتكاب الجرائم المعلوماتية.

الفَصل الثّانِي

الطبيعة القانونية للجريمة المعلوماتية

الفَصل الثّانِي: الطبيعة القانونية للجريمة المعلوماتية

تمهيد وتقسيم:

سبق وأن أشرنا إلى أن الجرائم المعلوماتية هي من الجرائم المستحدثة والتي ظهرت نتيجة التطور الهائل في مجال التقنية العالية، ولهذا فإن أمر تحديد طبيعة هذا النوع من الإجراء قد يكتنفه بعض الصعوبات العلمية والتقنية التي لا نتقنها جيدًا نحن أهل القانون.

وعمومًا تتميز الجريمة المعلوماتية بطبيعة قانونية خاصة لأنها تمثل ظاهرة إجرامية تتعلق بالقانون الجنائي المعلوماتي، وأن البحث عن النظام القانوني الملائم لطبيعة هذه الجريمة عبر التقنية المعلوماتية يهدف بشكل أساسي إلى معرفة أهم أقسامها، وكذا أركانها التي تقوم عليها في تقرير المسؤولية الجنائية للمجرم المعلوماتي، وفي مدى كفاية النصوص القانونية الوضعية التي يفترض تطبيقها على مثل هذه الجرائم المستحدثة في مجال التقنية المعلوماتية، وخصوصًا لتأرجح موقف الدول بهذا الشأن[1]، وحسب قدرة المشرعين في إحتواء التقدم الحاصل ضمن إطار قانوني صحيح تحسبًا لأي إستغلال ضار للتطور التكنولوجي الحاصل في المجتمع[2].

وحتى نصل إلى مفهوم دقيق لوصف الطبيعة القانونية لهذه الظاهرة وأنها جريمة معلوماتية، وهذا ما سوف نبحث فيه من خلال هذا الفصل وذلك بتقسيمه إلى مبحثين إثنين على التوالي:

المبحث الأول: الأركان القانونية العامة للجريمة المعلوماتية

المبحث الثاني: أقسام الجريمة المعلوماتية

[1]– **طوني ميشال عيسى:** التنظيم القانوني لشبكة الإنترنت، دار صادر للمنشورات الحقوقية، بيروت، لبنان، 2001، ص388.

[2]– **أحمد عبد الله المراغي:** المرجع السابق، ص66.

المبحث الأول: الأركان القانونية العامة للجريمة المعلوماتية

تمهيد وتقسيم:

مما لا شك فيه أن دراسة الجرائم بشكل عام، والجرائم المعلوماتية بشكل خاص، تدخل في نطاق دراسة القسم الخاص لقانون العقوبات، ذلك المجال المختص بدراسة كل جريمة على حدة،[1] متناولا عناصرها الأساسية وأركانها، وذلك حتى يتسنى معرفة أهم المبادئ والقواعد التي يقوم عليها النظام القانوني في مجال المسؤولية الجنائية للمجرم المعلوماتي.

وإنّ وصف سلوكيات هذه الجريمة موضوع الدراسة على أنها من الجرائم بالمفهوم القانوني، يقودنا حتما إلى البحث عن أركانها العامة والخاصة بها، فلا جريمة من دون أركان، فركن الجريمة جزء من ماهيتها، فبوجوده وقيامه تتواجد الجريمة وتكون لها قائمة، حتى يمكن الحديث بعدها عن المسؤولية الجنائية وتقرير العقوبة بشأنها.

لذا يجب أن تتوافر عناصر وأركان الجريمة المتمثلة في نص التجريم والسلوك غير المشروع والارادة الجنائية وأثرها على كل من الواقع والقانون، وهذا ما سنتناوله في المطالب الثلاثة الآتية:

المطلب الأول: الركن الشرعي للجريمة المعلوماتية

المطلب الثاني: الركن المادي للجريمة المعلوماتية

المطلب الثالث: الركن المعنوي للجريمة المعلوماتية

[1]– والواقع من الأمر أنّ الجريمة المعلوماتية تدخل في نطاق دراسة القسم الخاص لقانون العقوبات، ذلك الفرع الذي يدرس العناصر التكوينية لكل جريمة على حدة إعمالا لمبدأ "تفريد شرعية الجرائم والعقوبات".

المطلب الأول: الركن الشرعي للجريمة المعلوماتية

يقصد بالركن الشرعي للجريمة نص التجريم الذي يضفي على الفعل أو الإمتناع صفته غير المشروعة، فالجريمة لم تكتسب وصفها كجريمة إلا منذ تقرير تجريمها بنص قانوني، وبدون نص التجريم يصبح الفعل أو الامتناع مشروعًا مهما بدا ملومًا أو مستنكرًا من وجهة نظر الدين أو الأخلاق أو الأعراف الإجتماعية.[1]

والركن الشرعي للجريمة أو كما يسميه البعض "بمبدأ الشرعية الجنائية" هو أول وأهم ركن في الجريمة، حيث لا يمكن تصور جريمة أو الحديث عنها من دون وجود ركنها الشرعي،[2] فلا جريمة ولا عقوبة إلا بنص القانون وأنه ومن دون أن ينص القانون على النموذج القانوني للجريمة المعلوماتية فلا تتحقق إمكانية المساءلة الجنائية عنها، وهذا إستنادًا إلى القاعدة الشرعية التي توجب عدم جواز العقاب عند إنتفاء النص التشريعي، وسندا كذلك إلى أنّ القياس محضور في ميدان النصوص التجريمية الموضوعية.[3]

ولا شك في أن التجريم والعقاب يعد من أخطر الأمور التشريعية التي تمس بحقوق المواطنين وحرياتهم، وذلك بسبب خطورة الآثار والنتائج التي تترتب عليه، ولذلك فإن النصوص التشريعية التي تصدر به يتعين أن تصدر دائمًا وفقًا لمبدأ الشرعية الجنائية،[4] – مشروعية التجريم والعقاب – الذي نتولى إلقاء الضوء عليه في إطار الجرائم المعلوماتية، لذا تقتضي دراسة الركن الشرعي للجريمة المعلوماتية تناوله من عدة نقاط مهمة وهي على التوالي:

---

[1]– **سليمان عبد المنعم:** النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الاسكندرية، مصر، 2014، ص270.

[2]– ومع ذلك فإنه يوجد اتجاه فقهي يعارض فكرة الركن الشرعي للجريمة، وأنّ هذه الاخيرة لا تقوم إلاّ على ركنيين إثنين وهما "المادي والمعنوي" أما الركن الشرعي فليس من الأركان وإنما هو عبارة عن الصفة غير المشروعة للفعل، وهذا على أساس أنّ النص الجنائي الموجد للجريمة لا يمكن أنّ يكون احد أركانها، وأنّ هذا النص ليس إلاّ وعاء نموذج الجريمة، بالإضافة إلى امكانية ارتكاب السلوك المجرم بالنص ومع ذلك لا تقوم الجريمة إذا وجد معها سبب من أسباب الاباحة مثلا (المزيد من التفصيل في هذا الموضوع يراجع:

- ***GARE (Th), GINESTET (C) :*** *Droit pénal et procédure pénal, Imprimé par (I.M.E) paris, France,2012, P13.*

[3]– **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، الأردن، 2009، ص33.

[4]– والواقع من الأمر أنّ مبدأ الشرعية الجنائية لا يقتصر فقط على الشق الموضوعي للقانون الجنائي والمتمثل في قانون العقوبات فيما يقرره من شرعية الجرائم والعقوبات، بل إنه يشمل أيضا وفقا للفقه الراجح الشق الاجرائي للقانون الجنائي والمتمثل في قانون الإجراءات الجزائية وهو ما يعرف "بمبدأ الشرعية الاجرائية" ويتجلى ذلك في مجال التقيد بقواعد الاختصاص، وإحترام قرينة البراءة وغيرها كثير من القواعد الاجرائية (أنظر كل من: – **أحمد فتحي سرور:** الشرعية الدستورية وحقوق الانسان في الاجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، 1955.– **محمود علي أحمد مدني:** دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التي يقوم عليها النظام القانوني المصري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، مصر، 2015، ص349. – **هشام عبد السيد الصافي محمد بدر الدين:** الجرائم الالكترونية في مصر ودستورية مبدأ الشرعية الجنائية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، طرابلس، لبنان، العدد 14 لعام 2017، ص133).

الفرع الأول: مبررات مبدأ الشرعية الجنائية أمام الجرائم المعلوماتية

في سبيل إسباغ الشرعية الجنائية على الجريمة المعلوماتية هناك عدد من المبررات العقلية والمنطقية والتي عرضت نفسها من أجل الترويج لفكرة الشرعية الجنائية لهذا النوع من الجرائم والتي يمكن حصرها في الآتي:

أولاً- تحقيق فكرة العدالة الجنائية

إنّ احترام الذات الانسانية لا يمنعنا من القول أن الجريمة موجودة مع الانسان وجودًا وعدمًا، تقدمًا وتخلفًا، والإنسان مرتبط بالمجتمع فاعلاً ومنفعلاً، كما أن الصلة وطيدة بين الجريمة والمجتمع[1]، كذا القرابة وطيدة بين تطور المجتمع الحضاري والعلمي والتكنولوجي والجريمة، فقد تكون الصلة بين الجريمة والتطور مثيرة للدهشة ولكن سرعان ما تكشف هذه الدهشة ستارها عندما نعلم أن تطور المجتمع وما يصاحبه من تقدم علمي وتكنولوجي ينعكس أثره على تطور الجريمة والمجرمين[2].

فالجريمة بإعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تقدم وتطور، ومرجع ذلك أن مرتكب الجريمة عضو في المجتمع يتأثر بثقافة مجتمعه فأقصى ما يصل إليه المجرم اليوم من براعة ودراية يكون نتيجة لهذه الثقافة يحاول إستخدامها في جريمته، فالجريمة اليوم هي محصلة كل ذلك، لذلك يتطلب من المشرع داخل كل مجتمع من حصر الأفعال التي يستنكرها أفراده، وأن تحدد تحديدا دقيقا تحت طائلة العقوبة في إتيانها.[3]

وعمومًا فإن فكرة العدالة الجنائية يقصد بها بصفة عامة أن التشريع هو المختص بتحديد الجرائم والعقوبات دون السلطتين القضائية والتنفيذية، وأن القاضي مهمته تطبيق النصوص التي وضعها المشرع، ويعد مبدأ شرعية الجرائم والعقوبات أحد أهم تطبيقات فكرة العدالة الجنائية وبالتالي لا يجوز توقيع عقوبة إلا بناء على حكم قضائي، ومن هنا يعد هذا المبدأ من المبادئ الدستورية ذات الطابع العالمي.[4]

---

[1]- **حسني الجندي:** الوجيز في شرح قانون العقوبات، القسم العام، ط1، دار النهضة العربية، القاهرة، مصر، 2007، ص5.

[2]- **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017، ص45.

[3]- وهذا ما سعت الثورة الفرنسية لتؤكد عليه من خلال اعلان حقوق الانسان والمواطن لسنة 1789، ثم جاء بعدها الاعلان العالمي لحقوق الانسان لعام 1948 ليؤكد ذلك أيضا، كما تضمنته الاتفاقية الأوروبية لحقوق الانسان لعام 1950، ثم بعد ذلك العهد الدولي للحقوق المدنية والسياسية عام 1966.

[4]- يرجع الفضل في ظهور هذا المبدأ إلى الفقيه الايطالي (سيزار بكاريا ***Cezare Baccaria***) صاحب الكتاب الشهير: "رسالة في الجرائم والعقوبات" الذي أصدره سنة 1764، وقد جاء فيه أنّ: "القوانين وحدها هي التي تحدد العقوبات التي تقابل الجرائم، ولا يستطيع القاضي أن يوقع سواها". موجود على الموقع: ***www.neelwalurat.com***، تاريخ التصفح: 2017/04/30.

ثانيًا– تحقيق فكرة الردع العقابي والمساواة في العقاب

والردع العقابي بنوعيه العام والخاص يؤدي إلى إحجام الأشخاص عن إرتكاب مثل هذه الجرائم مخافة الحكم عليهم بمثل هذه العقوبة المقررة، كما يؤدي بإقتناع مرتكب الجريمة بعدالة العقوبة المطبقة عليه.

أما عن المساواة في العقاب يقصد بها أن النصوص الخاصة بالتجريم والعقاب تصاغ بشكل عام ومجرد بحيث تطبق على كافة المخاطبين بها، بل وحتى على جميع الواقع دون تمييز، وهذا سيؤدي حتما إلى تحقيق فكرة المساواة ين الأفراد أمام القانون، فلا يختلف تطبيق القانون على حسب الوضع الاجتماعي أو المركز القانوني لصفة الجاني، وهذا ما أكدته المادة (165) من الدستور الجزائري بقولها: "يقوم القضاء على أساس مبادئ الشرعية والمساواة". وكذا نص المادة (37) منه: "كل المواطنين سواسية أمام القانون"[1].

ثالثًا– تحقيق فكرة العلم بوجود النص الجنائي

وهذا معناه أنه لا يعذر أحد بجهله للقانون، بل العلم به مفترض فيه، وأنّ إعلام المخاطبين بالقانون يكون بموجب نصوص قانونية مكتوبة يتم نشرها بمختلف الوسائل المتاحة بعد نشرها في الجريدة الرسمية، وهذا ما أكدت عليه المادة (78) من الدستور الجزائري بقولها: "لا يعذر أحدًا بجهل القانون، ولا يحتج بالقوانين والتنظيمات إلاّ بعد نشرها بالطرق الرسمية، ويجب على كل شخص انّ يحترم الدستور وأن يمتثل لقوانين الجمهورية".

وعليه فإنه لمواجهة الجريمة المعلوماتية لا بد من وجود نصوص جنائية عامة وخاصة وإعلام المواطنين بها، بل يقتضي الأمر أكثر من ذلك وهو ضرورة وجود قانون خاص بالإجرام المعلوماتي، ومن هنا ووعيًا بخطورة الوضع أصدر المجلس الأوروبي سنة 1989 توصية تشجع من خلالها الدول الأعضاء على تبني نصوص جنائية جديدة للحد من هذه الظاهرة ولحل هذه المشكلة مؤقتًا، فهناك من قام بإدراج هذه النصوص الجديدة في إطار قانون العقوبات التقليدي، وهناك من قام بإدماجها ضمن جرائم الأموال باعتبار أنه يمكن إسباغ صفة المال على الكيانات المادية والمعنوية للحاسوب، ومثال ذلك قانون العقوبات الفرنسي وذلك ضمن الكتاب الخامس منه تحت عنوان الجنايات والجنح ضد الأموال.[2]

[1]– أنظر في ذلك: الدستور الجزائري لعام 2020.

[2] -***GASSIN (R) :*** *Le droit pénal de l'informatique, Op. Cit, P28.*

والبعض الآخر فضل إدماجها في إطار الجزء الخاص بالجرائم ضد الملكية باعتبار أن الكيان المادي للحاسوب قابل للتملك، كما أن الكيان المعنوي له يدخل في إطار الملكية الفكرية،[1] وهناك من يرى أنه من الأفضل إلحاق كل جريمة إلكترونية بما يقابلها في قانون العقوبات التقليدي، فمثلا جريمة السرقة المعلوماتية في باب السرقات والنصب، وجريمة الإتلاف والعبث المعلوماتي في باب جرائم الإتلاف للممتلكات، وجريمة التزوير المعلوماتي في باب تزوير المحررات، وجريمة القذف المعلوماتي في باب جرائم السب والشتم ... وهكذا.[2]

أما على المستوى الدولي، نجد أول إتفاقية حول الإجرام المعلوماتي كانت عام 2001 التي تضمنت التأكيد على وضع نصوص قانونية تجرم مختلف أشكال الإجرام المعلوماتي،[3] وتعتبر السويد أول الدول الغربية التي سنت التشريعات الخاصة بجرائم الحاسب الآلي والإنترنت، حيث أصدرت قانون البيانات الآلية السويدي لسنة 1973، كما تعتبر الولايات المتحدة الأمريكية أول الدول التي سنت قوانين خاصة بالجريمة الإلكترونية وذلك عام 1985، وتلتها بعد ذلك الكثير من الدول منها فرنسا عام 1988، وإنجلترا عام 1990، وإيطاليا عام 2000.[4]

وأيضًا ما قام به المشرع الجزائري من إضافة القسم السابع مكرر تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، وإدراجه ضمن قانون العقوبات في الجزء المتعلق بالجنايات والجنح ضد الاموال، ولقد أدمج المشرع الجزائري هذه الجرائم بموجب ثلاثة قوانين وهي القانـــون رقم (04-15) المؤرخ في 10 نوفمبر 2004 ثم عدل وتمم بموجب القانون رقم (06-23) والمؤرخ في 20 ديسمبر 2006، وكذا القانون رقم (16-02) والمؤرخ في 19 يونيو 2016، وكلها تعدل وتتمم من قانون العقوبات رقم (66-156) والمؤرخ في 08 يونيو 1966. وكل ذلك ولم يستحدث المشرع الجزائري قانون خاص ومستقل بالإجرام المعلوماتي، على الرغم من أن النص على هذه الجريمة كان إحدى البنود التي نص عليها الإتفاق الذي يؤسس الشراكة بين الجزائر والاتحاد الأوروبي والمنعقد بتاريخ 22 أفريل 2002 والذي تضمنته المادة الثامنة منه.

---

[1]- **غنية باطلي:** المرجع السابق، ص177.

[2] -***GASSIN (R) :*** *Le droit pénal de l'informatique, Op. Cit, P.30.*

[3]- أبرمت هذه الإتفاقية بتاريخ 2001/11/08 تحت إشراف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[4]- **مليكة عطوي:** الجريمة المعلوماتية، مجلة حوليات، جامعة الجزائر1، العدد21 لسنة 2012، ص18. - **مختارية بوزيدي:** ماهية الجريمة الإلكترونية، مجلة أعمال الملتقى الوطني، بعنوان آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، تحت إشراف مركز جيل البحث العلمي، الجزائر العاصمة 29 مارس 2017، ص12.

ومع ذلك وحتى الآن لا يوجد بالجزائر تشريع عقابي خاص بالجرائم المعلوماتية، كل ما هناك أنه توجد بعض النصوص القانونية المتناثرة في قوانين مختلفة كقانون العقوبات، والتي تتحدث عن بعض الجرائم الالكترونية والعقوبات المقررة لها،[1] حيث يقتضي الأمر ضرورة وجود قانون خاص لمواجهة الجرائم المعلوماتية.

رابعًا- تحقيق فكرة الأمن القومي والإقتصادي

إنّ الدراسات الحديثة للإجرام الحديث بينت أنّ هناك علاقة بين الأمن القومي والإقتصادي وظاهرة الإجرام، حيث إنجر على هذا التطور خسائر كبيرة جراء الجرائم الإلكترونية المتزايدة والمتسارعة، وتفاقم هذه الأخطار على المجتمع وأمنه القومي وإقتصادياته، مما يلزم الدولة من التدخل كل مرة لبسط حمايتها الجنائية على مشروعاتها القومية والوطنية ضد هذا النوع من الإجرام،[2] ولأنّ الفائدة الكبيرة المترتبة على المساس بالمعلوماتية قد تعاظمت في الوقت الحالي فأصبحت توازي إقتصاديات الدول، فكان من الضروري التدخل السريع للمشرع الجنائي لحمايتها،[3] وهذا ما ذكرته المادة (31) من الدستور المصري لعام 2014 والتي جاءت تشير إلى وجوب الحفاظ على المعلومات والبيانات الإلكترونية لأنها توازي أمن الوطن وإقتصادياته، حيث جاء نصها: "أمن الفضاء المعلوماتي جزء أساسي من منظومة الإقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"[4].

كما يجب أيضًا على الفرد تقييم الفعل الذي سيقدم عليه، أي الموازنة بين الفائدة التي سيجنيها منه والثمن الذي سيدفعه وهو العقوبة، فإذا غلب جانب مقدار العقوبة على جانب مقدار الفائدة وهذا أمر حتمي، فإنه سيتجنب الإقدام على مثل هذه الأفعال.

خامسًا- تحقيق فكرة التوازن بين الواقع والقانون

نظرًا للتطور الكبير الذي يشهده الواقع الإنساني اليوم في كافة المجالات لاسيما منها المجال التكنولوجي، فكان لابد أن يواكب هذا التطور نصوص قانونية مناسبة، والقانون الجنائي كان ولايزال يعيش هذا التطور بإستمرار، إذ يلعب دورًا كبيرًا من الناحية الموضوعية والإجرائية في

---

[1]- أنظر في ذلك: **الملحق رقم (05).**

[2]- **غنية باطلي:** المرجع السابق، ص145.

[3]- **محمد خليفة:** المرجع السابق، ص30.

[4]- الدستور المصري لعام 2014.

تحقيق حماية كافية للحقوق والحريات لا توجد في قوانين أخرى، وعليه كان لزامًا على المشرع الجنائي النص على تجريم مثل هذه الأفعال، وتفعيل إجراءات البحث عن مرتكبيها حتى يمكن القول بتوافر الركن الشرعي[1].

الفرع الثاني: الحماية الجنائية للمال المعلوماتي

إنّ المال المعلوماتي بطبيعته ينقسم إلى نوعين منفصلين وفقًا لخصوصية هذا المال، فهو إما مال معلوماتي ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أيًا كان نوعها، وإما أن يكون مال معلوماتي ذو طبيعة مادية ويتمثل في أدوات وآلات الحاسب الآلي الملموسة، إذ قد يترتب على إختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلافًا في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي، ولذلك ظهرت في هذا الشأن بعض الخلافات الفقهية وتبع ذلك عدم إستقرار الأحكام القضائية الصادرة[2].

فالإعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة تقنية ذات طبيعة خاصة يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الإعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للنظام المعلوماتي، وهي ما سميت في كل من فرنسا وكذا الجزائر "بجريمة المساس بنظام المعالجة الآلية للبيانات"، وهي جريمة مستحدثة تناولها كل من المشرع الفرنسي ونظيره المشرع الجزائري. فمعظم حالات إرتكاب هذا النوع من الإجرام تتم في مجال المعالجة الإلكترونية للبيانات، وذلك من خلال تجميع وتجهيز البيانات لإدخالها إلى الحاسب بغرض الحصول على معلومات ذات قيمة مالية، وهي طريقة أوتوماتيكية تمكن المستخدم من تأمين المعلومة على الحاسب أو الشبكة، مع توفير إمكانية التصحيح والتعديل والمحو والتخزين والإسترجاع والطباعة، وهي كلها عمليات وثيقة الصلة بإرتكاب الجرائم المعلوماتية.[3]

ومن هنا كان ولابد على المجرم المعلوماتي من إستيعابها، فضلاً عن أنه طور تعامله مع مفردات جديدة كالبرامج والمعطيات والمواقع الإلكترونية التي تشكل محل الإعتداء أو تستخدم كوسيلة له، ناهيك عن إفساح المجال واسعًا أمام المنحرفين لإقتناء وسائل إلكترونية تمكنهم

[1]– **غنية باطلي:** المرجع السابق، ص146.

[2]– **فخري محمود خليل:** جرائم البلطجة الإلكترونية، د.د.ن، 2019، ص14.

[3]– **أحمد خليفة الملط:** الجرائم المعلوماتية، المرجع السابق، ص79.

لإستخدامها في إرتكاب جرائم مختلفة سواء بالإعتداء على حق الخصوصية والحرية الشخصية أو حتى على أمن وإستقرار المجتمع في حد ذاته.[1]

ولقد إسقر الفكر القانوني على ضرورة إيجاد نصوص خاصة لحماية المال المعلوماتي وحماية الخصوصية المعلوماتية الرقمية، بحيث إستجابة فعلاً العديد من دول العالم لهذه الحاجة بسنها قوانين تناولت في طياتها أركان الجريمة المعلوماتية وعقوباتها المقررة لها، وهذا كله تحت بوتقة مبدأ مشروعية التجريم والعقاب.

وإنّ كانت بعض التشريعات بما فيها التشريع الجزائري تسعى إلى إيجاد قانون مستقل خاص بالمعلوماتية، وهذا نتيجة طبيعية للتطور الحاصل في هذا المجال، فإن هناك من يرى بإضافة قانون خاص بالجرائم الإلكترونية مستقل عن قانون العقوبات التقليدي، أو كما يسميه البعض "بالقانون الجنائي التقني" وهذا بإعتبار أن هذه الجرائم تتعلق بقيمة إجتماعية جديدة لها طابع خاص.[2]

أما المشرع الجزائري فقد تدارك هو الآخر ومن وقت بعيد نسبيًا الفراغ القانوني في مجال الجريمة المعلوماتية،[3] وذلك بإستحداث نصوص تجريمية خاصة لقمع بعض الإعتداءات الواردة على النظام المعلوماتي، وذلك بموجب تعديل قانون العقوبات، وهذا بإضافة القسم السابع مكرر تحت عنوان "المساس بأنظمةالمعالجةالآليةللمعطيات" بالمواد من(394مكرر) حتى (394 مكرر8) من (ق ع ج).[4]

كما أصدر المشرع الجزائري في مواجهته لهذا النوع من الإجرام القانون رقم (09-04) المؤرخ في 05 أوت 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.[5]

---

[1]– **محمود رجب فتح الله:** الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2019، ص163.

[2]– **غنية باطلي:** المرجع السابق، ص148

[3]– نجد أنّ المشرع الجزائري إتخذ هذه المبادرة في مواجهة الجريمة المعلوماتية، في وقت مبكر نوعًا ما وهذا مقارنة مع بعض الدول العربية، حيث شاركت الجزائر في الإتفاقية الأورو متوسطية والمؤرخة في 22 أفريل2002، والتي كانت تهدف إلى ربط الجهود بين الدول الأوروبية من جهة والدول المطلة على الحوض الأبيض المتوسط من جهة أخرى، وقد صادقت الجزائر على هذه الإتفاقية بتاريخ 25 أكتوبر 2003 والتي دخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم (07-375) المؤرخ في 01 ديسمبر 2007، (ج ر المؤرخة في 09 ديسمبر 2007 ع77).

[4]– وهذا بموجب القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004، ثم عدلت وتممت هذه المواد مرتين، الأولى بموجب القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006، والثانية بموجب القانون رقم (16-02) المؤرخ في 19 يونيو 2016. هذه القوانين وغيرها تعدل وتتمم الأمر رقم (156/66) المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات الجزائري.

[5]– القانون رقم (09-04) المؤرخ في 2009/08/05 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، (ج ر المؤرخة في 2009/08/16، ع 47). **الملحق رقم (06)**

الفرع الثالث: دستورية الشرعية الجنائية للجريمة المعلوماتية

ولما كان القانون ينشأ الحق ويحميه تبعًا للقاعدة الفقهية الشهيرة، فنجد أن الدستور بإعتباره الوثيقة العليا والقانون الأساسي في الدولة أن من ضمن ما ينظمه جملة الحقوق والحريات بإعتباره القانون الذي ينشأها، ثم يأتي القانون الجنائي لحماية هذه الحقوق والحريات، حيث أنّ العلاقة وثيقة بين القانون الدستوري والقانون الجنائي،[1] ذلك أن مبادئ الدستور تسهم في تحديد مضمون القانون الجنائي ذاته بحيث يتوقف تحديد الجرائم والعقوبات على قيمة تطوير المبادئ الدستورية والقيم والمصالح الإجتماعية.[2]

وفي ضوء ذلك يؤدي التشريع الجنائي الجزائري وظيفته في الدولة في إطار الشرعية الدستورية على النحو الذي يرسمه ويحدده الدستور مسبقًا، فقد أقيم القانون الجنائي على عدد لا بأس به من المبادئ الدستورية، والتي من أهمها "مبدأ الشرعية الجنائية" حيث جاء في سياق نص المادة (43) من دستور 2020 أنه: "لا إدانة إلاّ بمقتضى قانون صادر قبل إرتكاب الفعل المجرم" وكذا ما ذكرته المادة (167) منه بقولها: "تخضع العقوبات الجزائية لمبدأي الشرعية والشخصية"[3]، وهاتان المادتان تمثلان حجر الزاوية والأساس التجريمي والعقابي للنظام الجنائي بأسره، فهما بمثابة نقطة المركز التي يدور حولها كافة المبادئ والقواعد التي تحكم النصوص الجنائية موضوعية كانت أم إجرائية.

كما كفل الدستور الجزائري حماية الحقوق الأساسية والحريات العامة والفردية، على أن تضمن الدولة عدم إنتهاك حرمة الإنسان،[4] وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها القانون الجنائي في شقيه العقابي والإجرائي، وكذا قوانين خاصة أخرى والتي تجسد فعلاً مبدأ الشرعية الجنائية، حيث جاء في نص المادة الأولى من قانون العقوبات الجزائري أنه: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون".

---

[1]– **محمود رجب فتح الله:** المرجع السابق، ص178.

[2]– صدر الدستور الجزائري الحالي بموجب المرسوم الرئاسي رقم (20–442) المؤرخ في 30 ديسمبر2020، والمتعلق بالتعديل الدستوري (ج ر 82 المؤرخة في 30 ديسمبر2020).

[3]– **أحمد فتحي سرور:** القانون الجنائي الدستوري، دار الشروق، القاهرة، مصر، 2002، ص31.

[4]– ولعل من بين أهم هذه المبادئ والقواعد الدستورية التي كرسها الدستور الجزائري هو ما جاء في سياق المواد التالية:

– **المادة (39):** "تضمن الدولة عدم انتهاك حرمة الانسان، يحظر أي عنف بدني أو معنوي، أو أي مساس بالكرامة".

– **المادة (41):** "كل شخص يعتبر بريئا حتى تثبت جهة قضائية إدانته في إطار محاكمة عادلة".

– **المادة (44):** "لا يتابع أحد، ولا يوقف أو يحتجز، إلا ضمن الشروط المحددة بالقانون، وطبقا للأشكال التي نص عليها".

كما أقر أيضًا الدستور الجزائري لعام 2020 بعض المبادئ الدستورية ذات الطابع العلمي مواكب في ذلك التطورات التقنية والتكنولوجية فنذكر على سبيل المثال نص المادة (47) منه: "لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته وإتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة إلاّ بأمر معلل من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي، يعاقب القانون على كل انتهاك لهذه الحقوق" وزادت المادة (55) من نفس الدستور بقولها: "يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات، والحصول عليها وتداولها، لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم وبالمصالح المشروعة للمؤسسات وبمقتضيات الأمن الوطني، يحدد القانون كيفيات ممارسة هذا الحق".

المطلب الثاني: الركن المادي للجريمة المعلوماتية

يتطلب المشرع للقول بقيام جريمة ما توافر الركن المادي لها، والذي بدوره يتكون من عناصره الثلاثة وهم على التوالي السلوك المادي والنتيجة الإجرامية والعلاقة السببية ما بينهما.

ومن المشكلات العملية التي تثيرها الجريمة المعلوماتية هي طبيعة الركن المادي فيها، ذلك أن مناط التجريم ينصب على نظام إلكتروني يُساء إستعماله أو يتم إقتحامه على نحو غير مشروع، بما يكون لذلك الإستعمال أو الإقتحام من أثر مادي ملموس يظهر إما في صورة تدمير للنظام المعلوماتي أو في صورة التلاعب بالبيانات والمعلومات.

وعليه فإن إرتكاب الجريمة المعلوماتية يحتاج إلى منطق تقني يتمثل في سلوك مادي ونتيجة إجرامية وعلاقة سببية تجمع بينهما، وهذا ما سوف نتطرق إليه:

الفرع الأول: السلوك الإجرامي

الجريمة المعلوماتية ذات طابع موحد فهي تباشر من حيث السلوك أو النشاط المادي فيها بوصفه أحد أهم عناصر الركن المادي،[1] والسلوك الإجرامي في الجريمة المعلوماتية يرتبط دائمًا بالمعلومات المخزنة على الحاسب الآلي أو النظام المعلوماتي، أي ضرورة إستخدام الحاسب الآلي وسيطًا لإرتكابها مما يجعل هذا النوع من الإجرام من نوعية جرائم الوسيلة،[2] وهذا الأمر غير مقبول للقول بعدم مشروعية هذا الوسيط المستخدم لإرتكاب الجريمة وهو هنا الحاسوب أو الشبكة

[1]– **علي جبار الحسيناوي:** المرجع السابق، ص37.

[2]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص211.

أو الخادم... وهذه أدوات مشروعة بحس الأصل، لأنه من اللازم إستخدام الحاسوب لكي يمكن إرتكاب الجريمة التي ترتبط بإمكانية إستخدام الآلة أو الجهاز ومدى تمتع الشخص بالتقنية الكافية في هذا الشأن لإرتكاب الجريمة،[1] وأن كل من الحاسوب والإنترنت يدخلان في طائلة المشروعية ولا يمكن أن تقوم أي من الجرائم المعلوماتية سوى بإستخدامها، وهذا ما يجعل مسألة إستخدام الحاسوب والإنترنت جزءًا من النشاط المادي في الجرائم الناشئة عن سوء إستخدام كل من الحاسوب والإنترنت[2].

إن السلوك الإجرامي بوصفه عنصرًا في الركن المادي في الجرائم التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن مع صعوبة الجريمة المعلوماتية والركن المادي فيها خاصة وأن الجريمة ترتكب عن طريق تدفق معلومات عبر نظم الحاسب الآلي والتي لا يمكن الإمساك بها ماديًا، تمامًا فهي مثل التيار الكهربائي الذي يسري في توصيلة دون أن نراه وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط زِرْ في الحاسب فتقوم معه الجريمة، كما هو الحال في الجرائم الإلكترونية التي يتم فيها الإعتداء على المال العام أو الخاص.[3]

ويضاف إلى فلسفة السلوك الإجرامي في الجرائم المعلوماتية هو تدارك المشرع المقارن حينما نص على هذا النوع من الجرائم والتي ترتكب عبر الحاسوب نجد المشرع يقرر صراحة عبارات تدل على ذلك ومنها مثلاً: "... إذا إرتكب الجريمة بإستخدام الحاسوب" أو عبارة "... بإستخدام المعالجة الآلية للبيانات" ويكون المشرع بهذه الحالات مدركًا للقيمة في إرتكاب أو الشروع في إرتكاب جريمة عبر الإنترنت أو بإستخدام الحاسوب المرتبط بالإنترنت.[4]

مما تقدم نرى أن النشاط المادي يبنى على العلاقة التقنية بين مرتكب جريمة معلوماتية وبين الجهاز أو الآلة، وفي كيفية تحديد حدوث السلوك الإجرامي بإستخدام الإنترنت والحاسوب، ولقد وجد المشرع الأمريكي أنّ إستخدام الإنترنت ليس له هدف في ذاته فلا يستخدم الإنترنت لمجرد الإستخدام وإنما هو تحقق فوائد عظيمة في الوقت الذي يمكن أن تكون مهدًا لإرتكاب الجريمة أيضا، لذلك لم يمانع في تحديد طرائق السلوك الإجرامي بشكل تفصيلي لكي يمكن القول

[1]– **فخري محمود خليل:** المرجع السابق، ص23.

[2]– **علي جبار الحسيناوي:** نفس المرجع، ص38.

[3]– **فخري محمود خليل:** المرجع السابق، ص24

[4]– **محمد فهمي طلبة:** المرجع السابق، ص122.

بقيام النشاط الإجرامي بما يجعل النص الجنائي ينطبق على هذا النوع من الجرائم مع مراعاة تحقيق النتيجة الإجرامية المشار إليها[1].

الفرع الثاني: النتيجة الإجرامية

يقصد بالنتيجة الأثر الطبيعي المترتب على السلوك متى أعتبر من الوجهة التشريعية عدواناً على حق أو مصلحة يحميها القانون[2]. وتعني النتيجة الإجرامية ذلك التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي والذي يعتد به القانون فيجعله عنصر من العناصر المكونة لجريمة معينة فلا تقع الجريمة تامةً إلاّ بتوافره مع بقية العناصر الأخرى، فالنتيجة الإجرامية هي إحدى عناصر الركن المادي في الجريمة[3].

ويستخلص من تعريف النتيجة على النحو السابق أن لها مدلولين، أولهما طبيعي مادي يمكن إدراكه حسيًا[4] ويتجسد في الأثر أو الآثار المترتبة على السلوك، والنتيجة بهذا المعنى تغيير يحدث في العالم الخارجي، وثانيهما مدلول معنوي قانوني يتمثل في العدوان على الحق أو المصلحة التي إرتاءها المشرع جديرة بالحماية الجنائية،[5] ويترتب على النتيجة بهذا المعنى أحكام قانونية عديدة فيما يتعلق بتحقق صلة السببية، والشروع، والقصد الجنائي. ولكن النتيجة قد لا تكون عنصرًا في بعض الجرائم الأخرى التي تقوم وتكتمل دون تحقق النتيجة فيها، وقد درج الفقه على تسمية الجرائم التي يلزم فيها تحقيق نتيجة بالجرائم المادية أو جرائم الضرر، بينما يطلق على الجرائم التي لا يلزم فيها تحقيق نتيجة بالجرائم الشكلية أو جرائم الخطر[6].

ويواجه تحديد الخطر أو الضرر بوصفه نتيجة إجرامية عبر الحاسوب أو الإنترنت العديد من المشاكل كتلك المتعلقة بجرائم العدوان الفيروسي، إذ تثير هذه النوعية من الجرائم مشكلة تحديد حجم الضرر أو الخطر وهي من الصعوبات التي تواجه الفكر القانوني المعاصر في هذا المجال خاصة إذا كان المشرع الجنائي يتطلب تحقق نتيجة معينة في مثل هذه الجرائم[7].

---

[1]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص162. – **علي جبار الحسيناوي:** المرجع السابق، ص38.

[2]– **سليمان عبد المنعم:** النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، مصر، 2014، ص409.

[3]– **رمسيس بهنام:** النظرية العامة للقانون الجنائي، منشاة المعارف، الإسكندرية، مصر، 1997، ص377.

[4]– **محمود نجيب حسني:** شرح قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 1988، ص144.

[5]– **عمر السعيد رمضان:** فكرة النتيجة في قانون العقوبات، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، مصر، العدد 31 لسنة 1961، ص104.

[6]– **سليمان عبد المنعم:** المرجع السابق، ص410.

[7]– **علي جبار الحسيناوي:** المرجع السابق، ص40.

كما تثير النتيجة الإجرامية في جرائم الحاسوب والإنترنت مشاكل متعددة كمسألة مكان وزمان تحقق النتيجة الإجرامية، فهل تعد هذه الجريمة مرتكبة سلوكًا ونتيجةً في العالم الإفتراضي أو أن هناك إمتدادًا للنتيجة لكي يتحقق منتهاها في العالم المادي، أو يتحقق أولها في العالم الإفتراضي ومن ثم يكون هناك إمتداد في النتيجة من العالم الإفتراضي إلى العالم المادي، وذلك قياسًا على أثر النتيجة الإجرامية ذات البعد الدولي، سواء في شكل إمتداد الضرر أو الخطر إلى ما يتجاوز الحدود الإقليمية التي وقع فيها السلوك المجرم وتأخر حدوث النتيجة، حيث يأخذ هذا الإمتداد شكل العدوان على حق أو مصلحة قائمة ومشروعة في دولة أخرى أو دول متعددة[1].

وذلك مع الأخذ في الإعتبار أن هناك من الجرائم التي يكون لها وجود سواء عبر الإنترنت أو عبر الحاسوب أي كل جرائم التقنية التي لا يمتد أثرها إلى العالم المادي ويشمل ذلك بالطبع صعوبة إكتشافها وإقامة الدليل على إرتكابها، وهذا ما جعل القانون المقارن يتجه إلى محاولة إرساء رؤية قانونية في تقدير قيام المسؤولية الجنائية في كل محاولة إفساد أو إعاقة مصلحة معلوماتية، ومن ثم فإن النهج هنا ينطلق وفقا لهذه النظرية هو الأخذ في الإعتبار بضرورة أن تكون كل علاقة مشبوهة على تعطيل أو المساس بالخدمات التي تقدمها الانترنت أو الحاسوب للمستخدم الشرعي، كل ذلك يؤدي بالضرورة إلى الإهتمام بالنتيجة الإجرامية ذات النشاط المادي للجريمة من حيث كونه الخلاصة النهائية التي ما تحرك المشرع المقارن إلاّ بسببها[2]، ومن ثم يلزم الحال هنا التعرض لتأثير منطق العالم الإفتراضي في العالم المادي لكي يمكن ان نتعرف على نوعية النتيجة وهذا التأثير الذي إعترف فيه المشرع الجنائي.[3]

ومن هنا فإنّ كل جريمة تحدث بإستخدام الإنترنت أو الحاسوب إنما تحدث كلها أو بعضها حسب الأحوال في العالم الإفتراضي مع إمكانية تحقق النتيجة الإجرامية في العالم المادي، فمثلاً إذا تطلب المشرع تحديدًا القتل في جريمة إختراق قواعد بيانات المستشفى وذلك بقصد إرتكاب جريمة القتل فإنّ تمام النتيجة تقنيًا هو إكتمال تغيير بيانات الدواء، ويلزم هنا لكي يمكن القول بتمام الجريمة وفق النموذج القانوني للجريمة أن يتم إعطاء المريض الدواء الخاطئ فعلا، فإذا لم يتم إعطاؤه

---

[1]– **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي والأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص52.

[2]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص270.

[3]– **عمر محمد أبو بكر بن يونس:** المرجع نفسه، ص273.

الدواء الخاطئ فإن الجريمة ماديًا تضل في حالة شروع شكلي ومن الناحية العملية فإن النتيجة الإجرامية سوف تظل محلاً لجدل قانوني يجب أن يتم التطرق إليه من منطق التزاوج بين العالم المادي ونظيره الإفتراضي، بحيث يكون بناء الجريمة المعلوماتية حين هيكلة ركنها المادي بالأخذ في الإعتبار هذا التزاوج[1].

وهكذا نجد أنّ النتيجة الإجرامية عنصر هام من عناصر الركن المادي للجريمة المعلوماتية، ويتوقف عليها العديد من أحكام النظرية العامة لقانون العقوبات، فبدون المساس بالنظام المعلوماتي لا يتصور قيامها، ولا حتى البحث فيها، إلاّ إذا تعلق الأمر بإحدى جرائم الخطر الماسة بهذا النظام والتي يتطلب بناؤها القانوني حصول نتيجة في معنى العدوان الفعلي على حق أو مصلحة معلوماتية يحميها القانون، كما أن الشروع لا يكون متصورًا ومعاقب عليه إلاّ حين تصور حدوث نتيجة حيث يقع كل أو بعض السلوك وينتفي مع حدوث النتيجة وذلك في الجرائم العمدية، أما إذا لم يكن تصور حدوث نتيجة فلا عقاب على الشروع في الجرائم غير العمدية.[2]

الفرع الثالث: العلاقة السببية ما بين السلوك الإجرامي والنتيجة

مؤدى صلة السببية ***Le lien de causalité*** أنه لكي يكتمل البناء القانوني للجريمة في ركنها المادي لابدّ أن يرتبط السلوك فعلاً كان أو إمتناعًا في الحدود التي يعتد فيها بالإمتناع، بالنتيجة المحظورة التي تحققت بإرتباط السبب بالمسبب،[3] وهي إسناد ماديات النتيجة إلى مصدرها بشكل تسلسلي وهي من طبيعة مادية كأصل عام، فالعلاقة السببية هي علاقة مادية وليست علاقة قانونية، والمشرع يعترف بها قانوناً صراحةً أو ضمناً ولا يحيلها إلى الوصف القانوني، فهي ليست مجرد علاقة أو رابطة زمنية لكونها عنصر رئيسي في الركن المادي.[4]

وفي عبارة أخرى يجب توافر صلة السببية بين السلوك والنتيجة، بحيث أنه إذا أمكن ردّ هذه النتيجة إلى عامل آخر غير السلوك المجرم تنقطع حتما صلة السببية وتنتفي معها المسؤولية الجنائية، وهذا أمر منطقي إذ الشخص لا يتحمل التبعية القانونية لما اقترفه من فعل إلاّ إذا كان فعله

[1]– **علي جبار الحسيناوي:** المرجع السابق، ص42.

[2]– **سليمان عبد المنعم:** المرجع السابق، ص412.

[3]– **سليمان عبد المنعم:** المرجع نفسه، ص413.

[4]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص258.

وحده هو سبب حصول النتيجة المحظورة قانوناً، فليس من العدل مساءلة الشخص إذا كانت هذه النتيجة الإجرامية ثمرة عامل أو عوامل أخرى غير فعله.[1]

وهكذا نجد أنّ المبدأ العام الذي يحكم علاقة السببية أنّ الشخص لا يسأل إلاّ عن النتائج التي يكون لنشاطه دخلاً في إحداثها، فإستحقاق العقاب في القانون الجنائي رهن دائمًا بقيام الرابطة السببية بين نشاط الجاني وبين الواقعة الإجرامية التي تستوجب العقاب، لأنه ما دام الجاني مسؤول أمام القانون على النتيجة التي أدى إليها فعله، فإنه ينبغي لمساءلته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية.[2]

وتختلف صلة السببية في مفهومها القانوني[3] بوصفها عنصرًا في الركن المادي للجريمة عن فكرة النية الإجرامية المعتبرة بدورها عنصرًا في الركن المعنوي،[4] فصلة السببية إذن ذات طبيعة موضوعية تستخلص من الخواص المادية للسلوك ذاته في إحداثه النتيجة المحظورة قانوناً، بينما النية الإجرامية ذات طبيعة شخصية معنوية تستخلص من الموقف النفسي للجاني في مدى علمه بصلاحية السلوك لإحداث النتيجة ومدى رغبته ونيته تحقيق ذلك، وهذا الإختلاف في طبيعة كل من الفكرتين يقودنا بالضرورة إلى إختلاف معيار المسؤولية لدى كل منهما على نحو ما سوف نراه في الباب الثاني من هذه الدراسة.

ففي جريمة انتهاك الحق أو المصلحة المعلوماتية عبر الإنترنت أو الحاسوب يجب أن يكون هناك سلوك يتمثل في الدخول على الإنترنت بإستخدام حاسوب ثم بعد ذلك التعدي على خصوصية النظام، فهنا تكون علاقة السببية قائمة بمجرد ثبوت الضرر أو الخطر، فعلى سبيل المثال في الجريمة المتعلقة بحيازة صور دعارة الأطفال وإستغلالهم جنسيًا موجودة على جهاز حاسوب أو على موقع إلكتروني، فهنا صلة السببية تتحقق بقيام رابطة بين فعل الحيازة لهذه الصور وبين الترويج أو العرض أو التداول، فكل هذه الأفعال يجب لكي تتم أنّ تقوم علاقة سببية

---

[1]- ***GARRAUD (R) :*** *Traité théorique et pratique du droit pénal français (sériy2, tome 1) ED. D, Paris,1987, P74.*

[2]– **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، المرجع السابق، ص58.

[3]– المشرع الجنائي عادة لا يعرف علاقة السببية كعنصر في الركن المادي بل يبرز اشتراطها، ومع ذلك هناك قوانين جنائية تصدت لتعريف علاقة السببية نذكر منها قانون العقوبات اللبناني بموجب المادة (204) منه.

[4]– ويلاحظ رغم هذا أنّ صلة السببية يتناولها البعض في معرض دراسة الركن المعنوي للجريمة لا ركنها المادي. (أنظر: – **سليمان عبد المنعم:** المرجع السابق، ص413).

بيـــن مباشـــرة النشـــاط المادي فيها وبين النتيجة المـــقررة سواء حال كونها تامة أو الـــشروع في إرتكـــابها.[1]

المطلب الثالث: الركن المعنوي للجريمة المعلوماتية

لا يكفي لقيام الجريمة قانوناً ومساءلة فاعلها جنائيًا مجرد إرتكاب ماديات الجريمة المتمثلة في عناصر الركن المادي، بل ينبغي أنّ يتوافر لدى الجاني قدر من الخطأ أو الإثم[2] وهو ما أصطلح على تسميته بالركن المعنوي، فلا جريمة إذن دون خطأ أو إثم مهما كانت النتائج التي تمخضت عنها.[3]

والركن المعنوي يترجم الحالة النفسية للجاني وقت إرتكابه الفعل المجرم، لذلك نجد البعض يعرفه بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني،[4] فهو بمثابة المسلك الذهني أو النفسي للجاني بإعتباره محور القانون الجنائي في تقرير المسؤولية الجنائية.[5]

ومن هنا يمكن القول أنّ المسؤولية الجنائية للفاعل ترتكز على توافر صلة نفسية بين الفاعل والنتيجة بحيث يمكن نعت السلوك الواقع من هذا الفاعل بأنه سلوك خاطئ أو مؤثم، فإرتكاب ماديات الجريمة لا يكفي بذاته إذن لمساءلة فاعلها جنائيًا. [6]

والقول بتوافر الركن المعنوي في الجرائم الإلكترونية يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وطريقة تكييفه لتحديد النصوص القانونية التي يلزم تطبيقها عليه، لذا نجد في حالات كثيرة جرائم الحاسوب والإنترنت تواجه مشكلات تتعلق بمدى توافر الركن المعنوي فيها وبشكل يمكن أن يحقق غرض النص الجنائي لاسيما في مسألة الإدانة.

---

[1]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص267.

[2]– كما يتناوله الفقه الفرنسي في نطاق فكرة الاثم *La culpabilité* التي تضم لدى هذا الفقه نوعين من العناصر هما: (العناصر المادية كالعمد، والعناصر المعنوية كالخطأ). وقد تعددت التسميات الفقهية للتعبير عن الركن المعنوي، فقد وصف بانه الركن الأدبي للجريمة أو ركن الخطأ، أو الإثم، أو الذنب أو الخطيئة، وهذا كله لا يؤثر في جوهر الركن المعنوي، بل إنّ المشرع يشير فقط إلى هذا الركن إلاّ بكلمات كقوله: "من يرتكب عمدا" أو "مع علمه بذلك" أو "بإهمال منه".

[3]– **حسن المرصفاوي:** قواعد المسؤولية الجنائية في التشريعات العربية، معهد البحوث والدراسات العربية، القاهرة، مصر، 1972، ص64.

[4]– **عبد الله دغش العجمي:** المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الكويت، 2014، ص29.

[5]– **محمود نجيب حسني:** النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، مصر، ط2، 1971، ص90.

[6]– **سليمان عبد المنعم:** المرجع السابق، ص432.

لذا في السابق لم يستقر القضاء في تحديد ما إذا كانت جريمة الدخول غير المشروع إلى النظام المعلوماتي تتطلب قصدًا عام أم خاص في إستجلاء معالمها من النظرة الموضوعية إلى السلوك الشخصي ومجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية لمرتكب الجريمة.[1] إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة وهي جريمة الدخول أو الولوج غير المشروع لذلك النظام، حيث أنّ إتجاه القضاء المقارن في تطلب العمد كان بالنسبة لجريمة الولوج فقط، وهي من الموضوعات المنتقدة هنا، لأنّ التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة معلوماتية أخرى كتجاوز صلاحية الدخول مثلا يعد تمييزًا دقيقًا.

لكن في الأخير إستقر القضاء الفرنسي على إبتكار فكرة "سوء النية *Mauvaises intensions*" وإصباغها على كافة النصوص القانونية التي تطبق بشأن جرائم الإنترنت والحاسوب، حيث إشترط قانون العقوبات الفرنسي مبدأ "سوء النية" حين وجود عدوان حقيقي على النظام المعلوماتي، وأنّ هذه الجرائم لا يمكن أنّ تدخل حيز التطبيق ما لم يتوافر سوء النية في منطق القصد الخاص وإرادة الإضرار[2]. كما ألزم تقنين البريد والإتصالات الفرنسي[3] بالسهر على إحترام سرية الإتصالات وأنّ تطبيق النصوص العقابية الجديدة متوقف على ضرورة توافر سوء النية ووجود عدوان حقيقي على خصوصية الإتصالات ومن ذلك البريد الإلكتروني حيث يعد من أهم وسائل الإتصال الخاصة والتي تتطلب بالضرورة حماية قوية.

كما جرم المشرع الإنجليزي الدخول غير المصرح به للنظام الإلكتروني وذلك بموجب المادة الأولى من قانون إساءة إستخدام الحاسوب لعام 1990، والتي تؤكد على ضرورة الأخذ بمبدأ سوء النية حين جرم الدخول غير المصرح به إلى النظام الإلكتروني بنية إرتكاب جريمة أخرى[4].

---

[1]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص294. – **إبراهيم خالد ممدوح:** المرجع السابق، ص109.

[2]– **مصطفى محمد موسى:** دليل التحري عبر شبكة الإنترنت، دار الكتب القومية، القاهرة، مصر، 2010، ص143.

[3]– ومن ذلك ما هو مقرر في نص المادة (15–226) من قانون العقوبات الفرنسي الجديد، والتي تشترط سوء النية حين وجود عدوان على البريد الإلكتروني وهو ما يتطابق مع ما هو مقرر في نص المادة (5–1–32. L) من تقنين البريد والاتصالات الفرنسي والصادر بالقانون المؤرخ في 1996/07/26 والذي يلزم وزير الاتصالات الفرنسي بالسهر على مبدأ احترام وحماية سرية الاتصالات. (أنظر كل من: – **عبد الله دغش العجمي:** المرجع السابق، ص31. – **مصطفى محمد موسى:** المرجع نفسه، ص144).

[4]– لمزيد من التفصيل حول الموضوع راجع: (– **سامي الرواشدة وأحمد الهياجنة:** مكافحة الجريمة المعلوماتية بالتجريم والعقاب، مجلة القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد الأولى، العدد الثالث، 2009، ص128).

رأي الباحث:

بناءًا على ما تقدم ذكره تتضح الطبيعة القانونية الخاصة بالجريمة المعلوماتية، لاسيما من خلال المجال الذي يمكن أنّ ترتكب فيه، وكذا صور المحل الذي يمكن أن يقع عليه الإعتداء المذكور.

ومما لا شك فيه أيضًا أن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات، ومن ثم كان لابد من ضم هذا السلوك إلى نطاق القانون الجنائي والتي على الرغم من أنّ معظم نصوصه المقارنة عاجزة عن مواكبة التطورات المعلوماتية، أو لما يحويه من فراغ أو نقص تشريعي في هذا المجال.

ومن جانب آخر نجد أنّ هذه الجرائم تتخذ طبيعة قانونية خاصة من حيث تكييفها القانوني إذ لا تستطيع القواعد القانونية التقليدية مواكبة هذه الظواهر الإجرامية المستحدثة وهذا ما يثير مشكلات عديدة في مقدمتها مسألة الإثبات الجنائي، وكذا ملاحقة جناة الجرائم المعلوماتية، ومما يزيد من صعوبة الأمر هم الجناة الذين يقيمون في دولة أخرى ولا تربطها إتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وذلك في البحث وراء القانون الواجب التطبيق، وفي ضوء تلك الإعتبارات يمكن الجزم بأنّ هذه الجرائم تتمتع بطبيعة قانونية شديدة الخصوصية.

وأنّ النصوص الواردة في قانون العقوبات الجزائري وبعض القوانين المكملة له في مجال التجريم الإلكتروني في حقيقة الأمر أنها نصوص لا زالت قاصرة عن إيجاد التأمين الكافي للنظام المعلوماتي.

وأمام هذه المشكلة التي تواجه الجزائر ودول كثيرة نجد في الوقت نفسه أن دول أخرى قد قطعت شوط كبير في وضع إطار قانوني محكم لمواجهة ومكافحة الجريمة المعلوماتية، وهذا ما سوف نتطرق إليه في الباب الثاني من هذه الدراسة.

المبحث الثاني: أقسام الجريمة المعلوماتية

تمهيد وتقسيم:

الجريمة المعلوماتية ليست جريمة وحيدة فقط[1]، وإنما تتخذ عدة صور وأشكال وأنواع متعددة ومخلفة، ونظرًا لهذا التعدد لم يوضع لها معايير محددة من أجل تصنيفها، وذلك تأسيسًا على التطور السريع والمستمر لتكنولوجيا المعلومات والخدمات، وأن تصنيفها يكون ضمن فئات متعددة تختلف حسب الأساس أو المعيار الذي يستند إليه كل تقسيم لها.

ومع ذلك يتفق كثير من الفقه الجنائي الحديث حول مسألة تحديد أهم معيارين تقسم بهما هذه الجريمة، وذلك إما حسب موضوع الجريمة، وإما حسب طريقة إرتكابها، فهناك جرائم ترتكب بإستخدام وسائل إلكترونية وجرائم تستهدف الوسائل الإلكترونية[2]، أي تبعًا للوسائل المستعملة في إحداث هذا النوع من الجرائم سواء كانت وسائل مادية كجهاز الحاسوب أو وسائل معنوية كشبكة الإنترنت، وهذا ما يطلق عليه اليوم "بجرائم الحاسوب وجرائم الإنترنت"، وهذا التقسيم الفقهي للجريمة المعلوماتية يختلف تمامًا عن التقسيم القانوني لها[3].

وإذا كانت الإنترنت في وجودها تعتمد اعتمادًا كبيرًا على تقنية الحاسوب، وبما أن إرتباط الحاسوب بالإنترنت أمر لابد منه، فقد إرتأينا تسليط الضوء على هذين القسمين الأكثر شيوعًا والأكثر إثارة للجدل بين أوساط الباحثين والدارسين في هذا المجال، وكذا لما لهما من خصوصية وعلاقة بموضوع البحث، وعليه سيتم في هذا المبحث التطرق إلى كل من جرائم الحاسوب، ثم جرائم الإنترنت ،وهذا بغرض التمييز ما بينها بالرغم من الإرتباط الوثيق بين الإنترنت والحاسوب، وذلك وفق مطلبين إثنين على الشكل التالي:

المطلب الأول: جرائم الحاسوب

المطلب الثاني: جرائم الإنترنت

---

[1]– مثلها في ذلك مثل مصطلح الجريمة المنظمة، فهذه الأخيرة ليست هي المقصودة كجريمة بالمفهوم الضيق، وإنما ينطوي تحت إسمها عديد الصور والأقسام من الجرائم المنظمة، ومنها:(الجريمة الجمركية، والجريمة الاقتصادية والجريمة الإرهابية والجريمة الدولية ...).

[2]– **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، المرجع السابق، ص72. – **علاء الدين الإبراهيمي:** الجرائم الإلكترونية، الوسائل وطرق الوقاية، مكتبة عنابة للنشر والتوزيع، عنابة، الجزائر، 2016، ص67.

[3]– التقسيم القانوني للجريمة المعلوماتية مثله مثل التقسيم القانوني لباقي الجرائم التقليدية الأخرى، والمعيار المعتمد في كل من التقسيمين هو معيار "درجة الخطورة"، أي خطورة الفعل، حيث جاء في نص المادة (27) من (ق ع ج) أنه: "تقسم الجرائم تبعًا لخطورتها إلى جنايات وجنح ومخالفات..."، وهذا ما يطلق عليه بالتقسيم الثلاثي للجريمة، وهو تقسيم عالمي معتمد في كل القوانين الجنائية المقارنة.

المطلب الأول: جرائم الحاسوب

يشهد العالم وبشكل كبير تطورًا هائلاً ومتسارعًا في إلكترونيات عالم الحواسيب، حتى أصبحت هذه الحواسيب من أفضل الأسلحة الناعمة في أداء العمل الإجرامي بدون عنف أو إراقة دماء، وأصبحت نظم الحاسوب الآلي طبقا لهذا التقسيم هي الوسيلة المستخدمة بكثرة في إرتكاب هذا النوع من الجرائم والمعبر عنها بجرائم الوسيلة، ولفهم أكثر للهذه الجرائم سنتطرق لأهم أحكامها وهي:

الفرع الأول: مفهوم الحاسب الآلي– الكمبيوتر *Ordinateur–Computer*

يعتبر الحاسب الآلي من أبدع ما إبتكره عقل الإنسان على مدى الأزمان، هذه الآلة الصغيرة التي إرتبطت بها معظم نشاطات الإنسان وباتت تقدم له خدمات هائلة، كانت تتطلب منه في الماضي الكثير من الجهد والمال والوقت، وأصبح من غير الممكن أن يستغني عنها في مجالات شتى بالنظر للخدمات الكبيرة التي تقدمها له هذه الآلة، وهو في نفس الوقت وعلى وجه الخصوص الأساس الذي يبنى عليه أي نظام معلوماتي اليوم.

ويمكن الحديث عن مفهوم الحاسب الآلي من عدة نواحي، لكننا سوف نركز حديثنا هنا وفي هذه الجزئية عن هذا الجهاز من حيث تعريفه، وكذا خصائصه ووظائفه وأهم مكوناته.

أولاً– تعريف الحاسب الآلي

عرف الحاسب الآلي أو كما يطلق عليه بجهاز الحاسوب أو الكمبيوتر، بعد تعريفات مختلفة[1] سواء ما جاء في صدر التشريع أو ما تناولته الألسن الفقهية، والتي نذكر منها:

أ– في الفقه: لم يتفق الباحثون كثيرًا في مجال تسمية وتعريف الحاسب الآلي كجهاز يتولى معالجة البيانات بشكل آلي، وقد جرت العادة على إطلاق إسم الحاسب الآلي أو الحاسب الإلكتروني أو الحاسوب، وهناك من يسميه أيضًا بالعقل الإلكتروني[2] .

---

[1]– السبب الرئيسي في إختلاف التسميات التي أطلقت على هذا الجهاز الآلي يعود إلى الترجمة اللغوية للكلمات التي تدل على معناه، وعلى وجه الخصوص في اللغتين الفرنسية والإنجليزية التي نقلت عنها تسمية الحاسب الآلي إلى اللغة العربية، ففي اللغة الفرنسية يسمى هذا الجهاز (*Ordinateur*)، أما الإنجليزية فيسمى (*Computer*)، لكن جميعها يقصد بها "المعالجة الآلية للمعلومات *Informatique*".

Voir plus: ROBERT (P): *Le petit Robert, Dictionnaire Alphabetical et la anallogique logos de la langue française, (V 1, Ed. D), Paris, France, 1983, P1319.*

[2]– تسمية الحاسوب بالعقل الإلكتروني لم يوافق عليها الكثيرون، وهذا على أساس أن المدلول الظاهر لهذه التسمية لا يعبر عن مضمونها الحقيقي، كما لا يمكن أن تستوي آلة أو جهاز مع ما يتميز به العقل البشري، إذ أنه من سمات العقل هو التخيل والتفكير والإبتكار والتأمل والإبداع وكلها مواصفات لا يمكن لتلك الآلة القيام بها، وإنما هي بمثابة إمتداد للعقل البشري، لهذا لا يمكن وصفهـــا بالعقل الإلكتـــروني. (أنظر في ذلك: **محمد علي سويلم:** المرجع السابق، ص64).

ومع ذلك كله فقد إختلف الفقه في تعريفه للحاسب الآلي، ومن أهم هذه التعريفات نجد:

– فقد عرفه البعض بأنه: "جهاز إلكتروني يتكون من مجموعة مكونات ووحدات والتي تعمل بصورة متكاملة مع بعضها البعض بهدف تشغيل ومعالجة البيانات والبرمجيات داخله، طبقا لبرنامج محدد تم وضعه مسبقًا للحصول على نتائج معلوماتية معينة"[1].

– وعرفه آخرون بأنه: "مجموعة متداخلة من الأجزاء التي لديها هدف مشترك من خلال أداء التعليمات الإلكترونية المخزنة"[2].

– وذكره آخرون بأنه: "آلة حسابية إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج والمعطيات المطلوبة"[3].

– وعرف أيضًا بأنه: "جهاز إلكتروني يعمل طبقًا لتعليمات محددة سلفًا ويمكنه إستقبال البيانات وتخزينها والقيام بمعالجتها بدون تدخل الإنسان ثم إستخراج النتائج والمعطيات المطلوبة مرة أخرى"[4].

– وعرف كذلك أنه: "جهاز إلكتروني يمكنه القيام بالعديد من العمليات الحسابية والمنطقية طبقًا للتعليمات المدخلة إليه بسرعة كبيرة، ويمكنه التعامل مع قدر هائل من البيانات وتخزينها وإسترجاعها مرة أخرى في شكل معلومات وبدرجة عالية من الدقة"[5].

– وعرف أنه: "جهاز إلكتروني رقمي متعدد الوظائف يقوم بإستقبال البيانات ومعالجتها وتخزينها للحصول على المعلومات المطلوبة"[6].

– كما عرف أيضاً جهاز الحاسوب بأنه: "تلك الآلة المتفاعلة مع الأوامر الإنسانية ذات التقنية العالية والمتطورة في معالجة البيانات"[7].

---

[1]– **أحمد محمود مصطفى:** المرجع السابق، ص10.

[2]– **محمد علي العريان:** المرجع السابق، ص70. – **محمد علي سويلم:** المرجع السابق، ص65.

[3]– **هدى حامد قشقوش:** جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة 25 إلى 28 أكتوبر 1993، ص19.

[4]– **محمد السيد خشبة:** مقدمة في الحاسبات الإلكترونية، د. د. ن، القاهرة، مصر، 1984، ص 21. – **عاطف حليم،** الكمبيوتر: دار الكتب المصرية، القاهرة، مصر، 1987، ص15.

[5]– **محمد حسام محمود لطفي:** الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، القاهرة، مصر، 1987، ص10.

[6]– **فراس محمد العزة:** مهارات الحاسوب والبرمجيات الجاهزة، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2003، ص13.

[7] **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص55. – **إنتصار نوري الغريب:** أمن الكمبيوتر والقانون، دار الراتب الجامعية، بيروت، لبنان، 1996، ص17. – **محمد مأمون سليمان:** التحكيم الإلكتروني، دار الجامعة الجديدة، الاسكندرية، مصر، 2011، ص27.

- ويطلق البعض الآخر على الحاسب الآلي بأنه: "عبارة عن جهاز كمبيوتر يتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج معين"[1].

- وقد عرفته الموسوعة الشاملة لمصطلحات الحاسب الآلي بأنه: "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي، لتنفيذ عمليات إدخال البيانات ***DATA*** أو إخراج المعلومات ***Information*** وإجراء عمليات حسابية أو منطقية"[2].

ب- في التشريع: من بين المشرعين الذين تناولت قوانينهم الداخلية تعريف جهاز الحاسب الآلي نجد على سبيل المثال:

- تعريفه في قرار لوزير الثقافة المصري رقم (82 لسنة 1993) بأنه: "جهاز إلكتروني قادر على تخزين ومعالجة وتحليل وإسترجاع البيانات أو المعلومات"[3].

- وعرفه أيضًا قرار لوزير الاتصالات وتكنولوجيا المعلومات المصري رقم (109 لسنة 2005) بأنه:

- "جهاز إلكتروني قادر على تخزين ومعالجة البيانات والمعلومات بطريقة إلكترونية رقمية"[4].

- كما عرفته المادة (7/1) من القانون السعودي لعام 2007 والمتعلق بنظام التعاملات الإلكترونية بأنه: "أي جهاز إلكتروني ثابت أو منقول، سلكي أو لاسلكي، يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو إستقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له مسبقًا"[5].

- وعرفته المادة الأولى من القانون الكويتي رقم (63 لسنة 2015) في شأن مكافحة جرائم تقنية المعلومات بأنه: "مجموعة برامج وأنظمة معلوماتية معدة لتحليل المعلومات والبيانات والأوامر وبرمجتها وإظهارها أو حفظها أو إرسالها أو إستلامها، ويمكن أن تعمل بشكل مستقل أو بالإتصال مع أجهزة أو أنظمة معلوماتية أخرى"[6].

---

[1]- **خالد حمدي عبد الرحمن:** الحماية القانونية للكيانات المنطقية، برامج الكمبيوتر، دكتوراه، جامعة عين الشمس، مصر، 1992، ص16.

[2]- **علاء الدين فهمي وآخرون:** الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، ط3، مطابع المكتب المصري الحديث، القاهرة، مصر، 1991، ص108.

[3]- أنظر قرار وزارة الثقافة المصرية رقم (82 لسنة 1993) في شأن تنفيذ قانون حماية حق المؤلف، والذي عدل أكثر من مرة، والصادر بالقانون رقم (354 لسنة 1954) في المادة الثانية منه، والمنشور بالجريدة الرسمية، العدد 104، المؤرخة في 1993/5/9.

[4]- أنظر قرار وزارة الإتصالات وتكنولوجيا المعلومات المصرية رقم (109 لسنة 2005) في شأن إصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم (15 لسنة 2004) في مادته الأولى، والمنشور بالجريدة الرسمية، العدد 115، والمؤرخة في 2005/5/25.

[5]- راجع المادة (7/1) من القانون السعودي بشأن نظام التعاملات الإلكترونية، والصادر بموجب المرسوم الملكي، في 1428/03/08هـ الموافق لـ2007/12/27م.

[6]- راجع نص المادة الأولى من القانون الكويتي رقم (63 لسنة 2015) في شأن مكافحة جرائم تقنية المعلومات.

- وقد عرفته أيضًا المادة الأولى من القانون المصري رقم (175 لسنة 2018) بشأن مكافحة جرائم تقنية المعلومات بقولها: "الحاسب هو كل جهاز أو معدة تقنية قادرة على التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو إسترجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للإتصالات"[1].

رأينا الخاص:

من خلال كل هذه التعاريف الفقهية والتشريعية للحاسب الآلي، يمكن أن نستنتج أنها تختلف من حيث التعبير والصياغة، ولكنها جميعها تتضمن نفس المعنى، أي أنها آلة تقوم بمعالجة المعطيات والبيانات بطريقة أوتوماتيكية وتحويلها إلى معلومات إلكترونية بناء على مجموعة من الأوامر التي يزودها بها مبرمجوها، إذ تعتبر هذه الوظيفة الأساسية للحاسب الآلي إضافة إلى وظائف أخرى لا تقل أهمية خاصة لما يرتبط هذا الأخير بشبكة الإنترنت.

كما نعتقد أن التعاريف التي جاء بها التشريع المقارن هي الراجحة، حيث أنها تمتاز بشمولية لكافة مهام الحاسب الآلي وتوضيحها بإيجاز، كما أنها إستوعبت كل الوظائف التي يقوم بها هذا الجهاز من عمليات حسابية ومنطقية، وعلى هذا الأساس نذهب إلى ما ذهب إليه المشرع المقارن في تعريفه لجهاز الحاسب الآلي.

ثانيًا- خصائص ووظائف الحاسب الآلي

ينفرد الحاسب الآلي بعدة خصائص ووظائف تجعله جهاز فريد من نوعه، ومن جملتها نجد ما يلي:

أ- بالنسبة للخصائص: من بين أهم خصائص جهاز الحاسب الآلي نجد مثلاً:

- أنه جهاز ذو كفاءة عالية تعتمد على كفاءة العنصر البشري في المقام الأول[2].
- أنه نتاج عمل إنساني مشترك وخلاصة مجموعة من العلوم الإنسانية الدقيقة[3].
- أنه جهاز يتعامل مع كم هائل من المعطيات والبيانات والقدرة على تخزين وإخراج هذا كله بسرعة شديدة قد تصل لملايين العمليات في الثانية الواحدة[4].

---

[1]- راجع نص المادة الأولى من القانون المصري رقم (175 لسنة 2018) بشأن مكافحة جرائم تقنية المعلومات. **الملحق رقم (04)**

[2]- **سيد أحمد محمود:** دور الحاسب، الكمبيوتر، أمام القضاء المصري والكويتي نحو إلكترونية القضاء، دار النهضة العربية، القاهرة، مصر، 2009، ص78.

[3]- **محمد علي سويلم:** المرجع السابق، ص68.

[4]- **محمد عبد الله سلامة:** جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، مصر، 2006، ص23.

– أنه جهاز مزود ببرامج قادرة على تفسير وتنفيذ التعليمات وكل البرمجيات المتعلقة بعمليات التخزين والمعالجة والإسترجاع بشكل تلقائي دون تأخير[1].

– أنه جهاز له علاقة جد وثيقة مع الشبكة الدولية للإتصالات والمعلومات الإنترنت وهي علاقة بمثابة الروح في الجسد، لأنه من غير الممكن الإستفادة من خدمات الشبكة بدون حاسوب.

ب– بالنسبة للوظائف: كما يقوم الحاسوب بوظائف متعددة جعلته يتمتع بأهمية بالغة وتطبيقات لا حصر لها، ومن أهمها نجد:

– إمكانية إستخدام الحاسوب في كثير من مجالات الحياة تقريبًا، التكوينية والتدريبية والتعليمية ...إلخ[2].

– القيام بعمليات حسابية معقدة وبسرعة كبيرة، كما يساعد على تقليل التكاليف وتحسين نوعية العمل الذي يقوم به[3].

– أدى إلى عصرنة قطاعات كثيرة في الدولة بداية من الحكومة الإلكترونية مرورًا بعصرنة الإدارة والقطاعات الحساسة كقطاع القضاء والصحة والتعليم، ناهيك عن المجالات التجارية والاقتصادية، وذلك كله بإدخال جهاز الحاسوب في هذه التعاملات[4].

– القدرة الهائلة في فهرسة وتوثيق الأرشيف بطريقة إلكترونية، وهي طريقة شبكية ذكية تعتمد على إعمال المعرفة، وفي الغالب يكون مرتبطًا بإستخدام تكنولوجيا الإنترنت[5].

– تحسين الخدمات المقدمة إلى المواطن بإستخدام تكنولوجيا الحواسيب كطريقة للتعاون والتواصل مع الدولة بإستخدام الطرق المختلفة للإتصال، ووضع إطار إلكتروني لتحسين الخدمات المرفقية[6].

– يقوم معظم الناس بتسيير أعمالهم اليومية عن طريق إستخدامات الحاسب الآلي حتى أصبح لكل واحد منا تقريبا حاسبه الشخصي، بل يكاد لا يوجد اليوم عملاً على مختلف الأصعدة ليس للحاسب الآلي دور فيه[7].

---

[1]– **فاروق علي الحفناوي:** قانون البرمجيات، ط1، دراسة متعمقة في الأحكام القانونية لبرمجيات الكمبيوتر، دار الكتاب الحديث، القاهرة، مصر، 2003، ص28.

[2]– **محمد علي سويلم:** المرجع نفسه، ص69.

[3]– **عماد محمد سلامة:** الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل، عمان، الأردن، ط1، 2005، ص33.

[4]– **صليحة علي صداقة:** الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2017، ص141.

[5]– **صليحة علي صداقة:** المرجع نفسه، ص142.

[6]– **خالد ممدوح إبراهيم:** الإدارة الإلكترونية، الدار الجامعية، القاهرة، مصر، 2010، ص47.

[7]– **محمد علي سويلم،** المرجع السابق، ص69.

ثالثًا- مكونات الحاسب الآلي

تعد دراسة المكونات والأدوات التي ترتكب بها الجرائم المعلوماتية أو ترتكب عليها أمرًا ضروريًا لا غنى عنه لمعرفة الشرط البديهي والمفترض في قيام المساءلة الجنائية لمرتكبي هذه الجرائم.

ويتكون جهاز الحاسب الآلي – الكمبيوتر- من مجموعة متكاملة من الأجهزة والإلكترونيات المتنوعة والمختلفة[1]، وهذا بهدف تشغيل مجموعة البيانات المدخلة إليه بموجب برامج وضعت فيه مسبقًا للحصول على النتائج المطلوبة في شكل معلومات. ومن هنا وحسب ما إستنتجناه من التعاريف السابقة يمكننا القول أن جهاز الحاسوب يتكون من مكونات تنقسم بدورها إلى مكونات مادية وأخرى غير مادية أي معنوية.

أ- المكونات المادية للحاسوب *Hard Ware*: يقصد بالمكونات المادية للحاسوب تلك الأشياء الملموسة من أجزاء وأدوات صلبة أو مرنة، والتي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات والمعطيات آليًا[2].

وعليه، فالمكونات المادية للحاسوب *Hard Ware* هي ذلك الكيان المادي يمكن مشاهدته بالعين المجردة، والذي بدوره يشتمل على عدة وحدات بدء من وحدة التشغيل، ووحدات الإدخال *Units input* وهي الوحدات المصممة بإدخال البيانات والمعطيات المطلوب معالجتها إلى وحدة المعالجة الرئيسية، وتتألف هذه الوحدات بدورها من العديد من المكونات[3]، كما نجد وحدات الإخراج ***Units Out put*** وهي الوحدات التي نحصل منها على نتائج العمليات التي أنجزتها وحدات

---

[1]- لابد من الإشارة هنا بخصوص مكونات الحاسب الآلي أن هناك من يدرجها ضمن مكونات كل حاسوب بحسب شكل وحجمه ونوعه، وأن هناك من يدرجها ضمن مكونات النظام المعلوماتي ككل، لأن هذا الأخير لا يشمل فحسب الحاسب الآلي وحده، وإنما قد يشمل عدة حاسبات آلية مرتبطة في نفس الوقت بشبكة الإنترنت. (أنظر: - **محمد علي سويلم:** المرجع نفسه، ص 71).

[2]- كما تجدر الإشارة هنا إلى أن الجيل الحالي للحاسبات يعمل بواسطة ما يعرف بـــ "الذكاء الاصطناعي *L'intelligence artificielle*"، وبالتالي لا حاجة لاستخدام كلمة "آلي *Automatique*" بعد كلمة حاسوب. (راجع أكثر: - **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص20. - **بلال أمين زين الدين:** جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، مصر، 2008، ص22).

[3]- وهي أدوات لإدخال البيانات والأوامر والبرامج إلى الكمبيوتر، أي أنها وسيلة الإتصال بين الإنسان والحاسوب، ومن أشهرها نجد (الفأرة *Mouse*، لوحة المفاتيح *Board Key*، الماسح *Scanner*، القلم الضوئي *Pen Light*،الميكروفون *Microphone*، الكاميرا Camera).
(أنظر في ذلك: - **جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي:** الحاسب والمعلومات، الدار المنهجية للنشر والتوزيع، عمان، الأردن، 2016، ص32).

الإدخال وقامت بمعالجتها من أجل الوصول إلى نتائج معالجة البيانات وهو الحصول على العلومات بواسطة وحدات الإخراج المختلفة[1].

إضافة إلى وحدة الذاكرة الرئيسية ***Main Memory*** وهي المكان الذي تخزن فيه البيانات ***Data*** والمعلومات ***information*** والبرامج التي ندخلها إلى الحاسوب[2]، وكذلك توجد وحدة المعالجة المركزية ***Units processing Central***، والتي يمكن وصفها بأنها عقل الكمبيوتر لأنها تتولى إستقبال وتنفيذ جميع عمليات التشغيل ومعالجة البيانات وتنظيمها، بالإضافة إلى وحدة الضبط والتحكم ***Unit Control*** والتي تتولى عملية الضبط والتحكم في جميع الأوامر والتعليمات وحركة البيانات ونقلها بين أجزاء الكمبيوتر المختلفة لتنفيذ المعالجة المطلوبة، كما أنها مصدر الأوامر إلى بقية وحدات الحاسوب[3].

إضافة إلى وحدات أخرى كوحدة الحاسب والمنطق ***Unit Logic Arithmetic*** والتي تتولى تنفيذ جميع العمليات الحسابية والمنطقية وحتى المقارنة، كما يوجد وحدة تشغيل الأقراص الثابتة والصلبة والمرنة والمضغوطة ***DVD, CD, Disk Hard, Flash Disque***، والتي تعتبر من أشهر دعائم تخزين البيانات والمحافظة عليها[4].

ب- المكونات المعنوية للحاسوب *Soft Ware*: أما القسم الثاني من مكونات الحاسب الآلي نجد المكونات غير المادية أي تلك المكونات المعنوية ***Soft Ware***، فهي ذلك الكيان المنطقي للحاسوب[5]،

---

[1]- وهي الوحدات التي نحصل منها على نتائج العمليات التي أنجزها الحاسب وقام بمعالجتها وتنفيذها، وتسمى هذه النتائج بالمخرجات، وتكون هذه المخرجات في أشكال مختلفة (مرئية ومسموعة، ثابتة ومتحركة، وقد تكون نصوصًا مكتوبة أو صورًا أو رسومات، وغيرها من المخرجات). ومن أهم مكونات وحدات الإخراج نجد: (الطابعة *Printer*، السماعة *Speaker*، الراسم *Plotter* ... وغيرهـا). (أنظر: - **جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي:** المرجع السابق، ص33).

[2]- وتختلف البيانات عن المعلومات من حيث: (البيانات هي مجموعة الرموز أو الحروف أو الأشكال أو الأرقام التي تعبر عن ظاهرة أو مشكلة ما، أما المعلومات فهي جمع وتحليل وتنظيم وتلخيص تلك البيانات، لذلك فإن عملية تحويل البيانات إلى معلومات تسمى بـ "المعالجة الآلية للبيانات *Processing datd*").

[3]- **جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي،** المرجع نفسه، ص35.

[4]- **طارق إبراهيم الدسوقي عطية:** الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص88.

[5]- وتنقسم الكيانات المنطقية إلى نوعين هما: الأولى هي الكيانات الأساسية والتي تضم كل البرامج الضرورية من أجل إستخدام أفضل للحاسوب وملحقاته، وهي مندمجة في الجهاز ذاته، أما الثانية فهي الكيانات التطبيقية والتي بدورها تضم البرامج المصممة والمدخلة إلى الجهاز والتي تمكن المستخدم من أن ينفذ بواسطتها عملاً محددًا حسب احتياجات هذا المستخدم، فهي برامج مساعدة مثل برنامج التحليل الإحصائي، وبرامج التصميم الهندسي وغيرها. (أنظر: - **محمد عبد الظاهر حسين:** الإتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2001، ص17).

وهو بدوره عبارة عن مجموعة أوامر وتعليمات أو بيانات ومعطيات معبر عنها بأية لغة[1]، وهذا عن طريق البرامج والبرمجيات ***Program***، وهي الأخرى عديدة ومتنوعة[2]، وهذا كله بغية معالجة البيانات والحصول على المعلومات، والتي تعد مطلب أساسي للتعامل مع الحاسوب.

وتشكل المعطيات والبرامج معًا المكونات غير المادية لنظام المعالجة الآلية؛ إذ بدونها يعتبر الحاسب الآلي مجرد آلة كباقي الآلات، فهي بمثابة العمود الفقري وعصب عمل الحاسوب، فلها درجة كبيرة من الأهمية، ذلك أنها تعتبر الروح بالنسبة للحاسب الآلي[3]، فقيمة هذا الأخير من قيمة البرامج والمعلومات المخزنة به، والعدوان عليها هو الذي يشكل الجريمة المعلوماتية بالمعنى الدقيق[4].

الفرع الثاني: التطور التاريخي لجرائم الحاسوب

تمر المجتمعات في هذا العصر بتطورات وتغيرات تقنية وإجتماعية كبيرة مردها حدوث ما يسمى "بالثورة المعلوماتية أو الإنفجار المعلوماتي *Révolution de l'information*"، وهذا الجحم الهائل من التغيرات التي يمر بها العالم اليوم مردها الأساسي هو التطور الكبير والسريع في تقنيات المعلومات[5].

وتعد دراسة التطور التاريخي لهذه التقنية الإلكترونية من أهم الدراسات في مجال الحوسبة وتطورها وعلاقتها بالإجرام المعلوماتي، فكان لتطور الحاسوب وتقنية المعلومات وإستخداماتها الخطوة الأولى لبيان سمات هذه الجريمة وطابعها الخاص، كون محل هذه الجريمة معطيات الكمبيوتر بدلالاتها الواسعة، فهي جرائم ذات خصائص متفردة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة إرتكابها.

---

[1]– **محمد فهمي طلبة:** الموسوعة الشاملة لمصطلحات الحاسوب الإلكتروني، مطابع المكتب المصري الحديث للنشر والتوزيع، القاهرة، مصر، 1991، ص369.

[2]– ومن أهمها برامج النظام *System program* والتي تصمم لعمل نوع معين من التطبيقات والخدمات، ومن أشهرها برامج ميكروسوفت أوفيس *Office Microsoft* والذي يقوم بمعالجة النصوص والجداول وقواعد البيانات والرسومات والألعاب...، كما أن هناك البرامج التطبيقية *Application programs* والمعدة بواسطة المستخدم نفسه لعمل خدمة معينة لشركة أو مؤسسة أو منشأة مثل: برامج المحاسبة، برامج العقارات، برامج شؤون الموظفين ... وغيرها. (أنظر: **جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي:** المرجع السابق، ص43).

[3]– **يزيد بوحليط:** الجرائم الإلكترونية فى القانون الجزائري، دار الجامعة الجديدة، الإسكندرية ، مصر، 2019، ص24.

[4]– **محمد علي سويلم:** المرجع السابق، ص 73.

[5]– يقصد بتقنيات المعلومات: ذلك المزيج من تقنيات الإلكترونيات الدقيقة وتقنيات الحواسب الآلية وتقنيات الإتصالات الحديثة وتكنولوجيات حفظ المعلومات، والتي شهدت جميعها تطورًا كبيرًا وسريعاً في السنوات الأخيرة من القرن الماضي، ونتيجة لذلك تحولت المجتمعات في هذا العصر إلى مجتمعات معلوماتية بإمتياز يعتمد فيها إقتصادها ورفاهية شعوبها اعتمادًا كبيرًا على تقنيات المعلومات.
- ***Voir Plus : Guillaume Champy :*** *La fraude informatique (T 2. Ed. D), Paris, france, 1992, p 373.*

فبداية صناعة الحواسيب وإنطلاق ثورة الإلكترونيات كانت مستقلة عن عصر وسائل الإتصال الحديث بفترة من الزمن، والتي بدأت في أربعينيات القرن الماضي، حيث إقتصر إستخدام الحاسوب وقتها على المؤسسة العسكرية فقط، بالنسبة للدول المتطورة في ذلك الوقت، ومع مطلع الخمسينيات دخل الحاسوب في مجالات ضيقة لدى المؤسسات الكبرى التابعة لهذه الدول، كما بدأ بعدها الإستخدام التجاري للحواسيب، وفي ذلك الوقت لم يكن يتصور في الأذهان حجم الخطر الناجم عن إستخدامها، وإن وجد فلم يكن يتعلق بالإجرام، بل في البطالة التي قد تنجم عنها في قطاع الإنتاج والصناعة ومخاطرها على سوق العمل في الدولة[1].

ومع مجيء ثورة المعلومات والثورة الجديدة في عالم الإتصالات الحديثة وتكنولوجيا نقل المعلومات وبروز مصطلح عصر العولمة، أتاح للأفراد والمؤسسات فرصة الولوج إلى عالم الإلكترونيات على الصعيدين المحلي والدولي، فإنعكس هذا الأمر إيجابيًا على كل القطاعات الإقتصادية والتجارية كالبنوك والمؤسسات الإدارية وكل ما له علاقة بقواعد المعلومات، وصار الحاسوب مصدرًا غنيًا بالمعلومات لمراكز إتخاذ القرار[2].

ومع إقتراب نهاية خمسينيات القرن الماضي بدأت ظاهرة "جرائم الحاسوب"، أو كما كان يطلق عليها بـــ "جرائم الكمبيوتر" بالظهور، ولكن ضمن إطار واضح ومفهوم كانت تكيف وقتها على البعد الأخلاقي تحت مسميات عديدة منها "إساءة إستخدام الحاسوب"، وأيضًا "سرقة وقت الجهاز" وغيرها من المسميات[3]، فكانت الأنشطة الجرمية المتصلة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني، مما أدى إلى عدم التمييز بين الأنشطة الجرمية التي تستهدف مكونات الحاسوب المادية والمعنوية وبين الإعتداءات الجرمية ذات الدلالة للجرائم التقليدية سواء من حيث الإتلاف أو السرقة أو الإحتيال[4].

---

[1]– **يونس عرب:** موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، منشورات اتحاد المصارف العربية، ج1، ط1، القاهرة، مصر، 2002، ص 299.

[2]– **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2009، ص18.

[3] أُرتكبت أول جريمة بواسطة جهاز الحاسوب عام 1958، ومنذ ذلك التاريخ بدأ رصد ونشر تقارير من حالات إساءة إستخدام الحاسوب لاسيما في أمريكا مهد نشأة جرائم الكمبيوتر، حيث صنفت في بادئ الأمر إلى جرائم العبث أو التخريب الموجه إلى جهاز الحاسوب. (أنظر أكثر: – **محمد علي العريان:** الجرائم المعلواتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2011، ص69).

[4]– **نائل عبد الرحمن صالح:** واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والإنترنت، مجلة كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، 2004، ص155.

ثم تزايد بعد ذلك إنتشار الحواسيب مع بداية ستينيات القرن الماضي وتعددت إستخداماتها، وبدأت معها بالظهور جرائم الحاسوب، وكان العبث في الحواسيب محدودًا نسبيًا في ذلك الوقت، وأما في السبعينيات وبعد الإندماج ما بين الحوسبة والإتصالات ظهرت الأنشطة التي تستهدف المعطيات المخزنة داخل الكمبيوتر والتي أطلق عليها وقتها بـــ "جرائم الكمبيوتر"[1] كالتجسس المعلوماتي، والإستخدام غير المشروع للبيانات المخزنة، وثار الجدل مرة أخرى والتساؤل فيما إذا كانت هذه الأنشطة عبارة عن سلوكيات غير أخلاقية أم هي جرائم بالمعنى القانوني، ولكن بقي التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني[2].

وإذا كانت سبعينيات القرن الماضي قد حملت في طياتها بذور وملامح ظاهرة جرائم الحاسوب، فإن عقدي الثمانينات والتسعينات قد جلبا تحديدًا الإطار السليم لمفهوم وماهية هذه الجرائم، وإتسعت معها أهمية الشعور بعظمة وقيمة المعلومات وحجم المخاطر الناتجة عن الإعتداء عليها ووجوب حمايتها من خلال توفير أدوات قانونية فعالة وحماية وسائل معالجتها ونقلها، ومن هنا بدأ الحديث عن جرائم الكمبيوتر بوصفها ظاهرة جرمية مستحدثة لا مجرد سلوكيات مرفوضة[3].

ونتيجة هذا التطور في عالم المعلوماتية نشأت ونمت أنواع جديدة من الجرائم التي ما كانت لتبصر النور لولا ظهور الكمبيوتر، حيث شهدت أواخر التسعينات وبداية القرن الحالي أنواعًا فريدة من جرائم الكمبيوتر، وترافق ذلك مع إنتشار الإنترنت وبدأت معها أنشطة "الهاكرز ***Hakers***" بإختراق مواقع المعلومات والدخول إليها دون تصريح مسبق والعبث بالبيانات والمعلومات المخزنة فيها[4]، فبدأت هذه الجرائم تشكل خطرًا على الصعيدين الإقتصادي والأمني للدول، الأمر الذي إستدعى معه مراجعة شاملة للأحكام والنصوص القانونية التقليدية التي أصبحت قاصرة عن إحتواء وتغطية هذه الجرائم المستحدثة[5].

ونظرًا للخطورة الكبيرة لهذه الجرائم على كافة دول العالم وإنتشارها وتزايد حجم الأضرار الناشئة عنها وأخطار الإعتداءات على البيانات الشخصية للدول والمنظمات، ترتب على ذلك كله

---

[1]– **يونس عرب:** موسوعة القانون وتقنية المعلومات، المرجع السابق، ص 302.

[2]– **محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت، دار الثقافة، عمان، الأردن، 2004، ص70.

[3]– **نائل عبد الرحمن صالح:** المرجع السابق، ص160.

[4]– **علي جبار الحسيناوي:** المرجع السابق، ص20.

[5]– **محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت، دار الثقافة، عمان، الأردن، 2004، ص74.

إبرام إتفاقيات دولية في محاولة لترسيخ وجوب التعاون الدولي لمواجهة جرائم الكمبيوتر، وعلى رأسها منظمة الأمم المتحدة والمجلس الأوربي، وكذا بعض الهيئات والمنظمات الدولية الأخرى، فكانت بمثابة الأساس الذي إرتكزت عليه الإلتزامات الدولية للوقوف صفًا واحدًا لمجابهة هذا الخطر القادم.

ونشير هنا أن هذه الجرائم سرعان ما تنوعت وتضاعفت يومًا بعد يوم، وأصبح يختلف مرتكبوها عن المجرمين التقليديين لأنهم في الغالب أصبحوا أشخاص على مستوى عالي من العلم والمعرفة، هذا الوضع جعل بطبيعة الحال القانون يغير من نظرته للمجرم العادي إلى المجرم المعلوماتي.

الفرع الثالث: تعريف جرائم الحاسوب وأهم صورها

لجرائم الحاسوب تعاريف خاصة وصور متعددة نذكر من أهمها:

أولاً: تعريف جرائم الحاسوب

بإعتبار أن الجريمة المعلوماتية كل فعل أو إمتناع يجرمه القانون يرتكب بإستعمال الحاسب الآلي أو كونه هدف أساسي لقيام الجريمة، لذا سوف نحاول أن نتناول بعض التعريفات التي قيلت في جرائم الحاسوب نذكر منها:

– يقصد بجرائم الحاسوب أنها: "تلك الأفعال المجرمة والتي تشكل إعتداءًا على أجهزة الحاسب الآلي سواء على مكوناته المادية ***Hard Ware*** أو على مكوناته المعنوية *Soft Ware* كالبيانات والمعلومات المخزنة بداخله"[1].

– كما عرفها الفقيه الألماني "تيدمان *Tiedemann*" بأنها: "كل أشكال السلوك غير المشروع أو الضار بجهاز الحاسوب ومكوناته سواء كان الحاسب أداة أو هدفا لها"[2].

– وعرفها الفقيه الانجليزي "ليزي بول ***Lizzi Paul***" بأنها: "كل فعل إجرامي يستخدم الحاسب الآلي لقيامه وإتمامه"[3].

---

[1]– **ثامر علي النويران:** الجرائم الإلكترونية وطرق الحد منها، مجلة المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، كلية علوم الحاسب والمعلومات، جامعة محمد بن سعود الإسلامية، الرياض، السعودية، 2015، ص175.

[2]– **محمد علي سويلم:** المرجع السابق، ص98.

[3]– **يوسف حسن يوسف:** الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011، ص13.

– وعرفت أيضًا بأنها: "الفعل غير المشروع الذي يستخدم فيه الحاسب الآلي كأداة رئيسية ووسيلة لإرتكابه"[1].

– ومن الفقه من ذكر بأنها: "كل نشاط إجرامي يؤدي فيه الحاسوب دورًا إيجابيًا أو سلبيًا لإتمامه، أو أنه يقع على الحاسوب نفسه"[2].

– أو أنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[3].

– في حين عرفها مكتب تقييم التقنية والكمبيوتر في الولايات المتحدة الأمريكية، من خلال تعريفه لجريمة الكمبيوتر ***Computer Crime*** بأنها: "الجرائم التي تلعب فيها الحواسيب دورا رئيسيا في المساس بالبيانات الكمبيوترية والبرامج المعلوماتية"[4].

ثانيًا: صور جرائم الحاسوب

إن تحديد الأفعال المعتبرة أنماط وصور للسلوك الإجرامي للحاسوب هو أمر في غاية الصعوبة، وذلك بسبب ظهور عدد من الصور المختلفة لجرائم الحاسوب لاسيما مع ظهور أشكال وأنواع من الحواسيب الفائقة الدقة والمهارة والتعقيد[5]، ومع ذلك فإن من جملة صور جرائم الحاسوب التي إحتوها القانون الجنائي نجد مثلاً جرائم الإتلاف المعلوماتي، وجرائم التلاعب بالمعلومات المخزنة داخل الحاسوب، جرائم تعطيل نظام الحاسوب، جرائم إختراق وقرصنة شبكات الحاسوب، جريمة الإحتيال على الحاسوب ... وغيرها كثير.

رأينا الخاص:

نعتقد حسب رأينا المتواضع أن تعريف جرائم الحاسوب يتوقف عند العمل الأساسي فيها، وليس على مجرد الأداة المستعملة في إرتكابها، وهذا بسبب أن الوسيلة في إرتكاب الجرائم ليست معتبرة لدى المشرع الجنائي عند التجريم لكون كافة الوسائل متساوية، وإنما يعتد بها فقط في تشديد العقوبة من عدمه، كما أن البنيان القانون لأي جريمة كانت هو بتوافر أركانها، فهي محل الإعتبار

[1]– **سامي علي حامد عياد:** الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2007، ص38.

[2] شيماء عبد الغني عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، مصر، 2007، ص12.

[3] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار النهضة العربية، القاهرة، مصر، 2009، ص17.

[4] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، دار النهضة العربية، القاهرة، مصر، 2011، ص18.

[5] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2004، ص 40.

عند تطبيق نصوص التجريم، فضلاً عن أن الأخذ بهذه التعاريف كلها لجرائم الحاسوب سوف يؤدي حتمًا إلى التوسع في نطاق الجرائم المعلوماتية.

المطلب الثاني: جرائم الإنترنت

من الصعوبة الفصل بين جرائم الحاسوب وجرائم الإنترنت فلابد للأول لإرتكاب الثاني، وهذا الدمج والتزاوج بين وسائل الحوسبة ومواقع الإتصال أدى إلى نشوء فضاء جديد لكل منهما، وخلق إطار أوسع يعرف بتقنية المعلومات في وقتنا الحاضر.

ولما كانت شبكة المعلومات وفي مقدمتها الإنترنت العنوان الجديد لعصر الإتصالات الحديثة وبزوغ فجر الثورة المعلوماتية *La Revolution informatique* بدأ التوسع في إستخدامها في كافة المجالات والمعاملات الإلكترونية ودخول جميع فئات المجتمع إلى قائمة المستخدمين فيها، وقد اجتذبت الإنترنت الكثير من المستخدمين إليها في فترة زمنية قصيرة أكثر من أي وسيلة إتصال أخرى[1].

ومع التطور المستمر للإنترنت وتوفيرها السرية التامة للمستخدمين لها جعلها بيئة مثالية لتنفيذ العديد من الجرائم بعيدًا عن أعين الجهات الأمنية، حتى وصل الأمر إلى تكوين ما يسمى "مافيا جرائم الإنترنت *Mafia du crime sur internet*"[2]، ثم بدأت تظهر صور عديدة من الجرائم على الشبكة إزدادت مع الوقت وتعددت صورها وأشكالها، وهذه الجرائم يطلق عليها اليوم بالجريمة العالمية *Criminalité mondiale*[3]، وهي من أخطر التحديات التي تواجه المعاملات الإلكترونية اليوم.

---

[1]– يشهد التاريخ أن شبكة الإنترنت إستغرقت أربع سنوات فقط لكي تصل إلى خمسين مليون مستخدم ومستفيد لها، بينما إستغرقت التليفونات أربعة وسبعين عامًا والتلفزيون ثلاثة عشر عامًا للوصول إلى هذا الرقم الهائل، والذي لا يزال في تصـــاعد رهـــيب. (أنظـــر: – **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ط1، 2009، ص31).

[2]– **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص 106.

[3]– يطلق جانب كبير من الفقه على هذا النوع من الجرائم مصطلح "الجرائم العالمية *Criminalité mondiale*"، وهي تختلف بطبيعة الحال عن مصطلح "الجرائم الدولية *Crimes Internationaux*"، فالجريمة الدولية مصدرها القانون الجنائي الدولي وإختصاصها يعود إلى القضاء الدولي، بينما الجريمة العالمية مصدرها هو القانون الجنائي الوطني وإختصاصها يعود بطبيعة الحال إلى القضاء الوطني، وترجع هذه التسمية إلى زيادة مزاولة مجموعة من الأنشطة الإجرامية على مستوى عالمي وعبورها حدود الدول نتيجة للتقدم المذهل في وسائل الإتصال الحديثة، وذلك كله من منظور مبدأ عالمية الجريمة والنص الجنائي. (للمزيد من التفصل راجع: – **عمر الفاروق الحسيني:** المشكلات الهامة في الجرائم المتصلة بالحاسوب وأبعادها الدولية، دار النهضة العربية، القاهرة، مصر، ط2، 1995، ص133).

Voir plus : Sédallian (V) : *Droit de l'internet, réglementation, responsabilité, contrats net press, (Ed. D), paris, france 1997, p 19.*

ويمكن معرفة جرائم الإنترنت أكثر من خلال التطرق إلى تعريف شبكة الإنترنت (أولاً) ثم لمحة عن بدايتها تاريخ نشأتها (ثانياً) وأهم الخدمات التي تقدمها (ثالثاً)، ثم في الأخير إطلالة سريعة عن أنهم صور جرائم الإنترنت (رابعاً).

الفرع الأول: تعريف شبكة الإنترنت (الشبكة المعلوماتية)

نتطرق هنا إلى تعريف شبكة الإنترنت في كل من التعريف الإصطلاحي، ثم التعريف التشريعي.

أولاً: في الإصطلاح

الإنترنت *Internet* ليست كلمة عربية الأصل، بل هي كلمة لاتينية تداولت بين الألسن وعلى صفحات الجرائد والمقالات، بل وفي النصوص التشريعية والأحكام القضائية والمراجع الفقهية، وبشيوع إستخدام هذا اللفظ على حاله بات يشير ويثير في الذهن العربي وفي العقل القانوني إلى تلك الشبكة العالمية للملعومات التي تنتقل من خلالها المعلومات من أقصى الأرض إلى أقصاها، ولهذا كان لإستقامة منهج هذه الدراسة أن نبحث ولو قليلاً في أصل كلمة "إنترنت" حتى يتيسر لنا وضوح المعنى في الذهن القانوني.

فالإنترنت أو الشبكة أو الشابكة كما عرّبها وعرّفها مجمع اللغة العربية[1] أنها كلمة إنجليزية الأصل مركبة ومختصرة، مكونة من مقطعين إثنين، الأول (*Inter*) وهي اختصار لكلمة (*Inter Connection*) وتعني ربط داخلي، أو أنها تعني كلمة (*Inter national*) وتعني دولي، والثاني (*Net*) وهي إختصار لكلمة (*Net work*) وتعني شبكة[2].

والإنترنت بهذا المعنى هي "الشبكة العالمية للمعلومات"، أو كما يطلق عليها أيضًا "بالشبكة الدولية للإتصالات"، كما يصفها آخرون بـــ "شبكة الشبكات *Réseau des réseaux*"[3] وهي أكبر شبكة للمعلومات المتاحة حاليًا والتي تربط معظم دول العالم بنسيج من خيوط الإتصال[4] المتصلة

---

[1]– مجمع اللغة العربية بالقاهرة على موقعه الإلكتروني: ***www.arabicacademy.org.eg*** متاح بتاريخ 2017/03/23.

[2]– **نهلا عبد القادر المومني:** المرجع السابق، ص 34. – **محمد علي سويلم:** المرجع السابق، ص86.

[3]– *L'internet est un « réseau des réseaux » à l'échelle mondiale qui Sert à la communication d'informations numérisées. (Voir plus : Eatf- Gafi) group d'action financière sue le blanchiment de capitaux, rapport (2000-2001) sur les typologies du blanchiment de capitaux, (Ed. Cujas) Paris, France, 2001, P 06.*

[4]– فهي تتصل بتقنيات مختلفة من الأسلاك النحاسية كسلك التليفون العادي أو أي فرع آخر من الكوابل أو الألياف البصرية، وإذا كانت الحواسيب موجودة في أماكن بعيدة ومتفرقة فيمكن إستخدام الوصلات اللاسلكية عن طريق الأقمار الصناعية للربط بينها ليتحقق بذلك الإتصال الدولي عبر الإنترنت (أنظر أكثر: – **سهيل محمد الغرام:** الوجيز في جرائم الإنترنت، مكتبة الجامعة الأردنية، عمان، الأردن، 2009، ص6).

ببعضها، لذلك يطلق عليها "بالشبكة العنكبوتية"[1]، وهي عبارة عن شبكة ضخمة من الحواسيب المتصلة فيما بينها حول العالم والتي يتم من خلالها تبادل المعلومات الرقمية إلى كافة أنحاء المعمورة.

كما يمكن تعريف شبكة الإنترنت بأنها: "شبكة كمبيوتر عملاقة على سطح هذا الكوكب فأطلق عليها شبكة التشبيك"[2]، وهذا يعني أنها شبكة تربط مجموعة ضخمة جدًا من أجهزة الكمبيوتر والحواسيب عبر العالم والمتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها.

ولذلك فإن شبكة الحاسب الآلي يقصد بها محجموعة من الحاسبات الصغيرة أو الكبيرة المتصلة فيما بينها، بحيث يتاح لكل وحدة على الشبكة الاستفادة من الموارد –بيانات ومعلومات– التي تتيحها هذه الشبكة[3]، وغالبا ما تنطوي هذه الشبكة على جهاز حاسب رئيسي يطلق عليه اسم الخادم (*Servier*)، وتتمثل مهمته الأساسية في إتاحة التطبيقات والبرمجيات المختلفة لأي حاسبات أخرى على نفس الشبكة، والتي عادة ما يطلق عليها اسم محطات عمل *Work station*[4].

فالإنترنت عبارة عن أكبر شبكة حواسيب موسعة النطاق الجغرافي تغطي جميع أنحاء العالم، فهي تصل بين حواسيب شخصية (*PC*) وشبكات محلية (*L.A.N*) وشبكات عامة (*W.A.N*)[5]،

---

[1]– ومن حيث أنواع هذه الشبكات فهي عديدة ونذكر منها على سبيل المثال (شبكة الإنترنت *Internet*، وشبكة الإنترانت *Intranet*، وشبكة الاكسترانت *Extranet*)، وكلها شبكات معلوماتية إجتماعية إفتراضية (أنظر أكثر: – **مصطفى محمد موسى:** المرجع السابق، ص28).

[2]– **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، مصر، 2008، ص56.

[3]– **عياض راشد عياض المري:** مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود، دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1998، ص31.

[4]– **عماد مجدي عبد الملك:** جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011، ص22.

[5]– الشبكات من حيث النطاق الجغرافي تنقسم إلى: (شبكة محلية محدودة النطاق وشبكة عامة واسعة النطاق).

– **أما الشبكة المحلية (*L.A.N*) *Local Area Network*:** فهي شبكة تربط مجموعة حواسيب قريبة من بعضها البعض وتشترك في المعدات المادية وتشترك أيضًا في البرامج والبيانات، فقد تجمع كل إدارة أو مؤسسة أو شركة حواسيبها في شبكة محلية، وترتبط هذه الحواسيب المحلية عن طريق حاسوب واحد يكون يمتاز بالسرعة العالية والقدرة على تخزين كم هائل من المعلومات، والشبكة المحلية (*L.A.N*) نوعان:

• **النوع الأول: شبكة الخادم والعملاء *Client - server Architecture*:** وهذه الشبكة تتميز بوجود حاسوب أساسي يسمى الخادم *Server* والذي بدوره يقدم خدمات من الشبكة إلى حواسيب أخرى تسمى عملاء *Clients* ترتبط معه على نفس الشبكة.

• **النوع الثاني: شبكة نظير لنظير *Peer-To- Peer Architecture*:** وفي هذه الشبكة كل الأجهزة الحاسوباتية متساوية ومتكافئة، وبإمكان أي جهاز في الشبكة أن يكون خادمًا أو عميلاً في الوقت نفسه، أي أنه لا يوجد جهاز مميز عن الأجهزة الأخرى، وهي أقل كلفة من الشبكة التي سبقتها، وهي تستخدم في المنشآت ذات الأعمال البسيطة.

– **وأما الشبكات الموسعة أو العامة (*W.A.N*) *Wide Area Network*:** وهي شبكات تربط طرفيات حواسيب عديدة ومنتشرة في مناطق جغرافية واسعة كالمدن والدول وحتى القارات، حيث ترتبط هذه الحواسيب مع بعضها البعض عن طريق قنوات إتصال مثل خطوط التلفون والأقمار الصناعية، ويطلق على هذه الشبكات الموسعة إسم "شبكات نقل البيانات العمومية *Public data Network*"، وتعرف أيضًا بشبكة الحواسيب *Computer Network*. (لمزيد أكثر حـــول هـــذا الموضوع راجع كل من: – **نهلا عبد القادر المومني:** المرجع السابق، ص35. – **علي جبار الحسيناوي:** المرجع السابق، ص26. – **رشيدة بوكر:** المرجع السابق، ص52. – **محمد علي سويلم:** المرجع السابق، ص87).

بحيث يمكن لأي شخص أن يصبح عضوًا في هذه الشبكة من منزله أو أي مكان آخر، ويستطيع حينها الوصول إلى قدر هائل من المعلومات في أي موضوع كان، وهكذا أصبحت الإنترنت تربط ما بين ملايين الشبكات الخاصة والعامة في المؤسسات الأكاديمية والحكومية ومؤسسات الأعمال، وتتباين في نطاقها ما بين المحلي والعالمي.

ولقد تطورت الإنترنت من وسيلة إتصال الشبكات الحاسوبية إلى نظام يصل ما بين جميع الحواسيب حول العالم ببروتوكول موحد هو بروتوكول الإنترنت (*IP/TCP*)، وبما أنها تتكون من عديد الشبكات المتصلة معًا فإنها تستخدم جميعها نفس البروتوكول[1]، الذي يتم الإتصال بشبكة الإنترنت بسهولة ويسر من خلاله، كما يضمن هذا البروتوكول التحكم في الإرسال عبر الإنترنت فيحدد السرعة الملائمة لإرسال المعلومات إلى المتلقي، وكذا ضمان وصول المعلومات إلى متلقيها بصور سليمة وصحيحة، بالإضافة إلى بروتوكول نقل الملفات (*FTP*) وهو إختصار لعبارة " *File transfer protocol*"[2].

والحقيقة أن جميع هذه التعاريف وغيرها تعبر عن حقيقة الإنترنت والتي يمكن تعريفها ببساطة بأنها: "شبكة عالمية تربط عدد كبير من الأجهزة المتناثرة عبر العالم، عبر خطوط وتقنيات الإتصال عن بعد، والتي تستخدم تواصلها ببروتوكول تراسل الإنترنت"[3].

ثانيًا: في التشريع

من بين أهم التعريفات التشريعية التي عرفت شبكة الإنترنت نجد ما يلي:

– عرفت المادة الثانية من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 الشبكة المعلوماتية بأنها: "إرتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها".

---

[1]– تعمل شبكة الإنترنت على بروتوكول يعرف باسم (*IP/TCP*) أي بروتوكول اتصالات الإنترنت، وهو البروتوكول الذي يجمع بين بروتوكولي (*IP/TCP*) للاتصالات، والذي أصبح البروتوكول الرسمي والمعتمد لشبكة الإنترنت، وهو من وضع إدارة الدفاع الأمريكية.

– **فبالنسبة للبروتوكول الأول (*TCP*) فهو:** إختصار للكلمات الثلاثة التالية (*Transmission control protocol*)، وهذا البروتوكول هو الذي ينظم الإتصالات على شبكة الإنترنت، وهو المسؤول على كيفية تجزئة الرسائل إلى حزم إلكترونية تمهيدًا لإرسالها عن طريق بروتوكول الإنترنت (*IP*)، ثم يقوم بعد ذلك بتجميع الحزم الإلكترونية وقراءتها إلى رسائل يستقبلها مرة أخرى، والتحقق من خلوها من الأخطاء، على أن يطابق ذلك النقل للرسائل في النموذج المعتمد للمواصفات الدولية (*ISO*) أي الكود المعتمد من هيئة الإيزو.

– **أما بالنسبة للبروتوكول الثاني (*IP*) فهو:** إختصار لكلمتي (*internet protocol*) أي بروتوكول الإنترنت، وهذا البروتوكول هو الذي يتحكم في تقسيم الرسائل إلى حزم إلكترونية والسماح لها بالسير عبر شبكة الإنترنت، ثم تجميعها مرة أخرى عند محطة الوصول كالمواقع الإلكترونية والبريد الإلكتروني وغيرها.

[2]– **أنظر في ذلك:** نص المادة (4/2) من المرسوم التنفيذي رقم (98–257) والمتعلق بضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، والمؤرخ في 1998/08/25، ج ر عدد 63 بتاريخ 1998/08/26. **أنظر الملحق رقم (07)**

[3] **رشيدة بوكر:** المرجع السابق، ص54–55.

– ونصت المادة (3/3) من قانون جرائم المعلوماتية السوداني رقم (13 لسنة 2007) شبكة المعلومات يقصد بها: "أي إرتباط بين أكثر من نظام معلومات للحصول على المعلومات أو تبادلها"[1].

– وعرفت المادة (7/1) من المرسوم السلطاني العماني رقم (12 لسنة 2011) الشبكة المعلوماتية بأنها "إرتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على البيانات والمعلومات الإلكترونية وتبادلها"[2].

– وعرفت المادة (7/1) من المرسوم الإماراتي رقم (5 لسنة 2012) وال الشبكة المعلوماتية بأنها: "إرتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات"[3].

– وعرفت المادة (6/1) من القانون الكويتي رقم (63 لسنة 2015) الشبكة المعلوماتية بأنها: "إرتباط بين أكثر من منظومة إتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها"[4].

– وعرفت المادة (3/1) من القانون القطري رقم (14 لسنة 2014) الشبكة المعلوماتية بأنها: "إرتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية للإنترنت"[5].

– وعرفت المادة (11/1) من القانون المصري رقم (175 لسنة 2018) الشبكة المعلوماتية بأنها: "مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معًا، ويمكنها تبادل المعلومات والإتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكة المعلومات الدولية والتطبيقات المستخدمة عليها"[6].

– **موقف المشرع الجزائري:** ونشير هنا أن المشرع الجزائري لم يعرف الشبكة المعلوماتية بوضوح وإنما تطرق إلى ذلك تحت مسميات مختلفة نذكر منها:

– ما جاء في نص المادة (2/2) من القانون رقم (04 لسنة 2009) بقولها: "منظومة معلوماتية، أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين".

---

[1]– القانون السوداني رقم (13 لسنة 2007)، المتعلق بقانون جرائم المعلوماتية، والصادر بتاريخ 2007/06/20.

[2]– القانون السلطاني العماني رقم (12 لسنة 2011)، المتعلق بقانون مكافحة جرائم تقنية المعلومات، والصادر بتاريخ 2011/02/06.

[3]– القانون الإماراتي رقم (5 لسنة 2012)، المتعلق بقانون مكافحة جرائم تقنية المعلومات، والصادر بتاريخ 2012/08/26.

[4]– القانون الكويتي رقم (63 لسنة 2015)، المتعلق بقانون مكافحة جرائم تقنية المعلومات، والصادر بتاريخ 2015/07/12.

[5]– القانون القطري رقم (14 لسنة 2014)، المتعلق بقانون مكافحة الجرائم الإلكترونية، والصادر بتاريخ 2014/09/15.

[6]– القانون المصري رقم (175 لسنة 2014)، المتعلق بقانون مكافحة جرائم تقنية المعلومات، والصادر بتاريخ 2018/08/14.

– كما عرفت المادة (6/2) من نفس القانون، تحت مسمى "الإتصالات الإلكترونية" بأنها: "أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[1].

الفرع الثاني: تاريخ نشأة الإنترنت

الإنترنت كنظام حديث للإتصالات يعتبر الإمتداد الطبيعي لتكنولوجيا الإتصالات المعتمدة على الحاسبات الآلية، والإنترنت أيضًا نجد جذورها التاريخية في ظهور وتطور تكنولوجيا الإتصالات الإلكترونية بوجه عام، والتي بدأت بظهور التلغراف أو التليغرام *Télégramme*[2] سنة 1810، ثم بعد ذلك التليفون *Téléphone* سنة 1826، ثم موجات الراديو *Radio* سنة 1898، ثم الإرسال التلفزيوني *Télévision* سنة 1937.

وتؤكد البحوث والدراسات التي تمت في هذا الموضوع أن الإنترنت كفكرة تعود إلى سنوات خلت من ستينيات القرن الماضي إثر تكليف الحكومة الأمريكية لخبراء متخصصين في الكمبيوتر بغية إيجاد نظام للإتصال يمكن من خلاله سريان المعلومات المهمة عن طريق الربط بأجهزة الكمبيوتر، وهنا تولت وزارة الدفاع الأمريكية هذه المهمة وقامت بتطوير شبكة إتصالات جديدة أطلق عليها في بادئ الأمر إسم الأربانت *Arpanet*[3]، ثم بعدها توصلت إلى إنشاء نظام جديد خلافًا للأربانت وأطلق عليه لأول مرة أيضاً إسم الإنترنت عبر برنامج جديد وذلك بتطوير نظام الربط المفتوح بواسطة جهاز المودام *Modem*[4].

---

[1]– ما نلاحظه على هذه المادة أنها جاء بمصطلح يختلف تمامًا عن المصطلحات الموجودة تقريبًا في كل القوانين المقارنة، كما أن تسمية "الشبكة المعلواتية" تدل على الإنترنت كمصطلح دخيل على اللغة العربية، على عكس تسمية "الإتصالات الإلكترونية" و"منظومة معلوماتية".

[2]– **التليغراف أو كما يطلق عليه (التليغرام):** هو فرع من فروع الإتصالات المرتبطة بإستخراج نسخة طبق الأصل عن بعد في شكلها المكتوب فقط، ثم وصل تطوره إلى أن نشأ فيما بعد ما يسمى (بالفاكس *Fax*) وهو جهاز يقوم بإستقبال كل الإتصالات البعيدة وإستخراجها نسخة طبق الأصل في شكل مكتوب أو مطبوع أو مصوره.

[3]– **زيدان زيبحة:** الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص26.

[4]– **المودم *Modem*:** عبارة عن جهاز إلكتروني متسع النطاق، يمكنه الربط المباشر لمجموعة من الأجهزة عبر شبكة الإنترنت، بمعنى يستخدمه المشترك للربط بين حسابه الشخصي وجهاز الحاسوب الذي يستخدمه للإتصال بشركات الخدمة التوصيلية، أي أنه بمثابة عقل إلكتروني يقوم بنقل المعلومات والبيانات المخزنة بين الحاسبات الآلية وتوزيعها عبر خطوط التليفونات. والمودم نوعان: أحدهما داخلي يثبت داخل الحاسب الآلي نفسه في شكل (كارت *Carte* أو شريحة *Carte Sim*)، والثاني خارجي على شكل وحدة منفصلة توضع بجانب الحاسب الآلي لتصل به عن طريق كابل أو سلك توصيل، ولا يختلف النوعان في الوظائف التي يقومان بها. (أنظر أكثر كل من: – **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، 2012، ص4. – **محمد عبد الله العوا:** المرجع السابق، ص12).

وهكذا نجد الشبكة العالمية للمعلومات أو الإنترنت كفكرة ولدت من رحم وزارة الدفاع الأمريكية، وتم تطبيقها كتجربة داخل الولايات المتحدة بمعرفة الهيئات العلمية المتخصصة عام 1969، فكانت الفكرة في البداية تقوم على ربط الحواسيب الآلية ببعضها البعض في مراكز البحث، إلى أن قامت مؤسسة العلوم القومية "*NSF*" بشراء حواسيب آلية عملاقة وتزويد مركز البحث بها لتشمل كل مناطق الولايات المتحدة الأمريكية، وذلك حتى تعمل كل مراكز الأبحاث إقليميًا مع بعضها البعض في شكل شبكة معلومات قومية، وفي كل هذه المراحل الأولى كانت شبكة الإنترنت مخصصة لأغراض البحث العلمي الأكاديمي والعسكري فقط[1]، فكانت خدماتها في البداية مجانية وبغير مقابل، وكانت قاصرة على الإستخدامات العلمية والبحثية وليس لها صفة تجارية. وعندما إستقرت الإنترنت على مدى عشرين عامًا في بداياتها الأولى على هذا النمط، ظهرت الحاجة الماسة إلى إستخدامها لأغراض تجارية تستفيد منها المؤسسات والشركات وأصحاب المشاريع والأعمال، وفعلاً بدأت الشبكة تعمل بشكل تجاري عام 1993[2].

وقد يعتقد البعض أن شبكة الإنترنت تملكها دولة معينة أو منظمة دولية تقوم بإدارتها، فهي في الحقيقة لا يملكها أحد ولا يسيطر عليها أحد، إنما هي ملكية تعاونية للبشرية جمعاء بقدر إسهامهم فيها، بمعنى آخر لا توجد هيئة رسمية حكومية أو غير حكومية للإشراف على الإنترنت، ذلك لأن البنية الأساسية حين فتح الإنترنت على مجال واسع أنها تدار بإشراف جهات غير حكومية أخذت على عاتقها جعل الإنترنت مساحة حرة متاحة للجميع، وتصدرت هذه الهيئات "جمعيات الإنترنت *Internet society*"[3]، وكذا الإتحاد الدولي للإتصالات "*ITU*" الذي يشرف على منظومات الإتصالات العلمية بما فيها شبكة الإنترنت، وأيضًا نجد منظمة "الآيكان *ICANN*"[4]، وهي منظمة

---

[1]– **محمد علي سويلم:** المرجع السابق، ص87.

[2]– **عبد الفتاح بيومي حجازي:** مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص81–82.

[3]– وهي مؤسسة أمريكية أنشأت عام 1991، تهدف إلى تنسيق جميع عمليات الإتصال والإرتباط فيما بين الشبكات. (أنظر أكثر: – **عبد الحسن الحسيني:** القاموس الموسوعي في المعلومات والإتصالات والمعلوماتية القانونية، ط1، مكتبة صادر، بيروت، لبنان، 2004، ص454).

[4]– **الأيكان *ICANN*:** في السابق كان إسمها المختصر "الآيان *IANA*"، إذ تتولى تخصيص مجموعات المواقع في شكل أرقام لكل منطقة من مناطق العالم، بحيث يتولى مقدموا خدمات الإنترنت الرئيسيون توزيع حصص هذه الأرقام على مقدمو الخدمة الفرعيون، ثم يتم تخصيص الرقم الخاص بكل مستخدم للإنترنت مشترك في الخدمة على حسب موقعه الخاص، وعلى ضوء ذلك يتم تحديد مستويات للموقع Domain بتعدد المناطق، فأصبح لكل دولة مثلاً مستوى من الخدمة خاص بالموقع يرمز إليه برمز معين مثلاً الجزائر *Dz*، فرنسا *FR*، مصر*Eg*، وبعدها إتسعت المستويات العالمية للشبكة وتعددت معها المواقع حسب المجالات فمثلاً إستخدامات الدولة *Gov*، الاستخدامات التجارية *Com*، استخدامات التعليم *EDU*. ولقد عرف المشرع الجزائري "الموقع" في نص المادة الثالثة من المرسوم التنفيذي رقم (98–257) والمتعلق بشروط إقامة خدمات الإنترنت بأنه: "أي مكان يحتوي موزعًا أو عدة موزعات للمعطيات الضرورية لتقديم خدمات الإنترنت". (راجع المرسوم التنفيذي رقم (98–257) المؤرخ في 1998/08/25، ج ر عدد (63) بتاريخ 1998/08/26). **أنظر في ذلك الملحق رقم (07).**

تشرف على أسماء المواقع الإلكترونية وعناوينها أو ما يعرف بأسماء النطاقات الجغرافية *Zone Géographique*.[1]

كذلك قد يعجب الكثيرون حينما يعلمون أنه لا توجد إدارة مركزية للإنترنت، وهي بذلك شبكة وصفها البعض بأنها "فوضى تعاونية"[2]، لكن في الوقت الحالي تقوم شركات تجارية بإدارة شبكة الإنترنت على أسس تجارية، لذلك فمن الضروري أن يدفع المشترك مبلغًا من المال مقابل إستخدامه للشبكة وحصوله على المعلومات، وكذلك من أجل تطوير الشبكة نفسها والمحافظة على إستمراريتها وتحسين إستخداماتها[3].

وهكذا غيرت الإنترنت وجه عالم التجارة والأعمال، وقد ساهمت بشكل كبير في تحقيق الوجود الفعلي للتعاملات الإلكترونية في شتى مناحي الحياة الفردية والجماعية، ووفقًا للدراسات الإحصائية والتقارير الرسمية، فإن نموًا كبيرًا ومطردًا قد تحقق في سوق خدمات الإنترنت والتعاملات الإلكترونية بشكل عام، ففي الفترة الممتدة من 1998 وحتى 1999 إزداد مستخدموا الشبكة العالمية بنسبة 55%، كما إزدادت مواقع الخدمات الإلكترونية بنسبة 128%، وازدادت أيضًا عناوين المواقع الإلكترونية المسجلة بنسبة 137%[4].

لقد نمت الإنترنت بشكل مذهل خلال السنوات العشر الأخيرة، فبعد أن كانت مجرد شبكة أكاديمية صغيرة أصبحت تضم ملايين المستخدمين من كافة أنحاء العالم، وتحولت من مجرد شبكة أكاديمية إلى بيئة متكاملة للإستثمار والعمل والإنتاج والحصول على المعلومات، في البداية لم يكن ثمة إهتمام بمسائل الأمن بقدر مكان الإهتمام ببناء نظام الشبكة، ولكن هذه النظرة تغيرت اليوم بشكل جذري خاصةً بعد أن أصبحت هذه الشبكة بمثابة ميدان لإرتكاب جرائم تمس كل المناحي الحياتية للفرد والمجتمع وهو ما يطلق عليه اليوم بجرائم الإنترنت[5].

---

[1]– **رشيدة بوكر:** المرجع السابق، ص 56.

[2]– **محمد علي سويلم:** المرجع السابق، ص88.

[3]– **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009، ص28.

[4]– **رشيدة بوكر:** المرجع نفسه، ص57.

[5] **سليمة سعيدي، بلال حجاز:** جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الاسكندرية، مصر، 2017، ص88.

الفرع الثالث: ماهية جرائم الإنترنت وأهم صورها

في ماهية جرائم الإنترنت سوف نتطرق إلى كل من البيانات الأولى في ظهور هذه الجريمة، ثم نتطرق إلى تعريفها، وبعد ذلك نذكر أهم صورها.

أولاً: بداية جريمة الإنترنت

مع بداية عصر العولمة[1] وإنتشار شبكة الإنترنت وقتها لم يكن هناك قلق واضح تُجاه العبث الإلكتروني الذي يمكن أن ينتهك على الشبكة أو بواسطتها، وذلك نظرًا لمحدودية إستخدامها وتوسعها، حيث كانت قاصرة في بداياتها على أغراض البحث العلمي والأكاديمي فقط، ولكن سرعان ما ظهرت جرائم ترتكب عن طريق شبكة الإنترنت بإستخدام آداة الحاسوب، فأصبح هذا النوع من الإجرام المستحدث إمتداد لما عُرف فيما بعد بجرائم الكمبيوتر[2].

وتاريخيًا يمكن القول بأن جرائم الإنترنت بدأت مع مطلع عام 1988، حيث كانت أول تلك الجرائم هي "جريمة العدوان الفيروسي *Crime d'agression virale*"، فيما هو معروف في تاريخ هذه الجريمة بـــ "دودة موريس *Ver morris*"، وقد أطلق عليها لأول مرة مصطلح "جرائم الإنترنت *Internet Crime*" في مؤتمر الجريمة والإنترنت المنعقد في أستراليا في فبراير 1988[3].

وهكذا ومنذ ذلك التاريخ عرف رواج الإنترنت كوسيلة للإتصالات وإستعمالها في كثير المعاملات اليومية تقريبًا، ظهور سلبيات عديدة خاصة بعد إستغلال الكثير من المجرمين وذوي النفوس المريضة هذا التغيير في نمط المعاملات، مما أسفر عنه ظهور جرائم لم يكن يعرفها القانون الجنائي من قبل[4].

---

[1]– **عصر العولمة *l'ère de la mondialisation*:** أو كما يطلق عليه بعصر التكنولوجيات الرقمية أو عصر الثورة المعلوماتية أو عصر السموات المفتوحة ...، كلها أوصاف تعبر عن مدى ضخامة القفزات العلمية الهائلة التي حققها الإنسان، ومدى تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا اليومية لا سيما في الآونة الأخيرة.

[2]– **شرين دبابنة:** الجرائم الإلكترونية والقرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، مج 23، ع01، الأكاديمية العربية للعلوم المالية والمصرفية، القاهرة، مصر، 2015، ص19.

[3]– **نائلة عادل محمد فريد قورة:** المرجع السابق، ص26. – **محمد عبد الله العوا:** المرجع السابق، ص17. – **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص62.

[4]– **محمد السعيد رشدي:** الإنترنت والجوانب القانونية لنظم المعلومات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997، ص11 وما بعدها.

ثانيًا: تعريف جريمة الإنترنت

تعتبر جرائم الإنترنت من الأنواع الإجرامية الأكثر شيوعًا في الوقت الراهن، لذا إهتم الدارسين والباحثين لها بتعريفها، ومن جملة هذه التعاريف لجريمة الإنترنت نجد الآتي:

– عرفت بأنها: "جميع الأفعال غير المشروعة والمرتكبة بواسطة الشبكة عن طريق الحاسب الآلي"[1].

– وقالوا عنها: "كل نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت مثل المواقع الإلكترونية وغرف المحادثات والدردشة والبريد الإلكتروني وغيرها، والتي تقوم على قائمة متنامية من الجرائم المعلوماتية"[2].

– وعرفت أيضًا بأنها: "نمطًا مستحدثًا من أنماط الإجرام المعلوماتي والإلكتروني الرقمي كونها تطال في إعتداءاتها على المعلومات بإستخدام الشبكة"[3].

– وقيل فيها: " كل جريمة مستحدثة ينطوي تحتها جرائم كثيرة ومتنوعة يصعب حصرها وتكون جميعها عن طريق إستخدام شبكة الإنترنت، وبواسطة شخص على دراية واسعة بها"[4].

– ومنهم من عرفها أيضاً بأنها: "جريمة تتميز ببيئة خاصة مختلف عن الجرائم الإلكترونية الأخرى، كونها عابرة للحدود الوطنية بإمتياز، وهذا راجع إلى دور شبكة الإنترنت في إرتكابها، وهذا ما جعلها توصف بالجريمة عبر الوطنية"[5].

ثالثًا: صور جرائم الإنترنت

لقد صنف معهد العدالة القومي بالولايات المتحدة الأمريكية في عام 1985 صور جرائم الإنترنت بحسب علاقتها بالجرائم التقليدية إلى خمسة أصناف[6] وهي على التوالي:

– الصنف الأول: يتمثل في كل الجرائم المنصوص عليها في قانون العقوبات تتى أُرتكبت بإستخدامات الشبكة المعلوماتية للإتصالات أي الإنترنت.

---

[1]– **عمر محمد أبو بكر بن يونس:** المرجع السابق، ص223.

[2]– **محمد خليفة:** المرجع السابق، ص38.

[3]– **منير محمد الجهيني وممدوح محمد الجهيني:** المرجع السابق، ص35.

[4]– **محمد الشناوي:** جرائم النصب المستحدثة، دار الكتب القانونية، القاهرة، مصر، 2008، ص33.

[5]– **شرين دبابنة،** المرجع السابق، ص21.

[6]– **خالد حسن أحمد لطفي:** جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الإبتزاز الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2019، ص26.

- الصنف الثاني: ويتمثل فيما تلعبه شبكة الإنترنت من دور في دعم وتسهيل بعض الأنشطة الإجرامية، ويتعلق الأمر مثلاً بجرائم ترويج المخدرات، جرائم غسيل الأموال، الإتجار بالأسلحة...
- الصنف الثالث: يتمثل في جرائم المساس بنظام المعالجة الآلية للمعطيات، كالدخول غير المسموح به على النظم المعلوماتية وما ينجر عنه من إعتداءات على البيانات والمعلومات سواءً بتغييرها أو تعديلها أو محوها.
- الصنف الرابع: يتمثل في جرائم الإعلام والإتصال، وتشمل كل ما يرتبط بشبكات الهاتف وما يمكن أن يقع عليها من إنتهاكات بإستغلال شبكة الإنترنت.
- الصنف الخامس: الجرائم المتعلقة بالإعتداء على الخصوصية وحقوق الملكية الفكرية، ويتمثل ذلك في عمليات نسخ البرامج دون وجه حق، كالسرقات العلمية المعروضة على الشبكة دون إذن من صاحبها.

وهو نفس التصنيف تقريبًا الذي إعتمدته الإتفاقية الأوروبية الخاصة بجرائم الإنترنت لعام 2001، فقد عددت هي الأخرى صور جرائم الإنترنت إلى أربعة أصناف وهي كما يلي[1]:

- الصنف الأول: الجرائم المرتبطة بحقوق المؤلف والحقوق المجاورة.
- الصنف الثاني: الجرائم التي تستهدف عناصر المعطيات والنظم المعلوماتية.
- الصنف الثالث: جرائم التزوير والإحتيال على محتويات الكمبيوتر.
- الصنف الرابع: الجرائم الإباحية وغير الأخلاقية.

وأمام هذا التباين المطروح في تحديد أنواع وصور جرائم الإنترنت وتصنيفها بحكم أنها كثيرة ومتنوعة ويصعب حصرها، فإننا سوف نتناول جملة من صور جرائم الإنترنت نذكر منها على سبيل المثال:

- جرائم تخريب المعلومات وإساءة إستخدامها.
- جرائم تزوير المعلومات وتزييفها.
- جرائم الدخول غير القانوني للمواقع والشبكات قصد الإساءة.
- جرائم زرع الفيروسات وإرسالها بقصد تعطيل المواقع.
- جرائم سرقة البيانات والمعلومات.

[1]- **أحمد خليفة الملط:** الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ط2، 2006، ص180.

- الجرائم الماسة بحقوق الطبع والنشر والسرقات العلمية.
- جرائم الإحتيال المالي وسرقة الأرقام السرية والمتاجرة بها.
- جرائم المساس بحق الملكية الفكرية والحقوق المجاورة.
- جرائم قرصنة المواقع الإلكترونية والبرمجيات.
- جرائم إنتهاك الخصوصية كالتنصت والتجسس والتشهير.
- جرائم التحرش الجنسي والإباحية وكل المساسات غير الأخلاقية.
- جرائم الإستغلال الجنسي للأطفال القصر.
- جرائم الإبتزاز والإستفزاز الإلكتروني.
- جرائم الإرهاب الإلكتروني.
- جرائم تبييض الأموال.
- الجريمة المنظمة عبر الإنترنت.
- جريمة تزويج المخذرات.
- جرائم سرقة الهوية والمساس بالأسرار التجارية.

وغيرها كثير من الصور الإجرامية التي تسهلها شبكة الإنترنت، فهي جرائم منها ما هو بدافع المال، أو بدافع الإنتقام أو تلبية لأفكار وإديولوجيات إجرامية، أي أنها مسألة إما ذات أبعاد خاصة أو ذات أبعاد عامة، سيما إذا أدركنا أن العالم الإفتراضي هو نتاج إجتماع الإتصالات والمعلومات التي تتجاوز نطاق الحدود الدولية، وأنه بيئة مناسبة لإرتكاب أفعال يعدها المجرى العادي للأمور في عالمنا المادي أفعال غير مشروعة تصل إلى حد التجريم في النظم الجنائية المعاصرة.

البَاب الأَوّل

جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

البَاب الأَوّل: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

تمهيد وتقسيم:

تكتسي نظم المعالجة الآلية للمعطيات أهمية كبيرة في مجال الوسط الرقمي وتقنية المعلومات، وهو ما يعكس القدرة العملية والعلمية على صناعة ومعالجة وتخزين ونقل المعلومات من مادتها الخام إلى معلومات رقمية، وهذا من أكبر ما أنتجته العولمة التكنولوجية، فأصبحت الحواسيب والشبكات التي ترتبط فيما بينها بصورة سريعة جدًا تعكس مدى قدرة الإنسان وسيطرته على عديد المجالات تقريبًا وتذليل كثير الصعاب أمامه خدمةً للبشرية جمعاء في شتى الميادين والقطاعات.[1]

إلا أنه أصبحت هذه النظم المعلوماتية تتعرض لعديد الجرائم أُطلق عليها إسم "جرائم المساس بأنظمة المعالجة الآلية للمعطيات *Infraction aux systèmes de traitement automatisé de données (STAD)* الأمر الذي إستدعى معه إستحداث تعديلات جنائية جديدة بشأنها، وربما يرجع سبب ذلك إلى زيادة الوعي بخطورة هذا النوع المستحدث من الجرائم، بإعتبارها تؤثر على الأمن والإقتصاد الوطني من جهة، وكذا المساس بحرمة وخصوصية الأشخاص من جهة أخرى.

وإن التطور التقني والتكنولوجي والإعتماد عليه اليوم في كافة مجالات الحياة عمومًا، وفي مجال الإتصالات والمعلومات بوجه خاص، أثمر خدمات جد هامة وفرت الكثير من الجهد والوقت، زاد من تواصلنا وتقاربنا عبر عالم إفتراضي واسع المدى وأصبح العالم الحقيقي من خلاله قرية صغيرة، بيد أن ذلك التطور الإيجابي صاحبه جانبا آخر سلبي، جعل من الأنظمة المعلوماتية أداة ووسيلة لإرتكاب العديد من الجرائم والتي لم تكن معروفة من قبل، والغريب في الأمر أن هذه الجرائم إزدادت تطورًا وإكتسبت خصائص جديدة سهلت من إرتكابها ورفعت من سقف خطورتها، ولعل من أبرز هذه الجرائم وأكثرها إنتشارًا نجد جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي.

وعليه سوف نتناول في هذا الباب من الدراسة أهم الأحكام القانونية الموضوعية التي تطرق إليها المشرع الجزائري في قانون العقوبات بشأن المساس بأنظمة المعالجة الآلية للمعطيات، سواءً

[1]– ولعل من أهم هذه القطاعات التي سيطرت عليها تكنولوجيا الإعلام والإتصال نجد على سبيل المثال: "قطاع الإقتصاد العالمي الحر"، والذي أصبح بفضل هذه العولمة التكنولوجية والإلكترونية يحقق عائدات ضخمة قدرت مع بداية 2017 بحوالي 3.5 تريليون دولار أمريكي وهو في زيادة مستمرة. (أنظر في ذلك: – **يزيد بوحليط:** المرجع السابق، ص172).

تلك التي تقع بطريقة غير مشروعة على الأنظمة المعلوماتية ذاتها من حيث الدخول أو البقاء بداخلها أو تلك التي تمس بالمعلومات المعالجة آلياً، مع إبداء دراسة تحليلية مقارنة لبعض القوانين الأوروبية والعربية.

وترتيبًا على ذلك سوف نحاول من خلال هذا الباب الحديث عن هذه الجريمة بشيء من التفصيل، وذلك بإعتبارها الجريمة الرئيسية والتي أولت لها مختلف التشريعات الجنائية الحديثة أهمية كبيرة، لأنها وبكل بساطة هي بداية الجرائم المعلوماتية الأخرى الناتجة عن الجريمة الأم وهي جريمة الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات.

ومنه سوف نقوم بدراسة هذا الباب من خلال فصلين إثنين على التوالي:

الفصل الأول: الإطار المفاهيمي لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

الفصل الثاني: أركان وعناصر جريمة الدخول أو البقاء غير المشروع والعقوبات المقررة لها

الفَصل الأَوّل

الإطار المفاهيمي لجريمة الدخول
أو البقاء غير المشروع في النظام المعلوماتي

الفصل الأول: الإطار المفاهيمي لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

تمهيد وتقسيم:

تعد جريمة الدخول أو البقاء غير المشروع في المواقع الإلكترونية ومختلف الأنظمة المعلوماتية العديدة من أكثر الجرائم تأثيراً على السرية والخصوصية المرتبطة بتكنولوجيا المعلومات في مجال عالم الحواسيب والإنترنت، وبالرغم من أن هذه الجريمة تعد البوابة الرئيسية لإرتكاب بقية الجرائم المعلوماتية الأخرى الواقعة في فضاء التعامل الإلكتروني، إلا أن العديد من الدراسات الفقهية والقانونية لم تعطها حقها من البحث والدراسة.

لذا سوف نركز في هذا الفصل عن مفهوم هذه الجريمة وأهم خصائصها، مع التركيز على أهمية ضرورة وجود نظام المعالجة الآلية للمعطيات لقيام هذه الجريمة، وذلك من خلال مبحثين إثنين على التوالي:

المبحث الأول: مفهوم جريمة الدخول أو البقاء غير المشروع وإبراز أهم خصائصها.

المبحث الثاني: ضرورة وجود نظام المعالجة الآلية للمعطيات في قيام الجريمة.

المبحث الأول: مفهوم جريمة الدخول أو البقاء غير المشروع وإبراز أهم خصائصها

تمهيد وتقسيم:

أي جريمة كانت، ومهما كان شكلها ودرجة خطورتها، إلا ولها مفهوم خاص بها يحدد نوعها وجملة الخصائص التي تميزها عن غيرها، ومن ذلك جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، والتي إهتم بها كل من الفقه والقانون بتعريفها وإبراز وتبيان أهم خصائصها التي تمتاز بها.

ولقد أكدت الكثير من التشريعات الجنائية الحديثة أن جريمة الدخول أو البقاء غير المشروع في النظام بمثابة الحد الفاصل بين الجاني وبين إرتكابه لمختلف الجرائم الإلكترونية الأخرى ذات الصلة بها[1]، حيث أولت لها إهتمامًا كبيرًا وإعتبرها الجريمة الأساسية وما الجرائم المعلوماتية الأخرى إلاَّ نتاج يترتب عنها.[2]

وهذا ما سوف نتطرق إليه تباعاً في مطلبين إثنين هما:

المطلب الأول: تعريف جريمة الدخول أو البقاء غير المشروع

المطلب الثاني: خصائص جريمة الدخول أو البقاء غير المشروع

[1]– **عادل بوزيدة:** المرجع السابق، ص81.

[2]– **غنية باطلي:** المرجع السابق، ص135.

المطلب الأول: تعريف جريمة الدخول أو البقاء غير المشروع

لقد إهتم كلٌ من الفقه والقانون الجنائيين بمسألة تعريف جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي، وإن كان كل منهما له رؤيته الخاص وزاوية معينة ينظر من خلالها في تعريفه لهذه الجريمة، سواءً من حيث التعريف الإصطلاحي (فرع أول) أو التعريف الفقهي (فرع ثاني) أو التعريف القانوني (فرع ثالث).

الفرع الأول: التعريف الإصطلاحي للجريمة

تجدر الإشارة ونحن بصدد الإحاطة بأهم التعريفات الفقهية والقانونية لهذه الجريمة، إلى التنبيه أن هذه الجريمة تستعمل لها عدة مصطلحات ومسميات للدلالة عليها، وكلها لها معنى واحد وهو الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، ولعل من بين أهم هذه المصطلحات نجد على سبيل المثال ما يلي:

أولاً: الغش المعلوماتي والتواصل غير المصرح به مع النظام

وهو من أهم وأبرز المصطلحات التي تناولها وأخذ بها المشرع الجنائي في أكثر من موضع والمقصود به مجموعة الأفعال التي تتصل بطريقة غير مبررة بأنظمة المعالجة الآلية للمعطيات، فهي أفعال غير جائزة وغير مباحة من طرف مستخدميها، تنصب مباشرة على محل معين هو المعلومات المخزنة داخل الحاسب الآلي ونظم معالجتها.[1]

كما يقصد به كل عمليات الوصول والتواصل غير المصرح بها إلى أجهزة الغير وشبكاتهم الإلكترونية أو حتى إلى مواقع وصفحات التواصل الإجتماعي الخاصة، وذلك بواسطة حواسيب آلية أو برامج متطورة يستخدمها كل من لديه خبرة في إستعمالها[2]، مما يسمح له معرفة الطريقة الواجب إتباعها للحصول على كل ما يريده الفاعل من معلومات مخزونة في هذا النظام، وأكثر من ذلك فعملية التواصل غير المصرح به تسمح له أيضًا بالدخول إلى باقي الأنظمة المعلوماتية الأخرى المتصلة بهذا الجهاز الذي تم الدخول إليه بطريق الغش والمرتبطة معه على ذات الشبكة المعلوماتية[3]، وهكذا يكون الإتصال مع النظام بطريق الغش متى كان الجاني لا يحق له التواصل والدخول إليه لأي سبب من الأسباب.[4]

---

[1]– **نعيم مغبغب:** حماية برامج الكمبيوتر في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص234.

[2]– **خالد ممدوح إبراهيم:** أمن الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2008، ص84.

[3]– **نعيم مغبغب:** المرجع السابق، ص250.

[4]– **خالد ممدوح إبراهيم:** المرجع السابق، ص91.

فالغش المعلوماتي إذن هو ذلك الدخول غير المصرح به إلى النظام المعلوماتي عن طريق صوره المختلفة من إعتراض وإلتقاط وقرصنة وإختراق وغيرها من الصور غير المشروعة والماسة بسلامة النظام ومحتوياته، فمصطلح الغش المعلوماتي إذن هو تعبير يتسع ليشمل كل الصور والوسائل المستعملة للدخول إلى النظام ولكن بطريق غير قانوني، وهو نفسه المصطلح الذي جاء في سياق قانون العقوبات الجزائري، وكذا قانون العقوبات الفرنسي.[1]

ثانيًا: الإستعمال والإنتفاع المعلوماتي بدون وجه حق

تختلف فكرة الدخول أو البقاء غير المشروع إلى النظام عن فكرة الإستعمال والإنتفاع المعلوماتي بدون وجه حق، وبالتالي ينبغي علينا هنا أن نفرق بين الإستخدام والإستعمال والإنتفاع غير المصرح به لنظام الحاسب الآلي ذاته، وبين الإستخدام غير المصرح به للإطلاع على البيانات والمعلومات المخزنة داخل هذا النظام[2]، بمعنى أنه ينبغي أن نميز بين الإستخدام غير المصرح به لنظام الحاسب الآلي وبين الدخول أو البقاء غير المصرح بهما إلى النظام.

فالإستعمال غير المصرح به لجهاز الحاسب الآلي معناه الإنتفاع بدون وجه حق من الخدمات التي يقدمها هذا الحاسب الآلي، وبالتالي فإن المشرع الجنائي إذا جرّم فعل الدخول إلى النظام فإن ذلك لا يعني أن يقوم الفاعل بإستعمال الجهاز، وإنما دخوله هنا ينصب على إستمعماله للبيانات والمعلومات المخزنة داخل هذا الجهاز، فالأولى تدخل ضمن جريمة سرقة وقت الآلة، أما الثانية فتدخل ضمن جريمة سرقة المعلومات[3]، فالغرض من تجريم الدخول غير المشروع هو حماية المعلومات بغض النظر عن إستعمال الجهاز الذي يحتويها، فإذا ما تعدى الفعل حد إستعمال

---

[1]– أنظر نص المادة (394 مكرر) من (ق ع ج) بخصوص مصطلح "الغش المعلوماتي" والتي جاء فيها: "... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ...". **ينظر في ذلك الملحق رقم (05)**

- Article (323-1) : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

« - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

[2]– **أحمد محمود مصطفى:** المرجع السابق، ص263.

[3]- ***DEVEZ (J) :*** *Les qualifications pénales appliables aux fraudes informatiques, Acte du 8ème congrés de l'AFDP, grenoble 28-30 Novembre 1985, Ed Economica, Paris, France, 1986, PP 185-213.*

الخدمات التي يقدمها الحاسب الآلي إلى الوصول للمعلومات بطريقة غير مصرح بها، فإن الفعل هنا يدخل تحت طائلة النصوص التي تجرم الدخول غير المشروع للنظام[1].

فهكذا نجد أن دائرة فعل الدخول غير المشروع أضيق بكثير من دائرة الإستعمال غير المصرح به لجهاز الحاسوب[2]، بمعنى أنه نستطيع القول أن كل إستعمال للجهاز –نظام الحاسوب– دون موافقة صاحبه يشكل بلا ريب دخولاً فيه[3]، أما فعل الدخول فإنه لا يعني بالضرورة إستعمال بيانات النظام، فقد يتصل الشخص بالحاسوب أو الموقع ومن ثمة يكون قائمًا بالدخول فيه ولكنه لا يستعمل إمكانيات هذا النظام المعلوماتية، كأن يكتفي بالإطلاع على محتويات النظام دون إستعمالها.[4]

ولقد إنتشرت ظاهرة إستعمال تقنية المعلومات للإنتفاع بخدمات الإتصال بدون وجه حق وكذا الحصول على خدمات المواقع وقنوات البث المسموعة والمرئية بدون إذن مسبق بذلك، والتي قد تكون مشفرة في غالب الأحيان[5]، والتي يتطلب الحصول عليها بدفع مقابل الإشتراك، ومع ذلك يتم الإنتفاع بها وبخدماتها دون وجه حق عن طريق شبكة الإنترنت، مما يعرض الأفراد والشركات التي لها حقوق على هذه الخدمات لخسائر فادحة بما يؤثر على عمليات الإتصالات[6] وحقوق المستخدمين والمنتفعين من خدمات هذه الإتصالات.

لذلك حرصت العديد من التشريعات على تجريم فعل الدخول غير المشروع وكذا تجريم فعل الإستعمال والإنتفاع المعلوماتي غير المسوح به، فالإستعمال المعلوماتي هو ما يقصد به البقاء والتواجد داخل النظام بدون وجه حق، وهذا ما ذكرته جلُّ التشريعات الجنائية الحديثة تحت مسمى "جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي"[7]، وإن كان هناك بعض الهيئات الدولية والتشريعات الوطنية يرون أن فكرة الدخول غير المشروع تختلف عن فكرة إستعمال

---

[1]– **محمد علي سويلم:** المرجع السابق، ص266.

[2]- ***CHAMPY (G) :*** *Fraude informatique, thèse, université Aix- Marseille 3, France, 1990, P492.*

[3]– **إمام حسنين عطا الله:** جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر والتوزيع، الرياض، السعودية، 2017، ص182.

[4]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص106.

[5]– **عمر الشريف:** التنظيم التشريعي لجرائم الاتصالات في مصر، مجلة التشريع، السنة الأولى، العدد الثاني، القاهرة، مصر، 2004، ص32.

[6]– **إمام حسن عطا الله:** المرجع نفسه، ص185. – **رشيدة بوكر:** المرجع السابق، ص77.

[7]- ***SIEBER (U) :*** *Les crimes informatiques et d'autres crimes dans le domain de la technologie informatiqe, (R.I.D.P), 1993, P18.*

إمكانيات النظام دون إذن مسبق، ومن جملة هذه المواقف الدولية والتشريعات الوطنية نجد على سبيل المثال ما يلي:

أ- موقف الهيئات الدولية: من بين الهيئات الدولية التي دعت كل أعضائها إلى تجريم الإستعمال والإنتفاع المعلوماتي غير المشروع لنظام الحاسوب نجد:

1. موقف المجلس الأوروبي: أوصى المجلس الأوروبي الدول الأعضاء فيه بتجريم الإستخدام غير المشروع لنظام الحاسوب، وذلك حرصًا منه على حماية المصلحة الإقتصادية لمالك النظام أو للمرخص له بإستعماله، وكذا حماية النظام المعلوماتي ككل من أجل ضمان قيامه بالوظائف التي يقدمها على أحسن وجه.[1]

2. موقف منظمة التعاون الإقتصادي والتنمية: كما أوصت هذه المنظمة جميع الدول الأعضاء فيها بتجريم الإستخدام غير المشروع لنظام الحاسوب، ورأت هذه المنظمة ضرورة أن يقتصر التجريم على الحالات التي يعلم فيها الفاعل أنه يخترق بهذا الإستعمال الإجراءات الأمنية الموضوعة للحيلولة دون الدخول أو البقاء غير المصرح بهما لأنظمة الحاسبات الآلية[2]، ولقد إقترحت المنظمة في سبيل تجريم الإستعمال غير المصرح به أن تسلك الدول أحد الطريقين، إما أن يقوم المشرع بإفراد نص عام لتجريم الإستعمال غير المصرح به وجعله من قبيل جريمة الدخول أو البقاء غير المشروع، أو إفراد نص خاص لتجريم الإستعمال والإنتفاع غير المصرح به لأنظمة الحاسبات الآلية والذي يمكن أن يصاغ بعدة أشكال سواءً كان ذلك في صورة فقرة أو مادة مستقلة كما هو الحال في كثير من القوانين الوطنية.[3]

ويفرق البعض الآخر من المشرعين بين الإستعمال غير المصرح به لنظام الحاسب الآلي بصفة عامة وبين الإنتفاع المعلوماتي غير المصرح به من الخدمات التي يقدمها هذا النظام بإعتبار أن السلوك الأخير أحد المظاهر التي يتخذها السلوك الأول، فالإستعمال غير المصرح به لنظام الحاسب الآلي يدخل في تكوين الجرائم المعلوماتية بصفة عامة بما فيها جريمة الدخول أو البقاء

---

[1]- **عبد الجبار الحنيص:** الإستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي، دراسة مقارنة، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الأول، كلية الحقوق، جامعة دمشق، سوريا، 2011، ص202.

[2]- **أحمد محمود مصطفى:** المرجع السابق، ص268.

[3]- **عبد الجبار الحنيص:** المرجع نفسه، ص208.

غير المشروع داخل النظام، في حين أن الإنتفاع المعلوماتي من الخدمات التي يقدمها النظام وبغير مسوغ من القانون هو صورة مستقلة ومتميزة عن الاستعمال غير المصرح به.[1]

والواقع أنه إذا كان الإستعمال غير المصرح به لنظام الحاسب الآلي قد يكون مقصودًا لذاته لإستخدام الخدمات التي يقدمها، أو قد يكون وسيلة لإرتكاب نشاط إجرامي آخر، فلا يوجد مبرر لتأثيم الحالتين معًا وبنصوص مستقلة، لأن الإستعمال غير المصرح به ينصب دائمًا على الخدمات التي يقدمها الحاسوب، سواءً أكان مقصودًا في ذاته أو وسيلة لإرتكاب جريمة أخرى، وأن تجريم أي من السلوكين يكفي لتغطية الإثنين معًا[2].

ب- موقف التشريعات الوطنية: ومن جملة هذه التشريعات نجد على سبيل المثال:

1. التشريع الكندي: والذي حرص على معاقبة كل من يستعمل أو يتسبب في إستعمال نظام الكمبيوتر للحصول على الخدمات التي يقدمها متى تم ذلك بسوء نية أو بغير وجه حق، أو كان الإستخدام لهذا النظام بقصد إرتكاب جريمة أخرى، وذلك بموجب نص المادة (342) من قانون العقوبات الكندي لعام 1985، والتي بمقتضاها يتم تجريم الإستعمال غير المصرح به للنظام.[3]

2. التشريع الأسترالي: وفي أستراليا إتجه المشرع إلى تجريم الإستعمال غير المصرح به لنظام الحاسب الآلي، وذلك من خلال نص المادة (115) من قانون العقوبات الأسترالي لعام 1985، حيث تنص هذه المادة بمعاقبة كل من يستعمل بسوء نية حاسبًا آليًا، أو يساعد على هذا الإستعمال بنية تحقيق منفعة من وراء هذا الإستعمال له أو لغيره، أو إلحاق الخسارة بالمجني عليه.[4]

3. التشريع المصري: وفي هذا الصدد نصت المادة (13) من القانون المصري رقم (175 لسنة 2018) في شأن مكافحة جرائم تقنية المعلومات بقولها: "يعاقب ... كل من إنتفع بدون وجه حق عن

---

[1]- **محمد علي سويلم:** المرجع السابق، ص 252. - **أحمد محمود مصطفى:** المرجع السابق، ص264. - **نائلة عادل محمد فريد قورة:** المرجع السابق، ص380.

[2]- وهذا ما جاء في تقرير الأمم المتحدة لعام 1994 بشأن الجرائم المعلوماتية، معتبرًا أن تجريم أي من السلوكين يكفي لتغطية الإثنين معاً.

- *« Organisation des nations unies, manuel des nations unies sur la prévention et la représsion de la criminalité informatique, New York, Nations unies, 1994, P 15, Rev, inter, poli, crim, 1994, N°43-44 ».*

[3]- ***Canadian criminal code (C.C.C) :*** *computer crimes.*

[4]- مشار إليه عند: - **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2005، ص413.

طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة إتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي".[1]

4. التشريع الإماراتي: كما نصت المادة (34) من القانون الإماراتي رقم (5 لسنة 2012) بشأن مكافحة جرائم تقنية المعلومات بقولها: "يعاقب ... كل من إنتفع أو سهل للغير وبغير وجه حق الإنتفاع بخدمات الإتصالات أو قنوات البث المسموعة أو المرئية وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية المعلومات".[2]

5. موقف المشرع الجزائري: لم يضع التشريع الجزائري بخصوص هذه المسألة نصًا خاصاً بتجريم الإستعمال أو الإنتفاع المعلوماتي بدون وجه حق، كما هو الشأن في القوانين التي تم ذكرها سلفاً، وإن كان هناك إتجاه يذهب إلى القول بأن كل من الإستعمال والإنتفاع المعلوماتي يدخل ضمن جريمة الدخول أو البقاء غير المشروع، وليس هناك داعي إلى أن يكون هذا التجريم بصورة مباشرة وأن العقاب على الإستعمال غير المصرح به لنظام الحاسب الآلي قد يتم عن طريق تطبيق الفقرة الأولى من نص المادة (394 مكرر) من (ق ع ج) والخاصة بجريمة الدخول أو البقاء غير المصرح به داخل النظام المعلوماتي، وكذلك الأمر بالنسبة للمشرع الفرنسي بموجب المادة (323-1) من (ق ع ف).

ثالثاً: القرصنة المعلوماتية

قديمًا كانت تطلق كلمة "قرصان" على الشخص محترف السرقة والسطو على السفن وهي في عرض البحر[3]، وهكذا انتقلت تسمية القرصنة من عمليات إجرامية تجري في عرض البحار والمحيطات إلى مجال أوسع هو عالم الإتصالات الإلكترونية، ومنه سميت "بالقرصنة الإلكترونية" أو "القرصنة المعلوماتية"، ومن هنا أصبح يطلق على محترفي عمليات الإختراق والدخول إلى النظم المعلوماتية بطرق غير مشروعة "بالقراصنة" قياسًا على الأشخاص الذين كانوا يقومون في الماضي بإعتراض أموال الناس وأملاكهم الشخصية ويأخذونها بالغصب والقوة، ومثالهم قراصنة البحر.[4]

---

[1]– أنظر في ذلك نص المادة (13) من القانون المصري رقم (175 سنة 2018).

[2]– أنظر في ذلك نص المادة (34) من القانون الإماراتي رقم (5 لسنة 2012).

[3]– كتاب معجم القانون الصادر عن مجمع اللغة العربية، الهيئة العامة لشؤون المطابع الأميرية، القاهرة، مصر، 1999، ص508.

[4]– ***LAURE (Z) :*** *Enjeux et maitrise des cyber, risques, largus, 1ere Ed, Dalloz, Paris, France, 2014, P 63.*

ويشير مفهوم القرصنة المعلوماتية أو كما يحلو للبعض بتسميتها بالقرصنة الإلكترونية أو القرصنة الرقمية، إلى إستخدام وسائل الإتصال الحديثة وتكنولوجيا المعلومات في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات لكشفها والتأثير على سلامتها أو حتى إتلافها[1]، وفي عبارة أخرى فالقرصنة ما هي سوى عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية بإستخدام شبكة الإنترنت للقيام بعمليات الإختراق، أي توجيه هجمات إلى أجهزة الحاسوب بقصد المساس بسلامته أو المساس بسرية المعلومات أو الخدمات التي يحتوي عليها هذا النظام المعلوماتي، أو القصد منها تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها.[2]

حيث يقوم بهذه العملية إما شخص أو مجموعة من الأشخاص من لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة إستخدام برامج مساعدة من الدخول إلى حاسوب آخر مملوك للغير والتعرف على كل محتوياته المعلوماتية، ومن خلاله يستطيعون أيضا إختراق باقي الأجهزة الأخرى والمرتبطة معه في نفس الشبكة، والقرصان الإلكتروني أو هؤلاء القراصنة يتم تصنيفهم إلى نوعين إثنين وهما على التوالي:

أ- القراصنة الهواة (الهاكرز *Hackers*)[3]: أول ظهور للهاكرز بالمفهوم السيء كان مع مطلع عام 1981 ويتصادف ذلك مع ظهور أول حاسوب شخصي من إنتاج شركة "*IMB*"[4]، وتم تعريفهم وقتها بأنهم: "الأشخاص الذين لديهم القدرة الفائقة على إختراق الأجهزة والشبكات، أيًّا كانت إجراءات وبرامج الحماية الأمنية التي تم إتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي إلى الإضرار بالجهاز أو الشبكة نتيجة ذلك الإختراق".[5]

ويعتمد الهاكرز على برامج التجسس الجاهزة والمتاحة في كل مكان سواءً عن طريق شرائها أو تحميلها من شبكة الإنترنت، بحيث يقوم هؤلاء القراصنة بزرع ملفات التجسس في

---

[1]- **خالد حسن أحمد لطفي:** جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الإبتزاز الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، مصر، 2019، ص61.

[2]- **جميل زكريا محمود:** الجريمة المعلوماتية وأساليب التأمين، المؤتمر الدولي لأمن المعلومات الإلكترونية، جامعة عمان، 2005، ص147.

[3]- من أشهر من إكتسب هذه الصفة "دينيس ريتش" و"كين تومسون"، اللذان صمّما لأول مرة برنامج إختراق الحواسب العملاقة تحت إسم "برنامج أليونكس *Unix softwar*" وذلك عام 1969.

[4]- **شركة (أي.بي.أم *IBM*):** هي شركة عالمية متعددة الجنسيات تعمل في مجال تصنيع وتطوير الحواسيب والبرمجيات، مقرها بمدينة نيويورك الأمريكية، تعرف بإسم "المؤسسة الدولية للحاسبات الآلية".

[5]- **خالد حسن أحمد لطفي:** المرجع نفسه، ص64.

حواسيب الضحايا إما عن طريق البريد الإلكتروني أو بإستغلال ثغرات الويندوز "*Windows*" التي يكتشفها البرنامج، وهكذا تظهر أهداف الهاكرز في إثبات قدرته في التفوق والتفاخر بمواهبه التي يفتقدها بعضهم، فهؤلاء كل ما يشغلهم هو التسلل إلى حواسيب الآخرين وسرقة بريدهم الإلكتروني والتلاعب في إعدادات هذه الأجهزة مع ترك ما يفيد أنهم فعلوا ذلك كشكل من أشكال الغرور والتباهي بالنفس.[1]

ب- القراصنة المحترفون (الكراكز *Crackers*): أما عن فئة قراصنة الكراكز، فهم الفريق الأخطر لأنهم فريق منظم يعلمون ماذا يريدون وماذا يفعلون، ويرسمون مسبقًا كيفية الوصول إلى أهدافهم الإجرامية، وذلك بإستخدام ما لديهم من علم ومعرفة يطورونها بإستمرار بإستخدام البرامج والتقنيات المتطورة سواء من حيث لغة البرمجة والتشغيل والقدرة على تحليل البرامج بسرعة مذهلة، وتم تعريفهم بأنهم: "الأشخاص الذين لديهم القدرة الفائقة على إختراق الأجهزة والشبكات، أيًّا كانت إجراءات وبرامج الحماية التي تم إتخاذها من صاحب النظام، مع إمكانية أنهم يستطيعون القيام بكل أشكال العبث المعلوماتي على البيانات والمعلومات المخزنة على تلك الحسابات والشبكات من خلال إحترافية فائقة".[2]

ومن هنا يتضح أن أهداف هذه الفئة من القراصنة أكبر وأخطر من أهداف الفئة السابقة فأهدافهم مثلاً تكمن في سحب الأموال من الحسابات الخاصة بالعملاء داخل المصارف، أو الولوج إلى أخطر المواقع الإلكترونية وأكثرها حساسية والتلاعب ببياناتها ولَربما تدميرها بالمرة[3]، وعن طريقهم تعرضت الكثير من الشركات والمؤسسات المعلوماتية والمعروفة عالميًا إلى عمليات القرصنة، كما لم يسلم البعض من قرصنة بريده الإلكتروني أو صفحته الشخصية على مواقع التواصل الإجتماعي[4]، وهو ما يعد خرقًا للخصوصية والسرية، وأحيانًا يرتبط الأمر بخسائر مادية أيضًا وذلك عند إختراق البيانات البنكية والمصرفية عن طريق الإنترنت، فيعتبر التعرض لمثل هذه القرصنة بمثابة جرس إنذار للتأكد من سلامة برنامج الحماية الأمنية لمثل هذه الإعتداءات.

---

[1]- **خالد حسن أحمد لطفي:** المرجع السابق، ص65.

[2]- **ممدوح محمد الجهيني، منير محمد الجهيني:** المرجع السابق، ص28.

[3]- مثال ذلك ما أحدثه "روبرت موريس" أحد مشاهير الكراكرز *Crackers* عام 1988 حين قام بتطوير "أفعى اليونكس *Unix snake*"، مما تسبب وقتها في تعطيل حوالي 6000 جهاز حاسوب ومواقع إلكترونية، وقدرت الخسائر المادية حينها أكثر من 15 مليون دولار أمريكي، (أنظر: - **خالد حسن أحمد لطفي:** المرجع نفسه، ص67).

[4]- متاح على الموقع (***https://m.dw.com***) تاريخ التصفح 12 جانفي 2020.

رابعًا: الإعتراض الإلكتروني والإلتقاط الهوائي

يتفق كل من الدخول غير المشروع والإعتراض الإلكتروني غير المصرح به، في أن كل منهما يؤدي إلى نفس النتيجة، وهي الوصول إلى معطيات النظام المعلوماتي والتي لا يجوز للغير الوصول إليها، وبعبارة أخرى يمكن القول بأن الوصول إلى المعلومات الكائنة داخل النظام المعلوماتي قد يتم إما مباشرةً وذلك عن طريق الدخول إلى نظام الحاسب الآلي، أو بطريقة غير مباشرة وذلك مثلاً عن طريق الإعتراض الإلكتروني للنظام[1]، ويمكن تشبيه الإعتراض الإلكتروني للنظام المعلوماتي بالتنصت على المحادثات التليفونية مثلاً فهو يعني معرفة محتوى أي إتصال قد يتم داخل نظام معلوماتي واحد، أو بين نظامين مختلفين، أو بين عدة أنظمة تربط فيما بينها من خلال شبكة إتصالات محلية أو دولية، وذلك عن طريق ما يعرف "بالإلتقاط الهوائي للمعلومات" التي يتضمنها هذا الإتصال.[2]

والمقصود بالإعتراض الإلكتروني هو إعتراض المعلومات أو بالأحرى إعتراض النظام المعلوماتي، بحيث تعد الوسيلة الأساسية للإعتراض هي وسيلة الإلتقاط الهوائي، ويكون ذلك من خلال إلتقاط الموجات الكهرومغناطيسية *Radiation électromagnétiques* المنبعثة من الحاسب الآلي[3] في مرحلة إنتقال البيانات بين عدد من الحواسيب والأنظمة المعلوماتية، ومعناها عملية جمع المعلومات التي يتم إرسالها من خلال نظام الحاسب الآلي إلى جهات أخرى، فيقوم المعترض بإلتقاط الموجات الكهرومغناطيسية التي تحيط بالحاسب الآلي، والتي يستطيع تحويلها على شاشة عرض يتم توصيلها بجهاز تسجيل –جهاز فيديو– ومن هنا يتم قراءة هذه المعلومات المرسلة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى[4]، ولا يمكن في حالة الإعتراض الإلكتروني، أن يستطيع الجاني تحديد وإختيار المعلومات التي سوف يقوم بإلتقاطها من الجهاز، حيث يلتقط الجاني المعلومات التي يتم إرسالها دون أن يكون له أي دور في تحديدها، كما أن الجاني في هذه الحالة يقتصر دوره على مجرد إلتقاط المعلومات فقط، دون أن يكون بيده أي سلطة على المعلومات

[1]– **نائلة عادل محمد فريد قورة:** المرجع السابق، ص364.

[2]– **أحمد محمود مصطفى،** المرجع السابق، ص257.

[3]– لقد أشار القانون الإماراتي رقم (5 لسنة 2012) إلى ذلك وهذا حين جاء على تعريف مصطلح "إلكتروني" بموجب المادة (13/1) منه بقولها: "كل ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية ...".

[4]– **أحمد محمود مصطفى:** المرجع نفسه، ص258.

من حيث تعديلها سواءً بالحذف أو التغيير فهو يلتقطها كما هي، وهذا على عكس الدخول غير المشروع داخل النظام.[1]

وكذلك من قبيل الإعتراض نجد إلتقاط الإشعاعات الصوتية *Rayonnements vocal* والصادرة عن الكمبيوتر وذلك عن بعد، ومثاله إعتراض الرسائل الإلكترونية المكتوبة والتي ترسل بطريق الحاسوب سواءً بين جهازين عن طريق "شبكة مغلقة محلية *Réseau fermé local*" أو عن طريق "شبكة مفتوحة عالمية *Réseau ouvert mondial*" كالإنترنت[2]، وأيضًا من قبيل الإعتراض نجد إلتقاط الصور عن طريق كاميرات الحاسوب الخاصة بالمجني عليه وذلك من خلال التحكم فيها عن بعد بإستخدام شبكة الإنترنت، كما يشمل الإعتراض أيضًا عملية التنصت على التسجيلات الصوتية أو على محتويات الإتصال كوظيفة من وظائف نظام الحاسوب[3]، وهكذا ينصرف الإعتراض الإلكتروني في معناه الواسع إلى إعادة بناء البيانات والمعلومات المخزنة وتحويلها من بيانات مشفرة إلى بيانات مقروءة أو حتى إلى بيانات مسموعة، وفي كل الحالات قد يتوافق الأمر مع الإلتقاط الهوائي والتنصت المباشر.[4]

غير أن بعض الفقه يرى أنه لا يمكن إعتبار إعتراض وإلتقاط إرسال سلكي أو لاسلكي من نظام إلى نظام آخر من قرب أو عن بعد من قبيل جريمة الدخول أو البقاء غير المشروع في النظام والسبب في ذلك أن المجرم حين يعترض الرسائل الإلكترونية فهو هنا لا يدخل في وظيفة من وظائف النظام، لذا كان من الأجدر –حسب رأيهم– أن يخصص المشرع الجنائي نصًا خاصًا بالإعتراض الإلكتروني والإلتقاط الهوائي، وإن كان ذلك من قبيل جرائم التجسس المعلوماتي التي يقوم بها كثير من المجرمين مستخدمي شبكة الإنترنت لتحقيق ذلك وإن كان فيه مساس كبير بالحياة الخاصة للأشخاص.[5]

---

[1]– **فايز محمد راجح غلاب:** الجرائم المعلوماتية في القانون الجزائري والقانون اليمني، دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2009، ص495.

[2]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص104.

[3]– **طاهر محمود أبو القاسم:** المرجع السابق، ص332.

[4]– **وسيم طعمة:** السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، دمشق، سوريا، المجلد رقم 39، العدد 68، لعام 2017، ص174.

[5]– **فايز محمد راجح غلاب،** المرجع السابق، ص198.

بينما ترى طائفة أخرى من الفقه، أن كل من الإعتراض والإلتقاط ليس من قبيل جريمة الدخول أو البقاء غير المشروع في النظام ولكنهما جريمة من نوع خاص، فالإعتراض لا يتضمن تدخلاً أو دخولاً في نظام معلوماتي معين ولكنه يتمثل في التلصص على الرسائل الإلكترونية المكتوبة أو المسجلة صوتيًا والمرسلة بين جهازين أو أكثر، ثم يتم إلتقاطها بوسائل تكنولوجية حديثة سلكية أو لاسلكية[1]، الأمر الذي يستبعد معه هذا الوصف كنشاط يقصد منه الدخول في النظام نفسه، ومن هنا ظهرت أزمت مسايرة القانون الجنائي لمصطلحات ومعطيات التقدم التكنولوجي وتقنية المعلومات[2].

وما دام أن كل من فعل الإعتراض والإلتقاط هما من قبيل التجسس والتلصص، فهما لا يشكلان ولا يمثلان فعل الدخول أو البقاء غير المشروع في النظام، فهما لا يدخلان في عداد النشاط المعاقب عليه في المساس بسلامة المعلومات الموجودة داخل النظام، وإنما يمكن لكل من الإعتراض والإلتقاط أن يمس كل منها بالمعلومات الموجودة خارج النظام المعلوماتي وليس داخله[3]، وهكذا يرون أن فعل الإعتراض يختلف تمامًا عن فعل الدخول إلى النظام، على إعتبار أن الإعتراض جريمة مستقلة تمامًا تنصب على سلامة المعلومات المعالجة آليًا ولكن خارج النظام المعلوماتي، وهكذا إستبعدت بعض القوانين هذا الفعل من مجال التجريم المعلوماتي.[4]

وفي المقابل ظهر جانب آخر من الفقه الجنائي الحديث، للمطالبة بإدراج فعل الإعتراض والإلتقاط غير المشروع لنظام الحاسب الآلي والشبكات المعلوماتية ضمن جريمة الدخول بغير تصريح في النظام المعلوماتي بإستخدام وسائل تقنية المعلومات.[5]

ولقد أدت هذه الإختلافات بين الدخول إلى النظام وبين إعتراض هذا النظام، إلى الإتجاه نحو إفراد نص خاص لتجريم إعتراض النظام منفصل عن تجريم الدخول غير المصرح به، وقد أوصى المجلس الأوروبي بضرورة إفراد نص خاص لإعتراض النظام بمقتضاه يتم تجريم كل

---

[1]- ***HERBERT (M) :*** *droit de l'informatique et des télécommunication Ed, litec, Paris, France, 1989, p855.*

[2]- ***QUÉMÉNER (M), CHARPENEL (Y) :*** *Cybercriminalité et droit pénal appliqué, économica, Paris, France, 2010, P218.*

[3]- ***LARGUIER (J), CONTE (PH), FOURNIER (S) :*** *Droit pénal spécial, Op. Cit, P288.*

[4]– **وسيم طعمة:** المرجع السابق، ص168.

[5]– **وسيلة تقنية المعلومات:** كمصطلح ذكر لأول مرة بموجب المادة (10/1) من القانون الإماراتي رقم (5 لسنة 2012) بقولها: "أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين".

إعتراض أو إلتقاط لإتصال يتم من وإلى، أو يتم داخل نظام الحاسب الآلي نفسه، أو داخل شبكة للإتصالات.[1]

على إثر ذلك جاءت الإتفاقية الأوروبية الموقعة بمدينة بودابست بدولة المجر عام 2001 والمتعلقة بمكافحة الإجرام المعلوماتي[2] وذلك بموجب المادة الثالثة منها تحت عنوان "الإعتراض غير القانوني" بقولها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل إعتبارها جريمة جنائية، وفقًا لقانونه الداخلي، واقعة الإعتراض العمدي وبدون وجه حق، من خلال وسائل فنية للإرسال غير العلني، لبيانات الحاسب، في مكان الوصول، في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك الإنبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب ان ترتكب الجريمة بنية إجرامية بقصد الغش، أو أن ترتكب الجريمة في حاسب آلي متصلاً عن بعد بحاسب آخر".[3]

كما نصت الإتفاقية العربية لعام 2010 والموقعة بمدينة القاهرة بدولة مصر العربية بشأن مكافحة جرائم تقنية المعلومات[4]، حين عرَّفت مصطلح "الإلتقاط" بموجب المادة (8/2) بقولها: "الإلتقاط، مشاهدة البيانات أو المعلومات أو الحصول عليها".

كما ذكرت المادة السابعة من نفس الإتفاقية تحت عنوان "جريمة الإعتراض غير المشروع" بقولها: "الإعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو إستقبال بيانات تقنية المعلومات".[5]

وعلى إثر هاتين الإتفاقيتين قامت بعض القوانين المقارنة بالنص صراحةً على الإعتراض الإلكتروني والإلتقاط الهوائي للإتصالات والمراسلات الإلكترونية بين جهازين أو أكثر من

---

[1]– **أحمد محمود مصطفى:** المرجع السابق، ص259.

[2]– حرص المجلس الأوروبي على التصدي للإستخدام غير المشروع للحاسبات الآلية والشبكات المعلوماتية، وتجلى ذلك في إبرام إتفاقية بمدينة "بودابست" والموقعة في 23 نوفمبر 2001 في شأن الإجرام الكوني بمعنى مكافحة الإجرام المعلوماتي، وتتكون هذه الإتفاقية من (48) مادة.

[3]- ***Article (3) Interception illégale :*** *« chaque partie adopté les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne l'interception intentionnel et sons droit, effectuée par des moyens techniques, de données informatiques, lors de transmission non publique, à destination, en provenant ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenance d'un système informatiques. Transportant de telles données informatique, une partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique ».*

[4]– الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي حررت بمدينة القاهرة في جمهورية مصر العربية بتاريخ 21 ديسمبر 2010.

[5]– راجع المادة السابعة من الإتفاقية العربية، المشار إليها أعلاه. أنظر في ذلك: **الملحق رقم (02).**

الحواسيب وهذا من خلال الشبكات التي تربط بين تلك الأجهزة، حيث تنبهت بعض التشريعات الجنائية إلى ضرورة الإسراع في إيراد نص قانوني خاص لتجريم هذه الصورة من صور النشاط المعلوماتي غير المشروع، وذلك بمعاقبة كل من يعترض أو يتسبب في إعتراض وإلتقاط المعلومات بدون وجه حق وبسوء نية، وبأي طريقة كانت إلكترونية أو رقمية أو حتى ضوئية.[1]

وفعلا جَرَّمت بعض القوانين فعل إعتراض المعلومات أو إلتقاطها في حالة إنتقالها وذلك بموجب نصوص خاصة، ولعل من بين هذه القوانين نجد على سبيل المثال:

أ- القانون الأمريكي: لقد نص القانون الأمريكي لعام 1992 والمتعلق بجرائم الكمبيوتر والإنترنت، والذي إعتبر أن إلتقاط بيانات من نظام كمبيوتر أو شبكة معلوماتية، يعد ذلك بمثابة جريمة دخول غير مشروع في النظام المعلوماتي، حيث جعل هذا القانون من فعل الإعتراض والإلتقاط للرسائل الإلكترونية من ضمن أفعال الدخول غير المشروع نفسه، وذلك "إحترامًا وحمايةً للحق في نقل البيانات *The right of privacy of data communication*"[2]، وأن المساس بها يعتبر "إنتهاكا للحق في احترام الاتصالات *The privacy of communications*"[3]، مثل التنصت والتسجيل التقليدي للمحادثات التليفونية وكل أشكال إلتقاط النقل الإلكتروني للبيانات، سواء تم هذا النقل عن طريق التليفون أو الفاكس أو البريد الإلكتروني، وهذه الجريمة منصوص عليها في المادة الثالثة من هذا القانون، حين تعريفها لفعل الدخول بدون وجه حق في النظام بقولها: "هو كل وسيلة للولوج والإطلاع، أو لإعطاء تعليمات أو الإتصال أو لتخزين بيانات أو لإستعادة بيانات أو إلتقاط وإعتراض بيانات مرسلة ..."[4]، وهذه المادة تؤكد على وجوب إحترام المراسلات والإتصالات الإلكترونية وحماية حرية تنقلها.

ب- القانون البرتغالي: وفي نفس السياق جرم القانون البرتغالي رقم (109 لسنة 1991) والمعدل بالقانون رقم (94 لسنة 2009) والمتعلق بالجرائم المعلوماتية، وذلك بموجب المادة السابعة منه والتي تجرم وبشكل صريح كل إعتراض لعمليات الإتصال أو إلتقاط المعلومات أثناء إنتقالها داخل أنظمة الحاسبات الآلية أو خارجها بإستخدام وسائل تقنية المعلومات أو الشبكات المعلوماتية، كما حدد هذا القانون المقصود بمصطلح "الإعتراض" والتي جاء نصها: "الإعتراض هو كل عمل يهدف إلى

---

[1]- **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص101.

[2]- والتي تقابلها باللغة الفرنسية: "*Le droit au respect des données transmises*".

[3]- ويقابل ذلك في المصطلح الفرنسي: "*Le droit ou respect des communications*".

[4]- أنظر في ذلك قانون ولاية تكساس الأمريكية لسنة 1985 والمعدل في سنة 1992 والمتعلق بجرائم الكمبيوتر والإنترنت، والمتاح على الموقع التالي: **http://www.statutes.legis.state.tx.us/docs/pe/htm/pe.33.htm**، تاريخ التصفح: 2019/05/25.

الوصول للمعلومات التي تتضمنها أنظمة المعالجة الآلية للمعطيات بإستخدام أجهزة كهرومغناطيسية أو ميكانيكية أو غير ذلك من التقنيات الحديثة".[1]

ج- القانون السوداني: نص القانون السوداني رقم (13 لسنة 2007) والمتعلق بقانون الجرائم المعلوماتية وذلك بموجب نص المادة (1/3) منه، حيث عرّفت مصطلح "الإلتقاط" بقولها: "مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها"[2].

د- القانون العماني: كما نص القانون العماني رقم (12 لسنة 2011) بموجب المادة (13/1) منه حيث عرفت مصطلح "الإلتقاط" بقولها: "مشاهدة البيانات أو المعلومات الإلكترونية أو الحصول عليها"، كما نصت المادة (8) من نفس القانون على تجريم فعل "الإعتراض" بقولها: "يعاقب ... كل من إعترض عمدًا أو بدون وجه حق بإستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو إستقبالها أو تنصت عليها".[3]

هـ- القانون السوري: ذكر أيضًا القانون السوري رقم (17 لسنة 2012) جريمة إعتراض المعلومات وذلك بموجب المادة (18) منه بقولها: "يعاقب ... كل من إعترض أو إلتقط قصدًا بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها".[4]

و- القانون الإماراتي: كما جاء في سياق القانون الإماراتي رقم (5 لسنة 2012) حيث عرّف مصطلح "الإلتقاط" بنص المادة (17/1) بأنه: "مشاهدة البيانات أو المعلومات أو الحصول عليها"، كما نصت المادة (1/15) منه بقولها: "يعاقب ... كل من إلتقط أو إعترض عمدًا وبدون تصريح أي إتصال عن طريق أي شبكة معلوماتية".[5]

ز- القانون الأردني: كما نجد القانون الأردني رقم (27 لسنة 2015) هو الآخر نص بموجب المادة الخامسة منه: "يعاقب كل من قام قصدًا بإلتقاط أو بإعتراض أو بالتنصت أو إعاقة أو حوَّر أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات".[6]

---

[1]- راجع الموقع التالي: ***http://www.usdoj.gov/criminal/cybercrime/maxwelleplea.htm***، متاح بتاريخ: 23-06-2019.

[2]- أنظر في ذلك القانون السوادني رقم (13 لسنة 2007).

[3]- أنظر في ذلك القانون العماني رقم (12 لسنة 2011).

[4]- راجع أيضًا القانون السوري رقم (17 لسنة 2012).

[5]- أنظر في ذلك القانون الإماراتي رقم (5 لسنة 2012).

[6]- أنظر أيضًا القانون الأردني رقم (27 لسنة 2015).

ح- **القانون المصري:** وهنا أيضًا ذكر القانون المصري رقم (175 لسنة 2018) تعريف لمصطلح "الإعتراض"[1]، وذلك بموجب المادة (17/1) بقوله: "مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الإستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق". بينما نصت المادة (16) منه تحت عنوان "جريمة الإعتراض غير المشروع" بقولها: "يعاقب ... كل من إعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكها".[2]

خامسًا: الإختراق *Piratage*

مصطلح الإختراق من أبرز ما أنتجته تكنولوجيا تقنية المعلومات، وهو من أخطر صور الدخول غير المشروع والمخالف لأحكام الترخيص للوصول إلى النظام المعلوماتي ومحتوياته[3]، فالإختراق عمومًا هو عبارة عن عملية دخول غير مصرح بها لأجهزة الغير وشبكاتهم وصفحاتهم الإلكترونية، وذلك بواسطة برامج جد متطورة يستخدمها كل من يملك خبرة في إستعمالها[4]، بحيث لم يحدد المشرع الجنائي الوسيلة أو الطريقة التي يتم بها الدخول إلى النظام المعلوماتي، لذا تتسع كلمة الدخول أو الولوج على إطلاقها لتشمل كافة فنيات الدخول بطريق الغش والإحتيال في منظومة معلوماتية محمية كانت أم غير محمية[5]، لذا يتفق كل الباحثين والدارسين في هذا المجال أن أهم شكل يتخذه الدخول غير المشروع هو ما يطلق عليه في عالم الإنترنت "بالإختراق *Piratage*"[6].

والإختراق كما قيل عنه: "أنه إمكانية الدخول بالقوة إلى النظم المعلوماتية للوصول لأهداف معينة بطرق غير شرعية، مستغلاً في ذلك ثغرات موجودة في نظم الحماية الأمنية"[7]، وبذلك فهو

---

[1]- هنا مصطلح الإعتراض وقع سهوًا من المشرع المصري وإنما المقصود هنا هو مصطلح "الإلتقاط" مثل ما فعله بقية المشرعين العرب في تعريفهم للإلتقاط.

[2]- أنظر في ذلك القانون المصري رقم (175 لسنة 2018).

[3]- **محمد علي سويلم:** المرجع السابق، ص270.

[4]- ***FOREST (D) et KAUFMAN (G) :*** *Droit de l'informatique, édition gualino extenso, Paris, France, 2010, P95.*

[5]- **أحسن بوسقيعة:** الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، ط14، ج1، 2012، ص453.

[6]- ***El AZZOUZI Ali:*** *La cybercriminalité au maroc 1ere Ed (Bishoop Solution) casablanca, Maroc, 2010, P42.*

[7]- **فخري محمود خليل:** جرائم البلطجة الإلكترونية تتحدى التشريعات والقضاء وتدعم المجرم والجريمة المستحدثة، دراسة مقارنة، د.د.ن 2019، ص170.

أشهر أنواع المخاطر المعلوماتية وأكثرها إنتشارًا، لأن المخترق إذا ما نجح في عملية إختراق الجهاز فإنه بذلك يستطيع فعل أي شيء يريده كالتنصت والتجسس والتزوير وغيرها[1]، وهي سمة سيئة يتسم بها المخترق، وذلك لقدرته على دخول أجهزة الآخرين عنوة ودون رغبة منهم.[2]

وعملية الإختراق لأنظمة الحاسوب أو النظام المعلوماتي غالبًا ما تتم عبر شبكة الإنترنت، لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة العالمية، وعادةً ما يتم الإختراق عبر شبكات محلية يرتبط فيها أكثر من جهاز حاسوب[3]، بحيث يستطيع من خلالها المخترق التطفل والوصول إلى أجهزة الآخرين بسهولة وذلك عن طريق معرفة الشفرات والأكواد السرية الموجودة في ذلك النظام[4]، وهذا من خلال برامج متطورة يستخدمها القراصنة أو كل من يملك خبرة في إستعمالها مثل القنابل المنطقية والفيروسات أو بواسطة الإغراق بالرسائل[5]، وغيرها.

وبهذا المعنى ينقسم الإختراق إلى ثلاثة أقسام هي:

أ- إختراق الأجهزة الخادمة: بحيث يتم ذلك عن طريق المحاكاة بإستخدام مسارات المصدر، وفيها يتم إعطاء حزم عناوين "*IP*" شكلاً معيناً لتبدو وكأنها صادرة عن حاسوب مصرح له بالدخول[6].

ب- التعرض للبيانات أثناء إنتقالها: بحيث تتم هذه الطريقة من خلال التعرف مثلاً على أرقام البطاقات الإلكترونية أثناء إستعمالها من طرف العميل كإستخدام بطاقة الإئتمان في مراكز التسويق والبنوك وغيرها، حيث يقوم الجاني بإستعمال هوية مؤسسة مالية وبريدها الإلكتروني ثم يقوم بإرسال رسالة إلكترونية للمجنى عليه يطلب منه حجز بياناته المصرفية، ثم يقوم الجاني بإستعمال هذه البيانات لسحب أموال المجنى عليه.[7]

---

[1]- **طارق عبد الله الشدى:** آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، السعودية، 2000، ص274.

[2]- **سليمة سعيدي، بلال حجاز:** المرجع السابق، ص96.

[3]- **فخري محمود خليل:** المرجع السابق، ص178.

[4]- **يعتمد الإختراق *Piratage***: على السيطرة عن بعد بما يعرف *Remote*، وهي لا تتم إلا بوجود عاملين مهمين، الأول يعرف بالعميل *Client* وهو البرنامج المسيطر، والثاني هو الخادم *Server* الذي يقوم بتسهيل عملية الإختراق ذاتها، بمعنى أنه لابد من توفر برنامج على كل من جهازي المخترق والضحية، ففي جهاز الضحية يوجد برنامج الخادم أما في جهاز المخترق يوجد برنامج العميل، إلا أنه قد تختلف طرق وأسس الإختراق بإختلاف الأجهزة والنظم المراد إختراقها ووسائل هذا الإختراق، ولكنها جميعها تعتمد على فكرة توفير إتصال عن بعد بين جهازي كل من الضحية والمخترق. (أنظر أكثر: - **سليمة سعيدي، بلال حجاز:** المرجع السابق، ص96).

[5]- وهي إحدى أهم طرق إختراق الحاسوب، وذلك يتم عن طريق إرسال كم هائل من الرسائل عبر البريد الإلكتروني بهدف تعطيل نظام الحماية عن العمل، بحيث تتسبب هذه الرسائل في غلق منافذ الإتصال وملئ قوائم الإنتظار. (أنظر: - **منير محمد الجهيني، ممدوح محمد الجهيني:** المرجع السابق، ص181).

[6]- ***El AZZOUZI Ali:*** *La cybercriminalité,Op. Cit, P47.*

[7]- **يزيد بوحليط:** المرجع السابق، ص181.

ج- إختراق الأجهزة الشخصية: وهي الطريقة الأكثر شيوعًا وإنتشارًا في مجال تقنية المعلومات نظرًا لتوفير الأسواق والمحلات التجارية العديد من أنواع وأشكال أجهزة وبرامج الإختراق والتي يمكن أن يقتنيها المجرم بسهولة من هذه الأماكن.[1]

وكثيرًا ما تنشأ الجرائم المعلوماتية وتتحقق داخل الفضاء الإفتراضي، وهذا من خلال الإختراق لحدود الحاسب الآلي أو المواقع والصفحات الإلكترونية الموجودة على الشبكة العنكبوتية، وذلك بغية مباشرة مجموعة من الأنشطة اللامشروعة، والتي من أبرزها:

- دخول الجاني لصفحات المواقع الإلكترونية والإطلاع على البيانات والمعلومات الموجودة بداخلها دون أن يكون مصرحًا له بذلك.
- الدخول إلى ساحة النظم الحاسوبية وشبكة الهواتف بأنواعها لإستغلال الموارد المالية الموجودة بداخلها وتحويلها إلى حسابات مجهولة.
- التلاعب بالبيانات والعبث فيها وتغيير محتويات ملفات الغير الإلكترونية.
- تزوير المعلومات أو تزييفها أو نقلها ونشرها، ولربما إتلافها بالمرة، وتدمير قواعد البيانات والبرمجيات والنظم التطبيقية.
- سرقة البرامج أو إستغلالها دون وجود إذن مسبق بذلك.
- فك الرموز والكلمات السرية وكسر الحواجز الأمنية، وإستكشاف مواطن الضعف في جهاز الحاسوب أو نظام الشبكة المعلوماتية.
- فك شفرات البرمجيات التطبيقية المحمية أو الملفات المشفرة.
- مباشرة أعمال القرصنة على الخدمات العامة والخاصة والمتاحة على المواقع الإلكترونية.
- زج الفيروسات الحاسوباتية لإحداث خلل في آداء وظيفة المنظومة وإتلاف مواردها المعلوماتية.
- تهريب موارد معلوماتية من نظام إلى آخر.
- إحداث ثغرات في النظام المعلوماتي تمهيدًا للكشف عن مواطن الخلل والضعف به.
- ممارسة أنشطة إرهابية بمختلف مستوياتها ضد أمن الدولة أو المؤسسات أو الأفراد.
- ممارسة الإبتزاز الإلكتروني والترويع والإباحية.[2]

---

[1]- ***El AZZOUZI Ali:*** *La cybercriminalité, Op. Cit, P*50.

[2]- لمزيد من التفصيل حول هذا الموضوع يراجع في ذلك كل من: **(- عبد الله الكرجي، صليحة حاجي:** التعاقد الرقمي ونظم الحماية الإلكترونية، مطبعة الأُمنية، الرباط، المغرب، 2015، ص131-132. - **عبد الفتاح بيومي حجازي:** التجارة الإلكترونية العربية، الكتاب الثاني، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة، مصر، 2003، ص115).

وعلى العموم إذا كان المخترق غير مخرب ولا يبتغي إحداث أي ضرر أو إرتكاب أي نشاط من الأنشطة السالف ذكرها، ففي هذه الحالة يعد مجرم هاوي *Hacker*، أما عندما يقوم المخترق بإحداث ضرر وإرتكاب نشاطات غير مشروعة فهو مجرم محترف *Cracker*.[1]

في الأخير يمكننا القول أن مصطلح "الإختراق" لم يأخذ حصته من القانون الجنائي، ولم يعرفه المشرع الجنائي بوضوح، ما عدا ما جاءت به بعض التشريعات مثل التشريع المصري من خلال القانون رقم (175 لسنة 2018) وذلك بمـــوجب المادة (18/1) منه بقولها: "الإختراق هو الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حساب آلي أو شبكة معلوماتية وما في حكمها"[2]. وهكذا ومن خلال هذا النص القانوني نجد أن مصطلح "الإختراق" هو الترجمة السليمة لفعل الدخول أو البقاء غير المشروع داخل النظام.

الفرع الثاني: التعريف الفقهي للجريمة

ذكر العديد من الفقهاء والباحثين والدارسين في مجال الإجرام المعلوماتي بعض المحاولات التي قيلت بشأن تعريف جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي والتي سوف نذكر هنا البعض منها:

– عُرِّفت هذه الجريمة بأنها: "الولوج داخل النظام المعلوماتي أو البقاء فيه بغير تصريح من المسؤول عنه، وذلك إضرارًا إما بسرية أو سلامة أو تكامل أو موفورية هذا النظام ومحتوياته".[3]

– وعرفها آخرون بأنها: "عملية الولوج غير الشرعي إلى نظام التشغيل في الحاسب الآلي من قبل أشخاص لا يملكون صلاحية هذا الدخول أو التواجد، وذلك بهدف القيام بأعمال غير قانونية كالتجسس أو السرقة أو التلاعب أو التخريب، مع الأخذ بعين الإعتبار قدرة هؤلاء الأشخاص على نقل أو مسح أو إضافة ملفات أو برامج لم تكن موجودة من قبل في النظام، وكذا قدرتهم على التحكم بنظام التشغيل وإعطاء الأوامر له".[4]

---

[1]– **فخري محمود خليل:** المرجع السابق، ص171.

[2]– أنظر في ذلك نص المادة (18/1) من القانون المصري رقم (175 لسنة 2018).

[3]– **محمد خليفة:** جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2011، ص15.

[4]– **عزيزة رابحي:** المرجع السابق، ص161. – **رشيدة بوكر:** المرجع السابق، ص178.

– وجاء تعريفها أيضًا: "كل عمليات الولوج إلى المعلومات السرية بواسطة الإختراق الذي يحدث للنظام المعلوماتي بأكمله أو لجزء منه وذلك عن طريق التوصل للأرقام أو الكلمات أو الحروف أو الشفرات التي بواسطتها يفتح الجهاز من أجل الوصول إلى المعطيات المخزنة داخله".[1]

– وهناك من عرَّفها بأنها: "ذلك الدخول المجرد إلى النظام المعلوماتي، إذ أن هذا الدخول يمكن أن يترتب عليه الوصول إلى البيانات السرية والإطلاع عليها أو حتى إستخدامها مجاناً بما يجعله مخالفاً للقانون".[2]

– وقالوا عنها أيضًا بأنها: "كل إساءة لإستخدامات الحاسب الآلي وما في حكمه عن طريق شخص غير مرخص له بإستخدامه والدخول إليه والبقاء بداخله بغية الوصول إلى المعلومات والبيانات المخزنة بداخله، أو حتى لمجرد التسلية والرغبة في الإستطلاع".[3]

– كما عرّفوها أيضًا بأنها: "الدخول غير المصرح به مسبقًا إلى أنظمة المعالجة الآلية للمعطيات والتي تقع عدواناً على سرية المعلومات الموجودة بداخلها، والتي تتم بغض النظر عمّا تم الإطلاع عليه من معلومات داخل هذا النظام، وبغض النظر عن طبيعة هذه الأخيرة".[4]

– وذكرت بأنها: "كل دخول أو تواجد داخل نظام المعالجة الآلية للمعطيات، ضد إرادة من له الحق في السيطرة والمسؤولية على هذا النظام".[5]

– عرفت كذلك أنها: "الولوج غير المرخص به وبأي شكل من الأشكال غير المشروعة مع إمكانية البقاء داخل نظام المعالجة الآلية للبيانات وذلك بإستخدام الحاسب الآلي ونظام الشبكة المعلوماتية.[6]

– كما قالوا عنها بأنها: "إساءة إستخدام الحاسب الآلي من طرف شخص غير مسموح له بالدخول إليه أصلاً ومع إمكانية التواجد داخله، وذلك في سبيل الحصول على معلومات أو معطيات لها علاقة بسرية وخصوصية ذلك النظام وصاحبه".[7]

---

[1]– **بلال أمين زين الدين:** المرجع السابق، ص259.

[2]– **عبد الله هلالي:** المرجع السابق، ص69.

[3]– ***SIEBER (U) :*** *Les crimes informatiques, Op. Cit, P48.*

[4]– ***LINANT (Xav), HOLLANDE (Al) :*** *Pratique du droit de l'informatique, 5eme Ed, Dalloz, Paris, France, 2002, P57.*

[5]– **عبد المجيد جباري:** دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، 2012، ص111.

[6]– **فتحي محمد أبو عزت:** الحماية الجنائية الموضوعية والإجرائية للإعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007، ص128.

[7]– ***GASSIN (R) :*** *Le droit pénal de l'informatique, les systèmes de traitements automatique des données, commentaire de la loi N° (88-18) du 03/01/1988 relative à la fraud informatique, (J.C.P) Oct 1988, P 35.*
– ***DEVEZE (J) :*** *Les qualifications pénales applicables aux fraudes informatiques, Op. Cit, P 76.*

– وعرَّفوها أيضاً بأنها: "كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة والسيطرة على المعلومات التي يتكون منها أو حتى الخدمات التي يقدمها".[1]

– ومنهم من عرَّفها بأنها: "كل أنواع إساءة إستخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له بإستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله لإستعمالها في أغراض غير مشروعة إضرارًا بالغير".[2]

– وآخر تعريف ما ذكره الفقه الفرنسي ونحن نؤيد بدورنا هذا التعريف، والذي جاء فيه: "كل أشكال الولوج إلى المعلومات المعالجة آلياً والمخزنة داخل النظام المعلوماتي بدون رضا المسؤول عن هذا النظام، سواء كان ذلك بالدخول المجرد دون نية القيام بأي فعل آخر، أو بالدخول المقصود بنية القيام بأعمال العبث أو الإتلاف أو غير ذلك من الأفعال المجرمة".[3]

الفرع الثالث: التعريف القانوني للجريمة

تطرقت الكثير من التشريعات الجنائية المقارنة ومنذ وقت مبكر –لاسيما الأوروبية منها– إلى مسألة تعريف جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، وذلك بشكل ممهد لفهم بقية الصور الإجرامية المعلوماتية الأخرى[4]، الأمر الذي جعل من المشرع الجنائي في كل دولة ينظر إلى هذه الجريمة من زاويته الخاصة، لاسيما من حيث تعريفها القانوني، حتى وإن لم يختلفوا من حيث الوسائل المستخدمة في إرتكابها، لذا سوف نركز هنا على ما جاءت به الإتفاقيات الدولية من تعاريف بخصوص هذه الجريمةّ، ثم يليها القوانين الوطنية.

أولاً: في الإتفاقيات الدولية

من بين أهم الإتفاقيات الدولية التي تناولت تعريف هذه الجريمة من منظور قانوني نجد الإتفاقية الأوروبية للإجرام المعلوماتي، وكذا الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

---

[1]– **نائلة عادل محمد فريد قورة:** المرجع السابق، ص343.

[2]– **خالد ممدوح إبراهيم:** المرجع السابق، ص84.

[3]– ***GUAY (Pj) :*** *« la relation intelligence crime » le cas de d élinquants esxuels sous juridication fédérale, ph (D) thèse, universit é de montréal, France, 2001, P23.*

[4]– معظم التشريعات الجنائية الحديثة والتي تناولت مسألة الإجرام المعلوماتي، فإنها تعتبر جريمة الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي بأنها جريمة قائمة بذاتها، والتي يترتب على إتيانها عدد لا بأس به من جرائم تقنية المعلومات والتي من بينها العبث بالمعلومات أو التلاعب بها أو حتى إتلافها أو تزويرها أو سرقتها، أو القيام بإبتزاز أصحابها أو التشهير بهم، أو التجسس على خصوصيتهم، وغيرها كثير من الجرائم المعلوماتية والتي لا يمكن حصرها.

أ- الإتفاقية الأوروبية للإجرام المعلوماتي: حرص المجلس الأوروبي على التصدي لكل الإستخدامات غير المشروعة للحاسبات الآلية ونظم الشبكات المعلوماتية، ويتجلى ذلك في إتفاقية "بودابست" المشار إليها والموقعة في 23 نوفمبر 2001 والمتعلقة بما أطلق عليه وقتها "بالإجرام الكوني*Cyber Criminalité*" بمعنى الإجرام المعلوماتي، وهذا إيمـــاناً من الدول الأعـــضاء في هـــذا المـــجلس والدول الأخـــرى الموقعـــة على هذه الإتفاقـــية بحجم التغيرات التي حدثت بسبب الـــعولمة والرقمـــية *La mondialisation et numérisation*، ناهيك عن التطور الهائل في تكنولوجيا الإتصالات الذي أحدثته ومازالت تحدثه.

ومن هنا نصت هذه الإتفاقية على تعريف هذه الجريمة بموجب المادة الثانية منها تحت عنوان "الولوج غير القانوني *Accés illégal*" والتي جاء نصها كما يلي: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل إعتبارها جريمة جنائية، وفقًا لقانونه الداخلي، للولوج العمدي لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر".[1]

وعلى الرغم من أن هذه الإتفاقية جاءت بتعريف قانوني لهذه الجريمة بصورة ضمنية وليست صريحة، إلاَّ أنه يبقى هذا التعريف يمثل تلك الأرضية الخصبة التي نبتت وترعرعت عليها معظم القوانين الوطنية الأخرى في تعريفها لهذه الجريمة.

ب- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: الدول العربية هي الأخرى سعت سعيها تحت غطاء جامعة الدول العربية، وذلك رغبة منها في تعزيز التعاون العربي في مكافحة الإجرام المعلوماتي والذي أصبح بشكل أو بآخر يهدد أمن ومصالح وسلامة المجتمعات العربية، لذا تم التوقيع على إتفاقية عربية لمكافحة جرائم تقنية المعلومات بتاريخ 21 ديسمبر 2010 بمدينة القاهرة، ومن جملة ما نصت عليه هذه الإتفاقية هو تعريف هذه الجريمة، وذلك بموجب نص المادة السادسة تحت عنوان "جريمة الدخول غير المشروع" والتي جاء نصها: "الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به، وتشدد العقوبة إذا ترتب على هذا

[1]- راجع نص المادة الثانية من إتفاقية بودابست. **الملحق رقم (01)**

الدخول أو البقاء أو الإتصال أو الإستمرار بهذا الإتصال، محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الإتصال وإلحاق الضرر بالمستخدمين والمستفيدين، أو الحصول على معلومات حكومية سرية".[1]

ثانيًا: في القوانين الوطنية

كثيرةٌ هي القوانين الوطنية – الأوروبية والعربية – التي لم تتناول تعريف هذه الجريمة بشكل واضح وصريح بعيدًا عن ربطها بالعقوبة المقررة لها ما عدا بعض القوانين كالقانون الكويتي مثلاً والذي عرّفها بشكل واضح وصريح، وما عدا ذلك من قوانين فكلها كانت عبارة عن نصوص تجريمية وعقابية وفي نفس الوقت جاءت تعرف هذه الجريمة، ومن جملة هذه القوانين نجد على سبيل المثال:

أ- القانون الكويتي: عرف القانون الكويتي رقم (63 لسنة 2015) والمتعلق بمكافحة جرائم تقنية المعلومات، هذه الجريمة بموجب المادة (12/1) منه تحت عنوان "الدخول غير المشروع"، بقولها: "النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال إختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".[2]

ب- القانون العماني: كما ذكر القانون العماني رقم (12 لسنة 2011) هذه الجريمة بموجب المادة الثالثة منه بقولها: "... كل من دخل عمدًا وبدون وجه حق موقعًا إلكترونيًا أو نظامًا معلوماتيًا أو وسائل تقنية المعلومات أو جزءًا منها أو تجاوز الدخول المصرح به إليها أو إستمر فيها بعد علمه بذلك".[3]

ج- القانون الإماراتي: كما نص القانون الإماراتي رقم (5 لسنة 2012) بموجب نص المادة الثانية منه: "... كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة".[4]

د- القانون السوري: كذلك نص القانون السوري رقم (17 لسنة 2012) على تعريف هذه الجريمة بموجب نص المادة (15) منه تحت عنوان "الدخول غير المشرع إلى منظومة معلوماتية" بقوله:

---

[1]- راجع الفقرة الأولى والثانية من نص المادة السادسة من الإتفاقية العربية. **الملحق رقم (02)**

[2]- راجع المادة (12/1) من القانون الكويتي رقم (63 لسنة 2015).

[3]- راجع المادة (3) من القانون العماني رقم (12 لسنة 2011).

[4]- راجع المادة (2) من القانون الإماراتي رقم (5 لسنة 2012).

"...كل من دخل قصدًا بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك".[1]

هـ- القانون الأردني: كما عرّف القانون الأردني رقم (27 لسنة 2015) هذه الجريمة بموجب نص المادة (1/3) منه بقولها: "... كل من دخل قصدًا إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح".[2]

و- القانون المصري: وذكر أيضًا القانون المصري رقم (175 لسنة 2018) هذه الجريمة تحت عنوان "الدخول غير المشروع" وذلك بموجب نص المادة (14) منه بقوله: "... كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".[3]

ثالثًا: موقف المشرع الجزائري

المشرع الجزائري يعتبر من أول المشرعين العرب الذين حاولوا تعريف هذه الجريمة، هذا لو قارناه ببعض القوانين العربية، لاسيما من حيث سبقية الصدور، حيث جاء في نص المادة (394 مكرر) من القانون رقم (15 لسنة 2004) والتي جاء فيها: "... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"[4]، والتي تقابلها بنفس الصياغة ما ذكرته المادة (323-1) من قانون العقوبات الفرنسي.[5]

---

[1]- راجع المادة (15) من القانون السوري رقم (17 لسنة 2012).

[2]- راجع المادة (1/3) من القانون الأردني رقم (27 لسنة 2015).

[3]- راجع المادة (14) من القانون المصري رقم (175 لسنة 2018).

[4]- لقد إستحدث المشرع الجزائري ضمن قانون العقوبات (القسم السابع مكرر) تحت عنوان "المساس بأنظمة المعالجة الآلية للبيانات"، وذلك بموجب القانون رقم (04-15) والمؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، ثم عدل وتمم بموجب القانون رقم (06-23) والمؤرخ في 20 ديسمبر 2006، ثم عدل وتمم بموجب القانون رقم (16-02) والمؤرخ في 19 يونيو 2016، حيث تضمن هذا القسم المواد من (394 مكرر حتى 394 مكرر 8).

[5]- ***Article 323-1 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 :***

« - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

كما يلاحظ من تعريف المشرع الجزائري أنه أول من جرم المحاولة والشروع في إرتكاب هذه الجريمة بصريح العبارة كما سوف يأتي معنا بيانه.

رأي الباحث:

رغم كل ما قيل في جريمة الإعتراض من نصوص قانونية خاصة وصريحة، ومع ذلك لم يلقى كل من فعل الإعتراض الإلكتروني والإلتقاط الهوائي نفس الإهتمام الذي لقيه فعل الدخول إلى النظام المعلوماتي بغير تصريح، فمن القوانين مثلاً لم تجرم الإعتراض أو الإلتقاط للمعلومات ولم تأتي على ذكره لا في قانون العقوبات ولا في قوانين خاصة ومثالها المشرع الجزائري[1]، وهناك قوانين أخرى ذكرت صورة الإعتراض في معرض حديثها عن تجريم فعل الدخول غير المشروع، فيما خصصت بعض التشريعات نصًا خاصًا وصريح لكل من الإعتراض والإلتقاط، وحسناً فعلوا في ذلك.

وعليه نجد أن الموقف التشريعي لم يكن واحدًا في جميع الدول فيما يتعلق بتجريم فعل الإعتراض والإلتقاط، وبخصوص ذلك أشارت المذكرة التفسيرية لإتفاقية بودابست من أن: "الإعتراض غير القانوني ربما يكون في بعض البلدان مرتبطًا بدقة بجريمة الولوج غير المشروع للنظام المعلوماتي"[2]، وبناءًا عليه ذهبت بعض التشريعات إلى عدم تخصيص نص قانوني لفعل الإعتراض والإلتقاط غير المشروع، إلاَّ أنها في المقابل أعطت مفهومًا موسعًا لفعل الدخول، مما يسمح شموله للإعتراض والإلتقاط غير القانوني للمعلومات أثناء إنتقالها بإعتبار أنها في النهاية تمثل إنتهاكًا للحق في الإتصال المعلوماتي بين النظم والحواسيب المختلفة أثناء عملية التواصل، كما هو الحال بالنسبة للمشرع الجزائري والذي سار على نفس نهج المشرع الفرنسي.

---

[1]– لم يتطرق المشرع الجزائري لموضوع الإعتراض الإلكتروني والإلتقاط الهوائي لا في قانون العقوبات حين تكلم عن المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم (04-15)، ولا في قوانين خاصة لاسيما القانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. وإنما ذكر شيء من صور الإلتقاط في القسم الخامس من قانون العقوبات المتعلق "بالإعتداءات على شرف وإعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار" وهذا ما جاء في القانون رقم (06-23)، لاسيما بموجب المواد (303، 303 مكرر، 303 مكرر1، 303 مكرر2، 303 مكرر 3) منه، حيث نص في المادة (303 مكرر) على أنه:

"– يعاقب ... كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك: بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

– بإلتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه ...".

[2] – *« L'interception peut être étroitement liee à l'infraction d'accées non autorisé à un système informatique ».*

كما يتبين لنا من جملة هذه المصطلحات المتداولة في مجال جرائم تقنية المعلومات، بإعتبارها مرادفات لجريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، أنه من الصعوبة بمكان إيجاد مصطلح شامل يعبر عن هذه الحالة الجرمية المرتكبة، فإذا وصفنا مصطلح ما بعينه بأنه جريمة دخول، فليس بالضرورة أن يكون هذا المصطلح هو جريمة في حد ذاته، وإنما دوره يقتصر فقط على التعبير على جريمة الدخول أو البقاء غير المشروع، وأن هذه المصطلحات وغيرها كثير ما هي إلاَّ سلوكيات إجرامية يقوم بها المجرم المعلوماتي في المساس بأنظمة المعالجة الآلية للمعطيات بطريقة غير مشروعة.

كما يتبين لنا أيضًا من خلال كل التعاريف الإصطلاحية والفقهية والقانونية لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي، أنها قد بيّنت بدقة المفهوم الواقعي والحقيقي من هذا الفعل وما يترتب عنه من أفعال أخرى مجرمة، وهي الدخول إلى المعلومات المخزنة إما بالإختراق أو بالغش والإحتيال أو بالتواجد غير المسموح به، والتي من شأنها المساس بسلامة سير النظام المعلوماتي، ومع هذا تبقى كل هذه التعاريف مجرد محاولات للكشف عن حقيقة وخطورة وحداثة هذا النوع من الجرائم؛ وأكيد سوف نشهد مستقبلاً مفاهيم وتعاريف أخرى نتيجة التطور الهائل الذي يعرفه مجال تقنية المعلومات وتكنولوجية الإتصال.

وفي الأخير ما نلاحظه من هذه التعاريف كلها أنها لم تأتي على ذكر تعريف جريمة الدخول غير المشروع لمواقع التواصل الإجتماعي وصفحات الفايسبوك.

المطلب الثاني: خصائص جريمة الدخول أو البقاء غير المشروع

لاشك أن هذه الجريمة المرتكبة في العالم الإفتراضي والوسط الرقمي بإستخدام تقنية المعلومات لها من الخصائص ما يميزها عن غيرها من الجرائم المرتكبة في العالم المادي الفيزيائي، ولعل من جملة هذه الخصائص والتي تتميز بها هذه الجريمة يمكن أن نذكر هنا ما يلي:

الفرع الأول: من حيث إعتمادها على تقنية المعلومات والوسائل التكنولوجية في إرتكابها

إن إتساع حجم تقنية المعلومات وخاصة شبكة الإنترنت وسهولة الدخول إليها، والتزايد المستمر في إستخدام الوسائل التكنولوجية الحديثة، وتطور الحواسيب بمختلف الأشكال والأحجام، جعل منها مسرحًا لكثير من الأفعال الإجرامية الإلكترونية، وجريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي لا تخرج عن كونها من أبرز الجرائم المعلوماتية، وهذا بإعتبار أنها تقوم

أساسًا على إستخدام التقنية في إحداثها، فهي جريمة ذات تقنية تنسب إلى الجرائم المعلوماتية بحكم إستخدام تكنولوجيا الإتصالات في إرتكابها[1]، وهذا لأنها تعتبر من جرائم الوسيلة المطلقة؛ إذ لم يشترط المشرع الجنائي أن يكون الدخول أو البقاء غير المشروع والوصول إلى المعلومات الموجودة داخل النظام بطريقة أو بوسيلة تكنولوجية معينة، إذ جاءت معظم عبارات النصوص الجنائية مطلقة في هذا الخصوص وشاملة لكل طرق الدخول، دون تحديد طريقة أو وسيلة بعينها.

ووسائل الإتصال بالنظام عديدة، لكن ما يجمعها هو إفتراضها قدرًا من المعرفة بتقنية المعلومات وهو ما تنبهت له معظم التشريعات المقارنة حيث لم تحصر عملية الدخول بوسيلة بعينها بل جاءت شاملة لكل طرق الدخول[2]، سواء كان ذاك بواسطة الإختراق أو عن طريق إستخدام البرامج الخبيثة، أو عن طريق الإعتراض والإلتقاط بإستخدام شبكات الإتصالات السلكية واللاسلكية[3]، على أن يكون الحاسب الآلي هو الأداة الأساسية المستخدمة في إرتكاب السلوك الإجرامي المكون لها، سواء كنا أمام جرائم تقنية المعلومات بدون إستخدام وسائل الإتصال، أو أمام جرائم تقنية المعلومات بإستخدام وسائل الإتصال كالإنترنت مثلاً، وعند الحديث عن الحاسوب لا نقصره على شكله التقليدي في الكمبيوتر أو التليفون فقط، وإنما قد يكون شكل هذا الحاسوب ضمن الجوال الرقمي أو الجهاز المحمول أو في شكل ساعة يدوية إلكترونية وغيرها من الحواسيب الجديدة والمتطورة.[4]

وعلى الرغم من تنوع الوسائل التي ترتكب بها هذه النوعية من الجرائم، إلا أن الطرق المستخدمة في هذه الجريمة تتشابه في أمور كثيرة ومعقدة في نفس الوقت، ولهذا فإن أجهزة الأمن بحاجة إلى الكثير من العمل الميداني لتطوير قدراتها التقنية والتكنولوجية للتعامل مع جرائم الحاسوب والإنترنت، خاصةً وأن هذه الأخيرة هي مسرح الجريمة ذاتها، وهذا حتى تكون جهات البحث والتحري والتحقيق قادرة على التعامل مع مختلف الأدوات والوسائل الإلكترونية من أجهزة وبرامج تقنية المعلومات.[5]

---

[1]– **رشيدة بوكر:** المرجع السابق، ص60. – **أحمد حسام طه تمام:** المرجع السابق، ص20.

[2]– ***MICHEL Véron :*** *droit pénal spécial, 6eme édition Armand colin, Paris, France, 1998, P 258.*

[3]– **مدحت عبد الحليم رمضان:** الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2001، ص51.

[4]– **سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، 2013، ص25.

[5]– **محمد علي سويلم:** المرجع السابق، ص274. – **محمود رجب فتح الله:** المرجع السابق، ص275.

الفرع الثاني: من حيث صفة الفاعل في إرتكاب هذه الجريمة

من خصائص هذه الجريمة أنها تندرج أيضًا ضمن طائفة جرائم الصفة المطلقة لفاعلها؛ فلا يشترط توافر صفة معينة في الفاعل، ومن ثم يمكن أن يقع الدخول أو البقاء داخل النظام، من أي شخص سواءً كان محترفًا أم غير محترف في الجريمة، وسواءً أكان عاملاً في الجهة التي حدث فيها الدخول غير المشروع إلى النظام أم من غير العاملين[1]، ما عدا أنه من اللازم أن يكون مرتكبها من ذوي المعرفة والإختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على إستخدامها والتعامل معها.[2]

وهكذا نجد أن هذا النوع من الجرائم قد يرتكب بواسطة عدة فئات مختلفة، ولعل الفئة الأخطر من بين مرتكبي هذه الجريمة، هي فئة الجريمة المنظمة التي يستخدم أفرادها الحاسب الآلي لأغراض السرقة والسطو على المصارف والمنشآت التجارية الكبرى، وترويج المخدرات عبر وسائل التواصل الإجتماعي والإرهاب الإلكتروني وغسيل الأموال وغيرها.

وكما قد ترتكب هذه الجريمة من قبل أشخاص وفئات عادية، حيث تستخدم هذه الفئة الحاسب الآلي لسرقة الأرقام السرية أو الإطلاع على المعلومات ونشرها على شبكة الإنترنت، وغيرها من الدوافع الإجرامية الأخرى والأقل خطورة، كما أن إرتكاب هذا النوع من الجرائم ليس فقط من قبل الطبقة المثقفة بل ترتكب من قبل الجميع بمختلف الأعمار والمستويات التعلمية والمعرفية، وهذا نتيجة تبسيط وسائل تكنولوجيا المعلومات والقدرة على إمتلاكها والإعتماد على الحق في الإنترنت كوسيلة لنقل المعلومات وفي نفس المساس بها[3].

الفرع الثالث: من حيث طبيعة السلوك الإجرامي المكوّن للجريمة

يجمع الكثير على أن هذه الصورة من جرائم تقنية المعلومات تدخل ضمن طائفة الصور الشكلية، أو بالأحرى الجرائم ذات السلوك المحض، الذي يكفي لقيام الركن المادي معه إرتكاب أحد الأفعال أو الصور الإجرامية سواءً بفعل الدخول دون البقاء أو بفعل الدخول مع البقاء داخل النظام بحيث تقع هذه الجريمة بإرتكاب أحد هذه الأفعال دون أن يعد ذلك تعدادًا ماديًا للجرائم.[4]

---

[1]– **محمد علي سويلم:** المرجع نفسه، ص275.

[2]– **رشيدة بوكر:** المرجع السابق، ص62.

[3]– ***QUÉMÉNER (M), CHARPENEL (Y) :*** *Cybercriminalité, Op. Cit, P 75.*

[4]– **محمد علي سويلم:** المرجع السابق، ص274.

كما أن السلوك المجرَّم لهذه الجريمة يجعلها تندرج ضمن طائفة الجرائم الوقتية تحسب من وقت الدخول إلى النظام، فيترتب عليه تحديد بدء حساب مدة تقادم الدعوى الجنائية، كما أنها تضم فعل مستمر يتمثل في البقاء داخل النظام بدون وجه حق، ومن ثم يبدأ حساب تقادم الدعوى الجنائية من اليوم التالي لإنتهاء حالة الإستمرار[1]، فإذا كان فعل "الدخول" عبارة عن فعل وقتي، فإن فعل "البقاء" يكون ذو طبيعة مستمرة.

وقد تعتبر الجريمة مستمرة إذا إتخذ السلوك المكون لها صورة التواجد والبقاء داخل النظام المعلوماتي أو حتى في جزء منه، ويكون مرد هذا الإستمرار نابع من إرادة الجاني وأنه أخذ وقت طويل نوعًا ما من بعد الدخول إلى النظام، أما إذا إتخذ السلوك المكون للجريمة صورة الدخول فقط فإن الجريمة تكون وقتية أي فورية، لأن هذا السلوك المجرم يبدأ ثم يَتِمُّ ثم ينتهي في آن واحد، فضلاً على أنه غير قابل بطبيعته للإستمرار[2]. وقد يعتبر فعل الجاني جريمة متتابعة الأفعال تتحقق بتكرار فعل الدخول إلى الموقع أو إلى الحساب الإلكتروني أو النظام المعلوماتي.[3]

الفرع الرابع: من حيث علاقة الجريمة بالمعطيات المعالجة داخل النظام

نظام المعالجة الآلية للمعطيات ليس هو الهدف الرئيسي لما يريده المجرم المعلوماتي، وإنما يستخدمه كأداة لتحقيق نتيجته الإجرامية المبتغاة وهي الحصول على المعلومة بكل ما تحمله من معنى وهذا عن طريق الدخول غير المصرح به إلى مواقع الشبكات ونظم المعالجة الآلية.

وأحياناً أخرى تكون التقنية هي بيئة إتمام وتحقيق الهدف من وراء الجريمة، وإن كانت في أغلبها جرائم تقليدية لا تختلف عن الجرائم التي توالى حدوثها عبر التاريخ، ولكنها اليوم ترتكب في بيئة جديدة وبوسائل حديثة[4]، والتي لا يجوز أن تتم إلا بوجود نظام المعالجة الآلية بإعتباره شرطًا ضروريًا في مثل هذه الجرائم، كإستغلال النظام للإستيلاء على الأموال بإجراء تحويلات غير مشروعة، أو إستخدام النظام في عملية التزييف والتزوير، أو إستخدام النظام لإرتكاب جريمة غسل الأموال أو الترويج للمخدرات عبر شبكة الإنترنت.

---

[1]- **عزيزة رابحي:** المرجع السابق، ص161.

[2]- **محمد علي سويلم:** المرجع نفسه، ص275.

[3]- **حسني الجندي:** التشريعات الجنائية الخاصة، المرجع السابق، ص80.

[4]- **رشيدة بوكر:** المرجع السابق، ص63-64.

وهكذا نجد أن الإعتداء على النظام وما يحتويه من المعطيات المعالجة بداخله قد يتخذ أكثر من شكل، ولعل أهمها الدخول أو البقاء غير المشروع والتعدي على سلامة المعلومات والبيانات، لذلك كان من الطبيعي أن يحتاج هذا النظام إلى حماية جزائية في حد ذاته، ناهيك عن قيمة المعلومات التي يحتويها هذا النظام بداخله، وهو ما أدركته الكثير من التشريعات الجنائية المقارنة.

الفرع الخامس: من حيث عدم مشروعية الأفعال التي ترتكب بها الجريمة

مما لاشك فيه أن مجرد الدخول إلى نظم المعالجة الآلية للمعطيات لا يشكل فعلاً غير مشروع وإنما يستمد هذا الدخول عدم مشروعيته من كونه قد تم عن طريق الغش والإحتيال، ويكون كذلك في حالة ما إذا كان هذا الدخول ضد إرادة المسؤول عن النظام أو مالكه، أي بدون الحصول على تصريح مسبق منه، ومن ثم فإن توافر الرضا ينفي عن السلوك عدم المشروعية[1].

ذلك أن التطور المستمر الذي يطرأ على البيئة الرقمية من حيث إمكانية شمولها مظاهر رقمية جديدة، يجعل من مسألة تضييق معنى الدخول بإعداد نموذج ثابت لشكل التفاعل الناجح مع النظام من أكبر المشاكل التي تعيق حماية النظام من صور الإختراق والقرصنة الإلكترونية، وذلك بسبب أن مستخدم النظام يمكن أن يتفاعل معه بطرق وتقنيات لا تعد ولا تحصى، وإذا كانت الشبكات والنظم المعلوماتية المختلفة لا تميز بين المشروعية وعدم المشروعية في الدخول إليها فإن القانون يقوم بهذا التمييز فارضًا الحماية المشروعة ضد كل محاولة يفترض فيها اللامشروعية.[2]

لذا يلزم القانون أنه لقيام جريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات أن يكون فعل الدخول أو البقاء بصفة غير مشروعة وبدون وجه حق بغرض الإطلاع على البيانات والمعلومات المخزنة داخل هذه المواقع ورؤيتها وتصفحها ونقل ما بداخلها من محتويات معلوماتية كله بما يخالف القانون، وعليه فإنه وبمفهوم المخالفة فلا جريمة ولا عقوبة إذا كانت هذه الأفعال مصرح بها من قبل صاحب النظام، وكذلك الأمر إذا كان إستعمال النظام المعلوماتي بالمجان وبدون مقابل مادي وأنه متاح للعامة كشبكة الإنترنت مثلاً وما تتيحه من مواقع مفتوحة للجمهور[3]، تسمح لهم بالإطلاع عليها وتصفحها عن طريق الدخول والبقاء داخل هذه المواقع ونقل ما بداخلها

---

[1]– ***MICHEL Véron :*** *Droit pénal spécial, Op. Cit, P262.*

[2]– **رشيدة بوكر:** المرجع السابق، ص72.

[3]– عملية الدخول إلى شبكة الإنترنت قد تكون بطريقة مباشرة أو عن طريق غير مباشر، وهذا من خلال إستعمال ما يعرف "بالنص المتشعب" وهذا الأخير عبارة عن نص يحتوي على نقاط تحكم تتيح الإنتقال إلى أماكن أخرى من النص لتسيير ربط الموضوعات ببعضها البعض، وأهم ما يميز هذا الأسلوب في العرض هو خاصية عدم وجود ترتيب معين للبحث بل يسير وفقًا لما يتراءى للمستخدم.

بكل حرية، وفي هذه الحالة يصبح كل من فعل الدخول وفعل البقاء حق مشروع وغير مخالف للقواعد القانونية.[1]

وكذلك يخرج من إيطار التجريم ما يطلق عليه "بإستخدام البرامج الدعائية"[2]، وكذا ما يعرف "بصائدي المعلومات"[3]، ففي كل هذه الأمثلة السابقة فإن إستخدام أي من هذه الأدوات الفنية والبرامج التطبيقية لا يعد في ذاته دخولاً أو بقاءًا غير مشروع، حيث نجدهما قد تما بشكل صحيح قانوناً وأنه مصرح به، وبالتالي لا تقوم هذه الجريمة ولا يخضع مرتكبها للعقاب المنصوص عليه في القانون الجنائي[4].

ولقد عبر المشرع الجنائي عن عدم مشروعية الأفعال التي ترتكب بها هذه الجريمة للتوصل إلى المعطيات الموجودة بالمواقع أو النظام المعلوماتي بعديد العبارات والمصطلحات، فنجد مثــلاً عــبارة "بدون وجه حق" وأيضًا عبارة "عن طريق الإحتيال"، أو عبارة "بطريقة الغش"، ومن هم من ذكر عبارة "غير مأذون له" أو "بدون إذن مسبق" أو "غير مسموح له" أو "غير مصرح له"، أو "دون مسوغ من القانون" فكل هذه المصطلحات والعبارات وغيرها تدل على عبارة "عدم المشروعية".

وعبارة "عدم المشروعية" أو "غير مشروع" هو مصطلح واسع يستوعب جميع الأفعال المجرمة وكل العبارات الدالة عليها التي تستخدم في الحصول على المعلومات المعالجة والمخزنة داخل النظام المعلوماتي بما يخالف القانون، أي التواجد على غير رغبة وإرادة من له الحق في السيطرة على هذا النظام. لذا كان من السليم على المشرع الجنائي النص على هذه الأفعال المجرمة كلها من خلال عبارة واحدة فقط وهي عبارة "الحصول بصورة غير مشروعة".[5]

---

[1]– ***BENSOUSSAN Alain :*** *L'informatique et le droit, memento guide, édition (HERMES), Paris, France, Tome I, 1994, P211.*

[2]– وهو ما يطلق عليه أيضًا "بالروابط العميقة" أو ما يعرف "بتطبيق البيانات الدعائية"، والتي يقصد بها تلك البيانات التي ترد مجاناً على السلع والخدمات التجارية من أجل الدخول إليها من قبل المتعاملين مع شبكة الإنترنت.

[3]– **صائدي المعلومات:** مصطلح أطلق على عملية تحديد مكان البيانات ومن ثم إستخراجها بواسطة برنامج معروف بإسم "*Spider*" وهو عبارة عن برنامج يبحث بإستمرار عن المواقع الإلكترونية الجديدة "كصفحات الويب *Web*" والصفحات الإخبارية، فيحتفظ بعناوينها في قاعدة بيانات للإستعانة بها مرة أخرى في إيجاد المقالات الإلكترونية.

[4]– ***QUEMENER (M), CHARPENEL (Y)*** *: Cybercriminalité, Op. Cit, P161.*

[5]– وهذا ما جاءت به المادة (202–A–1) من قانون العقوبات الألماني والتي جاء فيها: "كل من يحصل بصورة غير مشروعة له أو لغيره على البيانات المحمية بفعل الدخول إلى النظام ..."، والتي تقابلها أيضًا في نفس السياق نص المادة (143) من القانون الجزائي السويسري والتي جاء فيها: "أي شخص يقوم بتحقيق مكاسب غير مشروعة لنفسه أو لغيره بالدخول إلى معلومات تم تخزينها أو بإستخدام أية وسيلة أخرى مماثلة". فهو هنا يقصد بوسيلة أخرى مماثلة، كل من فعل "الإعتراض والإلتقاط".

– ***QUEMENER (M), CHARPENEL (Y) :*** *Cybercriminalité, Op. Cit, P188.*

وعمومًا فقد حدد المشرع الجنائي في معظم التشريعات الجنائية – الغربية والعربية– أنّ وسيلة التواصل مع الموقع أو النظام المعلوماتي بطريقة غير مشروعة تكمن في الدخول أو البقاء دون وجه حق، بحيث ينصرف مدلول الدخول والبقاء في إطار تقنية المعلومات ليشمل كافة الأفعال التي تسمح بالوصول إلى موقع إلكتروني أو نظام معلوماتي والإحاطة به أو حتى السيطرة عليه، أو على ما يحتويه بداخله من معلومات.[1]

خلاصة القول:

خلاصة لما سبق الحديث عنه أن لجريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي إرتباط وثيق بجناحي بيئة تقنية المعلومات، وأنها جرائم مستحدثة ما بزغت إلا بظهور وسائل الحوسبة والإتصالات التكنولوجية الحديثة، وهذا لما لها من قوة في المساس بحرية الأشخاص وخصوصيتهم داخل المجتمع.

ومن هنا إتضح لنا أن لهذه الجريمة مفاهيم عديدة ومختلفة وخصائص تميزها إبتداءًا، لذا رأينا أننا نقدمها بإيجاز قبل الخوض في غمار هذا الفصل والحديث عن الأركان والعناصر القانونية لهذه الجريمة وكذا الإجراءات العقابية المقررة لها.

[1]– **حسني الجندي:** التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث، شرح قانون مكافحة جرائم تقنية المعلومات، ط1، دار النهضة العربية، القاهرة، مصر، 2009، ص78.

المبحث الثاني: ضرورة وجود نظام المعالجة الآلية للمعطيات في قيام الجريمة

تمهيد وتقسيم:

إنّ الشيء المشترك بين كل الجرائم المعلوماتية هو ضرورة وجود نظام للمعالجة الآلية للمعطيات[1] *Système de traitement automatisé de donnes (STAD)*، وهذا حتى يتم بحث ما إذا كان هناك إعتداء على هذا النظام من عدمه، بحيث إذا لم يتوافر هذا العنصر فلا يمكن الحديث في مدى توافر الأركان العامة للجريمة المعلوماتية ولا حتى البحث في هذه الجريمة أصلاً[2]، فهذا العنصر القانوني لابد من وجوده كشرط بديهي ومفترض في أغلب الجرائم المعلوماتية. بحيث يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في خبايا هذه الجريمة وكذا في توافر أو عدم توافر أركان أية جريمة معلوماتية أخرى، فإن ثبت تخلف هذا الشرط فلا مجال للحديث عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إذ أن هذا الشرط يعتبر عنصرًا لازمًا لكل منها.[3]

وجريمة الدخول أو البقاء غير المشروع وما يترتب عنها من جرائم معلوماتية أخرى، تفترض وجود عناصر أو شروط ضرورية ومفترضة لقيام مثل هذه الجرائم وتحديد المسؤولية الجنائية لفاعلها وهذه العناصر المفترضة في الجريمة تتمثل أساساً في وجود نظام معالجة آلية للمعطيات، وكذا مسألة أن يكون النظام مشمولاً بالحماية الأمنية.

وهذا ما يحتم علينا بالضرورة تقسيم هذا المبحث إلى مطلبين إثنين على الشكل التالي:

المطلب الأول: تعريف نظام المعالجة الآلية للمعطيات

المطلب الثاني: ضرورة خضوع نظام المعالجة الآلية للحماية الأمنية

---

[1]– عبارة "المعالجة الآلية *Automatisé*" ذاتها تدخل ضمن مصطلح "المعلوماتية *Informatique*" وهي بمثابة الترجمة السليمة لعبارة "المعالجة الآلية للمعلومات" والتي بدورها تتكون من شقين، الأول هو كلمة "معلومة *Information*" والثاني هو كلمة "آلي *Automatique*" وعلى ذلك نخلص إلى نظام المعالجة الآلية للمعطيات أو البيانات *Le système de traitement automatisé des données* (*STAD*)، أو كما كان يطلق عليه في السابق "بالمعالجة الآلية للكمبيوتر *Traitement informatique d'ordinateur*" (*TID*). (لمزيد من التفصيل حول الموضوع أنظر: – **مختارية بوزيدي:** ماهية الجريمة الإلكترونية، مقال منشور ضمن أعمال الملتقى الوطني، بعنوان "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص12).

[2]– ***GASSIN (R) :*** *Le droit pénal de l'informatique, Op. Cit, P95.*

[3]– **خثير مسعود:** المرجع السابق، ص108.

المطلب الأول: تعريف نظام المعالجة الآلية للمعطيات

من خلال قراءتنا لمصطلحات هذا العنصر نجده تعبير فني وتقني يصعب على المشتغل بالقانون إدراك حقيقته العلمية بسهولة، وهذا على عكس من هم متخصصين في مجال الإعلام الآلي فضلاً عن ذلك أنه تعبير علمي دقيق ومتطور بإستمرار يخضع للتقلبات السريعة والمتلاحقة في مجال صناعة الحواسيب وما في حكمها.[1]

ولقد ظهرت عدة تعريفات لنظام المعالجة الآلية للمعطيات، وإن كان هناك جدل واسع في تحديد المفهوم الدقيق والصحيح لهذا العنصر، لذا قبل أن نخوض في البحث والدراسة لهذه الجريمة، لابد علينا التعرض لأهم التعاريف التي جاءت بخصوص مفهوم نظام المعالجة الآلية للمعطيات، سواء من الناحية الفقهية (فرع أول) أو من الناحية القانونية (فرع ثاني).

الفرع الأول: التعريف الفقهي للنظام المعلوماتي (نظام المعالجة الآلية للمعطيات)

إنقسم الفقه بشأن تعريف نظام المعالجة الآلية للمعطيات إلى إتجاهين إثنين، إتجاه مقيد في تعريفه لهذا النظام (أولاً)، وآخر موسع له (ثانياً).

أولاً: الإتجاه المقيد في تعريف النظام المعلوماتي

يذهب أنصار هذا الإتجاه لاسيما البعض من الفقه الفرنسي إلى تعريف نظام المعالجة الآلية للمعطيات من خلال وضع مفارقة بين مصطلح "المعطيات" ومصطلح "المعلومات"، أي ما بين "الآلية *Automatisé*"[2] من جهة وبين "المعلوماتية *Informatique*" من جهة أخرى، وإنتهوا إلى القول أن المعلومات هي المحصلة النهائية للمعطيات، بمعنى آخر أن المعطيات الآلية هي عبارة عن مجموعة أدوات وأجهزة الحاسب الآلي المادية والمعنوية المكونة له، أما المعلوماتية فهي نتاج عمل هذا النظام وتشغيله[3]، فيؤكدون على أن الفرق واضح بين موضوع المعطيات نفسه وموضوع المعلومات، أي أن الثانية نتاج الأولى.

ويزيدون على ذلك أنصار هذا الإتجاه أنه في السابق لم يكن هناك إختلاف بين "المعالجة الآلية" و"المعالجة المعلوماتية"، حيث أن قانون العقوبات الفرنسي لعام 1978 لم يكن يفرق هو الآخر بين هذين المصطلحين، ولكن فيما بعد إتضح الإختلاف بين المعالجة الآلية والمعالجة المعلوماتية،

---

[1]– **علي عبد القادر القهوجي:** المرجع السابق، ص120. – **بلال أمين زين الدين:** المرجع السابق، ص264.

[2]– ***GASSIN (R) :*** *le droit pénal de l'informatique, Op. Cit, P89.*

[3]– **كلمة آلية *Automatisé*:** تعني دون تدخل بشري وهي ترادف كلمة "آلياً *Automatique*" كأن نقول المعالجة الآلية للمعلومات.

أي بين الأنظمة الآلية والأنظمة المعلوماتية، وهذا بسبب أن المعالجة الآلية تدخل في إطار تكوين وحدة وعناصر النظام كجهاز، بينما المعالجة المعلوماتية ما هي إلاَّ الحد الأدنى وخلاصة لعملية المعالجة الآلية[1]، هذا وقد أجمع الفقه الفرنسي وقتها من واقع الأعمال التحضيرية لهذا القانون أن نظام المعالجة الآلية للمعطيات يحتم التفرقة بين المعلومات والنظام الذي يحتوي عليها.[2] وفي الجانب العملي يذهب الفقه الفرنسي إلى القول أن كلمة "الآلية" هي الأكثر تطبيقًا في الممارسات الميدانية من كلمة "معلوماتية"، لأن هذه الأخيرة ما هي إلاَّ الحد الأدنى الذي يمكن التوصل إليه كنتاج عمل نظام المعالجة الآلية للمعطيات، ومع ذلك فإنهم يرون أن مفهومية نظام المعالجة الآلية للبيانات أو المعطيات محصورة في العملية المعلوماتية كخلاصة فقط لا غير.[3]

ولكن وجه إلى هذا الإتجاه عدة إنتقادات، وهو أنه ليس هناك إنفصال بين المعطيات الآلية والمعطيات المعلوماتية، وأن كل منهما في النهاية يشكل "النظام المعلوماتي" أي نظام المعالجة الآلية للمعطيات، الذي هو موضوع الحماية الجنائية في الكثير من القوانين الوطنية والإتفاقيات الدولية.

ثانيًا: الإتجاه الموسع في تعريف النظام المعلوماتي

يقوم هذا الإتجاه على تعريف نظام المعالجة الآلية للبيانات عن طريق تبيان وتحديد العناصر التي تدخل في تكوين هذا النظام ككل، بإعتباره علم قائم بذاته وسريع التطور بإستمرار في مجال المعلوماتية والذي بدوره يمزج بين مصطلحين في غاية الأهمية "المعلومة والآلية" ومعناها المعالجة الآلية للمعلومة، أما عن مصطلح "المعطيات" فهو خلاصة الفكر الآلي من خلال عمل المكونات والبرامج مع البيانات الموجودة في جهاز الكمبيوتر أو الحاسوب أو على شبكة الإنترنت، سواءً كانت هذه المعطيات فنية أو أدبية أو علمية أو تجارية أو صناعية، فهي تصنف كإنتاج ذهني لأصحابها في إطار المعلوماتية.[4]

لذا ذهب أنصار هذا الإتجاه وعلى رأسهم الفقه الفرنسي إلى تبني التعريف الذي أقرته الأعمال التحضيرية لقانون العقوبات الفرنسي لعام 1988 والمتعلق بالحريات والمعلوماتية *Liberté et information*، والذي مؤداه أن نظام المعالجة الآلية للمعطيات هو: "كل وحدة أو مجموعة من

[1]– **بلال أمين زين الدين:** المرجع السابق، ص276.

[2]– **رشيدة بوكر:** المرجع السابق، ص74.

[3]– **بلال أمين زين الدين:** المرجع نفسه، ص264.

[4]– **مختارية بوزيد:** المرجع السابق، ص13.

الوحدات المخصصة للمعالجة أو التخزين أو أجزاء الدخول والخروج والإرتباطات التي تهدف إلى نتيجة محددة في هذه المجموعة وتكون مشمولة بحماية نظام آمان"، وهذا التعريف هو الذي أيده وتبناه الكثيرون من أهل الفقه والقانون، وهذا بسبب توسعه في الفهم حول نظام المعالجة الآلية للمعطيات، والتي يرون بأنها ليست محصورة في العملية المعلوماتية كخلاصة فقط، وإنما تتكون من مجموعة من الأدوات والأجهزة المادية والبرامج المنطقية وبيانات ونظم تطبيقية وهندسية وغيرها، بحيث تتكاتف جميعها معًا من أجل الحصول على المستخرجات المقروءة والمرئية والمسموعة[1].

كما نجد تعريف فقهي آخر قريب من ذلك تمامًا مفاده أن هذا النظام هو عبارة عن: "كل مركب يتكون من وحدة أو مجموعة وحدات للمعالجة الآلية، كالذاكرة والبرامج والمعطيات وأجهزة الربط وغيرها، التي تعمل فيما بينها لتحقيق الهدف والغاية المرجوة، على أن يكون هذا النظام خاضع لنظام حماية فنية".[2]

ويستند أغلب الفقه الفرنسي في تبرير ذلك إلى أن كل من المصطلحين "الآلي والمعلوماتي" قد وَرَدَا في بادئ الأمر في قانون العقوبات الفرنسي لعام 1978 ثم جاء بعدها قانون 1988 الذي جرَّم الإعتداء على نظام المعالجة الآلية للمعطيات، والذي عُدّل هو الآخر بالقانون الصادر عام 1994 والذي جرم بدوره الإعتداء على الوثائق المعلوماتية من جهة وكذا المعالجة الآلية من جهة أخرى، الأمر الذي أثار الجدل الفقهي حول التفرقة بين المصطلحين، بإعتبار أن الإعتداء على أي منهما يشكل جريمة مستقلة عن الأخرى.

إلاّ أن الرأي الغالب في الفقه الفرنسي قد حدى إلى القول بأن المشرع الفرنسي لم يهدف أبدًا بنصه على هاتين الجريمتين إلى التفرقة بين "المعالجة الآلية للمعطيات" أو "المعالجة المعلوماتية" بل أن ما في الأمر أن أحد المصطلحين هو أشمل للآخر منه. وبالتالي يمكن القول بأن كلمة "الآلية" تجعلنا نفكر في النظام المعلوماتي ذاته كنظام حركي يتحرك ويدور بديناميكية محددة،

[1]– **بلال أمين زين الدين:** المرجع السابق، ص274.

[2]– **مريم مسعود:** مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم (09-04)، ماجيستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2013، ص35.

أما كلمة "معلوماتية" فتبين لنا أنها نتاج عمل هذا النظام والمتمثل في الوثائق المعلوماتية والمحررات الإلكترونية بأنواعها المختلفة، ولهذا فلا غنى عن إحداهما وأن كلاهما يكمل الآخر.[1]

كما يزيد أنصار هذا الإتجاه في توسيع شموليته على أساس أن أشكال المعالجات الموجودة والواردة في نظام المعالجة الآلية للمعطيات ليست واردة على سبيل الحصر وإنما هي واردة على سبيل المثال، إذ أنها تشمل كل من المعالجة الآلية وكذلك المعالجة المختلطة.[2]

وعليه فإن مصطلح "النظام المعلوماتي" أو كما يعرف بنظام المعالجة الآلية للمعطيات يدل على كل تركيب يتكون من وحدة واحدة أو عدة وحدات للمعالجة الآلية، والتي يتركب كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط وغيرها من الأجهزة الدقيقة والمختلفة، والتي تجمعها مجموعة من العلاقات الفنية والتقنية، بحيث تتيح لهذا التركيب أن يباشر نشاطًا تقنيًا مُعَيَّنًا.[3] فالمنظومة المعلوماتية تبعًا لهذا الوصف تبنى على عناصر مادية وأخرى معنوية؛ فأما عناصرها المادية فتشمل الدعامات التي تضم كل المكونات المادية ويطلق عليها "بالدعامات المادية" أما العناصر المعنوية فتشمل كل الأوامر والتعليمات والروابط المنطقية التي تجمع بين مختلف عناصر النظام المعلوماتي، ويطلق عليها هي الأخرى "بالدعامات المنطقية".[4]

كذلك هناك من يزيد من الإتساع في تعريف هذا النظام، بحيث يشمل كل من الشبكة الدولية للمعلومات "الإنترنت" وما تشتمل عليه من مواقع إلكترونية وحسابات خاصة، وأيضًا الشبكات المحلية للمعلومات "كشبكات البنوك والشركات التجارية والمؤسسات الإدارية"[5]، وحتى البطاقات

---

[1]– **بلال أمين زين الدين:** المرجع السابق، ص264.

[2]– للتوصل أكثر إلى المقصود العام بنظام المعالجة الآلية للمعطيات نذكر هنا بعض أنواع المعالجة الآلية والمستخدمة في مجال المعلوماتية، فنجد على سبيل المثال:

– **المعالجة الميكانيكية "*Traitement Mécanique*":** وتتم هذه المعالجة للبيانات عن طريق بعض الأجهزة الأقل تطورًا من الناحية الفنية والتقنية والتي سبقت ظهور الكمبيوتر والذي هو أساس الثورة المعلوماتية الحالية، ولعل من أهم أدوات المعالجة الميكانيكية نجد مثلاً "الآلة الكاتبة *Dactylo*" والتي كانت منتشرة في مرافق عمومية عديدة وهي تعمل بصورة يدوية.

– **المعالجة المختلطة "*Traitement mixtes*":** وهذه المعالجة تتم عن طريق جيل من الآلات الراقنة والمتطورة نوعًا ما، والتي تتمتع بميزتيْ المعالجة الآلية والمعالجة اليدوية في آن واحد، حيث تكون عبارة عن آلات كاتبة لها ذاكرة معلوماتية تستطيع من خلالها الإحتفاظ بالمعلومات التي تم كتابتها يدويًا مع إمكانية تعديلها وإستخراجها عند الحاجة، وهذا ما هو موجود في ثورة الحواسيب الآلية اليوم. **(**لمزيد من التفصيل أكثر حول الموضوع راجع: – **بلال أمين زين الدين:** المرجع السابق، ص263**)**.

[3]– **عادل بوزيدة:** المسؤولية الجزائية لمتعهدي إيواء المواقع الإلكترونية، المركز الأكاديمي للنشر، القاهرة، مصر، 2019، ص82.

[4]– **بلال أمين زين الدين:** المرجع السابق، ص265.

[5]– ذهبت بعض الدراسات إلى الإشارة أن أو التشريعات التي إعتبرت الشبكة الدولية للمعلومات كمحل ينصب عليه النشاط الإجرامي وأنها تدخل ضمن تركيبة النظام المعلوماتي، هو قانون العقوبات اليوناني، الذي يشير في ذلك صراحةً من خلال جرائم الإعتداء على نظام المعالجة الآلية للمعطيات. **(**أنظر أكثر: – **نائلة عادل محمد فريد قورة:** جرائم الكمبيوتر الإقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005، ص324**)**.

الإئتمانية[1] والتي كذلك تعتبر حسب رأيهم من أهم مكونات هذا النظام بما تشتمله من بيانات ومعلومات خاصة لاسيما إذا ما أدخلت في المكان المخصص للتوزيع الآلي للنقود، حيث تعد هذه الحالة الأخيرة أحد أهم عناصر النظام التي تسمح بالدخول المباشر في نظام المعالجة الآلية للبيانات، لكن حسب رأي البعض أن البطاقات الإئتمانية بمفردها لا تعد نظامًا معلوماتيًا إلاَّ إذا تم إدخالها في النظام نفسه[2].

ومع ذلك قدم وقتها وزير المالية الفرنسي تعريفًا لفكرة نظام المعالجة الآلية للمعطيات، وإستبدلها لأول مرة بفكرة "النظام المعلوماتي"، على أنه: "مجموعة من التجهيزات والبرامج التي تحتوي على حاسب آلي يقوم بمعالجة وإسترجاع المعطيات"، لكن وقتها أُنتقد هذا التعريف بشدة بحجة أنه خاص بالنظام المعلوماتي بينما نظام المعالجة الآلية للمعطيات أوسع بكثير من ذلك، وأن هذا التعريف ينقصه القيمة القانونية.[3]

الفرع الثاني: التعريف القانوني للنظام المعلوماتي (نظام المعالجة الآلية للمعطيات)

هذه النصوص القانونية والتي إهتمت بتعريف نظام المعالجة الآلية للمعطيات، منها ما جاء في بعض الإتفاقيات الدولية ذات الصلة (أولاً) ومنها ما ذكرته بعض القوانين الوطنية (ثانياً).

أولاً: في الإتفاقيات الدولية

لقد عرفت العديد من الإتفاقيات الدولية والإقليمية المتعلقة بمكافحة الإجرام المعلوماتي، نظام المعالجة الآلية للمعطيات، والتي من أهمها:

أ- إتفاقية بودابست: لقد عرفت إتفاقية بودابست والمتعلقة بمكافحة الإجرام المعلوماتي لعام 2001 نظام المعالجة الآلية للمعطيات، وذلك بموجب المادة (1/أ) بأنه: "النظام المعلوماتي يعني كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواءً بمفردها أو مع مجموعة عناصر أخرى، تنفيذًا لبرنامج معين، بأداء معالجة آلية للبيانات".[4]

---

[1]- تزداد قيمة وأهمية إعتبار البطاقات الإئتمانية أو كما يطلق عليها "الفيزا كارت ***Visa carte***" من أهم عناصر النظام المعلوماتي، إذا ما تعرضت لبعض التصرفات والأفعال الإجرامية في إستخدامها للولوج إلى النظام.

[2]- ***BOSSAN Gerome :*** *Le droit pénal confronté à la diversité des intermédiaires de l'internet, édition Dalloz, Paris, France, 2013, P291.*

[3]- **غـنية باطلي:** المرجع السابق، ص137.

[4]- ***ARTICLE (1/A) :*** «*Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent. En exécution d'un programme, un traitement automatisé de données*».

كما أوضحت الإتفاقية التفسيرية "*Rapport explicatif*" لإتفاقية بودابست[1]، أن المقصود بالنظام المعلوماتي كل جهاز يتكون من مكونات مادية *Matériels*[2]، ومكونات منطقية *Logiciels*[3] وذلك بغرض المعالجة الآلية للبيانات الرقمية *Données numériques* وهي تشمل على وسائل الإدخال *Les moyens d'acquisitions*، ووسائل الإخراج *Les moyens restitutions*، وكذا تخزين البيانات *Stockage*، وهذا الجهاز قد يكون منفردًا *Isolé* أو متصلاً *Connecté* بمجموعة من الأجهزة المماثلة *Dispositifs similaires* عن طريق شبكة *Un réseau*.

وأضافت نفس الإتفاقية التفسيرية أن مصطلح "معالجة البيانات *Le traitement des données*" معناه: "مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي *Programme informatique*، وأن هذا الأخير بدوره عبارة عن مجموعة من الأوامر التي يمكن أن تنفذ من خلال الحاسب الآلي *L'ordinateur* وهذا لتحقيق النتيجة المنشودة، كما يمكن لهذا الجهاز أن يقوم بتشغيل برامج عديدة ومختلفة"[4].

كما أقرت هذه الإتفاقية أيضًا أنه من مشتملات النظام المعلوماتي يوجد "الشبكة المعلوماتية" وهي عبارة عن أداة ربط بين حسابين أو أكثر[5]، وهذه الرابطة يمكن أن تكون أرضية *à la terre* أي سلكية عن طريق الأسلاك والكابلات، كما يمكن أن تكون لاسلكية مثل الراديو أو الأشعة تحت الحمراء *Infrarouge* أو عن طريق القمر الصناعي *Satellite*[6]، بحيث يطلق على الشبكة التي تستخدم الإتصالات اللاسلكية في نقل البيانات "*Wirless LAN - W.L.A.N*".

---

[1]– *Convention sur la cybercriminalité (S.T.E) N°185, rapport explicatif adopté le 8 novembre 2001, P8.*

[2]– أي كل معدات الحاسوب المادية أو الصلبة التي تستخدم في معالجة البيانات، وتضم أيضًا المعدات الآلية والتركيبات الكهربائية التي يتكون منها الحاسوب. (أنظر: – **علي يوسف علي:** معجم مصطلحات الحاسب، مطبعة الخوارزمي، القاهرة، مصر، د.ت.ن، ص329.

[3]– الكيانات المنطقية والبرمجيات أي كل المكونات غير المادية للحاسوب، فيقصد بها مجموعة البرامج التي تشكل نظامًا معينًا داخل الحاسوب أو النظام. (أنظر: – **علي يوسف علي:** المرجع نفسه، ص360).

[4]– *Convention sur la cybercriminalité (S. T. E),Op. Cit, P11.*

[5]– **ثائر موسى يونس:** شبكات الحاسب، دار الراتب الجامعية، بيروت، لبنان، 1994، ص19.

[6]– **القمر الصناعي:** عبارة عن مركبة فضائية مخصصة للإتصالات مع كوكب الأرض، تعطي سرعة ضد حركة الأرض وبنفس سرعة دورانها حول نفسها، فتبدو معها هذه الأقمار الصناعية ثابتة بالنسبة لموضع معين من الكرة الأرضية. (أنظر: – **علي يوسف علي:** المرجع السابق، ص585).

والشبكة المعلوماتية يمكن أن تكون مقتصرة جغرافيًا على منطقة صغيرة فتسمى "شبكة محلية *Réseau Local*"[1]، كما يمكن أن تغطي هذه الشبكة منطقة كبيرة فتكون واسعة النطاق فتسمى "شبكة ممتدة *Réseau étendu*"[2]، كذلك يمكن لهذه الشبكات المختلفة أن تكون هي الأخرى متصلة ببعضها البعض *Interconnectés*، وتعد شبكة الإنترنت *Internet* شبكة عالمية لأنها تتكون من العديد من الشبكات المتصلة معًا والمعقدة في تشبيكاتها، لذا يطلق عليها بالشبكة العنكبوتية، والتي تستخدم جميعها نفس البروتوكولات.[3]

ومن هنا نجد أن معظم النظم المعلوماتية إن لم يكن كلها، يمكن أن تتصل بالشبكة بوصفها نقاط نهائية أو نقاط خروج *Points de sortie*، أو كوسيلة سريعة لتسهيل نقل المعلومات المعالجة آليًا ومن الأهمية بمكان أن تصبح هذه البيانات المعلوماتية متبادلة عبر الشبكة[4].

ب- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: لقد جاء تعريف نظام المعالجة الآلية للمعطيات ضمن هذه الإتفاقية بموجب المادة (5/2) تحت عنوان "النظام المعلوماتي" بقولها أنه: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

كما عرَّفت هذه الاتفاقية "الشبكة المعلوماتية" بموجب المادة (6/2) على أنها: "إرتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها".[5]

---

[1]- **الشبكة المحلية:** عبارة عن "نظام إتصال للبيانات data communication" بحيث يسمح هذا النظام لعدد من الأجهزة المستقلة بالإتصال كلٌ مع الآخر في حيز معتدل ومن خلال قنوات إتصال فيزيائية وبمعدل مرور بينات معتدل. (- **ثائر موسى يونس:** المرجع السابق، ص23).

[2]- تختلف الشبكة واسعة النطاق أو الممتدة عن الشبكة المحلية في أمرين، الأول هو المسافة التي قد تكون بألاف الكيلومترات، والثاني هو وجود أجهزة خاصة تقوم بمهمة تنظيم وتوزيع عملية الإتصال كنقطة مركزية داخل الشبكات الممتدة لكي تنجز مهامها في الإتصال، وهذه الأجهزة تسمى "الأجهزة الموزعة *Interfaceace Massage processors* ومختصرها "*IMP*"، وهكذا تقوم هذه الموزعات "*IMP*" بعملية الإتصال بين محطات العمل المنتشرة في الشبكة الممتدة عبر العالم. (أنظر: - **ثائر موسى يونس:** المرجع نفسه، ص26).

[3]- تعمل شبكة الإنترنت على بروتوكولات تعرف بإسم "*TCP/IP*" أي بروتوكول إتصالات الإنترنت، ويقابل ذلك في المصطلح الإنجليزي *transmission control Protocol* وهذه الحروف الثلاثة "*TCP*" هي إختصار لهذا المصطلح، أما بالنسبة للبروتوكول الثاني "*IP*" فإن هاذين الحرفين يشكلان مصطلح "*Internet Protocol*" أي بروتوكول الإنترنت، فالأول هو الذي ينظم الإتصالات على شبكة الإنترنت وهو الذي يحدد كيفية تجزئة الرسائل إلى حزم تمهيدًا لإرسالها إلى وجهتها الأخيرة، أما الثاني هو الذي يقوم بتسيير هذه الحزم عبر شبكة الإنترنت ثم تجميعها عند محطة الوصول والتحقق من الخلو من الأخطاء، حيث ذكر هنا وفي نفس السياق القانون الإماراتي رقم (5 لسنة 2012) بموجب المادة (15/1) منه تحت عنوان "العنوان البروتوكولي للشبكة المعلوماتية" على أنه: "مُعرّف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، ويتم إستخدامه لأغراض الإتصال".

[4]- تشير المذكرة التفسيرية لإتفاقية بودابست إلى أن تعريف البيانات المعلوماتية *Données informatiques* والواردة في المادة (1/ب) من هذه الإتفاقية والمأخوذة من هيئة التوصيف العالمية (*ISO*) وهذه البيانات المعلوماتية هي التي تكون هدفًا في كثير الجرائم الإلكترونية.

[5]- راجع المادة (2) (إ.ع.م.ج.ت.م) المشار إليها سلفًا. **الملحق رقم: (02)**

ثانيًا: في القوانين الوطنية

لقد ذكرت تقريبًا كل القوانين الوطنية الغربية منها والعربية مسألة تعريف نظام المعالجة الآلية للمعطيات، لذا سوف نسرد بعض هذه التعريفات التي جاءت في هذه القوانين معتمدين في ذلك التسلسل الزمني في صدورها، حيث نجد على سبيل المثال:

أ- القانون الفرنسي: إن مصطلح نظام المعالجة الآلية للمعطيات أُستعمل لأول مرة في نص قانوني عن طريق قانون العقوبات الفرنسي، وهو ما ذهبت إليه المادة الخامسة من القانون رقم (17/78) والمؤرخ في 16 جانفي 1978 والمتعلق بالحريات والمعلوماتية، والذي أُعتمد لحماية المعلومات الإسمية والشخصية، حيث عرفت نظام المعالجة الآلية على أنه: "جميع العمليات التي تتم آليًا، والتي تتعلق بالتجميع والتسجيل والإعداد والتعديل والإسترجاع والإحتفاظ ومحو المعلومات، وكذا مجموعة العمليات التي تتم آليًا بغرض إستغلال المعلومات وخصوصًا عمليات الربط والتقريب وإنتقال المعلومات ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة"[1]، ومع ذلك فإن هذا القانون لم يتضمن تعريف دقيق لنظام المعالجة الآلية للبيانات، رغم أنه يمثل أساس النظرية العامة للقانون الجنائي المعلوماتي[2].

ثم بعد ذلك إقترح مجلس الشيوخ الفرنسي عند تبنيه القانون رقم (88-19) المعروف بقانون "*Godfrain*" الصادر في 05 جانفي 1988 والمتعلق بمحاربة الغش المعلوماتي، والذي يشكل هو الآخر القاعدة الأساسية للإجرام المعلوماتي وذلك من خلال الأعمال التحضيرية لهذا القانون، فذكر مفهومًا جديداً لنظام المعالجة الآلية للمعطيات على أنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات المادية والمعنوية التي عن طريقها تتحقق نتائج معينة وهي معالجة المعطيات وتخزينها، على أن يكون هذا المركب خاضع للحماية الفنية"[3].

---

[1]- عدلت هذه المادة أكثر من مرة، آخرها بالقانون رقم (2004/801) المؤرخ في 16 أوت 2004، ونصها كما يلي:

« *… constitue un traitement de données à caractère personnel tout opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, ou la modification, l'extraction, la consultation, l'utilisation, la mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction…*».

- مشار إليه لدى: (- **رشيدة بوكر:** المرجع السابق، ص75).

[2]- ***GASSIN (R) :*** *Le droit pénal de l'informatique, Op. Cit, P11.*

[3]- **عبد القادر القهوجي:** المرجع السابق، ص120. - **خثير مسعود:** المرجع السابق، ص109. - **غنية باطلي:** المرجع السابق، ص138.

وهذا التعريف القانوني الفرنسي هو أول تعريف أشار إلى العناصر المادية والمعنوية التي يمكن أن يتكون منها النظام المعلوماتي[1]، لكن فيما بعد عرفت عناصر جديدة أخرى، وهذا ما يدل على أن مكونات النظام في هذا التعريف ورادة على سبيل المثال لا الحصر، وهذا بحكم أنها مكونات مستجدة ولها قابلية للتطور السريع[2]، وهذا التعريف الأخير لم يكن هو نفس التعريف الذي تم صياغته في النص النهائي الموجود في القانون رقم (88-19) بموجب المادة (462-2) من (ق ع ف).

ب- القانون السوري: لقد عرفت المادة (5/1) من القانون السوري رقم (17 لسنة 2012) والمتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية، نظام المعالجة الآلية للمعطيات بقولها: "النظام المعلوماتي هو كل مجموعة متسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها".

كما عرف أيضًا نفس القانون مصطلح "الشبكة" وذلك بموجب المادة (6/1) بأنها: "ترابط من الأجهزة الحاسوبية والمنظومات المعلوماتية يسمح بتبادل المعلومات أو التشارك فيها بين مرسل ومستقبل أو مجموعة من المستقبلين وفق إجراءات محددة".

وعرف هذا القانون أيضًا "الموقع الإلكتروني" بموجب المادة (7/1) منه بقوله: "الموقع الإلكتروني هو منظومة معلوماتية لها إسم أو عنوان يُعرّفها وتتضمن معلومات أو خدمات يمكن الوصول إليها عن طريق الشبكة وخاصة الإنترنت".[3]

---

[1]- أهم ما يتكون منه نظام المعالجة الآلية للمعطيات، هو جملة من المكونات والعناصر المادية والمعنوية والتي يفترض وجودها في أي مركب إلكتروني (الحاسوب الآلي *L'ordinateur*)، والتي من أهمها نجد:

- **وحدة المعالجة الرئيسية *l'unité centrale*:** وهي الوحدة المسؤولة عن عمليات حفظ البرامج والبيانات ومعالجتها، ويمكن وصفها بأنها عقل الكمبيوتر، لأنها تستقبل وتتولى تنفيذ جميع عمليات التشغيل والضبط والتحكم، ومعالجة البيانات وتنظيمها، وهي بدورها تتكون من "ذاكرة رئيسية *Mémoire centrale*" وأيضًا "وحدة الحاسب والمنطق *L'unité de calculs et logique*"، وكذا "وحدة التحكم *L'unité de contrôle*".

- **الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات *Les périphériques*:** وهذه الوسائط عبارة عن آلات تؤدي وظائف معينة بالتفاعل مع وحدة المعالجة الرئيسية، مثال ذلك "(آلة الطباعة *Imprimante*" وكذا "شاشة العرض *Écran*" وأيضًا "أداة القراءة والنقر على الأقراص المدمجة الخاصة بذاكرة القراءة *Lecteur graveur de CD Rom*" وغيرها كثير من هذه الوسائط. (لمزيد أكثر من التفصيل حول الموضوع راجع: - **جبريل بن حسن العريشي، حميدة بنت عبيد الصبحي:** المرجع السابق، ص30 وما بعدها).

[2]- بما أن هذه العناصر واردة على سبيل المثال وليس الحصر، فإن ذلك يفتح المجال واسعاً لإضافة عناصر جديدة أو ممكن حذف عناصر كانت موجودة من قبل، وذلك حسب ما يستوجبه التطور التقني والفني في هذا المجال. (أنظر : - **سفيان سوير:** المرجع السابق، ص86).

[3]- أنظر في ذلك المرسوم التشريعي السوري رقم (17 لسنة 2012) والمتعلق بتطبيق أحكام التواصل على الشبكة ومكافحة الجريمة المعلوماتية، والمؤرخ في 2020/2/8.

ج- **القانون الأردني:** عرفت المادة (1/2) من القانون الأردني رقم (27 لسنة 2015) والمتعلق بقانون الجرائم الإلكترونية، نظام المعالجة الآلية للمعطيات بقولها: "النظام المعلوماتي عبارة عن مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيًا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية".

أما بخصوص "الشبكة المعلوماتية" فعرفتها المادة (4/2) من نفس القانون بقولها: "إرتباط بين أكثر من نظام معلوماتي لإتاحة البيانات والمعلومات والحصول عليها".

كما عرف أيضًا هذا القانون "المواقع الإلكترونية" بموجب نص المادة (5/2) بقوله: "الموقع الإلكتروني هو عبارة عن حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد".[1]

د- **القانون المصري:** عرف المشرع المصري نظام المعالجة الآلية للمعطيات وذلك بموجب نص المادة (11/1) من القانون رقم (175 لسنة 2018) بقولها: "النظام المعلوماتي هو مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية".

كما عرف المشرع المصري مصطلح "الشبكة المعلوماتية" بموجب المادة (12/1) من نفس القانون بقوله: "الشبكة مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معًا ويمكنها تبادل المعلومات والإتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية والتطبيقات المستخدمة عليها".

كما زاد المشرع المصري في تعريف كل من "المواقع الإلكترونية" و"الحساب الخاص" وكذا "البريد الإلكتروني"، وإعتبرهم كلهم من قبيل نظام المعالجة الآلية للبيانات وذلك بموجب كل من المادة (13/1): "الموقع الإلكتروني هو كل مجال أو مكان إفتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"، والمادة (15/1): "الحساب الخاص هو مجموعة من المعلومات الخاصة بشخص طبيعي أو إعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو إستخدامها من خلال موقع أو نظام معلوماتي"، وكذا المادة (16/1): "البريد الإلكتروني هو عبارة عن وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين

[1]- أنظر في ذلك القانون الأردني رقم (27 لسنة 2015) والمتعلق بقانون الجرائم الإلكترونية، الجريدة الرسمية رقم (5631) لعام 2015.

أكثر من شخص طبيعي أو إعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها".[1]

ونلاحظ هنا أن المشرع المصري هو الآخر أخذ بالإتجاه الموسع في تعريفه لنظام المعالجة الآلية للمعطيات، إذ أنه دمج بين مصطلحين معًا "الآلية والمعلوماتية"، كما زاد المشرع المصري في تعريف هذا النظام من خلال إبتكاره لمصطلح جديد وهو "المعالجة الإلكترونية" والتي عرفها هي الأخرى بموجب المادة (6/1) من نفس القانون بقوله: "المعالجة الإلكترونية هي أي عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو إستقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو إسترجاع أو إستنباط البيانات والمعلومات الإلكترونية، وذلك بإستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى".[2]

وكخلاصة لما سبق ذكره نجد أن العديد من المشرعين يذكرون إستقلالاً أن مفهوم نظام المعالجة الآلية للبيانات يشمل كل من المواقع الإلكترونية وكذا الشبكات المعلوماتية والحسابات الإلكترونية الخاص مثل البريد الإلكتروني والإيميل وغيرها، هي صورة نموذجية للمنظومة المعلوماتية الموصولة بالشبكة الدولية للمعلومات كالإنترنت، وهذا لأهمية هذه الأنظمة وشيوعها، وأن كل منها له إسم وعنوان تُعرف به، وتتضمن معلومات وخدمات يمكن الوصول إليها عن طريق الشبكة المعلوماتية وخاصةً الإنترنت.[3]

وعلى ذلك فإنه لا وجود لنظام المعالجة الآلية للمعطيات، ولا يمكن أن نتصور وقوع أي جريمة من جرائم الإعتداء على هذا النظام، في حالة مثلاً إذا وقع الإعتداء بالسرقة على عنصر بمفرده لا يشكل جزءًا من النظام كما لو وقع الإعتداء بالسرقة على برامج معروضة للبيع أو وقع الاعتداء على جهاز الحاسب لم يدخل الخدمة بعد، أو أنها لا تزال مودعة بالمخازن، أو أنه وقع الإعتداء على الأجهزة التي خرجت من الخدمة تمامًا، وهذا على عكس القرص النقال والقرص المرن والقرص المضغوط والتي تحتوي جميعها على قاعدة البيانات والمعطيات والبرامج

[1]– راجع القانون المصري رقم (175 لسنة 2018) والمتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسميـــة، العـــدد (32 مكرر ج) المؤرخة في 14 أغسطس 2018. **الملحق رقم (04)**

[2]– راجع المادة (6/1) من نفس القانون المصري. **الملحق رقم (04)**

[3]– **وسيم طعمة:** السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، دمشق، سوريا، المجلد رقم 39، العدد 68، لعام 2017، ص171.

المعلوماتية والتي بإستخدامها يمكن التواصل والدخول إلى الأنظمة المعلوماتية، فإنها تعتبر حسب القانون من قبيل نظم المعالجة الآلية للمعطيات.[1] بينما تقع الجريمة المعلوماتية إذا وقع الإعتداء مثلاً على النظام وهو خارج ساعات تشغيله العادية، أو حتى إذا كانت أحد عناصره أو مكوناته في حالة عطل مؤقت.[2]

ثالثًا: موقف المشرع الجزائري من تعريف نظام المعالجة الآلية للمعطيات

لم يعرف المشرع الجزائري هذا النظام في "الفصل السابع مكرر" من قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وذلك بموجب القانون رقم (04-15) والمشار إليه سلفاً، ولكن فيما بعد عرَّف المشرع الجزائري هذا النظام وذلك من خلال تبنيه للتعريف الذي جاءت به الإتفاقية الدولية الأوروبية للإجرام المعلوماتي، وهذا بموجب المادة (2/2) من القانون رقم (04/09) والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث أطلق هو الآخر على نظام المعالجة الآلية للمعطيات تسمية "منظومة معلوماتية" وعرفها بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين".[3]

يتضح من هذا التعريف أن هناك إختلاف واضح بينه وبين ما جاء به المشرع الفرنسي، لاسيما من حيث الصياغة والدقة في التعريف، كوْن أن القانون الفرنسي جاء يعرف نظام المعالجة الآلية للمعطيات بتعريف عام وغير دقيق، ومع ذلك نجد أن المشرع الجزائري كان على صواب إلى حد كبير، لأن أنواع الأنظمة المعلوماتية أصبحت كثيرة ولا تنحصر فقط في أجهزة الكمبيوتر والحاسوب، بل أنها تشمل كل نظام أو جهاز بإمكانه المعالجة الآلية للمعطيات معلوماتيًا.

وعليه وإن كان القانون الجزائري لم يأتي على ذكر مصطلحات الشبكة المعلوماتية أو الموقع الإلكتروني بصريح العبارة كما فعل ذلك نظرائه من المشرعين العرب، فإنه حسب التعريف السابق الذي جاء به المشرع الجزائري نجده يشمل أيضًا شبكة الإنترنت وكذا البريد الإلكتروني والمواقع الإلكترونية الموجودة على الشبكة وحتى البطاقات الإلكترونية، كل ذلك يعتبر من قبيل

---

[1]- **نسيم دردور:** الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2013، ص22.

[2]- **خثير مسعود:** المرجع السابق، ص110.

[3]- راجع في ذلك القانون رقم (09-04) والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمؤرخ في 5 أوت 2009، ج ر العدد 47، المؤرخة في 16 أوت 2009. **الملحق رقم (06)**

النظم المعلوماتية، وهذا ما تؤكده العبارة الواردة في تعريف النظام المعلوماتي بقولها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة" إلا أن المشرع لم ينص في هذا التعريف صراحة على وجوب توافر حماية فنية للنظام كي تقوم الجريمة، وحسناً فعل في ذلك.

مع الإشارة هنا أن المشرع الجزائري هو الآخر جاء بمصطلح جديد تحت إسم "المعطيات المتعلقة بحركة السير" وعرفه بموجب المادة (5/2) من نفس القانون بقوله: "أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة بإعتبارها جزءًا في حلقة إتصالات توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة".[1]

رأينا الخاص:

بالرجوع إلى المفاهيم الفقهية والقانونية السابقة في تعريفها لنظام المعالجة الآلية للمعطيات نجد أن كلها تتفق على أن هذا النظام يشتمل على عناصر مادية ومعنوية يتكون منها المركب والعلاقات التي تربط بين هذه العناصر المختلفة وتوحدها نحو تحقيق هدف واحد محدد ألا وهو المعالجة الآلية للمعطيات.

ومن هنا يمكننا القول أن هذه العناصر المادية والمعنوية والتي يتكون منها النظام المعلوماتي إنما جاءت على سبيل المثال لا الحصر، وهذا لفتح المجال أمام إضافة عناصر أخرى وجديدة، أو حذف بعضها حسب ما يفرزه التطور التقني والتكنولوجي في هذا المجال.

المطلب الثاني: ضرورة خضوع نظام المعالجة الآلية للحماية الأمنية

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكة المعلوماتية وبالأخص شبكة الإنترنت، فهم يسعون لتأمين سرية الإتصالات الإلكترونية[2]، وسرية البيانات المتناقلة خاصة منها الأعمال التجارية والإقتصادية الرقمية، ويرى الخبراء أن أفضل وسيلة للحفاظ على سرية هذه البيانات المتناقلة هي ضرورة إستخدام أسلوب التشفير لمنع الآخرين من الإطلاع أو الإعتداء على هذه الرسائل الإلكترونية.[3] وفي مسألة الحماية الأمنية أو كما يسميها

---

[1]– راجع نفس القانون الجزائري. **الملحق رقم (06)**

[2] لقد عرفت المادة (6/2) من القانون الجزائري رقم (04/09) المشار إليه سلفا، مصطلح "الاتصالات الإلكترونية" بقولها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

[3] **أمال قارة:** الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، 2006، ص103.

البعض "بالحماية الفنية"، فإن المهتمون بمسألة النظام المعلوماتي يقسمون هذا الأخير إلى أنواع (فرع أول) على أن تكون لها وسائل حماية أمنية (فرع ثاني).

الفرع الأول: أنواع النظم المعلوماتية من حيث توافرها على الحماية الأمنية

بدوره النظام المعلوماتي ينقسم إلى ثلاثة أنواع وهذا من حيث توافره على وسائل الحماية الأمنية وهي كالآتي:

أولاً: الأنظمة المعلوماتية المنفتحة بدون حماية

وهي عبارة عن أنظمة معلوماتية مفتوحة للجمهور، وهي ليست بحاجة إلى حماية أمنية أو فنية.

ثانيًا: الأنظمة المعلوماتية المنغلقة بدون حماية

وهي عبارة عن أنظمة معلوماتية قاصرة على أصحاب الحق فيها ولكنها غير محمية أمنيًا أي بدون حماية فنية.

ثالثًا: الأنظمة المعلوماتية المنغلقة والمحمية

وهي عبارة عن أنظمة معلوماتية قاصرة على أصحاب الحق فيها بالإضافة إلى تمتعها بنظام حماية أمنية أي أنها تتمتع بحماية فنية.

ومن خلال هذا التقسيم الثلاثي لأنواع النظم المعلوماتية، يرى بعض الفقه أن النوع الثالث فقط من تلك الأنظمة هو وحده ودون غيره الذي يتمتع بالحماية الجنائية أما النوعين الآخرين فلا يتمتعان بتلك الحماية، وحسب نظرهم أن هذه الحماية الجنائية يجب أن تكون مقصورة على الأنظمة المعلوماتية المنغلقة والمحمية أمنياً وفنيًا فقط، لأنه من الطبيعي في نظرهم أن من يدعي ملكية الشيء وجب عليه أن يضع له الوسائل اللازمة لحمايته ودفع الإعتداء عليه في مقدور الرجل الحريص، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، بينما من يجعل أمواله هكذا متروكة ومهملة ولا يوفر الحد الأدنى لحمايتها فلا تشمله الحماية الجنائية.

الفرع الثاني: وسائل الحماية الأمنية في النظم المعلوماتية

والمقصود بالحماية الأمنية والفنية هو وجود وسائل مادية وأخرى غير مادية لحماية المعلومات والأنظمة المعلوماتية من الدخول العشوائي والغير المنظم إليها، ولعل من أبرز هذه الوسائل المادية وغير المادية في تأمين النظام المعلوماتي نجد ما يلي:

أولاً: وسائل الأمن المادية

يقصد بها المحافظة على الأجهزة والحواسيب الآلية -كالكمبيوتر وملحقاته- وتحصين أماكن تواجدها عن طريق إتخاذ جملة من الإجراءات الأمنية المادية والملموسة كإستعمال الأقفال والمفاتيح والبطاقات الإلكترونية وغيرها من الوسائل الدفاعية المادية، وهي تعتبر وسائل تأمينية هامة، بحيث لا تسمح بالدخول إلى مكان تواجد الأجهزة والأنظمة المعلوماتية إلاّ بعد الخضوع لإختبارات من طرف أجهزة الحماية للتأكد من الشخصية الحقيقية لمستعمل النظام، ومثالها إستعمال كلمة السر أو بصمات الأصابع وغيرها[1]، ولعل الهدف من ذلك كله هو تأخير وعرقلة الدخيل الأجنبي عن النظام قدر المستطاع لحين إعطاء فرصة أكبر لأجهزة الأمن من الكشف عليه قبل وقوع الجريمة.[2]

ثانيًا: وسائل الأمن غير المادية

يكمن دورها في المحافظة وتأمين الأنظمة المعلوماتية من الدخول إليها بسهولة، بحيث يستطيع المسؤول على هذه الأنظمة أن يضع عدة طرق ووسائل أمنية غير مادية لحمايتها من الدخلاء ومنع الوصول إليها بسهولة، وذلك مثلاً عن طريق ما يسمى بـــ "الجدار الناري *Le par feu*"[3]، الذي يعرف بنظام التصدي لعمليات الدخول غير المرغوب فيها إلى النظام المعلوماتي، بحيث تعتبر هذه الوسيلة الأمنية الأنجع لحماية سلامة المعلومات المعالجة آليًا والموجودة داخل النظام[4].

كما توجد العديد من طرق الحماية الأمنية الغير المادية، كإستخدام الخصائص البيولوجية مثل بصمة حدقة العين أو بصمة نبرة الصوت أو إستخدام التوقيع الإلكتروني أو إستخدام عملية

---

[1]- **أحمد حسام طه تمام:** الجرائم الناشئة عن إستخدام الحاسب الآلي، دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 2001، ص293.

[2]- **أيمن عبد الحفيظ:** المخاطر التي تتعرض لها شبكة الإنترنت وسبل حمايتها، مجلة مركز بحوث الشرطة، العدد 20، القاهرة، مصر، 2001، ص452.

[3]- **يقصد "بالجدار الناري"**: ذلك النظام الأمني الحديث والجد متطور يقوم بتوفير حماية أمنية بين شبكة الإنترنت وجهاز الحاسوب، وذلك من خلال إجبار جميع عمليات العبور إلى الشبكة والخروج منها أن تمر من خلال هذا الجدار الناري، الذي بدوره يقوم بالتصدي لكل المستعملين المتدخلين والمتطفلين والتحقق من هويتهم وكذا التحقق من هوية جهاز الحاسوب المستعمل في النطاق المحلي أو الخارجي، وكذا تأمين نظام الدخول والخروج وتشفير المعلومات، ووضع حماية للبرامج من الفيروسات الخبيثة، فهذا الجدار الناري يعمل كجسر إلكتروني يراقب كل عمليات الدخول والخروج من وإلى الشبكة، ولعل من أشهر تطبيقات نظام الجدار الناري نجد على سبيل المثال "برنامج المنطقة المسلحة *Zone Alarm*" نظرًا لكفاءته في ضبط ورصد كافة محاولات إختراق الأجهزة والأنظمة المعلوماتية (لمزيد أكثر حول الموضـــوع أنـــظر كل مـــن: - **غنية باطلي:** المرجع السابق، ص142. - **رشيدة بوكر:** المرجع السابق، ص68).

[4]- **إسماعيل عبد النبي شاهين:** تأمين المعلومات في الإنترنت بين الشريعة والقانون، مجلة كلية الشريعة والقانون، العدد 19، جامعة طنطا، مصر، 2005، ص09 وما بعدها.

التشفير وغيرها، وكلها من الأفكار العلمية الرياضية التي ما زالت لحد الآن من الطرق الأكثر فعالية.[1]

ومع ذلك فإن نظم الحماية الأمنية أو الفنية وإن كانت هامة جدًا في الحد أو التقليل من الإعتداءات إلا أن وحدها غير كافية في حماية النظام المعلوماتي من سائر الجرائم الإلكترونية المختلفة، فالتجربة والتطور التقني والتكنولوجي أثبت أن مجرمي التقنية لهم القدرة الفائقة على إبتكار أنماط إجرامية بإستخدام برامج ووسائل وطرق جديدة بصفة مستمرة قد تجعل طرق الحماية الفنية عاجزة على إستيعابها[2]، وهذا ما خلق نوع من التحدي بين شركات تصنيع برامج الأمن الإلكتروني وبين المجرمين الذين يتمتعون بقدراتهم الفائقة على تطوير وسائل إختراقهم لمختلف الأنظمة المعلوماتية الحديثة والمتطورة.[3]

وعليه وإن كانت الحماية الفنية هامة ولازمة، فهي غير كافية لوحدها لضمان سلامة النظام المعلوماتي، بل كان لابد من تكملتها بنظم حماية من أنواع أخرى كالحماية المرفقية والإدارية وأبرزها على الإطلاق الحماية القانونية، وهذه الأخيرة هي الأخرى واسعة جدًا وناجعة إذا ما تم تفعيلها، ولعل أهم حماية قانونية يمكن توفيرها للنظام المعلوماتي ككل، نجد الحماية الجنائية لما توفره من نصوص تجريمية وعقابية رادعة لكل من تسوّل له نفسه الإعتداء على مثل هذه النظم المعلوماتية ذات القيم والمراكز القانونية والحقوق.

ثالثًا: الحماية الجنائية للنظم المعلومتية بين التضييق والتوسيع

في حقيقة الأمر أن إشتراط ضرورة وجود نظام أمان لحماية محتويات النظم المعلوماتية من الدخول إليها أو البقاء فيها بغير سند من القانون من أجل قيام الحماية الجنائية لهذه النظم، ليس محل إتفاق بين فقهاء القانون –لاسيما الفقه الفرنسي– لذا إنقسم الفقه الجنائي بخصوص هذه المسألة إلى إتجاهين إثنين، فمنهم من وسع مجال الحماية الجنائية لتشمل كل من الأنظمة المعلوماتية المحمية والأنظمة المعلوماتية غير المحمية، وهناك من قصر مجال الحماية الجنائية على الأنظمة

---

[1]– أشهرها إستخدام طريقة (*R.S.A*) وهي إختصار لكلمات (*Aldman. Shamir. Riverst*) وهي طريقة أمنية غير مادية تستعمل لحمايـــة النظام المعلومـــاتي مـــن الإختـــراق والدخول إليه. (أنظر كل من: – **أيمن عـــبد الحـــفيظ:** المرجع الـــسابق، ص466–467. – **غنية باطلي:** المرجع السابق، ص143. – **إسماعيل عبد النبي شاهين:** نفس المرجع، ص13. – **نائلة عادل محمد فريد قورة:** المرجع السابق، ص365).

[2]– **غنية باطلي:** المرجع السابق، ص143.

[3]– **محمد خليفة:** المرجع السابق، ص29.

المعلوماتية المحمية بنظام أمان دون غيرها من الأنظمة المعلوماتية غير المحاطة بنظام الأمان، وهذا ما سوف نتطرق إليها هنا.

أ- الإتجاه المضيق في الحماية الجنائية للنظم: يرى أنصار هذا الإتجاه أن نظام الحماية الأمنية داخل النظم المعلوماتية هو بالأهمية بمكان من أي حماية أخرى بما فيها الحماية الجنائية، بحيث يلزم مستخدمي النظام المعلوماتي -كالشركات مثلاً- وضع حد أدنى من الحماية الفنية الذي لا يمكن النزول عنه من قبل مستخدمي هذا النظام، حيث يؤدي التقصير في ذلك إلى تحمل هؤلاء مسؤولية هذا التقصير.

ولهذا كان على القانون الجنائي أن يلزم مستخدمي أو مالكي النظم المعلوماتية بوضع أي من الأطر الحمائية لأنظمة المعالجة الآلية للبيانات الخاصة بهم والتي تتناسب مع قدر وأهمية ما تحتويه من معلومات وأسرار[1]، ولا يتسنى ذلك إلاَّ بإشتراط أن تكون هذه النظم مشمولة بالحماية من قبل أصحابها ضد التسلل إليها بالولوج أو البقاء في محتوياتها أو بإرتكاب أي من الأفعال الإجرامية الأخرى، فوجود مثل هذه الأنظمة الأمنية سوف يسهل عملية الكشف عن الجريمة في حالة إختراق هذه الأنظمة لأنه في العادة يترك أثر يدل عليه، فهذا الإختراق يساعد على التحقق من وجود القصد الجنائي لدى الفاعل.[2]

ومن حججهم في ذلك أن الحماية الأمنية للنظم المعلوماتية هو إلتزام ضروري وقانوني نصت عليه بعض القوانين الجنائية بما فيها القانون الخاص بالحريات والمعلومات الفرنسي لعام 1978 والذي يعتبر سابقة تشريعية في هذا الأمر وهذا بموجب المادة (29) منه والتي تلزم كل شخص أو شركة أو أية منشئ برامج يعمل بمجال المعالجة الآلية للبيانات أو مالك النظام أو المسؤول عنه بضرورة إتخاذ الإحتياطات الأمنية اللازمة لحفظ وحماية هذه البيانات وتأمين نظامه ضد أي إعتداء عليها بواسطة أشخاص غير مصرح لهم الإطلاع عليها.[3]

---

[1]- **بلال أمين زين الدين:** المرجع السابق، ص266.

[2]- **غنية باطلي:** المرجع السابق، ص144.

[3]- لقد جعلت المادة (29) من قانون الحريات والمعلومات الفرنسي الصادر بتاريخ 1978/1/6 وكذلك نص المادة (226-17) من (ق ع ف) والتي تعاقب على كل إجراء أو معالجة آلية لمعلومات إسمية وشخصية دون إتخاذ الاحتياطات اللازمة لتأمين هذه البيانات، ولا ينحصر الأمر في المعلومات الشخصية والإسمية فقط، بل تشمل كل المعطيات بما فيها تلك التي تحميها المادة (323-1) من (ق ع ف) لعام 1988، وأن الإخلال بهذا الإلتزام جريمة يخضع مرتكبها للعقوبات المنصوص عليها بالمادة (42) من (ق ع ف) لعام 1994، وهذا ما يؤكد على أن الأعمال التحضيرية لقانون الغش المعلوماتي الفرنسي أثبت في العديد من المرات رغبتهم في ربط هذه الجرائم بضرورة وجود الأنظمة المعلوماتية المحمية بنظام أمان.

ويؤكد أنصار هذا الإتجاه أن المنطق السليم يقصر الحماية الجنائية على الأنظمة المعلوماتية المشمولة بنظم الحماية الفنية فقط، بحيث لا ينبغي حماية حق لم يحتط له صاحبه، وهذا ما يجعل الأشخاص يلجأون إلى القانون الجنائي في حالة عجز هذه التدابير الأمنية عن حماية أنظمتهم[1]، وهذا ما يؤكد أهمية النظم الأمنية والتي يرى أنها ضرورة ولابد منها في قيام جريمة الدخول أو البقاء غير المشروع داخل الأنظمة المعلوماتية والتي تعدُّ وبحق مدخلاً للجرائم الأخرى.

وعليه فإن التفسير السليم لنص تجريم الدخول أو البقاء غير المصرح به يقتضي قصره على إختراق الأنظمة المعلوماتية المحمية دون الأخرى[2]، وأن نظام الأمان شرط لازم لقيام جريمة الدخول أو البقاء غير المشروع في أنظمة المعلومات المعالجة آليًا، وأن القانون يجرّم الإعتداء على نظم الأمن التي يحتويها النظام المعلوماتي، فالإعتداء على نظم الحماية الأمنية هو بمثابة شرط ضروري في كافة الأفعال الإجرامية الإلكترونية[3]، أي أنها لا تحظى بالحماية سوى تلك الأنظمة المعلوماتية المحمية بأجهزة أمان.[4]

ب- الإتجاه الموسع في الحماية الجنائية للنظم: لقد أُنتقد الإتجاه المقيد والمضيق للحماية الجنائية بشدة، وهذا لأنه يبني فكره على أن المنطق والعدالة يتطلبان شرط الأمان والحماية الفنية للنظام المعلوماتي حتى يمكننا الحديث عن الحماية الجنائية ومعها قيام الجريمة المعلوماتية، لكن الواقع والحقيقة القانونية غير ذلك تمامًا. ومن هنا ورد على هذا الإتجاه جاء إتجاه آخر يوسع من مجال الحماية الجنائية لتشمل كل الأنظمة المعلوماتية المحمية منها وغير المحمية، وحجتهم في ذلك أن القانون الجنائي جاء لتوفير الحماية لكل الأملاك والأموال المحروزة بالحماية الأمنية والغير المحروزة، فمثلاً تمتع المال المسروق بحماية صاحبه أو عدم تمتعه بذلك فهذا لا يؤثر في قيام جريمة السرقة[5].

كما أنه لو سلمنا أن هناك من يتخذ اللازم من الاحتياطات والحذر والنواحي الأمنية لحماية أنظمتهم المعلوماتية ضد أفعال العبث والبلطجة والقرصنة الإلكترونية، فإنه في المقابل يجب أن لا

---

[1]- **محمد خليفة:** المرجع السابق، ص134.

[2]- **نائلة عادل محمد فريد قورة:** المرجع السابق، ص367.

[3]- **بلال أمين زين الدين:** المرجع السابق، ص267.

[4]- **غنية باطلي:** المرجع السابق، ص144.

[5]- **طارق عبد الله الشدى:** آلية البناء الأمني لنظام المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، السعودية، 2000، ص273.

ننسى ذلك الشخص الآخر الذي يفترض فيه أن يكون على قدر كبير من الذكاء أو بمعيار الرجل العادي متوسط الذكاء، والذي يستطيع بطريقة أو بأخرى خرق العديد من نظم الحماية الأمنية المعلوماتية، إذ يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في ذلك النظام، وبالتالي سوف يستوي في ذلك النظام المحمي مع النظام غير المحمي بأمان[1].

من هذا المنطلق ذهب الإتجاه الغالب في الفقه الفرنسي إلى القول بعدم ضرورة وجود هذا النظام الأمني كشرط لقيام جريمة الدخول أو البقاء غير المشروع داخل النظام[2]، لأن مثل هذا الشرط سوف يتجاهل الكثير من الحالات التي يتم فيها الدخول بطريقة وأخرى إلى النظام المعلوماتي، وبالتالي سوف يضيق من مجال تطبيق النص الجنائي.[3] وبالرجوع إلى النصوص القانونية المتعلقة بجرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات في كل التشريعات الجنائية الحديثة تقريبًا، لا نجدها تتضمن شرط الحماية الأمنية والفنية، حيث خرجت تلك النصوص خالية منه تمامًا.

إذ أنه من المبادئ العامة والمتعارف عليها والمستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص العام المطلق أو تخصص النص العام إلاَّ إذا وجد نص خاص يجيز ذلك، تحت مسمى القاعدة الفقهية الشهيرة "الخاص يقيد العام"، ولا يوجد في موضوعنا هذا نص خاص يقيد إطلاق النص العام أو يخصص عمومه، وما دام أن مثل هذا النص غير موجود فيفهم من ذلك أن المشرع الجنائي إنما أراد إستبعاد هذا الشرط –أي شرط الحماية الأمنية والفنية– وأنه جعل من نطاق الحماية الجنائية يمتد ليغطي كافة النظم المعلوماتية سواء كانت تتمتع بحماية فنية أم لا.[4]

---

[1]– **فخري محمود خليل:** المرجع السابق، ص170.

[2]– يستند هذا الرأي إلى نصوص قانونية مثل نص المادة (462–2) من قانون العقوبات الفرنسي لعام 1988 والتي عدلت بنص المادة (323–1) من قانون 1994، حيث لم تشترط هاتين المادتين في جريمة الدخول أو البقاء غير المشروع داخل النظام أي شرط كنظام الحماية الأمنية، كما أن مجلس النواب الفرنسي رأى أن من شأن النص على هذا الشرط في سياق النص القانوني من شأنه أن يحد من بسط الحماية الجنائية للنظم المعلوماتية الغير مشمولة بنظام للحماية الأمنية ضد أفعال الإعتداء، كما يستند أنصار هذا الرأي إلى تقرير جلسات البرلمان الفرنسي التي سبقت صدور قانون العقوبات الفرنسي لعام 1988 والتي إنتهت إلى عدم الأخذ بوجهة النظر التي كانت تنادي بإشتراط شمول نظام المعالجة الآلية للبيانات بأي من نظم الحماية، وهذا ما يفسر إرادة البرلمان في رفض تطلب مثل هذا الشرط، وأن الأعمال التحضيرية ليس لها قوة إلزامية على القانون وإنما يستعينان بها في تفسير النصوص الغامضة أو المتعارضة. (أنظر كل من: – **بلال أمين زين الدين:** المرجع السابق، ص 268. – **نائلة عادل محمد فريد قورة:** المرجع السابق، ص368. – **غنية باطلي:** المرجع السابق، ص145).

[3]– ***BENSOUSSAN Alain*** *: Internet « aspects juridiques » éd. Hermes, Paris, France, 1998, P198.*

[4]– **عبد القادر القهوجي:** الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الاسكندرية، مصر، 1999، ص28.

وتطبيقًا لذلك كله، فإنه لا يشترط لوجود الجريمة المعلوماتية أن يكون الإعتداء على النظام مقيدًا بوجود حماية أمنية وفنية، ولكن إذا نظرنا إلى الواقع الميداني والعملي نجد اليوم أن غالبية الأجهزة والحواسيب وكل أنظمة المعالجة الآلية للمعطيات أصبحت تتمتع بنظم حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية الأمنية سوف تساعد بالتأكيد على إثبات أركان الجريمة المعلوماتية وصفة مرتكبها وتحديد القصد الجنائي من عدمه.

رابعًا: موقف المشرع الجزائري من هذه المسألة

إن الأخذ بفكرة ضرورة وجود نظام أمان قد يطرح عدة تساؤلات وهي تحديد مواصفات نظام الأمان، وكذا الحد الأدنى من الأمان، وأيضًا كيفية تحديد هذا الأمان نوعًا وكمًا، كل هذا جعل الكثير من المشرعين يأخذون موقف من هذه المسألة بما فيهم المشرع الجزائري.

حيث يرى المشرع الجزائري أنه لا مانع من أن يكون النظام المعلوماتي مشمولاً بالحماية الأمنية أو أي من نظم الأمن التي لا تسمح بمحاولات التسلل أو التلصص أو الإطلاع أو التصنت، وذلك وفقًا لما أعطته إتفاقية بودابست للدول الأعضاء من الحرية في النص أو عدم النص على هذا الشرط في قوانينها الجنائية الداخلية.

والحقيقة أن ما جاء به المشرع الجزائري في نصوص قانون العقوبات بخصوص مسألة المساس بأنظمة المعالجة الآلية للبيانات، هو أكثر مرونة ودقة في فهم النص، فكل إعاقة وتعطيل لحركة الإتصالات سواء أكانت بالولوج إلى النظم المعلوماتية أو التأثير عليها وتشويشها دون الدخول إليها أصلاً، فإن مثل هذه الأمور يشملها النص الجنائي أيضًا.

فلو فرضنا أنه تم النص على هذا الشرط في سياق نص المادة (394 مكرر) من (ق ع ج) من شأنه أن يحد من بسط الحماية الجنائية للنظم المعلوماتية الغير مشمولة بنظام الحماية الأمنية ضد كل أفعال الإعتداء، وهذا ما قد يهدر بعض الشيء من قيمة المعلوماتية والحماية المرغوب فيها، ولهذا إكتفى المشرع الجزائري بالنص في المادة (394 مكرر) على أن يكون الدخول أو البقاء قد تم بشكل غير مشروع وحسنًا فعل في ذلك.

لذا يرى المشرع هنا أن نظام الحماية الأمنية لا يكون له دورًا إلا في مسألة الإثبات –أي إثبات القصد الجنائي– لدى مرتكب جريمة الدخول أو البقاء غير المشروع داخل النظام، والذي يمكن إثباته بأي من الطرق الإثباتية الأخرى التي يقتنع بها القاضي الجزائي، وهذا ما تطلبته كل

من المادتين (394 مكرر) من (ق ع ج) و(323-1) من (ق ع ف) وهو أن الدخول بطريق الغش هو أمر يتعلق بالركن المعنوي وليس بالركن المادي حتى يتبين القصد الجنائي لقيامها.

أضف إلى ذلك أنه من الناحية العملية فإن غالبية أنظمة المعالجة الآلية للمعطيات أصبحت تتمتع بنظام حماية فنية وأمنية، وأن وجود مثل هذا النظام سوف يساعد حتمًا قضاة الموضوع خاصةً في مسألة إثبات سوء النية لدى الجاني.[1]

وفي الأخير يمكننا القول أن سكوت المشرع الجزائري على هذا الشرط يقصد به خضوع جميع الأنظمة المعلوماتية للحماية الجنائية سواء كانت محمية بنظام أمان أم غير محمية، وهذا ما أكدت عليه أيضًا غالبية القوانين الجنائية المقارنة في أن مثل هذا الشرط ليس ضروريًا لأن المبدأ المستقر عليه في مجال المعلوماتية هو مبدأ الشرعية الجنائية فقط، أما بخصوص شرط الأمان فإن عدم ذكر المشرع له وعدم إشتراطه يعني أنه أراد إستبعاده صراحةً، وهكذا نجد أن المشرع الجزائري يسير بنفس النهج الذي ذهب إليه المشرع الفرنسي بخصوص هذه المسألة.

[1]- **مختارية بوزيدي:** المرجع السابق، ص15. - **عبد المجيد جباري:** المرجع السابق، ص110.

الفَصل الثّانِي

أركان وعناصر جريمة الدخول أو البقاء غير المشروع والعقوبات المقررة لها

الفصل الثاني: أركان وعناصر جريمة الدخول أو البقاء غير المشروع والعقوبات المقررة لها

تمهيد وتقسيم:

بعد أن بيّنا في الفصل الأول من هذا الباب مفهوم وتعريف جرمة الدخول أو البقاء غير المشروع في النظام المعلوماتي من الناحية الفقهية والقانونية، ومفارقتها ببعض المصطلحات المشابهة لها وذات الصلة معها، فتبين أنها جريمة يلزم لقيامها توافر أركان وعناصر قانونية محددة، وأنها جريمة ذات طبيعة خاصة لاسيما من حيث العقوبات المقررة لها.

حيث تعاقب غالبية التشريعات الجنائية الحديثة على هذه الجريمة، إلاَّ أن موقفها حيالها متباين فمن هذه التشريعات ما يلزم بتوافر شروط معينة سواء بخصوص أنشطة تمس الحاسب الآلي أو البيانات الموجودة فيه بنية الإستلاء والإستحواذ على المعلومات بطريق الغش المعلوماتي، وفي نفس الإتجاه تعاقب تشريعات أخرى على مجرد الدخول أو البقاء بغض النظر عن نية المتهم في إرتكاب هذه الجريمة ومهما كان الأسلوب المتبع في إتيان هذا الغش المعلوماتي سواءً كان بقصد أو بدون قصد.

ولمعرفة متى تتحقق هذه الجريمة لابد من تحديد أركانها وعناصر قيامها، ثم التطرق لأهم الإجراءات العقابية المقررة لها، وهذا ما سوف نعالجه في هذا الفصل من خلال التطرق إلى مبحثين إثنين على التوالي:

المبحث الأول: الأركان والعناصر القانونية لقيام جريمة الدخول أو البقاء غير المشروع

المبحث الثاني: الإجراءات العقابية والردعية المقررة لجريمة الدخول أو البقاء غير المشروع

المبحث الأول: الأركان والعناصر القانونية لقيام جريمة الدخول أو البقاء غير المشروع

تمهيد وتقسيم:

لقيام جريمة الدخول أو البقاء بدون تصريح في الأنظمة المعلوماتية، يتعين توافر عدد من الأركان والعناصر القانونية، وذلك هو الحال بالنسبة لمختلف الجرائم المعلوماتية الأخرى، فهناك أركان مشتركة بين جميع الجرائم، وهناك عناصر قانونية متطلبة في جريمة دون الأخرى حسب خصوصية كل منها.

ولعل من أهم الأركان التي يستلزم القانون توافرها لقيام أية جريمة نجد الركن الشرعي، وكذا الركن المادي، وأخيرًا الركن المعنوي، وهذا ما سوف نعالجه في هذا المبحث وفق ثلاثة مطالب على التوالي:

المطلب الأول: الركن الشرعي لجريمة الدخول أو البقاء غير المشروع

المطلب الثاني: الركن المادي لجريمة الدخول أو البقاء غير المشروع

المطلب الثالث: الركن المعنوي لجريمة الدخول أو البقاء غير المشروع

المطلب الأول: الركن الشرعي لجريمة الدخول أو البقاء غير المشروع

نظرًا لأهمية تجريم كل من فعل الدخول غير المصرح به وفعل البقاء غير المشروع داخل النظام المعلوماتي كجريمة إلكترونية مستحدثة، فقد أولت لها معظم التشريعات الجنائية الحديثة إهتمامًا كبيرًا على جميع الأصعدة، حيث جرمت غالبية الدول والتشريعات المقارنة هذه الجريمة[1]،

[1]– تم النص على هذه الجريمة من عديد الدول الغربية والعربية على حد سواء، ولعل من بين أهم هذه القوانين التي تم الحصول عليها نجد على سبيل المثال:

– **في الدول الغربية:** نصت عديد الدول الغربية على جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، ومن بين هذه القوانين نجد على سبيل المثال:

- المادة (21) من قانون العقوبات السويدي رقم (289 لعام 1973).
- المادة (145) من قانون العقوبات النرويجي لعام (1979).
- المادة (342–1) من قانون العقوبات الكندي لعام (1985).
- المادة (01) من القانون الإنجليزي لعام (1990) الخاص بإساءة إستخدام الحاسبات الآلية.
- المادة (202–1) من قانون العقوبات الألماني لعام (1991).
- المادة (07) من القانون البرتغالي لعام (1991) والمتعلق بجرائم الكمبيوتر.
- المادة (263) من قانون العقوبات الدانيماركي لعام (1992).
- المادة (138) من قانون العقوبات الهولندي لعام (1992).
- المادة (38–8) من قانون العقوبات الفنلندي لعام (1992).
- المادة (1030) من القانون الفيديرالي في الولايات المتحدة الأمريكية لعام (1992).
- المادة (76–2) من قانون العقوبات الأسترالي لعام (1993).
- المادة (323–1) من قانون العقوبات الفرنسي لعام (1994).
- المادة (509–1) من قانون العقوبات لدولة لكسمبورغ لعام (1995).
- المادة (143 مكرر) من قانون العقوبات السويسري لعام (1995).
- المادة (525) من قانون العقوبات التركي لعام (1996.)

– مشار إليه لدى كل من: (– **نعيم مغبغب:** المرجع السابق، ص235. – **عزيزة رابحي:** المرجع السابق، ص160. – **محمد علي سويلم:** المرجع السابق، ص256).

– **في الدول العربية:** كما نصت الدول العربية التي سعت إلى تجريم كل من فعل الدخول أو البقاء غير المشروع داخل النظام المعلوماتي والتي من بينها:

- المادة (276 مكرر 2) من قانون العقوبات العماني رقم (72 لسنة 2001).
- المادة (607–3) من القانون العقوبات المغربي رقم (07 لسنة 2003)
- المادة (394 مكرر) من قانون العقوبات الجزائري رقم (15 لسنة 2004).
- المادة (03) من القانون السعودي رقم (17 لسنة 2007) والمتعلق بجرائم تقنية المعلومات.
- المادة (02) من القانون الإماراتي رقم (05 لسنة 2012) والمتعلق بالجريمة المعلوماتية.
- المادة (04) من القانون السوداني (13 لسنة 2007) والمتعلق بالإجرام المعلوماتي.
- المادة (03) من القانون الأردني رقم (27 لسنة 2015) والمتعلق بجرائم تقنية المعلومات.
- المادة (02) من القانون القطري رقم (14 لسنة 2014) والمتعلق بالجريمة المعلوماتية.
- المادة (07) من قانون البحرين رقم (05 لسنة 2015) والمتعلق بالإجرام الإلكتروني والإنترنت.
- المادة (02) من القانون الكويتي رقم (63 لسنة 2015) والمتعلق بجرائم تقنية المعلومات.
- المادة (14) من القانون المصري رقم (175 لسنة 2018).

وإن كانت إختلفت فيما بينها من حيث الشروط المتطلبة في إعمال نصوصها على الدخول أو البقاء غير المشروع في النظام بإستخدام وسائل إلكترونية مختلفة.

لذا تؤثر الجرائم المعلوماتية على مصالح الدول الداخلية والخارجية إذا لم يتم مكافحتها؛ لذلك فإن إستفحال وإنتشار هذا النوع من الجرائم دون وضع ضوابط قانونية وإجراءات تحد من إنتشارها سيؤثر ذلك حتمًا على التركيبة الأمنية للمجتمعات، لاسيما في ظل توسع دائرة مستخدمي شبكات التواصل الدولية وكل الوسائل التكنولوجية الحديثة[1].

وعليه سوف نبحث بالدراسة والفهم في الركن الشرعي لهذه الجريمة، على كل من نطاق نص التجريم وكيف تناولته الإتفاقيات الدولية والقوانين الوطنية (فرع أول) ثم يليها بعد ذلك العلة من هذا التجريم (فرع ثاني).

الفرع الأول: نطاق نص التجريم

لقد أولت كل من الإتفاقيات الدولية والإقليمية إهتمام كبير في الحرص على وضع الإطار القانوني لجريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، وألزمت كل دولة عضو في هذه الإتفاقيات أن تسعى جاهدة إلى النص على تجريم مثل هذه الأفعال ومعاقبة مرتكبيها.

أولاً: في إطار الاتفاقيات الدولية

فهنا نذكر على سبيل المثال أهم إتفاقيتين دوليتين وهما:

أ- الإتفاقية الأوروبية لمكافحة الإجرام المعلوماتي:[2] والتي نصت على هذه الجريمة بموجب المادة الثانية منها تحت عنوان "الدخول غير القانوني" بقولها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل إعتبارها جريمة جنائية، وفقًا لقانونه الداخلي، للدخول العمدي لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر".[3]

---

[1]- **لورنس سعيد الحوامدة:** الجرائم المعلوماتية أركانها وآليات مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، 2016، ص26 وما بعدها.

[2]- راجع (إ.أ.م.إ.م) والمعروفة بإتفاقية بودابست والموقع عليها بتاريخ 23 نوفمبر 2001.

[3]- ***Article (2) : Accès illégal*** « *Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit inteme l'accès intentionnel et sons droit à tout ou partie d'un système informatique. Une partie peut exiger que l'infraction soit commisse en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique* ».

ب- الإتفاقية العربية لمكافحة الإجرام المعلوماتي: وكذا نصت المادة السادسة من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي جاء فيها: "الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به، جريمة يعاقب عليها القانون. وتشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمرار بهذا الإتصال محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة داخل الأجهزة والأنظمة الإلكترونية وشبكات الإتصال، أو إلحاق الضرر بالمستخدمين أو المستفيدين أو الحصول على معلومات حكومية سرية".[1]

ثانيًا: في إطار القوانين الوطنية

أما على المستوى الوطني، فقد أولت مختلف التشريعات الأوروبية والعربية إهتماماً كبيراً بمسألة حماية النظام المعلوماتي من فعل الدخول والبقاء غير المصرح به، ومن أبرز هذه القوانين نذكر:

أ- في القانون السويدي: ففي السويد مثلاً صدر لأول مرة القانون رقم (289 لعام 1973) والمتعلق بحماية البيانات والمعلومات المخزنة في الكمبيوتر، حيث جرم فعل الدخول ومجرد الوصول إلى نظم المعالجة الآلية للبيانات بطريق غير مشروع.

ب- في القانون النرويجي: وتبعه بعد ذلك القانون النرويجي لعام 1979 والذي عاقب هو الآخر على أي فعل من شأنه الدخول إلى نظام المعالجة الآلية للبيانات من أجل فتح أي مستند إلكتروني بدون إذن مسبق.[2]

ج- في القانون الفرنسي: وهو ما ذهبت إليه لأول مرة المادة الخامسة من القانون الفرنـــسي رقم (78-17) المؤرخ في 16 جانفي 1978 والمتعلق بالحريات والمعلومات، ثم جاء بعد ذلك القانون رقم (19 لسنة 1988)[3] والذي جاء بعدة جرائم معلوماتية وفي مقدمتها جريمة الدخول لنظام المعالجة الآلية للبيانات أو البقاء فيه بطريق غير مشروع، وذلك بموجب المادة (323-1) من قانون العقوبات الفرنسي والتي عدلت وتممت أكثر من مرة إلى غاية صدور القانون رقم (912 لسنة

---

[1]- راجع في ذلك (إ.ع.م.ج.ت.م) المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والتي صادقت عليها الجزائر بتاريخ 08 سبتمبر 2014، بموجب المرسوم الرئاسي رقم (14-252)، ج ر رقم (57) المؤرخة في 28 سبتمبر 2014 وذلك بقصد التعرف على جملة الجرائم الجديدة التي جاءت بها نصوص هذه الإتفاقية، والتي لازال المشرع الجزائري لحد الساعة لم يدرجها بعد ضمن قانون العقوبات أو في قانون خاص.

[2]- **محمد علي العريان:** الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2011، ص142.

[3]- *Rapp.de jacques thyraud, (J.O.R.F), doc, sénat, 1988, 1er section N°3. P51.*

2015) والتي جاء فيها: "يعاقب كل من دخل أو بقي عن طريق الإحتيال في نظام المعالجة الآلية للبيانات أو المعلومات أو في جزء منها، بالحبس سنتين، وغرامة مالية قدرها 60 ألف يورو، وإذا ترتب على ذلك حذف للبيانات الواردة في النظام أو تعديلها أو تعطيل أداء هذا النظام، فإن العقوبة تكون السجن ثلاث سنوات وغرامة مالية قدرها 100 ألف يورو".[1]

د- في القانون السوري: كما جاء بموجب المادة (5/15) من القانون السوري رقم (17 لسنة 2012) المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، حيث نصت على أنه: "يعاقب بالغرامة من عشرون ألف إلى مئة ألف ليرة سورية كل من دخل قصدًا بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت دون أي يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك".[2]

هـ- في القانون المصري: وعالج أيضًا المشرع المصري هذه المسألة حيث نصت المادة (14) من القانون رقم (175 لسنة 2018) في شأن مكافحة جرائم تقنية المعلومات على أنه: "يعاقب بالحبس مدة لا تقل عن سنة واحدة، وبغرامة لا تقل عن خمسين ألف ولا تتجاوز مائة ألف جنية، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا أو دخل بالخطأ غير العمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، فإذا نتج عن ذلك إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر البيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص او النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف أو بإحدى هاتين العقوبتين".[3]

و- في القانون الجزائري: أما بخصوص المشرع الجزائري، فقد أخذ بنفس النهج الذي تبناه نظيره المشرع الفرنسي، وهذا من خلال تعديله لقانون العقوبات وإستحداث القسم السابع مكرر تحت عنوان "جرائم المساس بأنظمة المعالجة الآلية للمعطيات" وذلك بموجب القانون رقم (04-15) حيث

---

[1]- ***Article 323-1 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 :***

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende ». - (JORF) N° 171 du 26 juillet 2015, page, 12735 texte N°=02, loi N° 2015-912 du 24 juillet 2015, relative au renseignement.

[2]- راجع المرسوم التشريعي السوري رقم (17 لسنة 2012) المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

[3]- راجع القانون المصري رقم (175 لسنة 2018) في شأن مكافحة جرائم تقنية المعلومات. **الملحق رقم (04)**

إشتمل هذا الأخير على جملة من المواد، بداية من المادة (394 مكرر حتى 394 مكرر 8).[1] حيث نصت المادة (394 مكرر) على أنه: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة[2].

– وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 300.000 دج".[3]

الفرع الثاني: علة نص التجريم

بالإضافة إلى ما سبق ذكره فإن قابلية المعلومات للوصول إليها بطريقة غير مشروعة، أصبح يفوق بكثير ما كان عليه الحال قبل عصر الحسابات الآلية، ذلك أن المعلومات الهامة والسرية والتي كانت مدونة في السجلات والملفات الورقية كان يتم حفظها في أماكن يصعب الوصول إليها بسهولة، مما يجعلها بمنأى عن التلاعب والعبث بها، وهذا على عكس ما هو حاصل الآن في عصر الإنترنت والعولمة.

لذا حاولت معظم التشريعات الغربية والعربية سعيها لوضع إطار قانوني لهذه الجريمة، لاسيما من خلال النصوص القانونية السالف ببيانها، وهذا حماية للبيانات والمعلومات المعالجة آليًا من كل أشكال الدخول غير المشروعة سواء كان هذا الدخول في جزء من النظام أم كله، كما قد يتحقق ذلك أيضًا من خلال إنتهاء مدة الدخول بعد الوقت المصرح به.[4] ومؤدى ذلك كله أن علة نص التجريم تكمن في عدة أمور نذكر من أهمها:

– حماية الأجهزة والمواقع الإلكترونية والأنظمة المعلوماتية من كل عمليات التطفل والقرصنة عن طريق ما يسمى بفعل الدخول غير المشروع.

– حماية خصوصية البيانات والمعلومات ومنع الوصول إليها من أشخاص ليس لهم حق الإطلاع عليها.

---

[1]– راجع القانون رقم (04–15) المؤرخ في 10 نوفمبر 2004 والذي عدل وتمم بالقانون رقم (06–23) والمؤرخ في 20 ديسمبر 2006، ثم عدل وتمم بالقانون رقم (16–02) المؤرخ في 19 يونيو 2016 المعدل والمتمم لقانون العقوبات الجزائري.

[2]– تعد الجزائر من بين الدول العربية الأولى التي سايرت التطور الحاصل في المجال المعلوماتي، وهذا من خلال تعديلها لقانون العقوبات الصادر بالأمر رقم (66–155) والمؤرخ في 08 يونيو 1966، ج ر رقم (49) المؤرخة في 11 يونيو 1966، المعدل والمتمم بآخر قانون تحت رقم (16–2) المؤرخ في 19 يونيو 2016،

[3]– أنظر في ذلك نص المادة (394 مكرر) من (ق ع ج) لاسيما القانون رقم (06–23). **الملحق رقم (05)**.

[4]– **محمد علي سويلم:** شرح قانون جرائم تقنية المعلومات المصري، دار المطبوعات الجامعية، الإسكندرية، مصر، 2019، ص262.

– مواجهة كل أشكال القرصنة الإلكترونية وردع المجرمين.

– التأكيد على أن فعل الدخول أو البقاء غير المشروع في النظام يستمد عدم مشروعيته من كونه غير مسموح وغير مصرح به، أي كونه مخالف للأحكام القانونية المجرمة له.

– التشديد في الجريمة ورفع سقف العقوبة إذا ترتب على ذلك الفعل أي إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات خاصة.

– أن المصلحة محل الحماية في مجال التجريم المعلوماتي، هي الحق في المعلومة ذاتها ككيان معنوي ذو قيمة مالية وإقتصادية عالية.

– توجه العديد من الدول بما فيها الجزائر نحو عصرنة قطاع الإدارة وكل القطاعات الأخرى، بما يفيد أنها تسعى إلى تطبيق الحكومة الرقمية والإلكترونية، ولعل من بين أهم الأسباب التي أدت إلى إزدياد الإجرام المعلوماتي على المستوى المحلي والعالمي، هو قيام الحكومات على مستوى العالم بإنشاء هذه الحكومات الإلكترونية، وعصرنة أكبر البنوك والشركات وربطها بشبكة الإنترنت، فكل هذا سيزيد حتمًا من فرض إرتكاب هذا النوع من الإجرام، وسوف يسهل الدخول إلى تلك الانظمة المعلوماتية والعبث بها من قبل محترفي إختراق الأنظمة الأمنية للمعلوماتية والقيام بأكبر جرائم المساس بالبيانات المعالجة آلياً.[1]

المطلب الثاني: الركن المادي لجريمة الدخول أو البقاء غير المشروع

الركن المادي في الجريمة لابد من توافره وبدونه لا يتصور قيامها، وبإستقرائنا النصوص القانونية التي عالجت هذه الجريمة فإن الركن المادي فيها يقوم وفقًا للأحكام الموجودة في القانون الجنائي المقارن وذلك بمجرد قيام الجاني بأي نشاط أو سلوك إيجابي من شأنه التواصل المباشر أو غير المباشر[2]، بغية الوصول إلى المعلومات المخزنة في الحاسب الآلي أو الموجودة على الشبكة بطريقة غير مشروعة.

وهو أن يقوم الجاني بإتيان فعل من الأفعال المجرمة –أحدهما أو مجتمعة– وهما فعل الدخول أو فعل البقاء بدون وجه حق، وهاذين النشاطين يتخذان الصورة البسيطة في الولوج والتواجد غير المصرح به في النظام (فرع أول)، وقد يتحول ذلك من صورة بسيطة إلى صورة

[1]– **سامي علي حامد عياد:** الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2007، ص09.

[2]– يتحقق التواصل المباشر بتواجد الجاني أمام جهاز الحاسب الآلي أو ما في حكه، أما التواصل غير المباشر فيكون عبر إستخدام شبكة الإتصال الدولية كالإنترنت مثلاً، وذلك كله عن طريق الغش والإحتيال على نظام المعالجة الآلية للمعطيات.

مشددة حينما يقترن أي من الفعلين بأعمال الحذف أو التغيير للمعطيات الموجودة داخل النظام، أو تصل إلى حد تخريب نظام اشتغال المنظومة ككل (فرع ثاني)، وهذا ما سوف نعالجه تباعًا.

الفرع الأول: الصورة البسيطة لجريمة الدخول أو البقاء غير المشروع

يتحقق الركن المادي لهذه الصورة البسيطة بفعل الدخول أو البقاء في النظام المعلوماتي دون وجود إذن مسبق بذلك، بحيث يلزم لقيام هذه الجريمة أن يقوم الجاني بنشاط خارجي ملموس، أي عن طريق إتيان فعل مادي يعبر به عن إرادته في الدخول وإنتهاك نظم الحماية الأمنية الموجودة في الحواسيب وما في حكمها، أو أنه يعبر بهذا السلوك عن نيته في البقاء داخل النظام وبدون وجود تصريح بذلك لتحقيق أي من الأهداف الإجرامية التي يريدها الجاني[1]. ويعني ذلك أن الصورة البسيطة لهذه الجريمة تتحقق بفعلين إثنين كل منهما متصل ومنفصل عن الآخر في آنٍ واحد وهما على التوالي "فعل الدخول" و"فعل البقاء" حيث يتفق الفقه الجنائي على أن الركن المادي لهذه الجريمة يختلف في هاذين الفعلين، أي بين جريمة الدخول غير المشروع (أولاً) وجريمة البقاء غير المشروع (ثانيًا) في النظام المعلوماتي، ثم موقف المشرع الجزائري من جريمة الدخول أو البقاء غير المشروع (ثالثاً) وعليه سوف نستعرض لكلا الجريمتين في الآتي:

أولاً: جريمة الدخول غير المشروع

تقوم هذه الجريمة بمجرد فعل الدخول إلى النظام المعلوماتي بدون وجه حق، والعلة من وراء تجريم الدخول المجرد غير المشروع هو منع أي إقتحام للنظام حمايةً لما يحتويه بداخله من معلومات وبيانات لها قيمة مادية أو معنوية لا تقل عن قيمة الوثائق والأموال والحقوق الأخرى والمحمية بموجب التشريعات النافذة.[2]

ومدلول كلمة "الدخول" تشير إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والوصول إلى المعطيات والمعلومات السرية والمخزنة التي يتكون منها هذا النظام[3]، أي أن الشخص يكون قد حاول الدخول أو أنه دخل بالفعل إلى النظام المعلوماتي.[4]

---

[1]– كثيرًا ما تنتهك نظم الحماية الأمنية للمعلوماتية التي تضعها المؤسسات والإدارات أو الشركات والبنوك أو حتى الأشخاص العاديين في حساباتهم الخاصة، وهذا بهدف إرتكاب أنواع مختلفة من الجرائم الإلكترونية كالعبث والتلاعب أو الإتلاف أو التزوير أو حتى سرقة المعلومات، أو ربما بغرض الإطلاع عليها أو إفشائها، وهذا كله لارتكاب جرائم أخرى مثل الإبتزاز المعلوماتي أو المتاجرة بالمعلومات، وهذا ما سوف نتناوله أيضًا بالدراسة والتحليل في هذه الرسالة في حينه.

[2]– **رشيدة بوكر:** المرجع السابق، ص80.

[3]– **أمال قارة:** المرجع السابق، ص343.

[4]– **عبد الفتاح بيومي حجازي:** جرائم الكمبيوتر والإنترنت، المرجع السابق، ص355.

وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي العادي إلى مكان أو منزل أو حتى إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول بإستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي، أي ذلك الدخول المعنوي الإلكتروني[1]، بمعنى يجب أن ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها النظام[2]، وهو دخول منطقي وكأنه يفتح الباب الذي يؤدي إلى نظام المعالجة الآلية بمكوناته المختلفة[3]، فالدخول إذاً إلى النظام المعلوماتي له طبيعة معنوية، هذه الطبيعة تشبه الدخول في ذاكرة الإنسان.[4]

وعلى العموم، فإن الدخول غير المصرح به وفق المعنى الذي سبق ذكره يقع من أي شخص وضد أي نظام دون إستثناء[5]، ويتساوى في هذا المجال إن تمَّ هذا الدخول بطريق مباشر إلى المعلومات أو تمَّ عن طريق الإعتراض غير المشروع لعمليات الإتصال من أجل الدخول إلى النظام المعلوماتي[6].

ولتحديد أكثر لجريمة الدخول غير المشروع، يجب علينا أن نبين التعريف الدقيق لفعل الدخول؛ ثم تحديد المعايير القانونية الخاصة بهذا الفعل، وهذا من خلال ما يلي:

أ- تعريف فعل الدخول غير المشروع *Accés illicite*: هنا سوف نبين ما توصل إليه كل من الفقه والقانون الجنائيين في تعريفهما لفعل الدخول غير المشروع إلى النظام المعلوماتي.

---

[1]- **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص158.

[2]- **سليمة سعيدي، بلال حجاز:** المرجع السابق، ص149.

[3]- والوضع هنا شبيه بجريمة الدخول إلى عقار مملوك للغير وإنتهاك حرمته، فهي تتم بالدخول إلى العقار بصرف النظر عما يحويه ذلك العقار بداخله وعن طبيعة هذا المحتوى.

[4]- **إدريس النوازلي:** جريمة النصب المعلوماتي، قانوناً وواقعًا وقضاءًا، دار الأفاق المغربية للنشر والتوزيع، مراكش، المغرب، 2015، ص138.

[5]- **رشيدة بوكر:** المرجع السابق، ص80.

[6]- عملية الدخول إلى النظام المعلوماتي قد لا تتطلب سوى تشغيل جهاز الحاسوب، وفي بعض الأحيان قد يتطلب ذلك أمور فنية وتقنية أكثر تعقيدًا كما هو الحال من خلال محاولة الحصول على الكود والرقم السري، حتى يكون بالإمكان الدخول إلى النظام، وأحياناً أخرى قد يتم ذلك بإستخدام برامج خبيثة يتم دمجها في أحد البرامج الأصلية لجهاز الحاسوب حيث تعمل كجزء منه، على أن تقوم هذه البرامج بتسجيل الشفرات التي يستخدمها أصحاب النظام للدخول وإستعمالها بعد ذلك في عملية الإختراق، وهناك وسائل أخرى تعتمد على ضعف الأنظمة المعلوماتية ذاتها أو على الأخطاء الناجمة عن عملية البرمجة، لذا فإن وسائل الدخول غير المصرح به من الصعب حصرها لأنها تعتمد بالأساس على التطور التقني والتكنولوجي في مجال المعلوماتية. (أنظر: - **نهلا عبد القادر المومني:** المرجع السابق، ص158).

1. التعريف الفقهي لفعل الدخول غير المشروع: فعل الدخول يسميه بعض الفقه بفعل "الولوج" أو فعل "الوصول" الذي يحدث من قبل الغير في المساس بالنظم المعلوماتية كلها أو في جزء منها[1]، ولم يحدد لا الفقه ولا التشريع الوسيلة أو الطريقة التي يتم بها الدخول والوصول إلى هذه النظم، بحيث يستوي أن يتم ذلك بطريقة مباشرة أو غير مباشرة.[2] وهذا النشاط المتمثل في الدخول إلى النظام –كما سبق وأن رأينا– لا يقصد من ورائه المعنى المادي الملموس والمحسوس كالدخول إلى المنزل، وإنما يقصد به المعنى المعنوي للدخول بطريق الغش إلى العمليات الذهنية الموجودة داخل نظام المعالجة الآلية للمعطيات.[3]

فيذهب الفقه الفرنسي إلى القول أن فعل الدخول له مدلول معنوي، حيث أن الدخول إلى النظام بمثابة الدخول في عقل الإنسان أو حينما نتكلم عن الدخول إلى الفكر أو ملكة التفكير لشخص ما[4]، وهذا ما قصده المشرع الفرنسي عندما إستعمل مصطلح "*Accéder*" بدلاً من مصطلح "*Entrée*"، ويزيد في ذلك القصد ما جاء على لسان الفقيه الفرنسي "*Gassin*" أن المشرع الفرنسي إستعمل عبارة "*Le fait d'accéder*" للتعبير على الدخول غير المشروع إلى الشيء كله أو جزء منه كظاهرة ليست مادية، وإنما كظاهرة معنوية من خلال الدخول إلى العمليات الذهنية للنظام المعلوماتي.[5]

وقد جرى على لسان الفقه محاولات عديدة في تعريفهم لفعل الدخول غير المشروع داخل النظام المعلوماتي، فنجد من أهم هذه التعاريف على سبيل المثال:

---

[1]– يستوي في ذلك أن يكون فعل الدخول لجزء من البرامج أو البيانات المخزنة كفهارس أو محتوى، أو أنه يشمل كامل النظام المعلوماتي، ولا عبرة في الحالتين بطريقة الولوج أو الوصول سواءً كانت عن بعد أم كانت على نطاق قريب. (أنظر أكثر: – **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص 92. – **بلال أمين زين الدين:** المرجع السابق، ص271).

[2]– يكون الدخول إلى النظام بطريقة مباشرة إذا كان هذا الأخير مَفتوحًا مُسبقًا، ولكن الأكثر منه هو الدخول بطريقة غير مباشرة كإستعمال الرمز السري أو كلمة مرور صحيحة من أجل الدخول، أو أثناء المعالجة باليد يتم فيها إدخال برنامج يخترق النظام على مستوى نفس الجهاز أو عن بُعد بإستخدام جهاز آخر مرتبط بشبكة الإنترنت.

[3]– جرائم الكمبيوتر عمومًا وجرائم الإنترنت خصوصًا، هي من الجرائم التي تتسم بسمات مخصوصة تميزها عن غيرها من الجرائم التقليدية الأخرى، فهي تستهدف الأمور المعنوية أكثر من إستهدافها الأمور المادية المحسوسة، وقد أثير في هذا النطاق مشكلة الإعتراف بحماية المال المعلوماتي المعنوي. (أنظر: – **نبيل صقر:** الوسيط في شرح جرائم الاموال، المرجع السابق، ص198).

[4]– **خثير مسعود:** المرجع السابق، ص115. – **غنية باطلي:** المرجع السابق، ص151.

[5]– ***GASSIN (R) :*** *Le droit pénal de l'informatique, Op. Cit, P 29.*

– عُرّف فعل الدخول غير المشروع بأنه: "كل وسيلة غير مشروعة للإطلاع أو الإتصال بالبيانات المخزنة، أو لإستعادة وإلتقاط هذه البينات من داخل نظام الكمبيوتر".[1]

– وعرف أيضًا أنه: "أي تفاعلات ناجحة مع النظام؛ مهما كان حجم هذا التفاعل في البيئة الرقمية سواءً كان الدخول بطريقة إيجابية أو سلبية".[2]

– كما يقصد به أيضًا: "أي عملية غير مصرح بها للدخول إلى أجهزة الغير وشبكاتهم الإلكترونية"[3].

– وذُكر أيضًا بأنه: "الدخول لمنظومة معلوماتية كليًا أو جزئيًا، وسواءً كانت عامة أو خاصة بهدف الإحتيال المعلوماتي".[4]

– وقيل عنه أيضًا أنه: "إساءة إستخدام الحاسب الآلي ونظامه المعلوماتي عن طريق شخص غير مرخص له إستخدامه للوصول إلى المعطيات والمعلومات المخزنة بداخله للإطلاع عليها أو لمجرد التسلية أو لإشباع الشعور بالنجاح.[5]

2. التعريف القانوني لفعل الدخول غير المشروع: لم يوضح المشرع الجنائي المعنى الحقيقي من فعل الدخول غير المشروع في نص قانوني خاص، وإنما ترك ذلك إلى كل من الفقه والقضاء الجنائيين في تعريف هذا الفعل، لكن هذا لم يمنع بعض المشرعين في مجال تقنية المعلومات من الإشارة إلى المعنى القانوني لفعل الدخول غير المشروع، وفق نصوص قانونية خاصة وصريحة، فنذكر منها على سبيل المثال:

– فنصت المادة (2) من إتفاقية بودابست تحت عنوان "الولوج غير القانوني *Accés illégal*" والتي جاء فيها: "... الولوج العمدي لكل أو لجزء من جهاز الحاسب بدون حق، بِنيَّةِ الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر".[6]

---

[1]– ***QUEMENER (M), FERRY (J) :*** *Cybercriminalité défimondial, economica, 2eme édition, Paris, France, 2009, P83.*

[2]– **رشيدة بوكر:** المرجع السابق، ص72.

[3]– **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2009، ص242.

[4]– ***NIDAL (Ch) :*** *La criminalité informatique devant la justice pénale, édition juridique sader, Beyrouth, liban, 2004, P112.*

[5]– **محمد خليفة:** جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2011، ص142.

[6]– ***Article (2) : Accés illégal :*** *« ... l'accés intentionnel et sans droit à tout ou partie d'un système informatique, ... dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique ».*

– كما نصت المادة (1/6) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومـــات بقولـــها: "الدخول ... هو كل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات ..."[1].

– وقد عني القانون الإنجليزي في تعريف الدخول غير المشروع بموجب الفصل الأول من قانون إساءة إستخدام الكمبيوتر المعدل بقانون العقوبات لعام 1990 وذلك بموجب المادة الأولى منه بقولها: "الدخول المأثم هو ذلك الدخول الذي يتسبب في أن يؤدي جهاز الكمبيوتر وظيفة من وظائفه بنية التوصل إلى الإطلاع على البرامج والمعلومات الموجودة بداخله".[2]

– وجاء المشرع المصري بموجب القانون رقم (175 لسنة 2018) والمتعلق بمكافحة جرائم تقنية المعلومات، من خلال الأحكام العامة من الباب الأول فيما يخص التعريفات، حيث نصت المادة الأولى منه حين ذكر مصطلح "الإختراق" فعرفه على أنه: "الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها".[3]

– **موقف المشرع الجزائري:** لم يُعرِّف المشرع الجزائري وكذا نظيره المشرع الفرنسي، فعل الدخول غير المشروع بنص قانوني خاص وصريح مثلما فعلته بعض التشريعات الجنائية المقارنة، وإنما إكتفى بتجريم هذا الفعل متى كان ذلك بطريق الغش المعلوماتي، حيث ذكر المشرع الجزائري بموجب المادة (394 مكرر) من (ق ع ج) والتي تقابلها المادة (323–1) من (ق ع ف)[4]، بقولها: "كل من يدخل ... عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

ب– المعايير القانونية الخاصة بفعل الدخول غير المشروع: إن فعل الدخول غير المشروع إلى النظام المعلوماتي، بإعتباره جريمة منصوص عليها قانوناً، فإنه تحكمه جملة من المعايير القانونية والمتمثلة في الآتي:

---

[1]– راجع في ذلك نص المادة (1/6) من (إ.ع.م.ج.ت.م). **الملحق رقم (02)**

[2]– حيث تضمن قانون العقوبات الإنجليزي قسم جديد إنطوى تحته (18) مادة جاءت موزعة على ثلاثة فصول، وذلك بموجب صدور قانون إساءة إستخدام الكمبيوتر والصادر في قانون العقوبات المؤرخ في 29 يونيو 1990، حيث بيّن هذا القانون جملة من الجرائم المتصلة بالكمبيوتر وحدد العقوبات المقررة على مرتكبيها. (مشار إليه عند: – **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص104).

[3]– راجع المادة الأولى من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

[4]– ***Article (323-1) du (C.P.F) :*** *« Le fait d'accéder… frauduleusement, dant tout ou partie d'un système de traitement automatisé de données ».*

1. معيار السلوك المجرم لفعل الدخول: من يقوم بفعل الدخول بطبيعة الحال هو شخص طبيعي؛ يدخل إما بصورة مستقلة أو مرتبطة بالشخص المعنوي، حيث يكون ممثله القانوني أي يقوم بفعل الدخول لحسابه[1].

وتتحقق جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش، أي الدخول إلى النظام بصورة إما مادية عن طريق إدخال وحدة أو وحدات النظام وربطها بوسائل الإتصال المادية كالأسلاك[2]، وكما يكون هذا الإدخال مادي، يمكن أن يكون بصورة منطقية[3]، على أن يتحقق ذلك من خلال الإستخدام غير المشروع لإحدى وحدات النظام أو خطوط الجهاز، أو إنتحال صفة شخص له حق الدخول إلى النظام، أو إستخدام كلمة المرور كالرقم السري مثلاً، الذي يسمح للجاني بالدخول إلى النظام أو الإتصال به "كمبيوتر أو شبكة"[4]، بالإضافة إلى ذلك فإنه يمكن أن يتحقق الدخول أيضًا عن بعد أي عن طريق الإتصال عن بعد، وهذا من خلال الإتصال بين الوحدة التي يعدها الجاني وبين النظام المراد الدخول إليه وإختراقه وذلك بإستعمال الوسائل التقنية والفنية اللازمة لهذا النشاط.[5]

وعلى هذا الأساس، فإن عملية الدخول كسلوك مجرم في الركن المادي لهذه الجريمة يتحقق عن طريق الوصول للمعطيات المعالجَة آليًا داخل النظام بمختلف الطرق والسبل، والتي يمكن أن تتحقق بطرق مادية كالأسلاك والخيوط "أي السلكية" أو عن طريق الإتصال عن بعد أي "اللاسلكية" وهذا الأخير هو الأسلوب الأحدث في هذا المجال.[6]

وبالرغم من أن الدخول غير المصرح به إلى النظام المعلوماتي يعد مرحلة سابقة وضرورية لإرتكاب الجرائم المعلوماتية الأخرى كسرقة المعلومات وتزويرها أو التجسس

---

[1]– معظم القوانين أقرَّت صراحة قيام المسؤولية الجنائية للشخص المعنوي بخصوص جريمة الدخول وحتى البقاء غير المشروع داخل النظام المعلوماتي، كالمشرع الفرنسي بموجب المادة (323-6) من (ق ع ف)، وكذا نظيره المشرع الجزائري في المادة (394 مكرر 4) من (ق ع ج). وهذا ما سوف نتناوله في حينه.

[2]– **لينا محمد الأسدي:** مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، دار الحامد للنشر والتوزيع، عمان، الأردن، 2015، ص161.

[3]– ***KENNETH (C) Brancik :*** *insider computer fraud, new york, U.S.A, 2008, P403.*

– مشار إليه عند لينا محمد الأسدي، المرجع نفسه، ص161.

[4]– ***CHUCH Eastton and JEFF Taylor :*** *Computer crime investigation and the law, Boston (U.S.A), 2011, P12.*

– **مشار إليه عند لينا محمد الأسدي:** المرجع نفسه، ص162.

[5]– **عبد الفتاح بيومي حجازي:** الجرائم المستحدثة، المرجع السابق، ص477.

[6]– **لينا محمد الأسدي:** المرجع نفسه، ص163.

المعلوماتي أو جريمة الإحتيال المعلوماتي أو المساس بحرمة الحياة الخاص، وغير ذلك من الجرائم، إلا أن مرتكب هذا الفعل قد يقصده بحد ذاته دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه.

وقد أثارت هذه الحالة خلافًا واسعًا في الفقه حول مدى إنطباق وصف الجريمة المعلوماتية عليها، وبالتالي إذا كانت تستوجب الحماية الجنائية وقيام المسؤولية الجنائية أم لا، وكان هذا الخلاف يدور بين إتجاهين إثنين وهُما:

1.1. الإتجاه الأول: يرى أنصار هذا الإتجاه أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول غير المصرح به إلى النظام المعلوماتي، وخاصة إذا لم يكن لدى الفاعل نية لإرتكاب جريمة لاحقة على هذا الدخول، وحجتهم في ذلك أنه سواء كان الدخول جزئيًا أو كليًا، فإنه يمكن أن نتصور فعل الدخول إلى النظام في فرضين إثنين وهما:

– الفَرَض الأول: يفترض أن يكون النظام المعلوماتي مملوك لصاحبه أو مستخدمه، سواء كانت ملكيته للنظام ملكية خاصة أو ملكية مشتركة، ومعناه أنه ليس بنظام مفتوح للجميع، وهذا أمر بديهي، وفيها أن الدخول يتم من قبل صاحب النظام –مالكه أو مستخدمه القانوني– أو كان بناءً على رضـــاء منه[1] ومثاله لو كان الدخول إلى النظام من الغير بناءً على رضا من صاحب النظام نفسه، كما لو سمحت الشركة لمندوب الصيانة أن يقوم بتصفح البرنامج أو المعلومات لمحاولة إصلاح ما بها من تلف أو محاولة إسترجاعها، أو حتى لصيانة ماديات الأجهزة المكونة للنظام المعلوماتي.[2]

فبهذا الفرض ليست هناك جريمة دخول غير مشروع أصلاً، وعليه يشترط القانون في فعل الدخول أو الولوج أن يكون من قِبَلِ شخصٍ آخر غير مالك النظام أو مستخدمه وعلى غير رضاء منه.

– الفرض الثاني: وفيها أن الدخول يتم من غير علم صاحب النظام ولا برضاه، وإنما من قبل شخص آخر ولكن دخوله كان بالخطأ أو بمجرد الصدفة فقط، وكذلك الأمر بالنسبة للأطفال

---

[1]– تكمن أهمية تحديد الشخص المسؤول على النظام في أن تعيينه يسمح بحصر نطاق الأشخاص المسموح لهم بالدخول إلى نظامه، والأشخاص الذين ينطبق عليهم وصف الدخول غير المصرح به، وهذا على إعتبار أن المسؤول على النظام هو الذي يملك حق الدخول إليه، أو أن يحصل منه على تصريح بهذا الدخول، ذلك ان توافر رضا صاحب النظام ينفي عدم المشروعية على الفعل، كأن هناك إتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة مما يفيد توافر الرضا الضمني بدخول مثل العاملين على الأجهزة المنتمية إلى ذات الشبكة. (أنظر كل من – **رشيدة بوكر:** المرجع السابق، ص77، 78. – **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص83).

[2]– وهذا ما ينطبق على جرائم الأموال بصفة عامة، وما لمالكها من سلطة واسعة بمنح ماله لشخص آخر وبرضاه، فلا تقوم معها جريمة السرقة أو النصب أو خيانة الأمانة، وذات الأمر ينطبق على الجريمة التي نحن بصددها.

والشباب الهواة الذين يرتكبون جريمة الدخول غير المشروع لتحقيق الغاية ذاتها كنوع من التحدي لا غير أو لمجرد التسلية.[1] وبالتالي في حالة حصول مثل هذا الدخول غير المقصود فهنا لا يمكن الحديث عن هذه الجريمة، لاسيما إذا بادر الشخص من فوره وقام بقطع الإتصال مباشرة.[2]

ومن هنا يبرر هذا الإتجاه رأيه بأن مثل هذا السلوك لا يخرج عن كونه مجرد طريقة لعرض القدرات التقنية والذهنية التي يتمتع بها الشخص الذي يتعامل كثيرًا مع مثل هذه الأجهزة، وأن هذا الفعل لا يشكل في حد ذاته جريمة تستدعي مسؤولية ومعاقب الفاعل.

2.1. الإتجاه الثاني: يذهب أنصار هذا الإتجاه إلى القول بضرورة تجريم الدخول غير المصرح به إلى النظام المعلوماتي، وكذا من يتجاوز حدود التصريح بالدخول[3]، حتى ولو لم يكن ذلك بقصد إرتكاب جريمة لاحقة فيما بعد، إذ يؤكد أنصار هذا الإتجاه أن جريمة الدخول غير المشروع هي نقطة البداية لأي جريمة معلوماتية أخرى.

وتختلف أفعال الدخول غير المشروع من قبل الجناة، كأن يقوم شخص ما بالدخول غير المشروع في النظام وهو غير مالك له وغير مسموح له بذلك، فهنا نكون أمام جريمة معلوماتية، إلا أن هذا الإتجاه يميز أيضًا بين حالتين وهما:

– الحالة الأولى: وفيها يقوم الجاني بالدخول إلى أماكن تواجد الأجهزة ثم يباشر بفتحها أي يقوم بإستعمال جهاز الحاسوب وتشغيله، حتى ولو كان هذا الشخص يعمل في نفس الجهة المالكة للنظام

---

[1]– **أحمد خليفة الملط:** المرجع السابق، ص190.

[2]– **فخري محمود خليل:** المرجع السابق، ص179.

[3]– من بين التشريعات العربية التي عبرت صراحة عن ذلك نجد التشريع الأردني وذلك من خلال المادة (3/أ) من القانون رقم (27 لسنة 2015) السالف الذكر، والتي جاء فيها: "... دون تصريح مسبق أو بما يخالف أو يجاوز ذلك التصريح..."، وهذا التجاوز يتحقق بأحد الأمرين وهما:

– تجاوز المجال الذي حدده التصريح: إذ تفترض هذه الحالة أن الشخص يملك تصريح بالدخول إلى جزء من النظام فقط، إلا أنه يدخل للجزء الممنوع الدخول إليه، وهذا التجاوز المقصود هنا هو "التجاوز في المكان"، وقد عبر عنه كل من المشرع الجزائري ونظيره الفرنسي بعبارة "... في كل أو جزء..." ويفهم من عبارة "جزء" أن المشرع جرَّم الدخول الجزئي للنظام بطريق غير مصرح به.

– تجاوز الغرض الممنوح من أجله التصريح: وهذه الحالة تفترض أن يكون الغرض متفق عليه مسبقًا مع تحديد المدة الزمنية لهذا التصريح، وهذا التجاوز المقصود هنا هو "التجاوز في الزمان"، وقد عبّر عنه المشرع المصري بموجب المادة (15) من نفس القانون المشار إليه، تحت عنوان "جريمة تجاوز حدود الحق في الدخول" بقولها: "... كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقاً مخوّلاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"، وأن عدم الإلتزام بالغرض الممنوح من أجله التصريح نكون أمام حالة الدخول عن طريق الغش والإحتيال. (ولمزيد أكثر حول الموضوع أنظر: – **رشيدة بوكر:** المرجع السابق، ص79–80).

المعلوماتي[1]، ثم يقوم بالدخول إلى النظام دون أن يكون مسموحًا له بذلك، فهنا تقوم جريمة الدخول غير المشروع، لأن هذه الجريمة ليست من الجرائم التي تتطلب صفة معينة في الجاني، فبإمكان أي شخص القيام بها سواء كانت له علاقة بالنظام المعلوماتي أم لا[2]، فمدام أن صاحب النظام قد أفصح عن عدم رضائه بدخول شخص الغير إلى نظامه المعلوماتي الذي ينتمي إليه، فإن هذا الدخول وبدون موافقته تتحقق به الجريمة مهما كانت صفة الجاني، سواء كان يعمل لدى مالك النظام أو ليس له علاقة به كونه ليس من العاملين أي أنه أجنبي عنه.[3]

وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكًا غير مشروع، وإنما يتخذ هذا الفعل وَصْفُه الجرمي إنطلاقًا من كونه قد تم بدون وجه حق أو عن طريق الغش أو بمعنى آخر دون تصريح مسبق، ومن الحالات التي يكون فيها الدخول غير مصرح به إلى النظام المعلوماتي نجد مثلاً دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسؤول عن النظام أو مالكه[4] وأحيانًا تكون للفاعل سلطة معينة على النظام في حدود الإستعمال المصرح به، ومن بعد ذلك يتجاوز حدود هذا التصريح، كأن يكون دخوله مشروعًا ثم ينتهي الوقت المحدد لبقائه فيه، فهنا تتحقق الجريمة لأن بقاءه غير المشروع[5] لا يعني أنه ملزم بإرتكاب جريمة أخرى لإثارة المسؤولية الجنائية ضده وإنما يكفي هنا تحقق الإستمرار غير المشروع على الرغم من أن دخوله إلى النظام كان مشروعًا ومصرحاً به.[6]

وقد يكون الفاعل مصرحًا له بالدخول إلى جزء فقط من النظام إلا أنه يتجاوز حدود التصريح الممنوح له ويدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول إليها، وهذا

---

[1]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص99.

[2]– **يزيد بوحليط:** المرجع السابق، ص183.

[3]– **سليمان أحمد فاضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، 2013، ص214.

[4]– عرف القانون الأردني رقم (27 لسنة 2015) مصطلح "التصريح" وذلك بموجب المادة (6/2) منه بقولها: "التصريح هو الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو الجمهور للدخول إلى النظام، أو إستخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الإطلاع ...".

[5]– تعني عبارة "غير المشروع" كون أن الدخول غير مسموح به وغير مصرح به من قبل من له سلطة على النظام المعلوماتي أي صاحبه أو مالكه، ومما لاشك فيه أن مجرد الدخول إلى النظام لا يشكل فعلاً غير مشروع، وإنما يستمد هذا الدخول عدم مشروعيته من كونه قد تم عن طريق الغش، ويكون كذلك في حالة ما إذا كان هذا الدخول ضد إرادة المسؤول عن النظام أي بدون تصريح مسبق منه، ومن ثم توافر الرضا ينفي عن الفعل عدم المشروعية.

[6]– **فتحي محمد عزت:** الحماية الموضوعية والجزائية والحق في الخصوصية للكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007، ص131.

الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي[1]، ومثاله كأن يتجاوز العامل أو الموظف داخل المؤسسة التي ينتمي إليها السلطة المخولة له بدخوله إلى النظام سواء في غير أوقات العمل المحددة أو الحالات غير المرخص له فيها بذلك، أو أنه يطلع على بيانات ليست من إختصاصه الوظيفي.[2]

وبناءً عليه فإن الجريمة تقوم مادام أن الدخول إلى النظام بدون رضاء من صاحبه قد تحقق، حتى ولو لم يقم صاحب النظام بإحاطة النظام بوسائل خاصة لحمايته من دخول الغرباء إليه، فيكفي فقط أن يكون قد عبر عن عدم رغبته في السماح للآخرين بالدخول.[3] كما يعتبر عنصر عدم الرضاء[4]، متوفرًا مثلاً إذا علق صاحب النظام إستخدام ذلك النظام على دفع إشتراكات مالية معينة نظير الإستفادة من الدخول، وكذلك الحالات التي يكون فيها الدخول مشروطًا بدفع ثمن محدد وبالرغم من ذلك يدخل الجاني إلى النظام دون أن يقوم بتسديد هذا الثمن، فهنا تقع الجريمة ممن يقوم بالدخول إلى هذا النظام دون تسديد المقابل المالي الذي حدده صاحب النظام نظير هذه الخدمة[5].

أما إذا كان الولوج إلى النظام المعلوماتي بالمجان وكان متاحًا للجمهور، ففي هذه الحالة يكون الدخول إليه حقًا من الحقوق، لأنه من البديهي أن هذا الدخول غير المصرح به لا يسري مثلاً على شبكة الإنترنت نفسها، حتى ولو تم ذلك دون الحصول على إشتراك مسبق في تقديم خدمات تلك الشبكة، وهذا لأن الإنترنت حق من الحقوق المستحدثة والخاصة بحقوق الإنسان.[6]

وفي الأخير وخلاصة لهذه الحالة الأولى يمكن القول أن الدخول إلى النظام يعد غير مسموح به وغير مصرح به في أمرين، الأول إذا كان هناك مسؤول عن النظام، وقام أحدهم بالدخول إلى النظام دون الحصول على إذن مسبق أو تصريح منه، حيث تشكل هذه الحالة النمط السائد في كل الجرائم المعلوماتية تقريبًا، أما الأمر الثاني إذا كان دخول الفاعل إلى النظام وهو

---

[1]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص159.

[2]– ***QUEMENER (M), CHARPENEL (Y) :*** *Cybercriminalité, Op. Cit, P161.*

[3]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص102.

[4]– هذا العنصر غير مختلف فيه، وللدلالة على عدم رضا صاحب النظام تستعمل معظم القوانين الجنائية تعابير عديدة ومختلفة تدل على هذا العنصر ومثالها: الدخول بغير وجه حق– الدخول بطريق الغش – الدخول غير القانوني – الدخول بالإحتيال – الدخول غير المشروع.

[5]– **أحمد عبد الله هلالي:** الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2003، ص73.

[6]– **شرين دبابنة:** جرائم الإنترنت في المجتمع من منظور إجتماعي، دار الحامد للنشر والتوزيع، عمان، الأردن، 2015، ص25.

مصرح له بذلك، ولكنه يدخل في غير الأوقات المرخص له فيها بذلك، أو أنه يتجاوز حدود التصريح الممنوح له بالدخول إلى المعطيات التي لا يشملها التصريح، حيث تشكل هذه الحالة النمط السائد في الجرائم داخل المؤسسات التي يعمل فيها الجاني.

– الحالة الثانية: ففي هذه الحالة يدخل الجاني إلى النظام المعلوماتي ليس في أماكن تواجد الأجهزة وإنما يدخل إلى النظام عن بعد، كأن يقوم الجاني بعمل توصيلة مع النظام بطريقة لاسلكية، أو أنه يدخل إلى النظام عن طريق إستخدام شبكة الإنترنت، وسواء كان هذا النظام محميًا بكلمة مرور أم غير محمي[1]، ومن التطبيقات على هذه الحالة ما يقوم به الفاعل من التداخل عن بعد في أنظمة الكثيرين من أصحاب الأجهزة، وهذا بعد تمكنه من معرفة أسماء المستخدمين، ومعرفة كلمات المرور، وقيامه بتهديدات للمجني عليهم بمسح ملفاتهم، ويعزز هذا الإتجاه رأيه بالإشارة إلى مدى الخسائر المادية التي قد تترتب على حالات الدخول غير المصرح به إلى النظام المعلوماتي عن بعد.[2]

لكن هنا يرى البعض من الفقه أن التداخل عن بعد ليس دخولاً في النظام ولكنه مجرد تجسس عليه، الأمر الذي يستبعد معه وصف التداخل كنشاط يقصد منه الدخول في النظام نفسه، ومن هنا تظهر أزمة مسايرة القانون الجنائي لمعطيات التقدم التقني والتكنولوجي.[3]

رأينا الخاص:

وعلى العموم فنحن من جانبنا نؤيد الإتجاه الثاني الداعي إلى تجريم هذا الفعل بحد ذاته لأنه يعد مرحلة أساسية لإرتكاب بقية الجرائم المعلوماتية الأخرى، كما أن المعلومات التي قد يقع عليها هذا السلوك تكوِّن معلومات على قدر كبير من الأهمية، كما هو الحال بالمعلومات المتعلقة بالأسرار العسكرية للدولة، وكذلك البيانات الخاصة بالعملاء في البنوك، أو البيانات الخاصة بالمواطنين في السجلات المدنية، وقد يطال هذا السلوك أيضًا الأبحاث العلمية أو الطبية وغير ذلك من المعلومات المختلفة؛ إذ أن مجرد الدخول في النظام المعلوماتي والإطلاع على المعلومات التي يحويها يعد مساس بها حتى لو لم يتم إرتكاب جريمة لاحقة على هذا الفعل، أو حتى لو كان الهدف من وراء

---

[1]– **نائلة عادل محمد فريد قور:** جرائم الحاسب الاقتصادية، ط1، دار النهضة العربية، القاهرة، مصر، 2004، ص327.

[2]– **نهلا عبد القادر المومني:** الجرائم المعلوماتية، المرجع السابق، ص157.

[3]– **جميل عبد الباقي الصغير:** القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن إستخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، مصر، 1992، ص66.

هذا الفعل هو مجرد إثبات الذات والقدرات التقنية أو القدرة على إختراق الحواجز الإلكترونية للنظام المعلوماتي، حيث أن ترك مثل هؤلاء الأشخاص دون مساءلة أو عقاب سوف يؤدي ذلك حتمًا إلى التمادي في الإعتداء على حرمة الأنظمة المعلوماتية.

2. معيار الشروع في جريمة الدخول: في الحقيقة أن الدخول غير المشروع يبدأ منذ اللحظة التي يصبح فيها الفاعل قادرًا على الإطلاع البصري والسمعي لمحتويات النظام المعلوماتي وتطبيقاته، ومع ذلك يصعب تحديد البدء في التنفيذ من عدمه في الحالات التي يتم فيها الدخول إلى النظام ومحتوياته إذا لم يكن هناك قواعد أمنية تساعد في تحديد وقت الإختراق والدخول[1].

ويمكن تصور الشروع في فعل الدخول غير المشروع إلى النظام على الرغم من أنها جريمة ذات وصف جنحي وهذا ما نصت عليه الفقرة الثانية من نص المادة (2/11) من إتفاقية بودابست المشار إليها سلفاً، بقولها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية للتجريم وفقاً لقانونه الداخلي كل شروع عمدي لإرتكاب إحدى الجرائم المشار إليها..."[2]، وأكدت على ذلك أيضًا نص المادة (2/19) من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات على أنه: "الشروع في إرتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية ...".

وقد عاقب عليه المشرع الجنائي في عديد القوانين الوطنية فنجد على سبيل المثال المشرع المصري تلكم عن ذلك من خلال الفصل التاسع من نفس القانون المشار إليه آنفاً، تحت عنوان "الشروع والإعفاء من العقوبة" وذلك بموجب نص المادة (40) منه بقولها: "يعاقب كل من شرع في إرتكاب الجنح المنصوص عليها في هذا القانون بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة"[3].

وعاقب كذلك المشرع الجزائري بنص المادة (394 مكرر) من (ق ع ج) بقوله: "... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

---

[1]– **وسيم طعمة:** المرجع السابق، ص168.

[2]– *« Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénal, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application ... ».*

[3]– راجع نص المادة (40) من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

وهكذا نجد أن المشرع الجنائي قد أقر بنظام العقاب على الشروع في إرتكاب الجرائم المنصوص عليها في هذا المجال ومنها جريمة الدخول بدون وجه حق، ومن أمثلة ذلك الشروع في الدخول إذا حاول الجاني إستعمال أكثر من كلمة مرور مثلاً ولكنه فشل في الوصول إلى الكلمة الصحيحة التي بها يفتح النظام المعلوماتي.[1]

إلا أنه في بعض التشريعات المقارنة بما فيها التشريع الجنائي الفرنسي قد أخرج جنحة الدخول غير المشروع من نطاق المحاولة والشروع، لأن المشرع الفرنسي يعتبر أن في ذلك مساس بالنظرية العامة للشروع في القانون الجنائي، والسبب في ذلك أن الأعمال التحضيرية لإرتكاب جريمة الدخول غير المشروع تشكل في حد ذاتها شروعًا أي محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع، وبالتالي لا عقاب على ذلك.[2]

3. معيار المحل في جريمة الدخول: من أجل إتيان السلوك الإجرامي في جريمة الدخول غير المشروع إلى النظام المعلوماتي، يتطلب الأمر وجود محل للجريمة، والمتمثل بطبيعة الحال في تلك البيئة الرقمية من حيث الجهاز الإلكتروني أي الحاسب الآلي بشكل خاص وإتصاله بشبكة الإنترنت في بعض الحالات.

وقد حدد المشرع الجنائي محل هذه الجريمة إما في موقع إلكتروني أو حساب خاص وإما في نظام معلوماتي محظور الدخول عليه، ولا يلزم أن يتحدد هذا المحل في الأمرين معًا، وإنما يكفي أن ينصب على أحدهما دون الآخر.[3]

حيث بينت المادة (2/1) من المرسوم السلطاني العماني رقم (12 لسنة 2011) والمتعلق بقانون مكافحة جرائم تقنية المعلومات أن "الموقع الإلكتروني" هو: "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد"[4].

وزادت على ذلك نص المادة (13/1) من القانون المصري رقم (175 لسنة 2018) في شان مكافحة جرائم تقنية المعلومات، أن "الموقع الإلكتروني" يقصد به: "مجال أو مكان إفتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات العامة أو الخاصة"، كما

---

[1]– **محمد علي سويلم:** شرح قانون جرائم تقنية المعلومات المصري، المرجع السابق، ص273.

[2]– **خثير مسعود:** المرجع السابق، ص130.

[3]– **محمد علي سويلم:** المرجع السابق، ص280.

[4]– راجع في ذلك نص المادة الأولى من المرسوم السلطاني العماني رقم (12 لسنة 2011) والمتعلق بقانون مكافحة جرائم تقنية المعلومات والمؤرخ في 06 فبراير 2011، الجريدة الرسمية رقم (929) الصادرة بتاريخ 15 فبراير 2011.

بينت المادة الأولى من القانون الإماراتي رقم (05 لسنة 2012) بشأن مكافحة الإجرام المعلوماتي على أن "المواقع الإلكترونية" يقصد بها: "مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الإجتماعي والصفحات الشخصية والمدونات"[1].

أما عن "الحساب الخاص" فعبر عنه نفس القانون المصري بأنه عبارة عن: "مجموعة من المعلومات الخاصة بشخص طبيعي أو إعتباري، تخول له دون غيره، الحق في الدخول على الخدمات المتاحة أو إستخدامها من خلال موقع أو نظام معلوماتي"[2].

ومع ذلك نجد أن معظم التشريعات الجنائية الحديثة قد تبنت الإتجاه الموسع في الدخول القائم على حماية النظام المعلوماتي ككل، وعلى عدم قصر محل هذه الجريمة على الشبكات المعلوماتية أو المواقع الإلكترونية دون الأخرى، أو على الحسابات الخاصة، أو على المعلومات السرية والرسمية فقط[3]، ووفقًا لهذا الإتجاه الموسع فإن المحل الذي ينصب عليه السلوك الجنائي في جريمة الدخول غير المشروع يتسع لإستيعاب المعلومات الموجودة داخل النظام، وكذا النظام الذي يتضمنها فضلاً عن المواقع والشبكات والحسابات الإلكترونية العامة والخاصة، كما يشمل هذا المحل إعتراض عملية تنقل المعلومات والتقاط الإشارات التي يحدثها جهاز إلكتروني من خلال وسائل إلتقاط إلكترونية، ويترتب على ذلك أن تصبح هذه الإشارات محلاً ينصب على سلوك الجاني في جريمة الدخول عن طريق الغش أو غير المصرح به إلى نظم المعالجة الآلية للمعطيات[4]، فمعيار المحل في جريمة الدخول غير المشروع هو كل ما تشتمل عليه المنظومة المعلوماتية من برامج ومواقع وحسابات بالإضافة إلى الشبكات المعلوماتية الدولية والمحلية.

وهذا كما أسلفنا بيانه أن المقصود بالأنظمة المعلوماتية سواء كانت موصولة بالشبكة أم لا، فهي مجموعة منسقة ومتناسقة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها سواء عن

---

[1]– راجع في ذلك نص المادة (13/1) من القانون الإماراتي رقم (5 لسنة 2012).

[2]– راجع نص المادة (15/1) من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

[3]– المعلومات المخزنة كمحل للجريمة الرقمية يقصد بها كل محتويات النظام المعلوماتي بشكل عام، أي المعلومات من جهة والخدمات من جهة أخرى، فأما المحتوى فيعرف بأنه: "كل المعلومات والخدمات التي يمكن الوصول إليها وتداولها في إطار التواصل على الشبكة أو النظام"، بينما المعلومات فهي: "تلك العلامات أو الإشارات أو حتى النصوص والرسائل الصوتية والمقروءة أو الصور الثابتة والمتحركة، التي تحمل معنى قابل للإدراك الحسي والمعنوي مرتبطًا بسياق محدد"، أما من ناحية نوعية المعلومات وعائداتها لم يقصّر المشرع الجنائي الحماية على المعلومات الرسمية أو السرية فقط، وكذلك لم يميز في هذه المعلومات بين ما تختص به الدولة أو الأشخاص، بل إنها تشمل كل المعلومات الرسمية وغير الرسمية، والسرية منها وغير السرية، سواء كان فيها مساس بمصالح الدولة أو حتى مصالح الأفراد الشخصية والمالية. (أنظر أكثر: – **وسيم طعمة:** المرجع السابق، ص175).

[4]– **رشيدة بوكر:** المرجع السابق، ص76.

طريق وسائل التوصيل أو عن طريق الشبكة، فالشبكة كمحل للجريمة هي الأخرى مشمولة بلفظ النظام المعلوماتي في كثير من التشريعات المقارنة.[1] ومؤدى ذلك أنه ينصرف محل هذه الجريمة إلى النظام المعلوماتي وكل مجموعة الإجراءات التي يتم من خلالها تجميع أو إسترجاع أو تشغيل وتخزين ونشر المعلومات، ولا ينصرف محل هذه الجريمة فقط إلى المكونات المادية للنظام المعلوماتي أو المعلومات ذاتها.[2]

أما عن المحل الجرمي في الإعتراض الإلكتروني أو الإلتقاط الهوائي، فإنه ينطبق على المساس بالبيانات في مراحل إنتقالها داخل الحاسب الآلي أو التي تتم عبر جهازين من قرب أو عن بعد عبر الشبكات المعلوماتية المختلفة، وينطبق أيضًا هذا المحل الجرمي على كل المحادثات والمراسلات التي تتم عن طريق وسائل الإتصال الحديثة، كالهاتف النقال والبريد الإلكتروني وصفحات الفايسبوك وغيرها.[3]

كما يكمن محل الدخول غير المشروع حسب المشرع الجزائري ونظيره الفرنسي وكذا المشرع المصري، في كل أو جزء من النظام المعلوماتي، بحيث لا يشترط لتحقق فعل الدخول أن يتم الإتصال بكل أجزاء النظام، وإنما يكفي فقط الإتصال بجزء أو عنصر منه أو من الشبكة، ولو كان ذلك بشكل ضيق، وحتى ولو كان ذلك الجزء أو العنصر لا يتضمن المعلومات التي يهدف الجاني الوصول إليها.[4]

ولقد حدد المشرع الجزائري موضوع محل الدخول غير المشروع بقوله: "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".[5] ويعني ذلك أن ما يتعلق بالأجزاء الأخرى للنظام فإن غالبية التشريعات الجنائية إعـتبرت أن الدخول إلى جزء من الأجزاء التي يتكون منها النظام، هو بمثابة الدخول غير المشروع إلى النظام ككل.

---

[1]– **وسيم طعمة:** المرجع السابق، ص170.

[2]– **محمد علي سويلم:** المرجع السابق، ص171.

[3]– **وسيم طعمة:** المرجع نفسه، ص175.

[4]– **لينا محمد الأسدي:** مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، دار حامد للنشر والتوزيع، عمان، الأردن، 2015، ص162.

[5]– راجع في ذلك الفقرة الأولى من نص المادة (394 مكرر) من (ق ع ج).

وبالتالي فإن هذه الجريمة لا تقوم إلا إذا كان الدخول غير مشروع أو البقاء كان بدون رخصة في نظام المعالجة الآلية للمعطيات، وعليه يخرج من مجال تطبيق هذا النص الدخول المشروع، كما لا تقع هذه الجريمة إذا كان الموقع مفتوح بدون ترخيص.[1]

4. معيار النتيجة في جريمة الدخول: تقع جريمة الدخول غير المصرح به داخل النظام بمجرد إتيان النشاط المؤثر، وهو هنا كما سبق وتحدثنا عنه، يقصد به الدخول في النظام المعلوماتي بطريقة غير مشروعة حتى وإن كانت عرضية وغير مقصودة، بحيث يعد مثل هذا الفعل وبكل بساطة من أخطر الأفعال التي تهدد تقنية المعلومات، سواء التي تمتلكها الحكومات أو التي لها خصوصية بالأفراد.[2]

وعليه تقع هذه الجريمة بمجرد أن يقوم الجاني بنشاط إيجابي غير مشروع، وأن إشتراط النشاط الإيجابي مستشف من إعتبار المشرع النظام محلاً لجريمة الدخول، لأن الولوج إلى هذا النظام المعلوماتي غر متصور بموقف سلبي أي نشاط الإمتناع، والنشاط الإيجابي المقصود هنا هو ذلك النشاط الإيجابي العام والذي يشمل الدخول غير المشروع كالإختراق الإلكتروني وسواء كان النظام محمي بقواعد أمنية أم لا.[3] وهذا المعيار في الحقيقة يتنازع فيه إتجاهين إثنين وهما على التوالي:

– الإتجاه الأول: والذي يرى أن جريمة الدخول غير المشروع هي من جرائم الخطر، لأنها لا تستلزم الوصول إلى المعطيات والمعلومات المخزنة داخل النظام حتى تقوم الجريمة، وإنما تقوم هذه الأخيرة بمجرد الإتصال غير المشروع بالنظام بأي طريقة كانت أي لا تتحقق الجريمة بمجرد الوصول إلى المعلومات.[4]

– الإتجاه الثاني: يعتبر جريمة الدخول غير المشروع من جرائم الضرر، لأنه يشترط أن يؤدي فعل الدخول إلى الوصول للمعطيات والمعلومات المخزنة داخل النظام، ومنه نستطيع القول معه المساس بسرية المعلومات وسلامتها من التزوير والإتلاف أو كمن يستخدم هذه المعلومات لإرتكاب جريمة أخرى لا تنصب على المعلومات في حد ذاتها، وإنما تستعمل في التشهير والإبتزاز مثلاً.[5]

---

[1]– **نبيل صقر:** الوسيط في شرح جرائم الأموال، دار الهدى، عين مليلة، الجزائر، 2012، ص218.

[2]– ومثاله الدخول غير المشروع على مواقع التواصل الإجتماعي، فقد يستغل نظام الفايسبوك *Facebook* في الدخول إلى بيانات الأشخاص وصفحاتهم والإطلاع على معلوماتهم وكذا التعرف على جهات الإتصال الخاصة بهم، ولربما الوصول إلى ملفاتهم الشخصية والسرية.

[3]– **وسيم طعمة:** المرجع السابق، ص171.

[4]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص99.

[5]– **وسيم طعمة:** المرجع نفسه، ص166.

والمشرع الجنائي هنا لا يستلزم لوقوع مثل هذه الجريمة أن تحدث نتيجة مادية معينة، وهذا ببساطة شديدة أن هذا النوع من الإجرام يدخل ضمن جرائم النشاط أي أنها جريمة خطر وليست جريمة ضرر، وبناءً عليه فإن الجريمة هنا تقوم بمجرد إستعمال الجاني للنظام دون موافقة صاحبه، حتى وإن لم يجد بداخله ما يبحث عنه من معلومات، وبدون أن يحدث أي ضررٍ كان.[1]

وعليه فالأصل أن جريمة الدخول غير المشروع إلى النظام المعلوماتي هي جريمة نشاط على أساس الخطر، وليست جريمة ذات نتيجة على أساس الضرر، وهذا ما هو موجود في غالبية التشريعات الجنائية المقارنة[2]، مادام أنه لا يلزم لوقوعها تحقق ضرر من نوع معين، ومما يدل على صحة هذا القول ما جاء به المشرع الجزائري في سياق نص المادة (394 مكرر) من قانون العقوبات، حيث تضمنت الفقرة الأولى ما نصه: "... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية أو يحاول ذلك..."، فهذه الفقرة تتماشى مع أن جريمة الدخول غير المشروع إلى النظام من جرائم النشاط على أساس الخطر أو كل من يهدد بالخطر، وليس بالضرورة أن يترتب عنها ضرر يمس الغير.

وخلاصة هذا القول أنه إذا كان الركن المادي في هذه الجريمة يقوم على النشاط الإجرامي، أي السلوك المجرم والمتمثل في فعل الدخول غير المشروع إلى النظام، فالجريمة إذاً من جرائم النشاط التي لا يلزم لتحققها حدوث نتيجة مادية معينة، فإن حدث وترتب عنها نتيجة ما فإنها حتمًا سوف تتحول إلى جريمة أخرى إضافة إلى جريمة الدخول غير المصرح به وهي الجريمة الأصلية[3]، أي أن الدخول غير المشروع من الصور الأولى للإجرام المعلوماتي، وهي بمثابة الأساس الذي إنطلقت منه معظم التشريعات الجنائية المقارنة في تأثيمها الكثير من الإعتداءات

---

[1]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص97.

[2]– أنظر على سبيل المثال: الفقرة الثانية من المادة (323–1) من (ق ع ف) السالف بيانها. **الملحق رقم (03)**

[3]– من المهم جدًا التعبير على أن هذه الجريمة هي الأصل في كل الجرائم المعلوماتية الأخرى، وهذا ما يعكس أيضًا مدى الأهمية الكبيرة للنص القانوني الخاص بتجريم فعل الدخول غير المصرح به إلى النظام في مختلف التشريعات الجنائية، مما يمكن القول معه أن هذا النص هو بمثابة نص إحتياطي بمعنى أنه في جميع الحالات التي لا تنطبق فيها على الفعل أي وصف جريمة إلكترونية كالإتلاف أو الإنتهاك أو العبث أو التجسس أو التلاعب أو التزوير أو السرقة أو الإحتيال... وغيرها، فإنه يمكن تطبيق نص الدخول غير المشروع بحسبان أن فعل الدخول هو مقدمة حتمية أو شبه حتمية لإرتكاب معظم الجرائم المعلوماتية الأخرى، وبالتالي سوف لن ولا يفلت أي مجرم معلوماتي من العقاب. (أنظر أكثر في ذلك: – **وسيم طعمة:** المرجع السابق، ص170).

المقترفة في البيئة الرقمية، وما يمكن القول معه في الأخير أن الدخول غير المشروع جريمة قائمة بذاتها ونتيجتها الضارة هي باقي الجرائم الرقمية الأخرى المترتبة عن هذا الدخول.[1]

أما البحث في مسألة العلاقة السببية، فلا يمكن الحديث عنها إذا كان فعل الدخول إلى النظام غير مشروع وبدون وجه حق، وإنما يكون الحديث والبحث في مدى توافر العلاقة السببية من عدمه متى كان الدخول مشروعاً ومسموحاً به ثم بعد ذلك وقعت جريمة داخل هذا النظام، فإن البحث هنا في قيام هذه الجريمة يتوقف على ما إذا كانت توجد فعلاً علاقة سببية بين الدخول المشروع والنتيجة الضارة وهي الجريمة المعلوماتية الأخرى، وكذا الإعتداء الحاصل على النظام برمته، ومدى توافر سوء أو حسن نية المتدخل.[2]

ثانيًا: جريمة البقاء غير المشروع

يقصد بفعل "البقاء" كل أشكال وحالات التواجد غير المصرح به في النظام المعلوماتي كربط الإتصال والإطلاع على البيانات أو القيام بعمليات مشابهة[3]، وهو السلوك الإجرامي الثاني في الركن المادي لهذه الجريمة والذي نصت عليه معظم القوانين الوطنية المقارنة، والمراد به البقاء والتواجد داخل نظام المعالجة الآلية للمعطيات دون إرادة صاحب الموقع الإلكتروني أو النظام المعلوماتي.[4]

وعلى العموم فإن البقاء داخل نظام المعالجة الآلية وفق المعنى الذي سبق ذكره مع فعل الدخول، يجعله يتميز هو الآخر بذاتية وخاصية مختلفة تمامًا عن التواجد والبقاء المادي في البيئة الواقعية، شأنه في ذلك شأن الدخول المادي، فكل من الدخول والبقاء في العالم الرقمي الإفتراضي له طبيعة معنوية وليست مادية.[5] ولإحاطة أكثر بفعل البقاء سوف نتطرق هنا إلى تعريفه، ثم نعرج على بعض الأحكام القانونية المنظمة له.

أ- تعريف فعل البقاء غير المشروع *Présence illégale*: لقد عرف أيضًا كل من الفقه والقانون الجنائيين مفهوم فعل البقاء غير المشروع داخل النظام المعلوماتي، وذلك في كل من الفقه والقانون.

---

[1]- ***VERGUTCH (P) :*** *La représsion des délits informatique dans une pérspéctive informtionale, thèse université de Montpellier (I), France, 1996, P169-171.*

[2]- **خثير مسعود:** المرجع السابق، ص110.

[3]- ***BENSOUSSAN Alain :*** *L'informatique et le droit,Op. Cit, P372.*

[4]- **أمال قارة:** الجريمة المعلوماتية، المرجع السابق، ص44.

[5]- **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص83.

1. التعريف الفقهي لفعل البقاء: ولعل من جملة هذه التعريفات نجد ما يلي:

– عرفه البعض بأنه: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام".[1]

– وعرفه آخرون بأنه: "سرقة وقت الآلة والأخذ من وقتها أكثر من الوقت المحدد وذلك بقصد الإضرار بالنظام".[2]

– وذكره البعض أنه: "عدم وضع حد للتشعب والتغلغل داخل النظام مع الإعتقاد أن ذلك يشكل خطأ غير مقصود".[3]

– ويقصد به أيضًا: "تجاوز المتدخل المدة المسموح له بها للبقاء داخل النظام المعلوماتي، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحًا له فيه الرؤية والإطلاع فقط".[4]

– وجاء ذكره أيضًا بأنه: "كل دخول عن طريق الخطأ وبدون قصد ولكن البقاء داخل النظام عن قصد وإرادة ووعي".[5]

– كما قيل عنه: "فعل البقاء هو كل تواجد أو تفاعل ناجح مع النظام، يكون ضد إدارة المسؤول عنه أو المسيطر عليه ومن يملك أحقية تنظيمه"[6].

2. التعريف القانوني لفعل البقاء: من بين القوانين التي تطرقت إلى تعريف فعل البقاء غير المشروع نجد:

– عرفته المادة السادسة من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بقولها: "كل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار بها".[7]

– وعرفه المشرع المصري تحت عنوان "بجريمة تجاوز حدود الحق في الدخول" وذلك بموجب المادة (15) من القانون رقم (175 لسنة 2018) المشار إليه سلفاً، على أنه: "... كل من دخل إلى

---

[1]– **هيام حاجب:** الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة إجازة مهنة القضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص12.

[2]– **زيدان زيبحة:** الجريمة المعلوماتية، المرجع السابق، ص50.

[3]– **محمد خليفة:** المرجع السابق، ص154.

[4]– **يزيد بوحليط:** المرجع السابق، ص184.

[5]– **غنية باطلي:** المرجع السابق، ص160.

[6]– ***VÉRON Michel:*** *Droit pénal spécial, 6ème édition, Armand colin, paris, France, 1998, P250.*

[7]– راجع المادة السادسة من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010. **الملحق رقم (02)**

موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"[1].

– وذكره المشرع الفرنسي في الفقرة الأولى من نص المادة (323-1) بقولها: "كل دخول أو بقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ..."[2].

– وعرفه أيضًا المشرع الجزائري في الفقرة الأولى من نص المادة (394 مكرر) من (ق ع ج) بقولها: "... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات..."[3].

ب– الأحكام القانونية لفعل البقاء غير المشروع: إذا كان فعل البقاء يتفق مع فعل الدخول كلما تم ذكره تقريبًا، فإنه لا يمكن تصور البقاء دون دخول إلى النظام المعلوماتي، مع إمكانية تصور الدخول دون بقاء في هذا النظام، ومع ذلك يرى كثير من الفقه أن فعل البقاء غير المشروع يختلف عن فعل الدخول في العديد من الأحكام القانونية التي تحكمه، سواء من حيث صوره وطبيعته القانونية ودرجة خطورته، وهي على النحو التالي:

1. صور فعل البقاء غير المشروع: تعد جريمة البقاء غير المشروع داخل المواقع الإلكترونية والأنظمة المعلوماتية من أكثر الجرائم تأثيرًا على السرية والخصوصية، وبالرغم من أن هذا النشاط يعد البوابة الرئيسية لإرتكاب بقية الجرائم الأخرى الواقعة في فضاء التعامل الإلكتروني، إلاَّ أن فاعله قد يكتفي بمجرد البقاء دون نية إرتكاب أي جريمة معلوماتية أخرى.

وتجدر الإشارة إلى أنه قد يتحقق فعل البقاء المعاقب عليه داخل النظام مستقلاً لوحده حين يكون الدخول إلى النظام مشروعًا، وقد تجتمعان الجريمتان معًا "الدخول والبقاء غير المشروعين"، لذا نجد أن لفعل البقاء غير المشروع صورتان وهما:

1.1. البقاء غير المشروع بفعل الدخول المشروع: يكون فعل البقاء معاقبًا عليه وحده حين يكون فعل الدخول إلى النظام مشروعًا ومن أمثلة ذلك:

---

[1]– راجع في ذلك نص المادة (15) من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

[2]– ***Article 323-1 :*** « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données …* ».

[3]– راجع في ذلك نص المادة (394 مكرر) من (ق ع ج). **الملحق رقم (05)**

أن يدخل الشخص سهوًا إلى النظام ودون قصد منه أو يدخله عن طريق الصدفة، ثم يتفطن أنه داخل منظومة معلوماتية دون ترخيص مسبق، ومع ذلك يبقى ولا يغادر النظام، فيجب عليه في هذه الحالة قطع الإتصال الذي تحقق عن طريق السهو والصدفة وأن يبادر بالإنسحاب والخروج فورًا من النظام[1]، وإلاَّ يكون أمام جريمة البقاء فقط دون الدخول لأن فعل البقاء هنا حدث عمدًا.[2]

وقد يدخل الشخص بالخطأ إلى النظام المعلوماتي، ويبقى داخله بالخطأ ولا يشعر بذلك، مما ينفي عنه جريمة الدخول أو البقاء غير المشروع، وذلك كما عبر عنه المشرع المصري بعبارة "عن طريق الخطأ"[3]، كإستخدام مثلاً شفرة خاطئة، أو حيازة كود العبور نتيجة خطأ في التعامل مع الملفات فإن هذا الواقع يستبعد الطابع المتعمد الذي يقتضيه القانون[4]، ومن ثم كان يتعين عليه الخروج من النظام بمجرد تبينه الخطأ الذي وقع فيه.

أما أن يستمر في البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مصرح له بالدخول فيه، فإنه في هذه الحالة يتوافر فعل البقاء المجرم ويسأل عنه[5]، حتى ولو حصل ذلك بصفة عرضية[6]، ومع ذلك فإن مجرد الخطأ في الدخول إلى النظام يمكن أن يقع تحت طائلة القانون الجنائي وهو ما يطلق عليه "بالخطأ غير العمدي" لأنه من الناحية التقنية يعتبر هذا الدخول مشروعًا، أما من الناحية القانونية فالدخول هنا غير مشروع لأنه يشكل بكل بساطة إنتحال للشخصية[7].

كما قد يكون للشخص الحق في الدخول والبقاء داخل النظام لمدة زمنية محددة، إلاَّ أنه يتجاوز هذه المدة المسموح له فيها بالبقاء، فهنا نكون أمام جريمة البقاء غير المشروع على الرغم من أن الدخول كان مشروعًا[8]، ويتحقق ذلك أيضًا بالنسبة للخدمات المفتوحة للجمهور على المواقع الإلكترونية والتي يستطيع الجاني فيها الحصول على الخدمة بالمجان دون أن يدفع المقابل الواجب

---

[1]– **محمد مزاولي:** المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة الدراسات والأبحاث القانونية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد01، لعام 2009، ص30.

[2]– **أمال قارة:** الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط2، 2007، ص110.

[3]– أنظر في ذلك نص المادة (14) من القانون المصري رقم (175 سنة 2018). **الملحق رقم (04)**

[4]– **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص82.

[5]– **محمد علي سويلم:** المرجع السابق، ص279.

[6]– **أحسن بوسقيعة:** الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، طبعة11، 2012، ص453.

[7]– ***CASILE Jean-François:*** *Le code pénal à l'épreuve de la délinquance informatique, presse universitaires (D'AIX) Marseille, (PUAM), France, 2002, P102.*

[8]– **هيام حاجب:** المرجع السابق، ص50-51.

دفعه، وكثيرًا ما يحدث ذلك إذا كان إستعمال النظام محددًا بوقت معين نظير أجر مالي[1]، فيتخطى المتهم هذا الوقت، وبالتالي يسمح هذا الفعل بتجريم ما يمكن أن نطلق عليه "سرقة وقت الآلة".

وفي نطاق موضوعنا فالمشرع يأمر الجاني بعدم الإبقاء على الإتصال مع النظام المعلوماتي لأن إمتناع الجاني عن الإنسحاب يشكل هنا إخلال بالواجب وهو علة العقاب على إبقاء الإتصال قائمًا، فالعبرة في هذه الحالة هو الإستمرارية والبقاء داخل النظام حتى ولو كان الدخول مبني على الخطأ أو المصادفة، إذ يتحقق ذلك بالنسبة للخدمات الهاتفية التي يستطيع بعض المجرمين فيها الحصول على الخدمة دون أن يدفع مقابل أو أنه يحصل على مدة أطول من المدة التي دفع مقابلها[2]، أو في حالة حصوله على خدمة أكثر من المدة التي دفع مقابلها عن طريق إستخدام تقنيات غير مشروعة، أو في حالة طبعه لنسخة من المعلومات في حين سمح له بالرؤية والإطلاع فقط، وفي كل هذه الحالات فإن الجاني يسأل ويعاقب على جريمة البقاء غير المشروع متى توافرت أركانها لاسيما منها الركن المعنوي.[3]

2.1. البقاء غير المشروع بفعل الدخول غير المشروع: قد يجتمع كل من الدخول غير المشروع والبقاء غير المشروع معًا، ومثالها أن لا يكون للجاني الحق في الدخول إلى النظام أصلاً، ومع ذلك يدخل إليه رغم إرادة من له حق السيطرة على النظام[4] ويقرر البقاء داخله وعدم قطع الإتصال به، ومن ثم يبقى ولا يغادر النظام لفترة زمنية معينة، فهنا يتحقق الإجتماع المادي والمعنوي للجريمتين معًا، وفعل البقاء بهذا المعنى لا يختلف كثيرًا عن فعل الدخول غير المصرح به من حيث كون الفعل في ظاهره غير مشروع مما يتعين معه التجريم[5].

ويعترض على ذلك بعضهم – ونؤيده في ذلك – بالقول أن كل من الجريمتين تقع مستقلة عن الجريمة الأخرى، ويستدل على ذلك بالقول أن المشرع عندما يستخدم كلمتين أو مصطلحين

---

[1]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص 121.

[2]– **محمد حامد المرهج الهايتي:** جـرائم الحـاسوب، دار المـناهج للنشـر والتوزيـع، عمـان، الأردن، 2006، ص191–192.
– **أمال قارة:** الجريمة المعلوماتية، المرجع السابق، ص44.

[3]– **غنية باطلي:** المرجع السابق، ص161. – **محمد خليفة:** المرجع السابق، ص154.

[4]– **صاحب السيطرة على النظام *Le maitre du système*:** هذه التسمية وضعها الفقه الفرنسي للدلالة على صاحب الموقع الإلكتروني أو النظام المعلوماتي ومن له سلطة عليه، وهو كل هيئة أو شخص يسمح بالدخول أو عدم الدخول إلى نظامه المعلوماتي، كما عرفته الإتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات لعام 1989 بأنه: "كل شخص طبيعي أو معنوي أو سلطة عامة أو كل مؤسسة أو جهاز يكون لهم حق التصرف في النظام المعلوماتي التابع لهم وكيفية تنظيمه والهدف منه".

[5]– **رشيدة بوكر:** المرجع السابق، ص82. – **يزيد بوحليط:** المرجع السابق، ص184. – **أمال قارة:** المرجع نفسه، ص111.

مختلفين فلابد أن يكون لكل مصطلح معناه ومدلوله المختلف عن المصطلح الآخر، فمثلاً مصطلح "بقاء" لا يحتوي مصطلح "دخول" والعكس كذلك صحيح، فلكل فعل من الفعلين نطاقه ومجاله الذي لا يتداخل فيه مع الآخر.[1]

2. الطبيعة القانونية لفعل البقاء غير المشروع: لقد إتجه غالبية الفقه إلى إعتبار أن الطبيعة القانونية لهذه الجريمة أنها سلوك مجرد، وهو كل سلوك شكلي لا يتطلب نتيجة مادية معينة، أي أنه لا يشترط أن يتم البقاء بقصد تحقيق غرض معين؛ وهذا بإعتبار أن هذه الجريمة من جرائم السلوك المجرد، بحيث يكفي فيها إرتكاب فعل البقاء غير المرخص به داخل النظام المعلوماتي، بغض النظر عن تحقق نتيجة معينة أو عدم تحققها، وعلى ذلك يكتمل الركن المادي للجريمة بمجرد دخول الجاني وبقاؤه في الموقع أو النظام[2]، أي أن الركن المادي لتلك الجريمة لا يشترط أن يضاف إليه ضرورة وقوع أي شكل من أشكال الضرر، لأنه لم يشترط المشرع في نموذجها القانوني أية نتيجة إجرامية[3]، إذ أنها تكتمل بمجرد الإنتهاء من السلوك المكون لها والمتمثل في فعل الدخول أو فعل البقاء.

وعليه تعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي من الجرائم الشكلية التي لا يشترط فيها المشرع حدوث نتيجة إجرامية معينة[4]، وعلى ذلك فإن الركن المادي لهذه الجريمة يتمثل في نشاط إيجابي يتطلب من الجاني القيام به هو قطع الإتصال مع النظام، وأن إمتناعه عن قطع الإتصال مع هذا النظام يحقق السلوك الإجرامي المتطلب لقيام الجريمة، ومن ثم فإن هذه الجريمة من جرائم النشاط الإيجابي الذي يتحقق بالترك أو الامتناع.[5]

إلاَّ أن بعض الفقه لم يتفق حول ما إذا كانت هذه الجريمة من الجرائم الوقتية أم من الجرائم المستمرة[6] أو أنها من الجرائم المتتابعة الأفعال، غير أن الرأي الغالب ذهب إلى إعتبار جريمة البقاء من ضمن الجرائم المستمرة، وهذا على عكس جريمة الدخول كون الفترة التي تستمر فيها

---

[1]– ***GASSIN (R)****: Fraude informatique, Ed, Dalloz, Paris, France, 1995, P117.*

[2]– **محمد علي سويلم:** المرجع السابق، ص279.

[3]– **جميل عبد الباقي الصغير:** جرائم التكنولوجيا الحديثة، المرجع السابق، ص28.

[4]– **نهلة عبد القادر المومني:** المرجع السابق، ص161.

[5]– أنظر كل من: (– **رشيدة بوكر:** المرجع السابق، ص82. – **أيمن عبد الله فكري:** المرجع السابق، ص238).

[6]– **الجرائم المستمرة *Les délits continu*:** هي تلك الجرائم التي لا ترتكب في لحظة واحدة بل يفترض فيها إتيان سلوك يتسم بالإستمرارية، أي إستمرارية الحالة الإجرامية، ومثال ذلك جريمة حمل سلاح ناري بدون رخصة أو مثلاً جريمة إخفاء الأشياء المسروقة، أو جريمة إستعمال وثائق مزورة. (أنظر: – **لحسن بن شيخ:** مبادئ القانون الجزائي العام، دار هومة، الجزائر، 2005، ص63).

هذه الأخيرة قصيرة نسبيًا فهي تعتبر من الجرائم الوقتية ذات أثر ممتد بدون ضرر، على عكس جريمة البقاء فإنها تبدأ من اللحظة التي يبدأ فيها الجاني بالتجوال داخل النظام حتى ولو بعد إنتهاء الوقت المسموح به[1]، وهذا ما يميزها عن سابقتها حيث تبقى الجريمة قائمة مادام الجاني على إتصال بالنظام لذا تعتبر جريمة البقاء من الجرائم المستمرة وأنها ليست من الجرائم الوقتية.[2]

وتتجلى حالة الإستمرارية في عدم قطع الإتصال مع النظام عند إدراك الجاني أن وجوده فيه غير مشروع وغير مرغوب فيهّ، فهي تبدأ من اللحظة التي كان يجب عليه فيها أن يغير وضعه بالخروج الفوري من النظام المعلوماتي. ولكن ما يميزهما أن فعل الدخول جريمة وقتية وهي تعني تخطي الحدود سواء كان فعلاً مجردًا أو أنه أدى إلى إحداث نتائج معينة، وعليه إذا لم ينص صراحةً على فعل البقاء فلا يمكن سحب أحكام جريمة الدخول إليه، في حين أن فعل البقاء جريمة مستمرة، وعلة تجريم حال الإستمرار تكمن في النشاط غير المشروع من وقت توافر العلم به والإرادة المتجهة إلى تحقيقه.[3]

وبناءً على ذلك ذهب البعض الآخر من الفقه – الفرنسي وكذا الجزائري على حد سواء – إلى إمكانية الجمع بين الدخول والبقاء، إذ أن جريمة الدخول جريمة وقتية تعقبها جريمة مستمرة هي فعل البقاء داخل النظام[4]، حيث يرى أصحاب هذا الرأي أنه ليس من العدالة أن يتساوى من دخل النظام ثم خرج من فوره مع من دخله ثم بقي فيه مدة معينة، أي بين من إرتكب جريمة واحدة ومن إرتكب الجريمتين معًا، وأن الأخذ بهذا الرأي يشجع على العدول عن جريمة البقاء لمن إرتكب جريمة الدخول.[5]

وهكذا فإن جريمة الدخول وإن كانت جريمة وقتية فإنها في نفس الوقت جريمة ذات أثار ممتدة ومستمرة في الزمان، وعليه فإذا تحققت جريمة الدخول فلا تقع جريمة البقاء لأنها في تلك

---

[1]– **عبد القادر القهوجي:** المرجع السابق، ص135.

[2]– **سعاد حميدي:** الجرائم الماسة بالنظم المعلوماتية في التشريع المغربي، مجلة المنارة للدراسات القانونية والإدارية، ع13، المغرب، 2016، ص38.

[3]– **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص83.

[4]– لقد طبق القضاء الفرنسي نص فعل البقاء غير المصرح به كجريمة يعاقب عليها القانون، في الحكم الشهير لمحكمة إستئناف باريس في [5] أفريل 1994، وجاء في حيثيات هذا الحكم "... أن القانون يجرم البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات، سواءً كان الدخول قد تم عن طريق الإهمال أو تم بطريقة مشروعة، إلا أنه إكتسب بعد ذلك صفة اللامشروعية، كما لو فقد الفاعل حقه في البقاء ...".
Voir plus : *« **C. A**. de Paris, 5 Avril, 1994, N C P, 104 E », édition, Dalloz, Paris, France, 2009, P 916.*

[5]– ***GASSIN (R)*** *: Fraude Informatique, Op. Cit, P118.*

الحالة هي أثر من آثار الجريمة وليست فعلاً إجراميًا مستقلاً، وإذا إنتفت جريمة الدخول فإن جريمة البقاء لا تنتفي.[1]

ويكفي لتحقق جريمة البقاء مجرد الإبقاء على ذات المعاني السابقة لفعل البقاء، ولا يتطلب في نموذجها القانوني حسب نص التجريم تحقق نتيجة مادية معينة لها بوجودها المحدد في العالم الخارجي، وهو نفس الوضع الموجود في قانون العقوبات الجزائري وكذا نظيره الفرنسي، ولكن هذا لا يمنع من تصور أن يترتب على إرتكابها حدوث نتيجة معينة منظورًا إليها وفق مدلولها المادي، من حذف أو تغيير المعلومات التي يحتويها النظام أو تخريب نظام إشتغال المنظومة[2]، كما سوف يأتي معنا في حينه.

وغالبًا ما يجتمع معًا كل من فعل الدخول وفعل البقاء غير المشروعين، كأن يكون الفاعل غير مصرح له بالدخول إلى النظام البتة، وبالرغم من ذلك يدخل إلى النظام فعلاً ضد إرادة من له حق السيطرة عليه ويبقى فيه بعد ذلك، ويتحقق بذلك الركن المادي للجريمتين معًا، فتثور مسألة جد هامة هنا وهي: – كيفية الفصل بين الجريمتين؟ أي متى تنهي جريمة الدخول غير المشروع؟ ومتى تبدأ جريمة البقاء غير المشروع؟

لم نجد في القانون الجزائري أو المقارن نصًا يحدد بدقة زمن إنتهاء جريمة الدخول وزمن بداية جريمة البقاء في كل المنظومة أو جزء منها، وإن كان المنطق يستدعي أن بدايتها تكون منذ اللحظة التي يبدأ فيها الجاني بالتجوال داخل النظام المعلوماتي.[3] ويبدو أن حل هذه الإشكالية قد إختلفت فيها هي الأخرى الآراء الفقهية:

فمنهم من يرى أن جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول إلى النظام، أي يفترض البقاء لفترة قصيرة، لكن يؤخذ على هذا الرأي أنه لم يحدد هذه الفترة بطريقة حاسمة، وكذا لحظة بداية جريمة البقاء.[4]

كما ذهب رأي آخر إلى القول أن تلك اللحظة تتحدد في الوقت الذي يعلم فيه الجاني أن بقاءه داخل النظام غير مشروع، ولكن يؤخذ على هذا الرأي صعوبة إثبات علم المتدخل.[5]

---

[1]– **أيمن عبد الله فكري:** جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، مصر، 2007، ص206.

[2]– **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص84.

[3]– **زيدان زيبحة:** المرجع السابق، ص50.

[4]– **محمد خليفة:** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص155.

[5]– **غنية باطلي:** المرجع السابق، ص161.

وذهب رأي ثالث وهو الصائب نوعًا ما[1] إلى القول أن جريمة البقاء تبدأ من الوقت الذي يبدأ فيه المتدخل بالتجول داخل النظام بعد إنتهاء الوقت المحدد للدخول المشروع، أما في الحالة التي يكون فيها الدخول غير مشروع ودخل الجاني وظل ساكناً ولم يبدأ بالتحرك والتجول بعد، فهنا لا تقوم جريمة البقاء غير المشروع بل تظل جريمة الدخول قائمة من لحظة الدخول إلى حين مغادرة النظام، مادام أنه لم يتم إلتقاط المعلومات إذ لا يشترط أي نتيجة فيكفي البقاء المجرد.[2]

أما عن مسألة التقادم فإنه تحسب مدته من وقت الدخول غير المشروع حتى ولو إستمر الجاني في البقاء داخل النظام، أما إذا كان الدخول غير مقصود أو أنه مشروع، ثم علم المتهم أن بقاؤه غير مرغوب فيه بتداخله ومع ذلك فضل البقاء، فإنه ينسب إليه جريمة البقاء غير المشروع وتحسب مدة التقادم من الوقت الذي فيه ينتهي هذا البقاء.[3]

3. درجة الخطورة في جريمة البقاء غير المشروع: إن الخطورة القائمة وراء الدخول أو الإختراق، هو البقاء غير المشروع داخل النظام، الأمر الذي ينجر عنه حتمًا الإطلاع على المعلومات أو البيانات المخزنة آليًا، والتي لا يمكن بأي حال الإطلاع عليها من قبل الغير إلاَّ من خلال إذن مسبق، حيث أن الوصول إليها وإفشاءها سوف يؤدي إلى إلحاق أضرار بالمجني عليهم[4]، كما قد يؤدي إلى إلحاق الخسائر بالنظام المعلوماتي في ذاته أو بالآلية التي يعمل بها.[5]

وتزداد خطورة هذا الفعل في محدودية النص المُجرَّم له، حيث أن ترك المعتدين دون عقاب سيؤدي إلى التمادي في الإعتداء على النظم المعلوماتية من مواقع إلكترونية وحسابات خاصة[6] حتى ولو كان الهدف من وراء هذا الفعل هو مجرد الإطلاع وإثبات الذات والقدرة على

---

[1]– وإن كانت هناك أراء كثيرة حول هذه المسألة ومنها من يرى أن جريمة البقاء داخل النظام تبدأ من اللحظة التي ينذر فيها المتدخل بأنه متواجد بطريقة غير مشروعة، لكن أُنتقد هذا أيضًا بسبب أنه لابد من وجود جهاز إنذار يقوم بهذه المهمة، وإن أمكن تحقيقه فإنه سوف يكون من نصيب المؤسسات والشركات الكبرى فقط دون الأنظمة الخاصة.

[2]– **عبد القادر القهوجي:** المرجع السابق، ص133. غنية باطلي، نفس المرجع، ص162.

[3]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص123.

[4]– ***LARGUIER (J), CONTE (Ph), FOURNIER (S) :*** *Droit Pénal Spécial, 15eme éd, Dalloz, Paris, France, 2013, P251.*

[5]– **لينا محمد الأسدي:** المرجع السابق، ص162.

[6]– في تطبيق أحكام القانون المصري رقم (175 لسنة 2018) أشار هذا الأخير إلى تعريف كل من المواقع الإلكترونية والحسابات الخاصة وذلك بموجب المادة الأولى منه بقوله:

– **الموقع:** "مجال أو مكان إفتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة".

– **الحساب الخاص:** "مجموعة من المعلومات الخاصة بشخص طبيعي أو إعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو إستخدامها من خلال موقع أو نظام معلوماتي".

إختراق الحواجز الإلكترونية[1]، لأن المشرع لا ينتظر حتى ينجم عن هذا الفعل أضرار فعلية، وإنما يراعي في ذلك أهمية الأخطار المحتملة التي قد تترتب عن البقاء غير المشروع والتي تعرض المصالح الأساسية للفرد والمجتمع إلى الخطر.[2]

ثالثًا: موقف المشرع الجزائري من جريمة الدخول أو البقاء غير المشروع

يعتبر قانون العقوبات الجزائري من بين القوانين السباقة إلى فكرة الحماية الجنائية المعلوماتية، بل إنه من التشريعات المواكبة للتطورات الحاصلة في هذا المجال إلى جانب التشريع الفرنسي، وقد تدارك المشرع الجزائري الفراغ القانوني الحاصل في هذا المجال وهذا من خلال تكريسه لحماية المواقع الإلكترونية من كل أوجه الإعتداء بالدخول أو الإطلاع عليها بدون وجه حق كما فعلته غالبية القوانين المقارنة والمنظمة لمسألة الحماية الجنائية للنظم المعلوماتية والمواقع الإلكترونية.

كما أدرك أيضًا المشرع الجزائري الطبيعة القانونية الخاصة بالدخول إلى النظام أو البقاء فيه دون إذن مسبق، وحرص بدوره على تجريم هذه الأفعال وكل النتائج المترتبة عليها. وفعلاً خطى المشرع هذه الخطوة بالمبادرة إلى تعديل قانون العقوبات بمقتضى القانون رقم (04-15) السالف الذكر، والذي جرم بمقتضاه المشرع فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية، وإعتبر هذا التصرف في حد ذاته يُشكِّل جريمة تقع بمجرد إختراق جهاز الحاسوب، سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية، فمهما كان الغرض من هذا الولوج يعد حسب المشرع الجزائري إنتهاكًا للنظام والمساس بسلامته.[3]

كما يمكن أن ترتكب جريمة الدخول غير المشروع بأي طريقة أو وسيلة كانت لأن المشرع الجزائري هو الآخر لم يحددها، لأن الدخول بإستخدام وسائل تقنية أو بإستعمال كلمة المرور حتى وإن كانت مسروقة فإنه يعتبر مشروعًا من الناحية التقنية، أما من الناحية القانونية فهو حسب المشرع يعتبر دخول غير مشروع لأنه وببساطة يشكل إنتحال للشخصية بالإحتيال على النظام.[4]

---

[1]- **رشيدة بوكر:** المرجع السابق، ص69.

[2]- **عبد الواحد العلمي:** المبادئ العامة للقانون الجنائي المغربي، مطبعة النجاح الجديدة، المغرب، 1998، ص276.

[3]- **زيدان زيبحة:** الجريمة المعلوماتية في التشريع الجزائري والدولي، المرجع السابق، ص49، 50.

[4]- **نائلة عادل محمد فريد قورة:** المرجع السابق، ص223. - **أمال قارة:** المرجع السابق، ص100. - **غنية باطلي:** المرجع السابق، ص160.

وحسب المشرع الجزائري ايضًا أن فعل الدخول إلى النظام المعلوماتي يتحقق بمجرد الوصول إلى المعلومات المخزنة داخلة دون علم صاحبها، لأن هذا النظام مهما كان إنتماؤه لا يسمح دخوله إلاَّ لأشخاص معينة، لأنه بمجرد الدخول البسيط إلى هذا النظام يمكن أن يقع ذلك تحت طائلة النص الجنائي، لاسيما إذا كان هذا الفعل وقع دون علم القائم على النظام أو غير مرخص له وفقًا لتعليماته، بحيث يكمن هذا الفعل في الإعتداء على خصوصية المعطيات وملكيتها، مما يمكن معه القول بأن الفقرة الأولى من نص المادة (394 مكرر) من (ق ع ج) تنص على إحدى صور الإعتداء على الخصوصيات والمتمثلة في دخول شخص غريب إلى نظام خاص بالمعلومات مملوك للغير ليس بنية التملك وإنما بغرض الدخول والإطلاع دون أن يكون له نية الحذف أو التغيير، لذا رأى المشرع هنا ضرورة تجريم هذا الفعل في صورته البسيطة[1].

فحسب مفهوم نص المادة (394 مكرر) فإن هذه الجريمة في صورتها البسيطة تتحقق بالصور التالية:

– بمجرد الوصول إلى النظام المعلوماتي ومحتوياته وذلك بطريقة غير قانونية، كما عبر عنه المشرع الجزائري "بطريق الغش" وهذا ما يجعل من الجريمة أن تكون عمدية متى توافر القصد الجنائي العام.

– أن يكون الجاني عالمًا بدخوله إلى منظومة معلومات لا تخصه وغير مرخص له برؤيتها ومع ذلك يُصِرُّ على البقاء داخلها.

وكما هو واضحٌ من نص المادة (394 مكرر) فإن جريمة الدخول أو البقاء غير المشروع تصبح قائمة حتى ولو لم يترتب عن ذلك أي أضرار بالبيانات والمعلومات المخزنة داخل النظام، لذلك المشرع الجزائري يعتبرها من الجرائم الشكلية التي لا يشترط لقيامها تحقق نتيجة معينة، بل يكفي معها الوصول إلى هذه البيانات والمعلومات.

كما أن المشرع الجزائري إعتمد على الإطار الزمني في تحديد طبيعة الجريمة إن كانت فورية "وقتية" أم مستمرة، فإعتبر جريمة الدخول غير المشروع من الجرائم الوقتية، بينما جريمة البقاء في المنظومة تعد من قبيل الجرائم المستمرة.

[1] نبيل صقر، جرائم الكمبيوتر والأنترنت، دار الهدى، عين مليلة، الجزائر، 2012، ص218.

وبإستقرائنا للفقرات (ف1 – ف2 – ف3) من نص المادة (394 مكرر) من (ق ع ج)، نجد أن الركن المادي لهذه الجريمة يحتوي على صورتين إثنتين وهما الصورة البسيطة والمتمثلة في فعل الدخول في النظام أو البقاء فيه بطريقة غير مشروعة، وكذا الصورة المشددة والتي تنطوي على حذف أو تغيير في المعطيات أو على أفعال من شأنها المساس بسيرورة النظام ككل.

وعليه فإن نص المادة (394 مكرر) جاءت بجريمتين وهما فعل الدخول أو فعل البقاء في النظام المعلوماتي، منها ما هو جريمة نشاط إذا ما بقي في مجرد الدخول أو البقاء وتعتبر حينها جريمة خطر ولها عقوبة محددة، أو أنها جريمة نتيجة لهذا النشاط إذا ما ترتب عليها الأفعال المذكورة آنفا وتصبح بذلك جريمة ضرر مشددة العقوبة.

رأينا الخاص:

إن فعل الدخول غير المشروع وفعل البقاء غير المشروع هما جريمتان مستقلتان تمامًا، أي كل منها يستبعد ويستثني الأخرى، وعلى الرغم من أنهما عنصران ماديان مختلفان فهما مكملان لبعضهما البعض في مفهوم الجريمة في البيئة الرقمية.

وما يعتبر أقرب إلى الصواب هو إما أننا نكون أمام دخول غير مشروع وغير مصرح به، أو أننا نكون أمام بقاء غير مشروع بعدما كان الدخول مشروعًا ومصرحًا به ولكنه إنتهت مدته ولم يتم الإنسحاب في اللحظة التي بدأت فيها عدم صلاحية الإتصال المرتبط بالتجوال داخل النظام.

حيث أنه وببساطة شديدة عندما يكون الدخول غير مشروع نكون أمام جريمة الدخول وما يترتب فيها من بقاء فهو نتيجة لها وليست جريمة بقاء، أما عندما نكون أمام جريمة البقاء غير المشروع فهذا يدل على أن الدخول كان مشروعًا أو أنه حدث عن طريق الصدفة أو الخطأ أو السهو مع البقاء بقصد وبإرادة حرة وواعية على الرغم من إنتهاء صلاحية الدخول.

حيث أن المشرع الجنائي عمومًا قد إستعمل كل من مصطلح الدخول والبقاء فجمع بينهما في نص واحد مما يجعل كل واحد منهما يحوي الآخر، مع أن كل مصطلح له مدلوله ومعناه القانوني، وإن كان في الغالب إجتماعهما في نص واحد أمر غريب. إذ أن القارئ لنص المادة (394 مكرر) في عبارتها "... كل من يدخل أو يبقى عن طريق الغش ..."، وكذا نص المادة (323-1) من (ق ع ف) من خلال عبارتها: «*Le fait d'accéder ou de se maintenir, frauduleusement…*».

إذ أن هاتين العبارتين لم تبين بوضوح أن جريمة الدخول غير المشروع مختلفة عن جريمة البقاء غير المشروع، وكما نلاحظ أن كل من الدخول والبقاء في الغالب يتم الجمع بينهما بحجة صفة الغش المرتبطة بهما معًا.

لذلك نحن ننتقد فكرة الجمع بين فعل الدخول وفعل البقاء في نص واحد، وهذا لإختلاف طبيعة كل منهما؛ بل كان جدير بالمشرع أن يجعل كل فعل في نص خاص به حتى وإن كانت المصلحة المحمية هي واحدة بالنسبة للفعلين معًا، وبالتالي فكل جريمة تقع مستقلة عن الأخرى ولكل واحدة سلوكها الإجرامي الخاص بها، كما تجدر الإشارة أن المشرع الجزائري أقر للجريمتين عقاب واحد الأمر الذي يستوجب التفريق بينهما حتى في نطاق العقوبة، وذلك مثل ما فعله المشرع المصري بموجب القانون رقم (175 لسنة 2018) بشأن مكافحة جرائم تقنية المعلومات، حيث فصل بين الجريمتين وذلك من خلال جعل جريمة الدخول غير المشروع بموجب نص المادة (14) منه، وتليها جريمة البقاء غير لمشروع بموجب نص المادة (15) منه على التوالي، وحسناً فعل المشرع المصري في ذلك.

الفرع الثاني: الصورة المشددة لجريمة الدخول أو البقاء غير المشروع

أما عن الصورة المشددة للجريمة فإنها تتحقق بتوافر الظرف المشدد لها، والمتمثل في حصول نتيجة جراء فعل الدخول أو البقاء غير المشروع، بحيث يمتد فيها إجرام الجاني إلى إحداث تغيرات داخل النظام المعلوماتي، لهذا نجد أن المشرع الجنائي قد ربط بينها وبين الجريمة الأصلية بإعتبارها ظرف تشديد لها.

ومع ذلك يتضح لنا أن هدف كل من المشرع الجزائري ونظيره الفرنسي كان واضحًا وهو حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة أو غير مباشرة، وأيضًا حماية المعطيات والبيانات الموجودة داخله، وحسناً فعل في تشديد العقوبة نظرًا للقيمة المستحدثة للمعلومات في شتى المجالات، وأن الإطار العام للنص جاء غير مميز لنوعية المعلومة بل جاء حماية لها على العموم وشاملاً لكل أنواع التلاعبات بمختلف الوسائل التي قد تمس بها.

والملاحظة التي يمكننا إبداؤها هنا، أن المشرع الفرنسي نص على هذه الجريمة كظرف تشديد لجريمة الدخول أو البقاء بغير حق في نظام المعالجة الآلية للمعطيات، وذلك من خلال نصين مختلفين أحدهما بموجب المادة (323-1) والتي تشدد من عقوبة الحبس والغرامة إذا ترتب على فعل

الدخول أو فعل البقاء أي إلغاء أو تعديل للبيانات المبرمجة داخل النظام[1]، والظرف المشدد الآخر بموجب المادة (323-2) والتي تنص على فعل إعاقة سير النظام المعلوماتي والإخلال به بصفة مستقلة[2].

أما المشرع الجزائري فقد إكتفى بالنص على هذه الجريمة كظرف مشدد لجريمة الدخول أو البقاء بموجب نص مادة واحدة وهي المادة (394 مكرر) والتي جمعت بين الصورتين البسيطة والمشددة، ومن خلال إستقراءنا للفقرتين الثانية والثالثة لنص المادة (394 مكرر) نجد أنها قد نصت على ظرفين تشدد بهما عقوبة الجريمة، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع حذف أو تغيير للبيانات التي يحتويها النظام، أو عدم قدرة النظام على تأدية وظيفته المعلوماتية، حيث جاء في سياق هاتين الفقرتين ما نصه: "... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة ...".

وعليه نستنتج من خلال ذلك أن هناك ظرفين إثنين يمكن أن تشدد بهما عقوبة هذه الجريمة شرط أن تكون هناك علاقة سببية بين هذه النتيجة والسلوك المجرم[3]، أي بين فعل الدخول أو فعل البقاء غير المشروع والنتيجة الضارة حتى وإن لم تكن مقصودة، لأن ظرف التشديد هنا يعتبر ظرف مادي يكفي أن توجد بينه وبين الجريمة الأساسية علاقة سببية للقول بتوافره، إلا إذا أثبت الجاني إنتفاء تلك العلاقة وأن ما حصل يرجع إلى قوة قاهرة أو حادث مفاجئ[4]، أو أنه راجع للخطأ غير العمدي[5].

---

[1]– ***Article 323-1 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4***

« - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

[2]– ***Article 323-2 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4***

« - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

- Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

[3]– **عزيزة رابحي:** المرجع السابق، ص162.

[4]– **أمال قارة:** المرجع السابق، ص114.

[5]– **محمد علي سويلم:** المرجع السابق، ص281.

ومن هنا نجد أن هذان الظرفين يشددان من عقوبة هذه الجريمة إذا ما ترتب عليهما ضرر فهي إذن تتماشى مع الجرائم ذات النتيجة على أساس الضرر متى حصل فعلاً ضرر معين يمس بالمعلومات ونظم معالجتها، ولا يشترط هنا أن تكون تلك النتيجة الضارة مقصودة أم لا، لأن تطلب مثل هذا الشرط يجعل هذا الظرف دون فائدة[1]، حتى ولو وقع على سبيل الخطأ غير العمدي والذي يتخذ صورة الإهمال أو عدم الإنتباه أو عدم الإحتراز أو الرعونة.[2]

أما بخصوص ضابط التفرقة بين حالة الحذف أو تغيير المعطيات أو تخريب النظام، تكمن من خلال تحليل كل ظرف على حدة، وهذا وفق ما يلي:

أولاً: حذف المعطيات *La Suppression des données*

الحذف يقصد به التخريب أي توقف الشيء تمامًا عن أداء وظيفته سواء كان هذا التوقف كليًا أو جزئيًا، مما يجعل الشيء غير صالح للإستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل[3]، ففعل الحذف يشير إلى إزالة المعطيات داخل النظام، وهو أقصى أنواع الضرر مما جعل العقاب عليه مشددًا[4].

كما عبر عنه المشرع المصري بموجب القانون السالف الذكر "بالإتلاف"[5]، وذلك من خلال إحداث أفعال مادية بالبيانات والمعلومات الموجودة على النظام، بحيث يكون من شأن ذلك الحذف أو المحو أن يُحدث إنقاص في المعطيات ومكوناتها أو أدائها لوظيفتها أو مهمتها.[6]

وجوهر الإتلاف لا يشترط أن ينصب الحذف على جميع المعطيات وإنما يكفي أن يحدث حذف جزئي لها[7]، ويتحقق ذلك بإحداث خلل في سلامة البيانات والمعلومات، كما يستوي أن يتحقق

---

[1]– **سليمة سعيدي، حجاز بلال:** المرجع السابق، ص150.

[2]– لأن نص الفقرتين الثانية والثالثة من المادة (394 مكرر) من (ق ع ج) لا تسمح بحدوث نتيجة ضارة سواء كانت مقصودة أم لا، ويفهم ذلك من خلال عبارة "إذا ترتب.."، بمعنى أن المشرع لا يشترط أن تكون تلك النتيجة مقصودة أم غير مقصودة لقيام الظرف المشدد.

[3]– **نبيل صقر:** الوسيط في شرح جرائم الأموال، دار الهدى عين مليلة، الجزائر، 2012، ص213.

[4]– **يزيد بوحليط:** المرجع السابق، ص185.

[5]– عاقب المشرع المصري بعقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف أو بإحدى هاتين العقوبتين، إذا نتج عن فعل الدخول أو البقاء إتلاف أو محو أو تغيير للبينات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، وهذا ما نصت عليه المادة (17) من القانون المصريي رقم (175 لسنة 2018) السالف الذكر. **الملحق رقم (04)**

[6]– **محمد علي سويلم:** المرجع السابق، ص283.

[7]– **عبد الوهاب ملياني:** أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقياد، تلمسان، الجزائر، 2017، ص187.

هذا الإتلاف والحذف بواسطة إستخدام البرامج الخبيثة كالفيروسات مثلاً، أو من خلال الدخول مباشرة على مكان تواجد المعلومة وإتلافها كليًا أو جزئيًا[1].

كما أن المشرع لم يشترط أن ينتج عن هذا الحذف تعطيل أو ضرر في سيرورة النظام، لأن التعطيل يكون بتوقف الشيء عن القيام بوظيفته فترة مؤقتة[2] وهذا على عكس الحذف، وبالتالي فبمجرد وقوع حذف في معطيات المنظومة كافٍ لتشديد العقوبة.[3]

ثانيًا: تغيير المعطيات *La modification des données*

يختلف التغيير عن الحذف، فهو يفترض فيه إستبدال معطيات مكان أخرى نتيجة الدخول أو البقاء غير المشروع، أي إحداث تعديلات فحسب في المعطيات دون أن يصل الأمر إلى حد إزالتها أو فنائها بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة، أو أنه لها معنى ولكنه مغاير لما كانت عليه قبل التغيير فيبقى النظام في هذه الحالة سليمًا لكن بوجود معطيات ومعلومات مغايرة[4]، لذلك يتفق الكثير من الفقه على أن مصطلح "التغيير" يقصد به "العبث المعلوماتي" أي إحداث خلل أو التلاعب بالبيانات والمعلومات الموجودة داخل النظام، بطريقة تؤدي إلى إختلاف معناها والإنقاص من مكوناتها أو أدائها لوظيفتها أو مهمتها[5]، وبعبارة أخرى يكون التغيير بإحداث تعديل في البيانات؛ بحيث تفقد قيمتها وحقيقتها التي كانت عليها.

كما أن التغيير لا يشترط أيضًا تعطيل النظام أو إفساده، إنما مجرد التغيير يجعل السلوك المجرم قائمًا، لأن فعل التغيير مجرم لذاته، فلا يهم بعدها إن حدث معه تعطيل للنظام أو تحسين أدائه بسبب ذلك التغيير، وهذا إحترامًا لمبدأ الشرعية الجنائية.[6]

---

[1]– **حسني الجندي:** قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، الكتاب الثالث، دار النهضة العربية، القاهرة، مصر، 2009، ص83.

[2]– **هدى حامد قشقوش:** جرائم الكمبيوتر والجرائم الأخرى، المرجع السابق، ص 564. – **عبد القادر القهوجي:** المرجع السابق، ص111.

[3]– **عبد الوهاب ملياني:** المرجع نفسه، ص187.

[4]– وتجدر الإشارة هنا أنه يقصد بالمعطيات والمعلومات بمعناها الواسع، فتشمل كل ما يمكن أن يحتوي عليه النظام المعلوماتي من بيانات مهمة وسرية كالسجلات الطبية والبيانات الخاصة بالعملاء في البنوك والبيانات الشخصية في سجلات الحالة المدنية، وكذا الأسرار الحكومية والعسكرية للدولة.

[5]– **محمد علي سويلم:** المرجع السابق، ص284.

[6]– **حسني الجندي:** المرجع السابق، ص83.

ثالثًا: تخريب نظام إشتغال المنظومة *L'altération du fonctionnement de système*

تخريب النظام يقصد به كل فعل من شأنه جعل النظام مصابًا بالشلل أو العجز كنتيجة لجريمة الدخول أو البقاء غير المشروع، وبالتالي تعطيله عن أداء مهامه، فمصطلح التخريب يشتمل على جميع الأوصاف المؤدية لعرقلة أو إفساد لوظائف النظام، والذي يحدث من خلال العبث في معطيات النظام المتعلقة بمنظومة سيره[1]، وذلك بإستعمال تقنيات ووسائل عديدة كإستخدام برامج الفيروسات أو بإستعمال تقنية التشبع *Saturation* أو تقنية الفخ *Trappe* ... وغيرها.[2]

لهذا فالتخريب أكثر ضررًا من فعل الحذف أو التغيير[3]، وهذا ما أكد عليه التقرير التفسيري المتعلق بشرح إتفاقية بودابست والمتعلقة بالإجرام المعلوماتي حيث تشترط أن يكون تخريب أو تعطيل النظام على درجة من الخطورة، بحيث يحرم صاحب النظام من الإستعمال العادي لنظامه مرة أخرى[4].

ويتكون الركن المادي في جريمة تخريب نظام إشتغال المنظومة في قيام الجاني بأحد النشاطين إما "الإعاقة" أو "الإخلال" بسير النظام وهما على التوالي:

أ- الإعاقة أو العرقلة *Entrave*: يقصد بالإعاقة منع النظام بصفة كلية أو جزئية من العمل، فقد ترد الإعاقة على برنامج من البرامج التي يحتويها النظام وليس على كل نظام الحاسوب[5]، فالمشرع الفرنسي لم يفرق بين حالة الإعاقة الدائمة أو المؤقتة أو على فترات.[6]

ويشير أيضًا التقرير التفسيري لإتفاقية بودابست السالف بيانها، أن العرقلة أو الإعاقة يجب أن تكون بدون وجه حق حتى تتحقق الجريمة، وأنه لا يشترط في العرقلة أن تكون إيجابية بل يمكن أن يتحقق ذلك عن طريق الإمتناع كأن يمتنع الجاني عن القيام بعمل يفرضه عليه القانون أو الإتفاق، غير أنه لا يعد من قبيل إعاقة النظام قيام العاملين مثلاً بالإضراب عن العمل، الأمر الذي يسبب توقف النظام – الكمبيوتر – عن العمل، فلا يسري هذا الوصف المؤثم في جريمة إعاقة

---

[1]- **يزيد بوحليط:** المرجع السابق، ص185. - **رشيدة بوكر:** المرجع السابق، ص231.

[2]- وما يجدر بنا الإشارة إليه هنا أن جريمة تخريب سير النظام يطلق عليها "الجريمة ذات الطابع الحر" حيث لا تتقيد بالوسيلة الواحدة التي يقع بها التخريب أو التعطيل، وإنما يستعمل فيها وسائل متعددة كإستخدام الفيروسات مثل: فيروس حصان طروادة والقنبلة الموقوتة والقنبلة المنطقية وبرامج الدودة ... وغيرها، أو من خلال التغيير في رقم التشغيل أو تعطيل برامج الدخول فينتج عنها توقف كامل أو جزئي للنظام، أو إستحالة مطلقة لإعادة إستخدام النظام المعلوماتي مرة أخرى.

[3]- **عبد الفتاح بيومي حجازي:** الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص41.

[4]- راجع في ذلك المادة الخامسة من نص إتفاقية بودابست المتعلقة بالإجرام المعلوماتي والمشار إليها سلفًا. **الملحق رقم (01)**

[5]- **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص283.

[6]- حيث تنص المادة (323-2) من (ق ع ف) على تشديد العقوبة في حالة القيام بالأفعال التي تعيق أو تخل بالسير الحسن لنظام المعالجة الآلية للمعطيات، وذلك بالحبس لمدة تزيد عن خمس سنوات والغرامة التي لا تزيد عن 100.000 أورو.

النظام، ولكن إذا حدث في أثناء الإضراب تخريب لأجهزة الكمبيوتر الخاصة بالعمل، عندئذ يمكن القول بوقوع جريمة الإعاقة بالإضافة إلى وصف آخر وهو الإتلاف المعلوماتي[1]، وهذا ما أكد عليه التقرير التفسيري السالف الذكر، أنه يجب على الأطراف الموقعة إختيار نظرية محددة لمعنى العرقلة والإعاقة في قوانينها الداخلية وذلك من أجل تحديد إلى أي مدى يمكن إعتبار الأفعال من قبيل العرقلة.[2]

وجدير بالذكر أن نص المادة الخامسة من الإتفاقية المشار إليها أعلاه، تترك للأطراف مهمة تحديد في أي الأحوال يعد عمل النظام معاقاً جزئياً أو كلياً، بشكل مؤقت أو دائم، حتى يمكن معرفة ما إذا كانت الإعاقة تستوجب جزاءًا إدارياً أم جزاءًا جنائياً بمقتضى قوانينهم الداخلية بشرط أن تكون الإعاقة قد أُرتكبت عمداً *Intentionnellement*، أي نية إحداث إعاقة جسيمة *L'intention causer une entrave grave*.

ب-الإخلال أو الإرباك *Perturber*: ويقصد به كل الأعمال التي من شأنها أن تمس بحسن سير النظام المعلوماتي، فهذا النوع من السلوك يجعل النظام غير قادر على أداء مهامه بصفة عادية، كالتقليل من سرعته التي برمج لأجلها أو حتى الزيادة في سرعته بشكل يخل بالعمل به، وقد يرد الإخلال في طريقة العمل على برنامج من البرامج وليس على كل النظام، بحيث يقوم الجاني في هذه الصورة من النشاط بإدخال ما من شأنه أن يسبب خللاً في نظام عمل الجهاز الإلكتروني، فالجهاز يعمل في هذه الحالة ولكن بصورة بطيئة أو بصورة مضطربة بحيث تبتعد عن الصورة المعتادة لعمل النظام.[3]

بعبارة أخرى يقصد بالإخلال تعييب النظام مما يؤدي إلى حصول نتائج غير تلك التي كان من الواجب الحصول عليها، ويشمل ذلك كل تشويه في سير النظام بحيث يؤدي إلى نتائج غير سليمة مخالفة للصورة المعتادة لعمل هذا النظام، مما يؤدي إلى إرباكه[4]. ولا يعتبر من قبيل النشاط المعاقب عليه في هذه الجريمة أن يحدث إخلال مثلاً بعقد من عقود صيانة أجهزة الكمبيوتر أو عدم توريد قطع غيار لتلك الأجهزة بما يؤدي إلى الإخلال بسيرها.

---

[1]- **شيماء عبد الغني محمد عطا الله:** المرجع نفسه، ص284. - **أمال قارة:** المرجع السابق، ص118.

[2]- **عبد الفتاح بيومي حجازي:** الحماية الجنائية لنظام الكمبيوتر، المرجع نفسه، ص42.

[3]- **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص129.

[4]- **عبد الفتاح بيومي حجازي:** الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص43.

وعليه فإن الإخلال المتعلق بنظام المعالجة الآلية حسب المفهوم السابق يختلف عن العرقلة أو التعطيل، فهو لا يؤدي إلى توقف عمل النظام أو إتلافه بالمرة، لكنه يجعل من هذا النظام غير قادر على الإستعمال السليم والصحيح.[1]

خلاصة القول:

وهنا كخلاصة لهذه الصورة المشددة لجريمة الدخول أو البقاء غير المشروع داخل النظام يمكننا القول، أن الظرف المشدد سواء كان متمثل في الحذف أو التغيير أو التخريب هو ظرف مادي يكفي لتحققه وجود علاقة سببية بينه وبين الجريمة الأصلية والبسيطة، أما إذا حدثت النتيجة من فعل آخر فلا وجود للظرف المشدد هنا، وأيضًا إذا أثبت الجاني إنتفاء تلك العلاقة، كأن يثبت أن الحذف أو التغيير أو تخريب النظام كان سببه القوة القاهرة أو الحادث المفاجئ[2]، وهنا يبقى للمتضرر خارج هذه النتائج الثلاثة سوى المطالبة بالتعويض وفقا للقواعد العامة للمسؤولية المدنية.[3]

المطلب الثالث: الركن المعنوي لجريمة الدخول أو البقاء غير المشروع

إن الركن المعنوي لجريمة الدخول أو البقاء غير المشروع داخل النظام، يحتم علينا أيضًا أن نميز بين الصورة البسيطة للجريمة (فرع أول) والصورة المشددة لها (فرع ثاني) من حيث توافر القصد الجنائي من عدمه.

الفرع الأول: من حيث الصورة البسيطة للجريمة

تعد جريمة الدخول غير المشروع أو البقاء غير المشروع داخل أنظمة المعالجة الآلية للبيانات من الجرائم العمدية[4]، أي يجب توافر القصد الجنائي العام دون القصد الجنائي الخاص، فهي من الجرائم المقصودة[5]، التي يتطلب لقيامها توافر القصد الجنائي بعنصرية "العلم والإرادة"، أي العلم بمكونات الجريمة والإرادة المتجهة إلى إحداثها.[6]

---

[1]– **عبد الوهاب ملياني:** المرجع السابق، ص189–190.

[2]– **عبد القادر القهوجي:** المرجع السابق، ص138.

[3]– **محمد خليفة:** المرجع السابق، ص162.

[4]– **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص 85. – **غنية باطلي:** المرجع السابق، ص166.

[5]– يقسم الفقه الجنائي الجرائم تبعًا للركن المعنوي إلى: "جرائم مقصودة *Infraction intentionnelles*" و"جرائم غير مقصودة *Infraction non intentionnelles*". ولمزيد أكثر حولا الموضوع أنظر كل من:

- ***GASTON (S), LEVASSEUR (G), BOULOC (B) :*** *Droit pénal général, 16eme édition, dalloz, Paris, France, 1997, P P231-232.*

- ***Voir plus : PHILPPE Conte, PATRICK Maistre du Chambon :*** *Droit pénal général, 7eme, édition, Armand collin, Paris, France, 2004, P120.*

[6]– **محمود نجيب حسني:** النظرية العامة للجريمة، دار النهضة العربية، القاهرة، مصر، 1988، ص60.

وعلم الجاني يجب أن يشمل كافة الوقائع التي يتطلبها القانون لبناء أركان الجريمة وإستكمال عناصرها، فلابد أن يحيط الجاني علمًا بأنه يأتي فعلاً غير مشروع يتمثل في الدخول والبقاء في النظام المعلوماتي المملوك لغيره والغير مصرح له بدخوله أو بالتجول في محتوياته من معلومات وأسرار وبرامج ونظم[1]. وأيًا كانت الوسيلة التي يلجأ إليها الجاني في الإحتيال على النظام في الولوج والبقاء، والتي قد تأخذ عدة أشكال وأساليب[2]، فضلاً عن التكييف الذي سوف تتصف به هذه الأساليب وتكتسب به أهميتها في نظر القانون.

وعليه يتوفر الركن المعنوي في هذه الجريمة في حال علم الجاني بكافة العناصر المشكلة لها، ومن قبيل ذلك علمه بأن فعله ينصب على نظام المعالجة الآلية للمعطيات، وأنه لا يملك حق الدخول إليه أو البقاء فيه، فضلاً عن علمه بخطورة فعله على المصلحة التي يحميها القانون، وأنه بذلك ينتهك سرية وخصوصية هذا النظام[3]، فيستوي في ذلك أن يكون غرض الجاني من الدخول مجرد التعرف والإطلاع على الأسرار أو لتمكين غيره من إستعمالها[4]، فإذا إنتفى العلم بالعناصر السابقة إنتفى تبعًا لذلك القصد الجرمي.

كما ينتفي العلم في حالة ما إذا كان دخول الجاني إلى النظام قد تم بناءًا على الصدفة المحضة أو أنه دخل بطريق الخطأ، فالجريمة هنا لا تتحقق بدخول الخطأ أو الصدفة لأنهما غير معاقب عليهما[5]، إلاَّ أنه يتحتم عليه الخروج من النظام بمجرد علمه أن دخوله غير مسموح به، فإذا لم يفعل ذلك توافر لديه القصد الجنائي منذ اللحظة التي تحقق فيها العلم، ويكون بذلك مرتكبًا

---

[1]– **بهاء فهمي الكبيجي:** مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2013، ص 33–34.

[2]– فقد تأخذ شكل حل الشفرة المتعلقة بالمعلومات أو البرامج أو النظام ككل، وهذا من خلال إستخدام كلمة المرور أو الرقم السري أو الكودات السرية التي يتم التوصل إليها إما عن طريق السرقة أو الإحتيال على صاحبها، أو حتى عن طريق التجربة لعدة أرقام أو كلمات أو حروف أو رموز أو شفرات مركبة من هذه الأشياء، كله بغية التوصل في النهاية إلى الوسيلة التي بها يستطيع الجاني كسر نظام الأمان الخاص بالنظام المعلوماتي، أو أنها قد تأخذ شكل إنتحال صفة مستخدم النظام، وبذلك يستطيع الدخول والبقاء، مع الإشارة أنه في هذه الحالة الأخيرة نكون بصدد تعدد مادي للجرائم وهما جريمة الدخول أو البقاء بغير حق وكذا جريمة النصب الإحتيالي على نظام المعالجة الآلية للمعطيات، فهنا تطبق العقوبة الأشد وفقًا لما نصت عليه المواد (32 و33 و34 و35) من (ق ع ج) وكذلك نص المادة (32) من (ق ع المصري).

[3] ***QUÉMÉNER (M), CHARPENEL (Y) :*** *Cybercriminalité et droit pénal appliqué,Op. Cit, P72.*

[4]– **نبيل صقر:** الوسيط في شرح جرائم الأموال، المرجع السابق، ص219.

[5]– **عزيزة رابحي:** الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018، ص167.

لجريمة البقاء[1]، عندئذ يمكن القول بأن جريمة الدخول لا تتوافر لإنتفاء القصد الجنائي بينما تتوافر جريمة البقاء في هذا الفرض[2].

وعليه لا يتوافر الركن المعنوي في حق الجاني إذا تمت هذه الأفعال في صورة الخطأ أو الصدفة، لكن يجب أن يثبت أنه لم يَرِدْ الوصول لهذه النتيجة، إلاَّ أن الواقع العملي أثبت أن علميات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها سواء بالخطأ أو بالصدفة هي عمليات تتكرر وتتزايد بشكل مذهل في اليوم الواحد، خصوصًا مع تزايد مستخدمي الإنترنت، وليس من المستبعد أن تكون هناك عمليات دخول وبقاء غير مصرح بها لكنها غير مقصودة، حيث لو كانت هذه العمليات من قبيل الجريمة العمدية لوقع كل مستخدمي هذه الشبكة تحت طائلة قانون العقوبات، وعلى هذا كان من اللازم أن تكون حالة الصدفة أو الخطأ في الدخول أو البقاء من الأمور غير العمدية، وهذا من أجل الموازنة بين حماية المعلوماتية والمعطيات من جهة وحرية الأفراد في إستخدام الإنترنت من جهة أخرى[3].

كما لا يتوافر القصد الجنائي إذا وقع الجاني في خطأ في الواقع، كأن يكون المتهم سبق له الإشتراك في النظام، ولكن بعد فترة إنتهت مدة الإشتراك ودخل مرة أخرى إلى النظام معتقدًا خطأ بأنه مزال له الحق في الدخول إليه، فإن ذلك يعد جهلاً بالواقع مما ينفي القصد الجنائي لديه[4]، سواء كان هذا الخطأ يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يعتقد خطأ أنه مسموح له بالدخول، لاسيما إذا لم تحدد صلاحيات النظام المستعمل بدقة[5]، لكن في كل الأحوال لابد عليه أن يخرج فورًا من النظام حال علمه بأن دخوله أو بقاؤه فيه غير مسموح به، فإذا لم يفعل ذلك هنا بالضبط توافر لديه القصد الجنائي منذ اللحظة التي تحقق فيها العلم فتقوم معها مسؤوليته الجنائية[6].

---

[1]– **رشيدة بوكر:** المرجع السابق، ص86.

[2]– **شيماء عبد الغني محمد عطا الله:** المرجع السابق، ص126.

[3]– **غنية باطلي:** المرجع السابق، ص 166.

[4]– **عزيزة رابحي:** المرجع السابق، ص 168.

[5]– **فيصل بدري:** مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر1، 2018، ص167.

[6]– أنـظـر في ذلك كل مـن: – **يزيد بوحليط:** المرجع السابق، ص 186–187. – **مريم أحمد مسعود:** المرجع السابق، ص36.
Voir : CHRISTIANE (F-S) : *Le droit à l'épreuve, de l'internet, 4eme édition, dalloz, Paris, France, 2006, P598.*

أما إن إختار الجاني سبيل البقاء في النظام بعد أن دخله بطريق الخطأ أو الصدفة، ثم قام بالعديد من الأفعال التي تشكل إنتهاكاً للنظام المعلوماتي كالإطلاع على الأسرار المعلوماتية والتنقل عبر قوائم البيانات والمعلومات، أو بأي من الأفعال الإجرامية الأخرى[1]، فإنه في هذه الحالة يكون قد إرتكب جريمة الدخول والبقاء المنصوص عليها في المادة (394 مكرر) من (ق ع ج) وهو ما يفهم من عبارة "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".[2]

إلى جانب العلم كعنصر في القصد الجنائي لابد من توافر الإرادة، وهي التي تبين الموقف النفسي للفاعل من سلوكه ومن النتيجة المترتبة عليه، أي أن تتجه إرادة الجاني إلى فعلي الدخول أو البقاء وإلى النتيجة الإجرامية وهي الإطلاع على البيانات والأسرار المعلوماتية بدون وجه حق، فإذا لم تتجه إرادة الجاني إلى فعل الدخول أو البقاء ولكن وجد نفسه داخل النظام بمحض الصدفة أو عن طريق الخطأ، ولم يتعدى سلوكه ذلك ووقف عند هذا الحد دون أن يتعداه في الإطلاع أو إستراق النظر إلى المعلومات، فإنه في هذه الحالة لا يتوافر القصد الجنائي لديه، وبالتالي لا قيام للركن المعنوي في هذه الجريمة ولا عقاب على فعله.[3]

ومادام أن هذه الجريمة في صورتها البسيطة لا يتطلب في قيامها تحقق نتيجة معينة فإن الإرادة تقتصر فقط على السلوك الإجرامي[4]، بمعنى أنه نظرًا لكون جريمة الدخول والبقاء من الجرائم الشكلية في التشريعات الحديثة، فإن عنصر الإرادة يقتصر على السلوك الإجرامي فتستغرقه بكل مقوماته ولا تمتد إلى النتيجة بغض النظر عن الباعث أو الغاية على إرتكاب الجريمة[5]، ولا يهم الباعث هنا سواءً كان ناتجاً عن مجرد الفضول الإلكتروني أو التنزه الإلكتروني أو إثبات القدرة على التفوق على الآلة.

---

[1]– كإستكشاف للمواقع الغير مسموح برؤيتها أو بالإطلاع عليها، أو القيام بنسخ الملفات والبرامج أو بتعديلها أو بإلغائها أو إتلافها أو محوها... وغيرها من الأفعال التي تشكل جريمة معلوماتية في حد ذاتها.

[2]– وهو نفسه ما جاء في سياق نص المادة (462–2) من (ق ع ف) لعام 1988 والمعدلة بالمادة (323–1) بموجب القانون الصادر عام 1994 فيما يخص الغش المعلوماتي.

[3]– ويقاس ذلك أيضًا على عنصر الإكراه على فعلي الدخول والبقاء بأي من وسائل الإكراه المادي أو المعنوي، كما لو قامت إحدى عصابات قراصنة المعلومات الإلكترونية، على إجباره وإكراهه على ذلك، نظرًا لما لديه من مهارة ودراية بفنون وتقنيات الحواسيب والنظم المعلوماتية، الأمر الذي جعله ينساق وفق إرادتهم لا إرادته هو، وبالتالي فالإرادة هنا معدومة ولا أساس لها من القانون. (أنظر أكثر: – **بلال أمين زين الدين:** المرجع السابق، ص279).

[4]– **غنية باطلي:** المرجع السابق، ص167.

[5]– **رشيدة بوكر:** المرجع السابق، ص86.

وعلى العموم فإنه يلزم توافر القصد الجنائي بعنصريه "العلم والإرادة" في جريمة الدخول أو البقاء في النظام المعلوماتي، وهذا لأنها جريمة تنتمي إلى زمرة الجرائم العمرية، وعلى أي حال فإنه لا يلزم توافر قصد من نوع خاص لوقوع هذه الجريمة، إذ يكفي توافر القصد الجنائي العام، أي أن يعلم المتهم بدخوله في النظام المعلوماتي الخاص بالغير مع إتجاه إرادته إلى تحقيق النتيجة الإجرامية المتمثلة في البقاء غير المشروع.[1]

حيث يتبين لنا من إستقراء نص المادة (394 مكرر) السالفة الذكر أن المشرع الجزائري لا يتطلب وجود قصد جنائي خاص لدى الجاني حتى تقوم هذه الجريمة، بل أنه يكفي لقيامها توافر القصد الجنائي العام القائم على العلم والإرادة معًا، والسبب في ذلك أن نظم المعالجة الآلية للمعطيات تتميز بأنها مناطق مفتوحة بعضها على بعض ومتشعبة نوافذها، لذا يلزم التأكد من توافر القصد الجنائي العام فقط لدى الفاعل في تجاوزه التصريح الممنوح له،أو حين إتيانه فعل الدخول أو فعل البقاء في النظام بغير وجه حق[2].

وإذا كان القانون يتطلب أن يكون الدخول قد تم بطريقة غير مشروعة، فيذهب البعض هنا إلى القول أن معيار التمييز هو وجود نظام الحماية الفنية والأمنية، لكن الإتجاه الغالب اليوم يرى عدم إشتراط توفر نظام الحماية الفنية لإثبات الركن المعنوي[3]، بمعنى أن دخول الشخص إلى الشبكة أو النظام أو حتى الموقع بدون ترخيص من الجهة المخول لها منح هذه الصلاحية، فإن مثل هذا الفعل يؤكد إرتكاب الجريمة عمدًا عن طريق خرق التدابير الأمنية بقصد الحصول على بيانات الكمبيوتر، وهو ما سار عليه كل من التشريع الجزائري ونظيره المصري وحتى الفرنسي.[4]

أما فيما يخص مسألة إثبات القصد الجنائي، فإنه يثبت إلى المتهم كلما توفر عنصر "الغش *Frauduleusement*"[5] وهو ما يقصد به عدم حصول الجاني على ترخيص مسبق من الجهة المختصة

---

[1]– ***BENSOUSSAN (A) :*** *Internet « aspects juridiques » Ed. Hermès, Paris, France, 1998, PP198-199.*

[2]– **محمد خليفة:** الحماية الجنائية لمعطيات الحاسب الآلي، المرجع السابق، ص150.

[3]– **أحمد حسام طه تمام:** المرجع السابق، ص292.

[4]– **فضيلة عاقلي:** المرجع السابق، ص09–10.

[5]– وهو أن يكون الدخول أو البقاء موصوفًا بالغش *Frauduleusement* والذي إستعمله لأول مرة القضاء الفرنسي، وصفة الغش هذه لها دلالات كثيرة في هذا المجال، فقد تعني أن الشخص ليس له حق الدخول، أوله ترخيص بذلك لكنه لم يحترم القواعد والإجراءات الفنية الموضوعة من طرف القائم على النظام.

Voir plus : - CASILE Jean-François: *Le code pénal à l'épreuve de la délinquance informatique, Op. Cit, P95.*

والتي لها سلطة ومسؤولية على المنظومة الرقمية ومعطياتها[1]، أي طالما تعمد إتيان هذا الفعل وبدون ترخيص مسبق من صاحب النظام المعلوماتي، وأحياناً يزداد الأمر تعقيدًا من حيث صعوبة إثبات القصد الجنائي وهذا نتيجة إحتجاج الجاني بأنه دخل عن طريق الخطأ أو الصدفة إلى النظام المعلوماتي المملوك للغير، وعند تفطنه لذلك حاول المغادرة إلا أنه لم يستطيع الخروج؛ نتيجة أسباب فنية يجهلها كتزويد النظام المعلوماتي بآليات تقنية وفنية تمنع خروج المتدخل إلى غاية التحقق من هويته وتحديد مكان تواجده[2].

فهناك خلاف فقهي حول كلمة "الغش – *Fraude*" والتي إستعملها المشرع الفرنسي ونظيره الجزائري، فيما إذا كان المشرع قد إكتفى بها للدلالة على القصد العام أم إستلزم إلى جانب ذلك توافر القصد الجنائي الخاص.[3] لكن هناك جانب آخر من الفقه الفرنسي من يرى أن لفظ "الغش" قد أُستعمل للدلالة على توافر القصد الجنائي الخاص، وهو مصطلح يختلف عن العمد أو القصد الإرادي بما يدل معه أن هذه الجريمة تتطلب قصد جنائي خاص.[4]

ومع ذلك يتفق جميع الشراح والباحثين في هذا المجال بأن قصد الإضرار والقصد الخاص غير متطلب هنا، وأن المقصود بالغش هنا ليس نية الإضرار فهي ليست مطلوبة ولا ضرورية، وإلاَّ يكون هناك تناقض بين الركن المادي الذي لا يتطلب نتيجة والركن المعنوي، فمفهوم الغش الذي إعتمده القانون والقضاء الفرنسي بالنسبة لهذه الجريمة هو في الحقيقة مفهوم مستعار من معنى الغش في جريمة السرقة، وقد عرفه الفقه الفرنسي[5] كما يلي:

– *«Il y a accès ou maintien frauduleux lorsque l'agent a su qu'il agissait sans droit, qu'il n'était pas autorisé ou encore qu'il agissait contre le gré du maitre du système».*

كما إعتبر القضاء الفرنسي توافر الركن المعنوي وإثبات القصد الجنائي في حق المتهم بجريمة معلوماتية كالدخول أو البقاء في النظام بغير حق، تتحقق حتى ولو قام الجاني بتلك الأفعال

---

[1]– **نسيم دردور:** جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجيستير، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2013، ص 27.

[2]– **أيمن عبد الله فكري:** جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص204.

[3]– **زيدان زيبحة:** الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص61.

[4]– **غنية باطلي:** المرجع السابق، ص167.

[5] ***VIVANT (M), AUTRES :*** *l'informatique et le droit pénal (les biens informatiques, objets d'une fraude). Lamy informatique, France 1991, P1511, N° 3443.*

بحسن نية، لأن القصد الجنائي في مثل هذا النوع من الجرائم مفترض[1]، وأن الجريمة لا تكون مؤسسة أمام القاضي الجزائي إلاَّ بإثبات عملية الدخول أو البقاء بطريق غير مشروع.[2]

ومن جانب آخر يمكن للقاضي الجزائي أن يستخلص من وقائع الدعوى أن الجاني قام عمدًا بإرتكاب هذه الجريمة وهذا من خلال القرائن والأدلة الموجودة[3] مثل "إستعمال برامج الإختراق المصطنعة أو ضبط المعطيات المعالجة والمتعلقة بالنظام بحوزة الفاعل ... وغيرها"، وعليه فإن مسألة إثبات القصد الجنائي في مثل هذه الجرائم هي مسألة تقديرية تعود سلطتها لقاضي الموضوع من أجل قيام المسؤولية الجنائية للمجرم المعلوماتي.[4]

الفرع الثاني: من حيث الصورة المشددة للجريمة

أما بخصوص الصورة المشددة للجريمة فإن المشرع يستلزم توافر القصد الجنائي الخاص لدى الجاني كَنِيَّة إرتكاب جريمة أخرى إلى جانب الجريمة الأصلية، أما إذا ترتب على جريمة الدخول أو البقاء غير المشروع نتيجة لا إرادية أي لم تتجه نية الفاعل إلى الإضرار بالمعطيات أو النظام وحدث ذلك فهنا نكون أمام نتيجة غير مقصودة، وعليه فالنتيجة هذه تدخل ضمن عناصر الركن المادي للجريمة وليس الركن المعنوي، أي أن المسؤولية عن الظرف المشدد هنا تكون عبارة عن مسؤولية مادية وموضوعية فقط، وبالتالي لا تقوم جريمة الدخول أو البقاء غير المشروع في صورتها المشددة إلا إذا حدثت هذه النتيجة عن قصد خاص.[5]

حيث يرى كثير من الفقه أن مثل هذه الآثار المترتبة عن جريمة الدخول أو البقاء غير المشروع والتي تتضمن الأضرار التي يمكن أن تلحق المعطيات بالحذف والتغيير أو تخريب نظام

---

[1] ***LARGUIER (J), CONTE (Ph) :*** *Droit pénal spécial, 13eme édition, Dalloz, Paris, France, 2005, P240.*

[2]– **عزيزة رابحي:** الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018، ص167.

[3]– أنظر في ذلك ما جاء في حيثيات قرار محكمة باريس المؤرخ في 5 أفريل 1994، بخصوص توافر سوء النية المفترض في إرتكاب الجريمة، مشار إليه عند رشيدة بوكر، المرجع السابق، ص86.

[4]– حيث أسندت محكمة باتنة في حكمها رقم 10/05272 والصادر بتاريخ 2010/06/01 على أنه "... ثبت للمحكمة من خلال أوراق القضية لاسيما فيما يتعلق بالخبرة الفنية الخاصة بتحليل البريد الإلكتروني للمتهم، وبعد تفحصه ثبت لمحكمة الموضوع أنه كان يقوم بالدخول عن طريق القرصنة والتحايل وإستخدام الغش هذا بإستعمال برامج متنوعة ... وجمع بعض المعطيات والمعلومات المعالجة آليًا والخاصة بإحدى الشركات وإستعمالها في تهديد هذه الأخيرة في مقابل حصوله على مبالغ مالية ... حيث نجد أن عملية الدخول للمنظومة المعلوماتية كانت عن طريق الغش، وهو ما يؤكد سوء نية الجاني للحصول على هذه المعطيات لإستعمالها ونشرها مقابل مبالغ مالية". (مشار إليه عند: – **يزيد بوحليط:** المرجع السابق، ص186).

[5]– **غنية باطلي:** المرجع السابق، ص171.

تشغيل المنظومة قد تكون في إعتداءات غير عمدية، ناتجة عن عدم الإحتياط أو عدم الإنتباه[1]، وعلى الجاني هنا أن يثبت إنتفاء العلاقة السببية بين السلوك الإجرامي – الدخول أو البقاء غير المشروع – والنتيجة الإجرامية المشددة، وأنا ما حدث يرجع إما لقوة قاهرة أو حادث مفاجئ خارج عن إرادته ونطاق سيطرته، فهنا تنتفي العلاقة السببية ومعها النتيجة الإجرامية المشددة وينتفي بذلك معهم القصد الجنائي الخاص.[2]

أما إذا قصد الجاني فعلاً هذه النتيجة الإجرامية وثبت ذلك من خلال الموقف النفسي للفاعل تجاه هذه الظروف المشددة، فهنا نكون أمام جريمة التلاعب في المعطيات الموجودة داخل النظام حسب ما هو منصوص عليه في المادة (394 مكرر 1) من (ق ع ج) أما بخصوص النتيجة المتعلقة بتخريب نظام المعالجة وثبت أنها هي الأخرى مقصودة فهنا نكون أمام جريمة إعاقة النظام والمنصوص عليها في المادة (323-2) من (ق ع ف)، والتي ليس لها ما يقابلها في قانون العقوبات الجزائري.[3]

[1]– **عز الدين طباش:** شرح القسم الخاص من قانون العقوبات الجزائري، الجرائم الواقعة ضد الأشخاص والاموال، دار بلقيس، الدار البيضاء، الجزائر، د.ت.ن، ص289.

[2]– **عزيزة رابحي:** المرجع السابق، ص163.

[3]– **محمد خليفة:** المرجع السابق، ص169-170.

المبحث الثاني: الإجراءات العقابية والردعية المقررة لجريمة الدخول أو البقاء غير المشروع

تمهيد وتقسيم:

لقد نصت المادة (13) من الإتفاقية الدولية للإجرام المعلوماتي بوجوب أن تكون الإجراءات العقابية والردعية المقررة نتيجة إرتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات صارمة سواء كانت عقوبات أصلية أو تكميلية[1]، كما نصت هذه الإتفاقية إلى جانب معاقبة الشخص الطبيعي على وجوب تطبيق عقوبات على الشخص المعنوي، وهذا بناءًا على مبدأ مساءلة الشخص الإعتباري الوارد ذكرها في المادة (12) من نفس الإتفاقية.[2]

وبإستقراء نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري من المادة (394 مكرر) إلى غاية المادة (394 مكرر 8) نجد أن المشرع قد تبنى جملة من الإجراءات العقابية والمقررة في تطبيقها على كل من الشخص الطبيعي والشخص المعنوي، مع مراعاة أحكام الشروع والإشتراك في هذا المجال، وذلك ما سوف نتناوله تباعًا في هذا المبحث من خلال مطلبين إثنين على التوالي:

المطلب الأول: العقوبات الأصلية والعقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع

المطلب الثاني: أحكام عقوبة الإشتراك والشروع في جريمة الدخول أو البقاء غير المشروع

[1]– **سفيان سوير:** جرائم المعلوماتية، المرجع السابق، ص98.

[2]– مبدأ مساءلة الشخص المعنوي والتي وارد ذكرها في نص المادة (12) من الاتفاقية الدولية للإجرام المعلوماتية، حيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحسابه وبواسطة أحد أعضائه أو ممثليه.

المطلب الأول: العقوبات الأصلية والعقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع

لقد إعتمد المشرع على سياسة عقابية تقوم على معيار أساسه الخطورة الإجرامية لكل جريمة على حدة، بحيث إتبع مبدأ الهرمية في تدرج سلم العقوبات، فنص على جريمة الدخول أو البقاء غير المشروع في صورتيها البسيطة والمشددة – وهذا ما سوى نعالجه في هذه الجزئية – ثم نص على جريمة الإعتداء على سلامة المعطيات الموجودة داخل أو خارج النظام بإعتبارها أشد خطورة من سابقتها – وهذا ما سوف نتطرق إليه لاحقا في الباب الثاني– وعليه سوف نقف على جملة الإجراءات العقابية المقررة لجريمة الدخول أو البقاء غير المشروع داخل النظام.

وقد نص المشرع الجزائري هنا على مجموعة من العقوبات لجريمة الدخول أو البقاء غير المشروع والماسة بالنظام المعلوماتي والمتمثلة في عقوبات أصلية (فرع أول) وأخرى عقوبات تكميلية (فرع ثاني) لكل من الشخص الطبيعي والشخص المعنوي.

الفرع الأول: العقوبات الأصلية لجريمة الدخول أو البقاء غير المشروع

هذه الجريمة لا تخلوا من وجود تدرج داخل النظام العقابي، وهذا التدرج في العقوبات كما أسلفنا ذكره يحدد الخطورة الإجرامية حتى في الجريمة الواحدة والمركبة من صورتين "البسيطة والمشددة"، إذ نجد سلم الخطورة التي قدرها المشرع لهذه التصرفات ضمن درجتين من العقوبة، سواءً من حيث الصورة البسيطة للجريمة أو من حيث الصورة المشددة لها، وهنا سوف نفرق بين عقوبة الشخص الطبيعي (أولاً) ثم يليها عقوبة الشخص المعنوي (ثانياً).

أولاً: عقوبة الشخص الطبيعي

متى توافرت أركان الجريمة على النحو السالف بيانه، فإن المشرع الجنائي يقرر عقوبات ضد الشخص الطبيعي تختلف بإختلاف الصورة والحالة التي تكون عليها جريمة الدخول أو البقاء غير المشرع داخل النظام.

أ– بالنسبة لعقوبة الصورة البسيطة: لقد أعطى المشرع الجنائي وصف الجنحة لهذه الجريمة وحدد عقوبتها بالحبس زائد الغرامة.

فمثلاً نجد المشرع الفرنسي يعاقب عليها بالحبس سنتين (2) وبغرامة قدرها 60.000 يورو.[1]

[1] أنظر الفقرة الأولى من المادة (323–1) من (ق ع ف). **الملحق رقم (03)**

أما المشرع الجزائري فعاقب عليها بالحبس من ثلاثة (3) أشهر إلى سنة (1) واحدة وبغرامة مالية من 50.000 دج إلى 200.000 دج.[1]

ب- بالنسبة لعقوبة الصورة المشددة: تضاعف العقوبة المقررة في الجريمة البسيطة إذا ترتب عن فعل الدخول أو فعل البقاء غير المشروع أيُّ حذف أو تغيير في المعطيات أو أنه وصل إلى حد تخريب نظام إشتغال المنظومة.

فتكون العقوبة حسب المشرع الفرنسي، إذا ترتب على نشاط الجاني حذف أو تغيير في المعطيات بالحبس ثلاثة (3) سنوات وبغرامة قدرها 100.000 يورو، وفي حالة ما إذا أُرتكبت الأفعال السابقة ضد نظام المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تقوم به الدولة فالعقوبة هنا تصل إلى حد خمسة (5) سنوات وغرامة قدرها 150.000 يورو.[2]

أما إذا ترتب على فعل الدخول أو فعل البقاء غير المشروع تخريب النظام أو إعاقته وإفساده، فإن المشرع الفرنسي يعاقب عليها بالحبس لمدة خمسة (5) سنوات وبغرامة قدرها 150.000 يورو، وفي حالة ما إذا أُرتكبت هذه الأفعال المشددة ضد نظام للمعالجة الآلية للمعطيات ذات الطابع الشخصي التي تقوم به الدولة فهنا تكون العقوبة الحبس سبعة (7) سنوات وغرامة قدرها 300.000يورو.[3]

أما المشرع الجزائري فموقفه غير واضح كما هو الشأن بالنسبة للمشرع الفرنسي في تحديد مقدار ضعف العقوبة، إذ ذهب إلى مضاعفة العقوبة في حالة ما إذا ترتب على ذلك حذف أو تغيير المعطيات، وهذا حسب ما جاء في الفقرة الثانية من المادة (394 مكرر)، مع أنه كان من المفروض ذكر قيمة الغرامة ومدة الحبس في حالة التشديد، فإذا سلمنا مع ذلك فإنه تصل العقوبة في حالة التشديد هنا إلى ضعف العقوبة وهي الحبس من ستة (6) أشهر إلى سنتين (2) وغرامة مالية من 100.000 دج إلى 400.000 دج لأن مضاعفة العقوبة تمس الحد الأدنى والحد الأقصى لكل من العقوبة السالبة للحرية والعقوبة المالية معًا.

---

[1]- أنظر الفقرة الأولى من المادة (394 مكرر) من (ق ع ج). **الملحق رقم (05)**

[2]- أنظر الفقرتين الثانية والثالثة من المادة (323-1) (ق ع ف). **الملحق رقم (03)**

[3]- أنظر الفقرة الأولى والثانية من نص المادة (323-2) من (ق ع ف). **الملحق رقم (03)**

أما إذا إنجر عن هذا الدخول أو البقاء تخريب نظام إشتغال المنظومة فإن العقوبة تكون الحبس من ستة (6) أشهر إلى سنتين والغرامة المالية من 50.000 دج إلى 150.000 دج، فنلاحظ أيضًا هنا أن المشرع قام بمضاعفة مدة الحبس ولم يضاعف قيمة الغرامة.

وعليه نجد أن المادة (394 مكرر) جاءت بثلاثة فقرات حسب تركيبتها الصياغية وطريقة كتابتها، ضف إلى ذلك أن المشرع أشار إلى أنه تضاعف العقوبة فقط دون أن يذكر قيمة ومقدار هذه العقوبة، بيد أنه ضاعف في الفقرة الأخيرة من عقوبة الحبس ولم يضاعف عقوبة الغرامة، وهذا ما يفتح المجال واسعًا أمام قاضي الموضوع في إستخدام سلطته التقديرية بأوسع وجه أمام أخطر الجرائم الرقمية التي يعيشها العالم اليوم.

ثانيًا: عقوبة الشخص المعنوي

في إطار مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وما تشكله من خطورة على المصالح المحمية قانوناً، وتجاوبًا مع نص المادة (12) من (إ.أ.م.إ.م)[1]، وأيضًا نص المادة (20) من (إ.ع.م.ج.ت.م) والتي جاء فيها: "تلتزم كل دولة طرف مع مراعاة قانونها الداخلي بترتيب المسؤولية الجزائية للأشخاص الإعتبارية عن الجرائم التي يرتكبها ممثلوها بإسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيًا".[2]

وذهب المشرع الفرنسي بدوره إلى تقرير عقوبة الشخص المعنوي وذلك بموجب المادة (323-6) التي تقرر المسؤولية الجزائية للشخص المعنوي وفقًا للشروط المحددة في نص المادة (121-2) من قانون العقوبات الفرنسي.[3]

وإلى جانب ذلك نجد المشرع الجزائري يقر بدوره مسؤولية الشخص المعنوي في مجال المعالجة الآلية للمعطيات، وذلك بموجب نص المادة (394 مكرر 4) بقولها: "يعاقب الشخص

---

[1] ***Article (12) : Responsabilité des personnes morales*** *« chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein… ».*

– Convention européenne de la cybercriminalité, Op. Cit, P 7.

[2]– أنظر في ذلك نص المادة (20) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات. **الملحق رقم (02)**

[3]– ***Article 323-6 : Modifié par LOI N°2009-526 du 12 mai 2009 - art. 124***

« - Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

- L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ».

المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".[1]

وتجدر الإشارة هنا إلى أن تطبيق نص المادة (394 مكرر 4) فإنها تخضع في ذلك لأحكام نص المادة (18 مكرر) من قانون العقوبات الجزائري، وهذا بإعتبار أن الجريمة موضوع الدراسة من فئة الجنح، إذ نصت هذه المادة الأخيرة على أنه: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي: الغرامة التي تساوي من مرة (1) إلى خمسة (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة...".[2]

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين سواء بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة، وهذا ما جاء في نص المادة (51 مكرر) من (ق ع ج) بقولها: "بإستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولاً جزائيًا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك، إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال".[3]

أما بخصوص صرامة المشرع في الردع فنلتمسها من خلال تشديده العقوبات الأصلية لكل من الشخص الطبيعي والشخص المعنوي، وذلك متى كانت المعلومات التي تم العدوان عليها تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، حيث أصبحت هذه الأخيرة تعتمد في تسيير شؤونها على التقنية المعلوماتية بشكل كبير، ونظرًا للخطورة البالغة التي تنجم عن الإعتداء عليها[4] وكذلك نظرًا إلى أن هذه المؤسسات والهيئات تمثل سيادة الدولة، فإن إرتكاب مثل هذه الجرائم من شأنه الإخلال بأمن وسلامة الدولة ومؤسساتها، خاصة وأن الجزائر ماشية وبخطوات سريعة وثابتة نحو تحقيق الحكومة الإلكترونية بغية عصرنة خدماتها والقضاء على مشكل التماطل في الخدمات والبيروقراطية[5]، حيث نصت هنا المادة (394 مكرر 3) من (ق ع ج)

---

[1]– راجع في ذلك نص المادة (394 مكرر 4) من (ق ع ج) الصادرة بموجب القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004.

[2]– أنظر في ذلك نص المادة (18 مكرر) من قانون العقوبات الجزائري والصادرة بالقانون رقم (06-23).

[3]– أنظر في ذلك نص المادة (51 مكرر) من (ق ع ج) والصادرة بالقانون رقم (04-15).

[4]– **رشيدة بوكر:** المرجع السابق، ص121.

[5]– **يزيد بوحليط:** المرجع السابق، ص197.

على أنه: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".[1]

والمقصود من عبارة "... دون الإخلال بتطبيق عقوبات أشد" الواردة في النص أعلاه، هو حرص المشرع الجزائري على توفير الحماية المطلقة لمؤسسة الدفاع الوطني وكل مؤسسات الدولة، مع إمكانية تكييف هذه الجريمة على أنها من جرائم الخيانة والتجسس الواردة في المواد من (61) حتى (64) من (ق ع ج)[2]، أو جرائم التعدي على الدفاع الوطني أو الإقتصاد الوطني الواردة في المواد من (65) حتى (76) من (ق ع ج)[3]، وعليه يمكن للقاضي هنا تطبيق العقوبات الأشد والمنصوص عليها قانوناً بشرط أن تكون لها علاقة بهذه الجريمة المعلوماتية.[4]

مع العلم أن المشرع الفرنسي أكد هو الآخر على صرامة تشديد العقوبات الأصلية إذا كانت الإعتداءات ضد نظام المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تنفذها الدولة[5]، وهذا حسب نص المادتين (323-3) و(323-4-1) من (ق ع ف) ولعل ما جعل المشرع الفرنسي ينتهج هذا السبيل في تشديد العقوبة هو المواجهة الشرسة لتفشي وانتشار ظاهرة الإجرام

---

[1]– أنظر نص المادة (394 مكرر 3) من (ق ع ج) الصادرة بالقانون (04-15). **الملحق رقم (05)**

[2]– أنظر في ذلك الفصل المتعلق بالجنايات والجنح ضد أمن الدولة حيث تضمن القسم الأول منه جرائم الخيانة والتجسس بموجب المواد من (61) حتى (64) من (ق ع ج) وذلك بموجب القانون رقم (06-23) المشار إليه سلفًا، حيث جاء في سياق نص المادة (63) منه ما يلي: "يكون مرتكبًا للخيانة ويعاقب بالإعدام كل جزائري يقوم:

– بتسليم معلومات أو أشياء أو مستندات أو تصميمات، يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الإقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما وبأية وسيلة كانت.

– الإستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها.

– إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معاونة دولة أجنبية أو ترك الغير يتلفها".

– مع العلم أن هذه المادة (63) من (ق ع ج) لم يطرأ عليها أي تعديل منذ أن صدرت بالأمر رقم (75-47) والمؤرخ في 17 يونيو 1975 والمعدل والمتمم لقانون العقوبات الجزائري.

[3]– أنظر في ذلك القسم الثاني من نفس الفصل أعلاه والمتعلق بجرائم التعدي على الدفاع الوطني أو الإقتصاد الوطني، وذلك بموجب المواد من (65) حتى (76) من (ق ع ج).

[4]– أنظر كل من: (– **يزيد بوحليط:** المرجع السابق، ص 198. – **زيدان زيبحة:** المرجع السابق، ص 100. – **عبد الله عبد الكريم عبد الله:** المرجع السابق، ص28).

[5]– ***Article 323-3 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 :***

«- Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

- Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

– Article 323-4-1 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 :

« Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende ».

المعلوماتي، وتعدد صور الاعتداءات على أنظمة المعالجة الآلية للبينات التابعة للهيئات والمؤسسات الاقتصادية والأمنية والتي أصبحت معظم أنشطتها وتعاملاتها اليومية ترتبط إلى حد واسع بالنظام المعلوماتي، وتقنية المعلومات.[1]

الفرع الثاني: العقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع

بالإضافة للعقوبات الأصلية تظهر جدية وصرامة المشرع كذلك من خلال وضعه عقوبات تكميلية إلى جانب العقوبات الأصلية[2]، والسبب في ذلك أن تجريم السلوك الذي يهدد نظم المعالجة الآلية في سريتها وسلامة بياناتها ليس كافيًا لمعاقبة وردع الجناة من خلال عقوبة الحبس والغرامة فقط، لأن بعض هؤلاء المجرمين حتى وإن تم توقيفهم وإدانتهم، فسوف يكون بوسعهم حيازة الأشياء التي إستخدموها في إرتكاب جرائم وأغراض أخرى، وهذا ما يُولِّد لديهم شعور أنه على الرغم من توقيع العقوبات الأصلية فسوى يظل قوام الجريمة مثمراً في مثل هذه الظروف.[3]

لذلك كان من الضروري أن يتضمن حكم الإدانة إلى جانب العقوبات الأصلية عقوبات أخرى تكميلية تتخذ بشأنها آليات وتدابير عملية للحيلولة دون إفادة المجرمين من الأشياء التي إستخدموها في تحقيق جريمتهم.

وعليه فإنه في حالة ضبط أي أجهزة إلكترونية أو أي مواد لها صلة بهذه الجريمة، فللمحكمة أن تحكم بمصادرة هذه الأشياء وإتلافها أو تعطيل أي أنظمة أو مواقع إلكترونية أُستخدمت فعلاً في الجريمة[4]، كما أن بعض التشريعات جعلت الحكم بمصادرة الأجهزة والمعدات أو النسخ المقلدة في الجرائم الإلكترونية وجوبيًا، وإلاَّ كان الحكم معيبًا مستوجبًا نقضه لشموله للخطأ في تطبيق القانون.[5]

وهذا ما أكد عليه المشرع الجزائري بموجب المادة (394 مكرر 6) من (ق ع ج) بقولها: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع الإلكترونية التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقًا لهذا القسم،

---

[1]– **بلال أمين زين الدين:** المرجع السابق، ص282.

[2]– **رشيدة بوكر:** المرجع السابق، ص122.

[3]– **عبد الوهاب مليايني:** المرجع السابق، ص230.

[4]– **يوسف خليل يوسف العفيفي:** الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة، رسالة ماجيستير، كلية الشريعة والقانون، جامعة غزة، فلسطين، 2013، ص53.

[5]– **محمد علي العريان:** المرجع السابق، ص248.

علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أُرتكبت بعلم مالكها"[1]. ويفهم من هذه المادة أن العقوبات التكميلية المقررة في هذا النوع من الجرائم تتمثل في كل من المصادرة (أولاً) والغلق (ثانياً) وهما على التوالي:

أولاً: المصادرة *La confiscation*:

وهي كل إجراء الغرض منه تمليك الدولة أشياء مضبوطة ذات صلة بالجريمة قسرًا وبدون مقابل، أو كما يقصد بها الإستلاء على مال المحكوم عليه وإنتقال ملكيته إلى الدولة بدون أي تعويض[2]، فالمصادرة بهذا المعنى هي عقوبة مالية ينطق بها كعقوبة تكميلية إلى جانب الغرامة في حكم واحد.

ويتضح من خلال عبارة "... يحكم بمصادرة ..." الواردة في المادة أعلاه أن عقوبة المصادرة وجوبية[3] متى تعلق الأمر بالأجهزة والبرامج والوسائل المستخدمة هذا من جهة، ومن جهة أخرى يفهم من عبارة "... الوسائل المستخدمة..." أن موضوع المصادرة لا يقتصر على وسيلة معينة أو محددة وإنما يتسع ذلك ليشمل أية وسيلة مستجدة مهما كان نوعها أو طبيعتها سواء كانت وسيلة معلوماتية أو تقليدية، بشرط أن تكون هذه الوسائل أُعتمدت وأُستخدمت فعلاً لإرتكاب تلك الجريمة[4]، أضف إلى ذلك أنه يجوز أن تطبق المصادرة كتدبير أمني وإحترازي بغض النظر عن طبيعة الحكم الصادر في الدعوى العمومية.[5]

ثانيًا– الغلق *La fermeture*:

إلى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية أخرى هي "عقوبة الغلق"، وهذه العقوبة وإن كانت تتفق مع المصادرة من حيث كونها إجراء قانوني وقضائي، إلاَّ أن عقوبة الغلق تبقي المنشأة أو المكان أو المحل المراد غلقه ملكًا لصاحبها حتى ولو صدر في حقه

---

[1]– راجع في ذلك نص المادة (394 مكرر 6) من (ق ع ج). **الملحق رقم (05)**

[2]– حيث عرف المشرع الجزائري "المصادرة" بموجب المادة (15) من (ق ع ج) بقوله: "المصادرة هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الإقتضاء...".

[3]– وهذا ما نصت عليه المادة (15 مكرر 1) من (ق ع ج) في فقرتها الثانية بقولها: "... وفي حالة الإدانة لإرتكاب جنحة أو مخالفة، يؤمر بمصادرة الأشياء المذكورة في الفقرة السابقة وجوبًا إذا كان القانون ينص صراحة على هذه العقوبة، وذلك مع مراعاة حقوق الغير حسن النية".

[4]– **عبد الوهاب ملياني:** المرجع السابق، ص231.

[5]– وهذا تبعًا لنص المادة (16) من (ق ع ج) بقولها: "يتعين الأمر بمصادرة الأشياء التي تشكل صناعتها أو إستعمالها أو حملها أو حيازتها أو بيعها جريمة، وكذا الأشياء التي تعد في نظر القانون أو التنظيم خطيرة أو مضرة. وفي هذه الحالة تطبق المصادرة كتدبير أمني مهما يكن الحكم الصادر في الدعوى العمومية".

غلق نهائي وليس مؤقت[1]. وكما هو ملاحظ من نص المادة (394 مكرر 6) أن المشرع الجزائري قد جعل لعقوبة الغلق محلين إثنين وهما:

أ- إغلاق المواقع *Les sites*: والتي تكون محلاً لجريمة من الجرائم الماسة بالأنظمة المعلوماتية وإن كان إستعمال المشرع عبارة "إغلاق المواقع التي تكون محلاً للجريمة..."، وهو تعبير غير سليم وهذا لأن المواقع التي تم الإعتداء عليها والتابعة للضحية هي التي كانت محلاً للجريمة، والقول بذلك يجعل هذا الموقع عرضة للغلق وهو قول غير صحيح، لذلك كان أولى بالمشرع أن يستعمل مثلاً عبارة: "إغلاق المواقع التي تستعمل في إرتكاب الجريمة".[2]

ب- إغلاق المحل أو مكان الإستغلال *Lieux d'exploitation*: وهو أي محل أو مكان إستعمله الجناة في إرتكاب جريمتهم، وكان بداخله الوسائل الإلكترونية التي أُستعملت في إتيان الجريمة المعلوماتية كما هو الحال بالنسبة لمقهى الأنترنت *Cyber café* الذي ترتكب فيه مثل هذه الجرائم أو يتم التعامل معها بواسطة هذه الوسائل الموجودة داخل هذا المحل[3]، بشرط توافر عنصر العلم لدى مالكه.

وفي كل الأحوال فإن عقوبة المصادرة أو الغلق يجب ألاّ تخل بحقوق الغير حسن النية، حيث أن هذه المادة إستثنت هذا الأخير بحفظ حقوقه، وأن إحترام المشرع للغير حسن النية يأتي منسجمًا مع مبدأ الشرعية العقابية وشخصية العقوبة[4]، وهو ذلك الشخص الذي يجهل حقيقة العلاقة بين ملكه الذي له حق عليه والجريمة المرتكبة[5]، حيث عرفته المادة (15 مكرر 2) من (ق ع ج) بقولها: "يعتبر من الغير حسن النية، الأشخاص الذين لم يكونوا شخصيًا محل متابعة أو إدانة من أجل الوقائع التي أدت إلى المصادرة، ولديهم سند ملكية أو حيازة صحيح ومشروع على الأشياء القابلة للمصادرة".[6]

---

[1]- وهنا ذكرت المادة (16 مكرر 1) من (ق ع ج) أنه: "يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي أُرتكبت الجريمة بمناسبته، ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر (10) سنوات في حالة الإدانة لإرتكاب جناية، وخمس (5) سنوات في حالة الإدانة لإرتكاب جنحة".

[2]- **عبد الوهاب مليايني:** المرجع السابق، ص232.

[3]- **محمد خليفة:** المرجع السابق، ص123. - سفيان سوير: المرجع السابق، ص99.

[4]- وهذا ما كرسته المادة (167) من الدستور الجزائري لعام (2020) بقولها: "تخضع العقوبات الجزائية لمبدأي الشرعية والشخصية".

[5]- **باسم شهاب:** مبادئ القسم العام لقانون العقوبات وفقًا لأحدث التعديلات بالقانون رقم 23 لسنة 2006، دار المطبوعات الجامعية، وهران، الجزائر، 2007، ص279.

[6] أنظر في ذلك نص المادة (15 مكرر 2) من (ق ع ج).

كما تجدر الإشارة هنا أن المشرع الجزائري قد أقر إلى جانب العقوبات التكميلية المطبقة على الشخص المعنوي أن قرر له عقوبات أخرى وذلك ما جاء في الفقرة الثانية من نص المادة (18 مكرر) من (ق ع ج) بقولها: "... واحدة أو أكثر من العقوبات التكميلية التالية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس(5) سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر، نهائيًا أو لمدة لا تتجاوز خمس (5) سنوات.
- مصادرة الشيء الذي أُستعمل في إرتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي أُرتكبت الجريمة بمناسبته".[1]

أما عن المشرع الفرنسي بدوره قد نص على العقوبات التكميلية والمتمثلة في المصادرة والغلق وذلك بموجب الفقرتين الثالثة والرابعة من نص المادة (323-5) من (ق ع ف)[2]، بل أن المشرع الفرنسي وفضلاً عن عقوبة المصادرة والغلق راح ونص على غيرها من العقوبات التكميلية الوجوبية الأخرى، وهذا سعيًا منه لتحقيق مبدأ تفريد العقوبة[3]، حيث نص على عدة

---

[1]– راجع في ذلك نص المادة (18 مكرر) من (ق ع ج).

[2]– **Article 323-5 :** « *Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :*
- L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
- L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
- La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
- La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
- L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
- L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 ».

[3]– **مبدأ تفريد العقوبة:** يقصد به تحديد مقدار العقوبة الواجب فرضها على الجاني بمقابل الجرم الذي إقترفه، وهذا المبدأ يعتمده أحياناً المشرع في وضع عقوبات للسلوك الجرمي في نفس نص المادة الواحدة، لذا نجد العقوبات التكميلية لجرائم الإعتداء على نظم المعالجة الآلية للمعطيات في القانون الفرنسي لم تكن تقرر إلاَّ عقوبة تكميلية واحدة وهي عقوبة المصادرة بموجب المادة (462-9) الصادرة بقانون 1988، ثم أقر بعد ذلك عقوبة الغلق من خلال تعديله لقانون العقوبات سنة 1994 ثم 2004 بموجب المادة (323-5) التي جاءت بقائمة للعقوبات التكميلية المطبقة على المجرم المعلوماتي.

عقوبات تكميلية بموجب المادة نفسها، وهذا من شأنه أن يضع خيارات عديدة أمام القاضي الجزائي تمكنه من إختيار ما يتناسب منها والقضية المعروضة أمامه وفق سلطته التقديرية.

لذا كان بإمكان المشرع الجزائري أن ينتهج نفس المبدأ ويضيف عقوبات تكميلية أخرى، بدل من تضييق نطاقها وحصرها في المصادرة والغلق فقط، لأن هذا لا يحقق فكرة الردع بنوعيه – العام والخاص– ناهيك عن إختلاف واقع الجريمة المعلوماتية وتنوعها وتفاوت مستويات السلوك الإنساني في إرتكابها.

المطلب الثاني: أحكام عقوبة الإشتراك والشروع في جريمة الدخول أو البقاء غير المشروع

أمام سهولة وسرعة الإتصال بين الأفراد في ظل تطوير وسائل الإتصال التي بات العالم فيها قرية صغيرة وما ترتب عليها من عولمة الجريمة، أصبح هناك تخوف كبير من إنتشار الشبكة الإجرامية وإتساع دائرتها، والحقيقة أن مجرمي المعلوماتية وجدوا ضالتهم في تنسيق جهودهم وربط نواياهم لإرتكاب الجرائم المعلوماتية عبر أماكن مختلفة من العالم[1]، وفي مواجهة ذلك لم يقصر المشرع الجنائي في مجابهة هاته الجماعات والشبكات الإجرامية.

وفي خضم ذلك نصت المادة (11) من الإتفاقية الدولية للإجرام المعلوماتي على تجريم التحضير للجرائم الماسة بالأنظمة المعلوماتية، وهذا من خلال وضع عقوبات على كل أشكال الإتفاق الجنائي المجسد في الأعمال التحضرية والمادية، وكذا العقاب على الشروع في هذا النوع من الجرائم.[2]

وقد تبنى كل من المشرع الجزائري ونظيره الفرنسي نطاق هذا التجريم[3]، وذلك طبقًا للمواد (394 مكرر 5) و(394 مكرر 7) من (ق ع ج) وكذا المواد (323-4) و(323-7) من (ق ع ف) والتي جميعها تعاقب على المشاركة (فرع أول) أو الشروع (فرع ثاني) في إرتكاب أحد الأفعال المنصوص عليها في هذا المجال، وفيما يلي سنتطرق إلى هذه الأحكام المشتركة:

---

[1]– **زيدان زيبحة:** المرجع السابق، ص104.

[2]– **غنية باطلي:** المرجع السابق، ص195.

[3]– ويبدوا هنا أن المشرع الجزائري سار على درب التشريعات العالمية وأقتفى أثرها بل أنه عمل على تجسيد إلتزاماته الدولية من خلال المصادقة على الإتفاقيات الدولية والإقليمية التي تم إرساؤها في مجال مجابهة الجرائم المعلوماتية والتي من أهمها: الإتفاقية الدولية حول الإجرام المعلوماتي والمبرمة بمدينة بودابست في 23-11-2001 والتي خلصت من بين ما تم الاتفاق عليه إلى تجريم "الإتفاق الجنائي" وإيلاء الصرامة اللازمة في معاقبته.

الفرع الأول: عقوبة الإشتراك في الجريمة (الإتفاق الجنائي)

هناك من يرى أن الإتفاق الجنائي هو بمثابة جريمة خاصة ومستقلة بذاتها وليست مجرد ظرف إجرامي، ودليل ذلك أن الإتفاق الجنائي ظاهرة إجرامية خطيرة تهدد المجتمع تهديدًا فعليًا، لذا نجد القانون يؤكد في العقاب على الإتفاق بغيت تجسيد صرامة الجزاء على مجرد تكوين الإتفاق الجنائي من جهة، ومن جهة أخرى الوقاية منه نتيجة إحباط كل محاولات الإتفاق الجنائي والحيلولة دون تحقيق الجناة لمخططاتهم الإجرامية.[1]

والحكمة التي إرتآها المشرع من تجريم الإشتراك أو الإتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية يتمثل في كون أن مثل هذه الجرائم تتم عادة في إطار إشتراك جماعي[2]، لذا نجد أن العقاب يطال كل من يشارك في مجموعة أو في إتفاق الغرض منه التحضير أو الإعداد لإرتكاب مثل هذه الجرائم المعلوماتية المنصوص عليها قانونًا.[3] ومما يستخلص أيضًا أن المشرع حرص على أن مجرد المشاركة في عمل إجرامي أو الإتفاق عليه والمجسد بفعل مادي يوحي بالتحضير للجريمة سوف يعاقب عليه القانون بنفس العقوبة المقررة لذات الجريمة، وذلك تحسبًا لسهولة الإتفاق وسرعته في تنفيذ الجريمة من قبل المجرمين، حتى وإن لم تكن بينهم معرفة مسبقة أو إتصال مباشر، وعليه فإن مبرر العقاب هنا يتطلب على الأقل البدء في نشاط إجرامي يؤدي مباشرة إلى إرتكاب الجريمة، أما الأعمال التحضيرية التي تسبق البدء في تنفيذها فلا يعاقب عليها كقاعدة عامة إلاَّ في حالة وجود نص خاص.[4]

أما في مجال الإجرام المعلوماتي نجد أن المشرع أراد توسيع نطاق العقوبة فأخضع الأعمال التحضيرية لنفس العقوبة المقررة للجريمة التي تم التحضير لها إذا تمت في إطار إتفاق جنائي، أما عن الأعمال التحضيرية المرتكبة من طرف شخص منفرد فهي غير مشمولة بهذا النص.[5]

ونجد أن كل من المشرع الجزائري ونظريه الفرنسي لم يقم بتجريم مجرد العزم على الإتفاق في إرتكاب هذه الجرائم، إنما تطلب أن يكون هذا العزم مجسدًا في أفعال مادية، أي الإنتقال

---

[1]– **غنية باطلي:** المرجع السابق، ص196. – **محمد خليفة:** المرجع السابق، ص112.

[2]– **سفيان سوير:** المرجع السابق، ص101.

[3]– **زيدان زيبحة:** المرجع السابق، ص105.

[4]– **أمال قارة:** المرجع السابق، ص66.

[5]– **سفيان سوير:** المرجع نفسه، ص101.

من المرحلة النفسية إلى المرحلة المادية وهي مرحلة الأعمال التحضيرية المنجرة وراء الإتفاق، وعليه فقد أراد كلاً من المشرعين الجزائري والفرنسي عدم التوسع في تجريم الإتفاق في مادة الجنح بإستثناء الجنايات[1]، ومنه رفع سقف التجريم إلى الأعمال التحضيرية بدل من تجريم مجرد العزم على الإتفاق.[2]

ولقد نص المشرع الجزائري على عقوبة الإشتراك والإتفاق الجنائي وذلك بنـــص المادة (394 مكرر 5) من (ق ع ج) بقولها: "كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

ومن خلال إستقراءنا لنص المادة أعلاه نجد أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك حيث رصد لها نفس عقوبة الجريمة التامة[3]، ذلك أن جرائم الإعتداء على نظم المعالجة الآلية للمعطيات، أغلبها تتم في شكل جماعات، حتى وإن لم يسبق ذلك إتفاق بين هاته المجموعة على إرتكاب هذه الجريمة، ولكن النتيجة الجرمية تبين وجود إتفاق ضمني بين أفراد المجموعة، إذ أن مثل هذه الجرائم لا تتطلب إجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الإتفاق الجنائي بمجرد إنتقال مثلاً كلمة السر أو معلومة مخزنة من شخص إلى آخر وإن لم يكن بينهما معرفة سابقة، كما أنه يستوي في ذلك أن يكون أفراد الإشتراك مجموعة من الأشخاص الطبيعية أو المعنوية.[4]

ويقابل هذا النص، نص المادة (323-4) من (ق ع ف) والتي تعاقب هي الأخرى على هذا النشاط الإجرامي بعقوبة الجريمة التي تم التحضير لها[5]، فإذا ساهم أعضاء الإتفاق في الجريمة التي

---

[1]– أنظر في ذلك المواد من (176) حتى (179) من (ق ع ج) فيما يتعلق بالإتفاق الجنائي في تكوين جمعية الأشرار.

[2]– **غنية باطلي:** المرجع السابق، ص197.

[3]– حيث نصت المادة (42) من (ق ع ج) أنه: "يعتبر شريكًا في الجريمة من لم يشترك إشتراكًا مباشرًا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك".

– كما نصت المادة (44) من (ق ع ج) على أنه: "يعاقب الشريك في جناية أو جنحة بالعـقوبة المقـررة للجنايـة أو الجنحـة ..." قانـون رقـم (82-04) مؤرخ في 13 فبراير 1982 المعدل والمتمم لقانون العقوبات الجزائري.

[4]– **خثير مسعود:** المرجع السابق، ص129.

[5]– ***Article 323-4 : Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004 :***

- « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

تم التحضير لها فنكون أمام تعدد مادي للجرائم، لأن الجريمة الأولى مستقلة عن الجريمة الثانية، أما إذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.[1]

ومما يجب ملاحظته هنا هو أن المادة (394 مكرر 5) من (ق ع ج) وكذا المادة (323-4) من (ق ع ف) تؤكدان على أن قوام جريمة الإتفاق الجنائي في هذه الجرائم يستدعي توافر ركنين مادي ومعنوي، أما عن الركن المادي فإنه يقوم على نشاط الإتفاق ذاته، وهو إنعقاد إرادتين أو أكثر وإجتماعها على موضوع معين مما يجعل لهذا الإتفاق طبيعة مادية ملموسة[2] مضمونها الإجتماع بهدف التحضير لإرتكاب الجريمة.

كما يلاحظ حرص المشرع على وجوب توافر شروط معينة منها ما يتعلق بفعل المشاركة بعد حصول الإتفاق أو الإجتماع أي تشكيل فريق أو مجموعة وهو ما يطلق عليه بالتعدد الضروري للجناة فيتخذ شكل "الجمعية الإجرامية" مع تحديد دور كل واحد منهم، بحيث يستشف من عبارة نص المادة (176) من (ق ع ج) بقولها: "كل جمعية أو إتفاق مهما كانت مدته وعدد أعضائه ..."[3] أي أن الإتفاق يتطلب الحد الأدنى للجناة وهو إثنان ولم يحدد الحد الأقصى[4]، ويستوي في ذلك أن يكون أعضاء الإتفاق في صورة شخص طبيعي أو شخص معنوي[5] كالشركة أو المؤسسة، وسواء كانوا يعرفون بعضهم البعض أو لا، المهم أنهم إتفقوا على القيام بالنشاط الإجرامي المشار إليه.[6]

ومن جهة أخرى وإستناداً لنفس المادة، فإنه يشترط أن يكون هذا الإتفاق موجه نحو هدف محدد وهو التحضير لإرتكاب جريمة من جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات والمنصوص عليها في هذا القسم. أي قسر الأمر فقط على جعل موضوع الإتفاق الجنائي هو الإعداد الفعلي لتلك الجرائم والتحضير لها، لأنه لم ينص المشرع على الإتفاق على إرتكابها، فيكفي أن يجسد التحضير للجريمة فعل مادي أو عدة أفعال تستهدف مثلاً سرقة البيانات أو تعطيل شبكة

---

[1]- أنظر في ذلك الفصل الثالث من قانون العقوبات الجزائري فيما يتعلق بتعدد الجرائم بموجب المواد من (32) إلى (38) منه.

[2]- **غنية باطلي:** المرجع السابق، ص198.

[3]- حيث جاء النص الكامل للمادة (176) من (ق ع ج) على أنه: "كل جمعية أو إتفاق مهما كانت مدته وعدد أعضائه تشكل أو تألف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس (5) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

[4]- هناك من القوانين من يتطلب الحد الأدنى في ثلاثة أشخاص كالقانون الإيطالي مثلاً والذي يشدد العقوبة إلى أقصاها إذا بلغ العدد عشرة أشخاص فأكثر، بشرط عدم توافر موانع المسؤولية الجنائية بين الجناة كصغر السن لأن هذا يحول دون قيام الإتفاق ويبقى الشخص البالغ معاقب وحده على الإتفاق. (أنظر أكثر كل من: - **غنية باطلي:** المرجع السابق، ص201. - **محمد خليفة:** المرجع السابق، ص116).

[5]- أنظر في ذلك نص المادة (177 مكرر 1) من (ق ع ج) الصادرة بالقانون رقم (04-15) السالف الذكر.

[6]- **أمال قارة:** المرجع السابق، ص68.

الإنترنت أو عرقلة سير المعلومات داخل النظام أو بث الفيروسات[1]، إذًا فبمجرد الإتفاق والمشاركة المقرونة بالتحضير المجسد بأفعال مادية يشكل الجريمة المعلوماتية.[2]

وإن كان بعض الفقه يرى أنه من الصعب تصور الإتفاق الجنائي في الجرائم المعلوماتية، وهذا لأن الأفعال المادية قد تختلط مع الأفعال المرتكبة في مرحلة البدء في التنفيذ، ويذهبون إلى أبعد من ذلك في القول أنه يجب التمييز هنا بين الركن المادي لجريمة الإتفاق والركن المادي للجريمة المتفق على إرتكابها، لأن الأولى تستكمل عناصرها بتوافر الإرادات حتى ولو لم تنفذ الجريمة المتفق عليها، وأن عدولهم عنها لا يحول دون العقاب على جريمة الإتفاق الجنائي لأن العدول لا يمس بالركن المادي الذي توافرت عناصره[3]، أما الثانية فإنها تقوم على مرحلة البدء في التنفيذ كمرحلة فاصلة بين الأعمال التحضيرية غير المعاقب عليها والشروع المعاقب عليه[4]، وقد يبدو حسب هذا الإتجاه الفرق واضحًا في بعض الجرائم وفي بعض الحالات.

أما بخصوص الركن المعنوي في الإتفاق الجنائي يفترض فيه توافر القصد الجنائي لدى أعضاء الجماعة، أي يجب توافر عنصر العلم لدى كل عضو من أعضائها بماهية هذا الإتفاق[5]، أما من كان يجهل الغرض من هذا الإتفاق ولا يعلم أن الأعمال التحضيرية تعد مسبقًا لإرتكاب الجريمة، فهنا لا يعد القصد الجنائي متوافرًا لديه، ومثالها من ينظم إلى جماعة على أساس الإتفاق معتقدًا منه أنها تتاجر في تقليد أو تصميم برامج الحاسوب، ثم يتبين له أنهم يتاجرون ببرامج خبيثة أو برامج إختراق، فهنا العلم غير متوفر في حقه.[6]

إضافةً إلى عنصر العلم يجب أن تتجه إرادة كل عضو من أعضاء الإتفاق إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري، ولا يشترط أن يكون كل واحد منهم عالمًا بنشاط الآخر، على أن تكون هذه الإرادة جادة، وليس كالذي ينخرط في المجموعة بناءً على إتفاق من أجل الكشف

---

[1]– **زيدان زيبحة:** المرجع السابق، ص105.

[2]– فحسب نص المادة (394 مكرر 5) من (ق ع ج) إذا كان موضوع الإتفاق مجرد أعمال تحضيرية والإعداد لتلك الجرائم فإن الإتفاق هنا يكسب صفته الجنائية ولو كانت الأعمال في ذاتها مشروعة، ومثال ذلك الإتفاق على تصميم المعطيات فهو مشروع في الأصل، لكنه يصبح غير مشروع إذا كان الإتفاق على تصميم ذلك بغية إستعماله في الجرائم المنصوص عليها في كل من التشريعين الجزائـــري والفرنســـي. (أنظر في ذلك كل من: (– **سفيان سوير:** المرجع السابق، ص102. – **غنية باطلي:** المرجع السابق، ص200).

[3]– **عبد القادر القهوجي:** المرجع السابق، ص129.

[4]– **عبد الرحمن خليفي:** القانون الجنائي العام، المرجع السابق، ص263–264.

[5]– **سفيان سوير:** المرجع نفسه، ص102.

[6]– **غنية باطلي:** المرجع نفسه، ص201.

للسلطات عن حقيقة هذه المجموعة الإجرامية، بشرط أن يكون ذلك قبل الشروع في إرتكاب الجريمة وقبل البدء في التحقيق فيها[1]، فهنا لا يعد قاصدًا جنائيًا، كما أن إنتقاء الإرادة عند أحد الشخصين المكونين للإتفاق ينفي الجريمة عن كليهما.[2]

الفرع الثاني: عقوبة الشروع في الجريمة (المحاولة الجنائية)

إضافة إلى العقاب على الإتفاق الجنائي في هذه الجرائم، فقد نص المشرع على عقوبة الشروع في الجريمة، حيث تعد النتيجة الحاصلة من الفعل المجرم ضرورية لإكتمال بنيان الجريمة، ورغم ذلك قد يكون مجرد السلوك كافيًا أحيانًا ليكون هناك محاولة تستوجب المتابعة والعقاب رغم عدم إنتهاء الجاني إلى مراده من الجريمة.[3]

والعلة من العقاب على الشروع هي أن قانون العقوبات حين يحمي المصالح الإجتماعية لا يقف عند حمايتها من الأضرار فقط، وإنما يشملها أيضًا بالحماية ضد أي خطر يصيبها ويهددها، فإنه لم يقصر دائرة التجريم على العدوان الكامل بالجريمة التامة، بل شمل أيضًا العدوان الناقص على هذه المصلحة بالشروع في الجريمة، فصورة الخطر المترتبة على الشروع هي العلة الأساسية أو السبب الرئيسي للتجريم.[4]

فقد يحدث في بعض الأحيان بالنسبة للجرائم ذات النتيجة التي يتطلب المشرع لتمام ركنها المادي سلوك ونتيجة وعلاقة سببية، وأحياناً يبدأ الجاني في إرتكاب السلوك الإجرامي كاملاً ثم بعدها يتدخل ظرف خارج عن إرادته يحول بينه وبين إتمامه السلوك فلا تتحقق النتيجة، وقد يصل الجاني بالسلوك الإجرامي إلى نهايته ولكن لسبب خارج عن إرادته لا تتحقق النتيجة الإجرامية أيضًا، ففي هذه الأحوال السابقة لا ينسب إلى الجاني إرتكاب جريمة تامة لعدم تحقق النتيجة الإجرامية، وإنما الذي ينسب إليه هو إرتكاب جريمة ناقصة، وتسمى هذه الحالة بالشروع أو المحاولة في إرتكاب الجريمة.[5]

---

[1]– حيث جاء في نص المادة (179) من (ق ع ج) أنه: "يستفيد من العذر المعفي وفقًا للشروط المقررة في المادة (52) من نفس القانون أنـــه: "من يقوم من الجناة بالكشف للسلطات عن الإتفاق الذي تم أو عن وجود الجمعية وذلك قبل أي شروع في الجناية موضوع الجمعية أو الإتفاق وقبل البدء في التحقيق".

[2]– **محمد خليفة:** المرجع السابق، ص117.

[3]– **فرج القصير:** شرح القانون الجنائي العام، مركز النشر الجامعي، تونس، 2006، ص99.

[4]– **عبد الله سليمان:** شرح قانون العقوبات، القسم العام، دار الهدى، عين مليلة، الجزائر، د.ت.ن، ص198.

[5]– **عبد الرحمن خليفي:** القانون الجنائي العام، المرجع السابق، ص262.

مع الإشارة هنا أن المشرع الجزائري لا يجرم كل محاولة لإرتكاب الجريمة بل يجعل ذلك نسبيًا لا يتعدى إلى كل الجرائم، وبالرجوع إلى القواعد العامة للقانون الجنائي نجد أن مسألة الشروع في الجنايات هو الأصل نظرًا لخطورتها، بينما هذا الأمر لا يكون في الجنح إلاَّ في الخطيرة منها وبموجب نص خاص وصريح. ولأن المشرع رأى في جرائم المساس بأنظمة المعالجة الآلية للمعطيات خطورة كبيرة مع العلم أن هذه الجرائم من فئة الجنح، لذا قرر إخضاعها لنظام الشروع بعدما نص عليها بنص خاص، وذلك رغبة منه في توفير حماية أكبر وفعالة لهذا النظام.

وفي تعريف الشروع وبيان مجال تطبيقه نص المشرع الجزائري تحت عنوان "المحاولة" في نص المادة (30) من (ق ع ج) أنه: "كل المحاولات لإرتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى إرتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلاَّ نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"[1]، وجاء في نص المادة (31) من (ق ع ج) ما نصه: "المحاولة في الجنحة لا يعاقب عليها إلاَّ بناءً على نص صريح في القانون، والمحاولة في المخالفة لا يعاقب عليها إطلاقًا".

من هذا يُفهم أن الشروع في الجريمة يراد به أن الجاني يفشل في تحقيق جريمته فلا تتحقق لديه النتيجة المادية المقصودة، رغم أنه بدأ فعلاً في تنفيذ جريمته بما ينطوي سلوكه من تهديد للمصالح المحمية قانوناً، وإستنفذ في ذلك كل الفعل أو جزء منه ومع ذلك لا تتحقق النتيجة الإجرامية. لهذا يطلق الفقه على الشروع عبارة "الجريمة الناقصة"، وهذا النقصان لا يعتري الركن المعنوي فيها لأن القصد الجنائي ثابت فيها، بينما يمس الركن المادي لأن الفاعل يقوم بأفعال تعتبر بدءًا في التنفيذ لكنه لا يتوصل إلى النتيجة لأسباب خارجة عن إرادته.[2]

ولم يخرج المشرع الجزائري من نظام العقاب الذي رسمته الإتفاقيات الدولية كما أشرنا لها سلفاً، وإستقرت عليه القوانين الداخلية بما فيها التشريع الجزائري ونظيره الفرنسي، فقد نصت المادة (394 مكرر 7) من (ق ع ج) على أنه: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، وتقابل هذه المادة في القانون الجنائي الفرنسي المادة

[1]– والتي تقابلها نص المادة (97) من قانون العقوبات الفرنسي.

[2]– سليمان عبد المنعم: النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، مصر، 2014، ص498.

(323-7)[1]، ولولا هذا النص الصريح لما أمكن العقاب على الشروع في إرتكاب جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات.

وعليه ومن خلال إستقرائنا لنص المادة المذكورة أعلاه نستنتج أن نطاق المتابعة الجزائية لم يتوقف عند ردع الفعل التام فقط، بل تعداه إلى المحاولة في إرتكاب الجنح المعلوماتية والتي أصبحت مشمولة بالنص الصريح المعاقب على الشروع فيها، وهذا رغبة من المشرع في تغطية أكبر قدر ممكن منها بالحماية.

ولأن المشرع قد جرَّم الإتفاق الجنائي المجسد في أعمال تحضيرية بصفتها مرحلة من مراحل الجريمة تسبق الشروع، فكان لزامًا عليه ومن باب أولى أن يجرم الشروع لأنه مرحلة لاحقة ووسط.[2]

ورغم إستحسان هذا التجريم بالنسبة للجنح السابقة في الذكر بموجب نص خاص، فإن مسألة تطبيق الشروع في بعضها يتنافى والقواعد العامة، وذلك كون أن معظمها تعتبر جرائم شكلية مما لا يتصور فيها الشروع[3]، لذا يرى بعض الفقه وبعض التشريعات المقارنة أن هناك جرائم معلوماتية كفعل الدخول أو فعل البقاء غير المشروع داخل النظام، بأنها جرائم شكلية تتحقق بمجرد وقوع النشاط المادي دونما حاجة لتحقق نتيجة إجرامية معينة، وبالتالي لا يكون هناك مجال للحديث عن فكرة الشروع، فلا يعد مثلاً مجرد حيازة كلمة السرّ أو الكود من قبل مَنْ ليس له الحق فيها شُرُوعًا في هذه الجريمة.[4]

رأينا الخاص:

أنه وخلافًا للقواعد العامة التي لا تقرر العقاب إلاَّ في الجرائم التامة، أو تلك التي تقف عند حد الشروع أو المحاولة، بمعنى أن مبدأ العقاب يتطلب على الأقل مرحلة البدء في إتيان نشاط إجرامي يؤدي لا محالة إلى الإرتكاب الجريمة. أما الأعمال التحضيرية التي سبق البدء في تنفيذها فلا يعاقب عليها القانون كقاعدة عامة إلا في حالة وجود نص خاص.

---

[1]– ***Article 323-7 : Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004 :*** *« La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines ».*

[2]– **سفيان سوير:** المرجع السابق، ص103.

[3]– **غنية باطلي:** المرجع السابق، ص204.

[4]– **عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن إستخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس القاهرة، مصر، 2004، ص337.

وعليه فإن المادة (394 مكرر 5) من (ق ع ج) والمادة (323-4) من (ق ع ف) تغيران من هذه القاعدة العامة، وتضعان إستثناء بموجب نص خاص، حيث إستوجب تمديد ميدان المتابعة الجزائية إلى المرحلة المادية التي تتوسط العزم والبدء في التنفيذ وقرر كل منهما عقوبة الإتفاق الجنائي والأعمال التحضيرية بالعقوبة المقررة للجريمة ذاتها المعد لإرتكابها والتحضير لها.

والغرض من ذلك هو وضع نوع من الحماية المتقدمة والوقائية لنظم المعالجة الآلية للمعطيات ضد المخاطر التي تهدد بإرتكاب الجرائم المشار إليها في هذا القسم، وكذلك حتى لا يفلت أي مجرم معلوماتي من العقاب.

ويبقى لنا هنا أن نشير أنه وعلاوةً على العقوبات السابق الإشارة إليها، فإن مسألة التفرقة بين الأعمال التحضيرية والبدء في التنفيذ – المحاولة – تبقى مسألة جد صعبة في هذا النوع من الجرائم خصوصًا مع محاولات الدخول عن بعد والتي تحدث يوميًا في كل ساعة وفي كل دقيقة، وهذا ما أدى بالمشرع إلى تبني مبدأ المعاقبة على الإتفاق الجنائي بهدف كشف كل ما من شأنه التحضير لإرتكاب مثل هذه الجرائم.

وفي الأخير يمكننا القول أن السياسة العقابية التي إنتهجها المشرع لمواجهة مثل هذه الجرائم، سواء كانت هذه العقوبات مقررة للشخص الطبيعي أو المعنوي، فإنها حققت قفزة نوعية في مجال التجريم المعلوماتي تستحق التشجيع، لأن الخطورة الإجرامية التي تنبأ بها هذه الظاهرة تتعدى في جسامتها بعض أشكال الإجرام التقليدي خاصة وأنها تستهدف مجالات حساسة للغاية كالشركات المالية والتجارية ومؤسسات الدولة.

ونظرًا لوعي المشرع بخطورة المساس بنظم المعالجة الآلية التي تقوم عليها جميع التعاملات الإلكترونية، وما يترتب عن ذلك من تهديد جدي للمصالح المرتبطة بها، أورد المشرع الجنائي في كل من الجزائر وفرنسا نظام حماية جزائي يتميز بأنه واسع من حيث نطاق المتابعة وصارم من حيث العقوبات.

ومع ذلك تبقى ناقصة من جهة لأنها لم تتناول بعض أشكال الجرائم المعلوماتية المستجدة ذات المفهوم الواسع والدقيق كجريمة الإعتداء والمساس بالملعومات الموجودة داخل وخارج النظام المعلوماتي، وهذا ما سوف نسعى جاهدين إلى معرفته بالبحث والدراسة في الباب الثاني من هذه الرسالة إنشاء الله.

البَاب الثّانِي

جرائم المساس بالمعطيات المعالجة آليًا والموجودة داخل وخارج النظام المعلوماتي

البَاب الثّانِي: جرائم المساس بالمعطيات المعالجة آليًا والموجودة داخل وخارج النظام المعلوماتي

تمهيد وتقسيم:

لقد إضطر المشرع الجزائري في ظل وجود فراغ تشريعي في مجال مكافحة الإجرام المعلوماتي إلى سن تشريعات حديثة وإضافة مقتضايات جديدة لمجموعة الجرائم الموجودة في قانون العقوبات، والتي تتلاءم ولو نسبيًا مع خصوصية هذا النوع من الجرائم، والتي يطلق عليها المشرع الجزائري "بجرائم المساس بأنظمة المعالجة الآلية للمعطيات"، أو كما يسميها الفقه "بجرائم الإعتداء على المعلومات" والتي قد تكون موجودة داخل النظام نفسه أو موجودة خارجه.

وحتى نعالج بشكل شمولي التجربة الجزائرية في هذا المجال، إرتأينا أن نقسم هذا الباب إلى فصلين إثنين على النحو التالي:

الفصل الأول: جريمة التلاعب بالمعلومات الموجودة داخل النظام المعلوماتي.

الفصل الثاني: جريمة التعامل غير المشروع في المعلومات الموجودة خارج النظام المعلوماتي.

الفَصل الأَوّل

جريمة التلاعب بالمعلومات
الموجودة داخل النظام المعلوماتي

الفصل الأول: جريمة التلاعب بالمعلومات الموجودة داخل النظام المعلوماتي

تمهيد وتقسيم:

بإزدياد أهمية المعلومات المعالجة آليًا داخل النظم والشبكات المعلوماتية، وأمام إنتشار التقدم التكنولوجي وتنوعه في مجال التعاملات الإلكترونية، إزدادت معه خطورة الإعتداءات التي تهدد هذه المعلومات والتعاملات الإلكترونية.

ولمواجهة ذلك عمدت معظم التشريعات الجنائية الحديثة إلى حماية سلامة وتكامل هذه المعطيات والمعلومات، فجرمت كل أنواع التلاعب والعبث المعلوماتي غير المشروع، وكذا كل صور الإتلاف المعلوماتي من تزوير وإحتيال التي من شأنها الإضرار بالمعلومات الموجودة داخل النظام.

ولنبحث أكثر في غمار هذه الجريمة سوف نقسم هذا الفصل إلى مبحثين إثنين على التوالي:

المبحث الأول: مفهوم جريمة التلاعب المعلوماتي.

المبحث الثاني: أركان جريمة التلاعب المعلوماتي والعقوبات المقررة لها.

المبحث الأول: مفهوم جريمة التلاعب المعلوماتي

تمهيد وتقسيم:

إضافة إلى الجرائم المعلوماتية التي تقع بإستخدام النظام المعلوماتي بوجه عام، هناك نوع آخر من الجرائم المعلوماتية تستهدف النظام المعلوماتي في حد ذاته، وهذا من خلال المساس بمكوناته المنطقية والمعنوية المدرجة والمخزنة بداخله، وهو ما يطلق عليه بجريمة التلاعب المعلوماتي.

ولمفهوم أكثر لهذا النوع من الجرائم سوف نأتي في هذا المبحث على تبيان أكثر لتعريفها وذكر بعض خصائصها، وثم تحديد الطبيعة القانونية لها، وهذا وفق مطلبين إثنين فيما يلي:

المطلب الأول: تعريف جريمة التلاعب المعلوماتي وأهم خصائصها

المطلب الثاني: الطبيعة القانونية لجريمة التلاعب المعلوماتي

المطلب الأول: تعريف جريمة التلاعب المعلوماتي وأهم خصائصها

وهذا المطلب بدوره سوف يعالج تعريف جريمة التلاعب المعلوماتي (فرع أول) ثم نعرج بعد ذلك إلى الحديث عن أهم خصائص هذه الجريمة (فرع ثاني).

الفرع الأول: التعريف بالجريمة

لم يعرف المشرع الجزائري جريمة التلاعب المعلوماتي[1]، لذا سوف نكتفي بما جاء به الفقه الوطني والمقارن من تعريفات لهذه الجريمة.

– عرفت جريمة التلاعب المعلوماتي بأنها: "كل أشكال العبث بالبيانات المعالجة آليًا والموجودة داخل النظام المعلوماتي، وذلك من خلال إدخال بيانات غير مصرح بها للدخول إلى النظام أو تعديل بيانات موجودة داخل النظام أو إلغاء هذه البيانات بالمرة"[2].

– وعرفت أيضًا بأنها: "التلاعب بالبرامج أو البيانات الموجودة داخل النظام أو الشبكة، يرتب عليها إيهام الغير بصحتها والتسليم بها"[3].

– وزاد آخرون في تعريفهم لها أنها: "ذلك الإتلاف الذي تتعرض له البيانات والمعلومات الموجودة على المواقع الإلكترونية وفي الحواسيب أو الصفحات الشخصية للأفراد والتي تحتويها شبكة الإنترنت، على أن يكون كلي من خلال محو هذه البيانات والمعلومات وتدميرها، بحيث لا يمكن الإستفادة منها مرة أخرى، أو أن يكون بشكل جزئي من خلال تشويه المعلومة كوضع بعض الرموز أو تشفير بعض الكلمات بشكل يجعلها تبدو غير مفهومة عند قراءتها"[4].

– كما عرفت هذه الجريمة بأنها: "كل ما من شأنه الإحتيال والعبث والتلاعب العمدي في الأوامر والتعليمات التي تحكم عملية البرمجة والمعالجة، من شأنها التأثير على الكيانات المنطقية للحاسب الآلي وما بداخله، حتى يقوم بمعالجة البيانات بناءً على هذه الأوامر والتعليمات الجديدة من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير"[5].

---

[1]– في جريمة التلاعب والإحتيال المعلوماتي ينظر مثلا: (– **نائلة عادل محمد فريد قورة:** المرجع السابق، ص415. – **محمد أمين الشوابكة:** المرجع السابق، ص180، – **أيمن عبد الله فكري:** المرجع السابق، ص571، – **غنام محمد غنام:** المرجع السابق، ص243، – **محمد علي العريان:** المرجع السابق، ص123، – **بلال أمين زين الدين:** المرجع السابق، ص125).

[2]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص135.

[3]– **عمار عباس الحسيني:** المرجع السابق، ص71.

[4]– **لينا محمد الأسدي:** المرجع السابق، ص58.

[5]– **محمد طارق عبد الرؤوف الخن:** جريمة الإحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011، ص38.

– كما جاء في تعريف لوزارة العدل الأمريكية بأن: "التلاعب المعلوماتي شكل من أشكال التخطيط الإحتيالي الذي ينتهج منهج الحوسبة للمساس بمحتويات النظام المعلوماتي بهدف كسب فائدة أو مصلحة من أي نوع كانت"[1].

– وهذا التعريف الأخير قريبٌ جداً مما جاءت به لجنة المراجعة البريطانية بعد أربع دراسات مختلفة قامت بها بشأن هذه الجريمة، حيث عرفتها بأنها: "كل سلوك غير مشروع من شأنه الإحتيال والتلاعب بالبيانات المخزنة داخل النظام، بنية الحصول على إمتياز مالي أو أي فائدة أخرى"[2].

وهنا يمكننا أن نضع من جهتنا بخصوص هذه الجريمة تعريف متواضع وهو أنها: "جريمة تقوم على التلاعب في المدخلات والتلاعب في البيانات والمعلومات الموجودة داخل النظم المعلوماتية، يلجأ إليها الجناة في سبيل تحقيق ما يرمون إليه".

الفرع الثاني: خصائص الجريمة

تتسم هذه الجريمة بجملة من الخصائص نذكر منها:

أولاً– أنها من جرائم الدخول المسموح به

تتميز هذه الجريمة بصفة عامة من كونها تقع في غالب الأحيان بمعرفة المسؤول عن النظام المعلوماتي أو الشخص المصرح له بالدخول والمسند إليه وظائف معينة على النظام كالمحاسبة والمعاملات المالية، لأنه يكون في أفضل وضع يؤهله لإرتكاب هذا النمط من التلاعب غير المشروع[3].

ثانيًا– أنها من جرائم الوسيلة الحاسوباتية

تتميز بأنها من جرائم الوسيلة المطلقة، ولم يشترط إرتكابها عن طريق وسيلة معينة[4]، تتميز أيضًا بأنها من الجرائم التي يلعب فيها الحاسب الآلي دورًا جوهريًا وهامًا في التلاعب المعلوماتي،

---

[1]– **محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت –الجريمة المعلوماتية–، دار الثقافة للنشر والتوزيع، القاهرة، مصر، 2001، ص180.

– **عبد الله سيف الكيتوب:** الأحكام الإجرائية لجريمة الإحتيال المعلوماتي، دار النهضة العربية، القاهـرة، مصـر، 2013، ص31.

– **عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن إستخدام الإنترنت، المرجع السابق، ص411.

[2]– **عمار عباس الحسيني:** المرجع السابق، ص71.

[3]– **عبد الفتاح بيومي حجازي:** مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص378. – **رشيدة بوكر:** المرجع السابق، ص98.

[4]– **حسني الجندي:** التشريعات الجنائية الخاص في دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، مصر، 2006، ص135.

بحيث يكون وسيلةً وهدفًا بالإعتداء، بمعنى أن يستهدف الفعل المجرم المعطيات المعالجة والمخزنة بواسطة الحاسب والشبكات[1].

ثالثاً- أنها من جرائم الدخول غير المسوح به

يرتكبها الجاني بإرتكاب أفعال دون وجه حق ودون أن يكون مصرحًا له بذلك، أو بطريقة غير مشروعة أو على وجه مخالف للقانون، وهذا يعني أن الجاني ليس له سلطة على البرامج والبيانات أو المعلومات المعالجة والمخزنة على النظام المعلوماتي وما في حكمه، ولم يحصل على تصريح مسبق أو رضاء صاحب الحق في القيام بالسلوك[2].

رابعًا- أنها من جرائم الإعتداء على المعلومات

الحماية الجنائية في هذه الجريمة تقتصر فقط على المعلومات والبيانات التي تم معالجتها داخل النظام، أو التي هي في طريقها إلى المعالجة[3]، وأن هدف الجاني من هذه الجريمة هو الوصول إلى نتائج ومعطيات غير تلك المرجوة من طبيعة وبيئة النظام المعلوماتي، وذلك بدافع الإنتقام أو تحقيق مصلحة له أو لغيره[4].

خامساً- أنها من الجرائم ذات النشاط الإيجابي

أي تتحقق الجريمة بطريق إرتكاب الفعل الإيجابي لها، ومن ثم لا تتحقق بسلوك سلبي أو بمجرد الإمتناع[5].

سادساً- أنها من الجرائم المستقلة عن جريمة الدخول أو البقاء غير المشروع

ومن مميزاتها أيضًا نجد الفارق بينها وبين جريمة الدخول أو البقاء غير المشروع، فجريمة التلاعب في المعطيات الموجودة داخل النظام المعلوماتي هي جريمة مستقلة تمامًا عن جريمة الدخول على الرغم من أن بدايتها كانت بقيام جريمة الدخول أو البقاء، ضف إلى ذلك أن جريمة التلاعب المعلوماتي تكون دائمًا مقصودة بمعنى يريدها الفاعل ويقبلها على الأقل متى أُرتكبت بطريق الغش، بينما جريمة الدخول أو البقاء لا تقع كذلك، إذ لا يريدها الفاعل أحياناً[6].

---

[1]- **محمود رجب فتح الله:** المرجع السابق، ص318.

[2]- **محمد علي سويلم:** المرجع السابق، ص307.

[3]- **عبد الفتاح بيومي حجازي:** الجريمة في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي، الاسكندرية، مصر، 2008، ص96.

[4]- **جباري عبد المجيد:** دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، 2012، ص115.

[5]- **محمد علي سويلم:** المرجع نفسه، ص306.

[6]- **محمد خليفة:** المرجع السابق، ص161. - **يزيد بوحليط:** المرجع السابق، ص190.

المطلب الثاني: الطبيعة القانونية لجريمة التلاعب المعلوماتي

على الرغم من عدم وجود مصطلح قانوني دقيق ومحدد للدلالة على هذه الجريمة التي نحن بصدد الحديث عنها وعن طبيعتها القانونية، فالبعض يطلق عليها إسم "جرائم التلاعب الإلكتروني" والبعض الآخر يطلق عليها إسم "جرائم العبث المعلوماتي"، ومنهم من يسميها "بجرائم التزوير والإحتيال المعلوماتي"، ومع ذلك فهي كلها تسميات لجريمة واحدة المقصود من ورائها المساس العمدي بالمعلومات المخزنة داخل النظام المعلوماتي.

لذا سنتحدث هنا عن نقاط في غاية الأهمية، وهذا بالتطرق إلى موضوع تغيير الحقيقة المعلوماتية بإحدى الطرق المنصوص عليها (فرع أول)، ثم الحديث عن المعلومات داخل النظام المعلوماتي والجديرة بالحماية الجنائية (فرع ثاني) ويلي ذلك موضوع ضرورة إستحداث نصوص خاصة لحماية المعلومات داخل النظام المعلوماتي (فرع ثالث).

الفرع الأول: تغيير الحقيقة المعلوماتية بإحدى الطرق المنصوص عليها

التلاعب المعلوماتي معناه تغيير الحقيقة المعلوماتية بوسيلة أو طريقة مادية يترتب عليها أثر يدركه البصر والحواس الأخرى[1]. كما يقصد بالتغيير في هذه الجريمة هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة[2].

ولا يكفي مجرد تغيير الحقيقة في محرر إلكتروني لقيام هذه الجريمة، وإنما يشترط القانون أن يتم هذا التغيير بإحدى الطرق التي حددها، على الرغم من تعدد الأساليب التي يستخدمها قراصنة المواقع والإنترنت في المساس بالبيانات الموجودة على هذه المواقع والشبكات الإلكترونية، ولهذا يتطلب القانون دائمًا أن يتضمن الحكم الصادر بالإدانة في جرائم العبث الإلكتروني تعيين وتبيان الطريقة التي توصل بها الجاني في تغيير الحقيقة الإلكترونية أو المعلوماتية، وإلا كان هذا الحكم قاصرًا عن التسبيب ومعيبٌ نقصه وجب نقضه[3].

بمعنى آخر أنه لا يكفي في جريمة التلاعب المعلوماتي أن يقع تغيير للحقيقة المعلوماتية في وثيقة إلكترونية، وإنما يلزم أن يكون هذا التغيير قد وقع فعلاً بإحدى هذه الطرق المحددة قانونًا، حيث كان دائمًا يثار التساؤل حول طرق التزوير والتلاعب الإلكتروني، هل أنها تخضع لمبدأ

---

[1]– **أحمد فكري طه:** المرجع السابق، ص253.

[2]– **محمود نجيب حسني:** شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1986، ص219.

[3]– قرار محكمة النقض المصرية، الطعن رقم (17639) جلسة بتاريخ 1998/12/17، عن (مج، ق، ق)، ج6، لسنة 2000، ص3.

الحصر السابق أم أنها واردة على سبيل المثال، وبالتالي فإن مبدأ الشرعية الجنائية يقتضي دائمًا أنه يجب على المشرع الجنائي أن يتداخل بنصوص قانونية يحدد بها هذه الطرق والأساليب التي من شأنها تغيير الحقيقة المعلوماتية الموجودة داخل النظم الإلكترونية[1].

وتغيير حقيقة المعلومة الإلكترونية يتضمن العديد من أفعال الإعتداء على المعلومات المعالجة آليًا، وهي تشمل عدد لا بأس به من الأنشطة التي تتعلق بالنظم المعلوماتية[2]، والتي يمكن إجمالها في إحداث تعديل في مضمون المعلومة سواء بطريق الإضافة إلى ما هو مكتوب أو بطريق الإزالة والمحو لبعض ما هو مكتوب، أو تعديل وإستبدال ما هو مكتوب بما من شأنه تغيير مضمون المعلومة أو بإدخال بيانات ومعلومات جديدة منافية للحقيقة تمامًا حتى وإن كانت تحمل بعض أوصاف الوثيقة الإلكترونية الأصلية، وهذا ما يطلق عليه في لغة القانون "أسلوب التلاعب والعبث بالمعلومات والمعطيات المعالجة آليًا داخل النظام المعلوماتي"[3].

وحتى وإن إختلف شكل المحرر الإلكتروني، فإن العبرة في تغيير الحقيقة المعلوماتية يكون بالمساس بحقوق الغير ومراكزهم القانونية الثابتة لهم في هذه المعلومات والمحررات[4]، وبالتالي يعتد بهذه الجريمة إذا وجد في المحرر الإلكتروني الذي شمله التغيير ما يخالف إرادة صاحب الشأن الذي يستأثر بالمعلومة لنفسه، حتى وإن كان ذلك التغيير يعبر بصدق عن الواقع[5].

وهكذا نجد أن أسلوب التلاعب في المعلومات هو الأكثر شيوعًا في إرتكاب الإجرام المعلوماتي، بما يحققه ذلك من تغيير في حقيقة المحررات والوثائق الإلكترونية، وهذا من خلال صور العبث في البيانات المعالجة آليًا، إما عن طريق مدّ وتغذية النظام بمعلومات غير صحيحة وإدخالها فيه أو القيام بتعديل هذه المعلومات بالحذف أو بالإضافة أو أنه يزيلها ويمحوها من على الدعامة الإلكترونية، وهذا ما يطلق عليه "بأفعال الإدخال والإزالة والتعديل".

الفرع الثاني: المعلومات داخل النظام المعلوماتي والجديرة بالحماية الجنائية

تظهر جدارة المعلومات المبرمجة آليًا والمدرجة داخل النظام المعلوماتي بأحقيتها في الحماية الجنائية وهذا مقارنة بالمعلومات التي تحتويها الملفات الورقية، وهذا لأهميتها في مجال

---

[1]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص89.

[2]– **أحمد فكري طه:** المرجع السابق، ص253. – **عماد مجدي عبد الملك:** المرجع السابق، ص136.

[3]– **بلال أمين زين الدين:** المرجع السابق، ص339.

[4]– **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص325.

[5]– **أشرف توفيق:** الحماية الجنائية للمستند الإلكتروني، المرجع السابق، ص14.

التعاملات الإلكترونية، كما أن المعلومات المعالجة آليًا ضعيفة داخل النظام المعلوماتي عنها داخل الملفات الورقية، فهذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات الموجودة داخل النظام المعلوماتي[1].

كما أن المعلومات المعالجة آليًا تتميز بالضخامة والتنوع، ومنها ما هو خطير الكشف عنه كالتي تتعلق بالحياة الخاصة للأشخاص[2] أو المؤسسات، كل هذه الإعتبارات وغيرها دعت مشرعي كثير من الدول إلى إستحداث صور من التجريم لحماية المعلومات الموجودة داخل النظم المعلوماتية سواء من حيث الإطلاع عليها أو المساس بها[3].

كما تعتبر النظم المعلوماتية على مختلف أنواعها وأحجامها الوسيلة الأساسية للقيام بالتعاملات الإلكترونية، بحيث تتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت وجيز، فمن الطبيعي إذن أن تحتاج هذه النظم إلى حماية جنائية بما يضمن عدم إنتهاك حرمة المكان الإفتراضي وقد أدركت كثير من التشريعات المقارنة هذه الحقيقة، فأدخلت نصوص خاصة لحماية هذه النظم وما تحتويه بداخلها من معلومات قيمة.

الفرع الثالث: ضرورة إستحداث نصوص خاصة لحماية المعلومات داخل النظام المعلوماتي

إن السلامة في مجال أمن التعاملات الإلكترونية تعني الحفاظ على المعلومات من كل أشكال التلاعب من طرف أشخاص غير مخول لهم القيام بذلك[4]، وإزاء تعدد صور الإضرار بالمعلومات التي تحتوي عليها المواقع والنظم الإلكترونية ونتيجة إزدياد العبث بها، تنبهت معظم

---

[1]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص 94.

[2]– لا شك بأن حرمة الحياة الخاصة للإنسان أو كما يطلق عليها "الحق في الخصوصية"، هو حق معترف به لكل شخص طبيعي كان أو معنوي، لاسيما الشخص الطبيعي، وهذا بصفته كإنسان يعيش داخل الجماعة وأحد أهم دعائم المجتمع، وهذا الحق يعد من أهم الحقوق الدستورية الملازمة للفرد، لذلك حظيت الحياة الخاصة للأفراد بحماية قانونية متميزة في كل القوانين المقارنة، مستمدة ذلك من نص المادة (12) من الإعلان العالمي لحقوق الإنسان والصادر في 1948/12/10، والتي جاء نصها: "لا يعرض أحد لتدخل تعرسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحص في حماية القانون من مثل هذا التدخل أو تلك الحملات"، كما نصت أيضاً المادة (17) من العهد الدولي للحقوق المدنية والسياسية الصادر في 1966/12/16 والتي جاء فيها: "لا يجوز التدخل بشكل تعسفي أو غير قانوني لشرفه أو سمعته، ولكل شخص الحق في حماية القانون ضد التدخل أو التعرض"، ولقد إنضمت الجزائر إلى هذا العهد الدولي بموجب المرسوم الرئاسي رقم (89–67) والمؤرخ في 1989/05/16، ج ر، ع20، في 1989/05/17، ص531.

[3]- ***HUET (J), MAISL (H) :*** *Droit de l'informatique et des télécommunications, édition, LITEC, Paris, France, 1989, P111.*

[4]– **عطاء الله وارد خليل:** أمن المعلومات في ظل الإنفتاح المعلوماتي، مجلة كلية الحقوق، جامعة بنها، مصر، ع 6، لعام 2011، ص612.

التشريعات الجنائية المقارنة إلى ضرورة مجابهتها بنصوص قانونية خاصة، كون هذا العدوان جديد من نوعه ولم يسبق تجريمه من قبل[1].

ونظرًا لقصور القواعد الجنائية التقليدية في قانون العقوبات عن حماية هذا النظام، إستشعر المشرع الجنائي في دول عديدة الحاجة الماسة إلى إستحداث نصوص تجريمية جديدة تحمي المعلومات داخل النظام المعلوماتي، وتعاقب كل من تسوّل له نفسه الإعتداء أو المساس بهذه المعلومات سواء لمن له أحقية الإطلاع عليها أو لغير المصرح له بالإطلاع عليها من مجرد الدخول أو التواجد غير المشروع داخل النظام المعلوماتي إلى التعمد في المساس بمحتويات هذا النظام من إتلاف أو تغيير أو حتى تعديل[2].

[1]– **رشيدة بوكر:** المرجع السابق، ص96.

[2]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص94.

المبحث الثاني: أركان جريمة التلاعب المعلوماتي والعقوبات المقررة لها

تمهيد وتقسيم:

لا تكتسب هذه الجريمة صفتها الجرمية إلا وفق ما يستلزمه القانون لقيامها، فيلجأ إلى تحديد أهم أركانها وعناصرها القانونية التي تقوم عليها، ثم يرصد لفاعلها الجزاء المقرر قانوناً أيًّا كانت صورته، وذلك ما سوف نتناوله في مطلبين إثنين كما يلي:

المطلب الأول: أركان جريمة التلاعب المعلوماتي

المطلب الثاني: العقوبات المقررة لجريمة التلاعب المعلوماتي

المطلب الأول: أركان جريمة التلاعب المعلوماتي

وإنطلاقًا من مقتضيات النصوص القانونية الموجودة في التشريع الوطني والمقارن، سنتطرق إلى هذه الجريمة من خلال أركانها العامة، ولقيام جريمة التلاعب المعلوماتي كغيرها من الجرائم المستحدثة أو التقليدية لابد من توافر أركان أساسية وعناصر قانونية بداية بالركن الشرعي لها (فرع أول)، ثم الركن المادي (فرع ثاني) وأخيرًا الركن المعنوي لهذه الجريمة (فرع ثالث).

الفرع الأول: الركن الشرعي للجريمة

تقتضي دراسة الركن الشرعي لجريمة التلاعب المعلوماتي تبيان نص التجريم الواجب التطبيق (أولاً) ثم الغاية من علة هذا التجريم (ثانياً).

أولاً- بالنسبة لنص التجريم

جريمة المساس بالمعلومات أو كما يطلق عليها أيضًا بجريمة التلاعب المعلوماتي، هي ثاني جريمة ينص عليها المشرع الجزائري بعد جريمة الدخول أو البقاء غير المشروع داخل النظام المعلوماتي، حيث جرم المشرع الجزائري التلاعب غير المصرح به في المعلومات بموجب المادة (394 مكرر 1) من (ق ع ج) بقوله: "... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1].

أما المشرع الفرنسي فقد نص عليها بموجب المادة (323-3) من (ق ع ف) على عقاب كل من أدخل بسوء نية بيانات في نظام المعالجة الآلية للمعطيات أو قام بإلغاء أو تعديل هذه البيانات بالحبس...[2].

كما دعت إلى تجريمه أيضاً إتفاقية بودابست (إ.أ.م.إ.م) بموجب المادة الرابعة (4) منه[3]، وكذا الإتفاقية العربية (إ.ع.م.ج.ت.م) بموجب المادة الثامنة (8) منه[4].

---

[1]- أنظر في ذلك: **الملحق رقم (05)**.

[2] ***Article : (323-3). Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4***

- « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

[3]- تنص المادة الرابعة من (إ.أ.م.إ.م) على أنه "التدخل البيانات: - تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما أرتكبت عمداً، إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها. - يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة الأولى في ضرر جسيم". **أنظر في ذلك الملحق رقم (01)**

[4]- تنص المادة الثامنة من (إ.ع.م.ج.ت.م) المتعلقة بالإعتداء العمدي على سلامة البيانات والمعلومات المخزنة داخل النظام المعلوماتي على أنه: "تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدًا أو بدون وجه حق، وعلى الأطراف الإلتزام بتجريم الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة"، **أنظر في ذلك الملحق رقم (02)**

أما عن المشرع المصري فقد نص عليها بموجب المادة (18) من القانون رقم (175 لسنة 2018) في شأن مكافحة جرائم تقنية المعلومات بقوله: "يعاقب بالحبس... كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا، متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيًّا كانت الوسيلة التي أُستخدمت في الجريمة"[1].

ثانيا- بالنسبة لعلة التجريم

يتضح جليًّا مما سبق ذكره من مقتضيات النصوص القانونية السالفة الذكر أن المشرع الجنائي يحمي النظام المعلوماتي بكل ما يشتمل عليه من برامج وتطبيقات وحتى بيانات ومعلومات، أي أنه يوفر الحماية الجنائية لما هو موجود داخل النظام المعلوماتي ذاته، وذلك ضد أي فعل إجرامي، وعلى هذا الأساس فإن النص الجنائي هنا جاء ليحمي المعلومة المعالجة والمخزنة داخل النظام، أو تلك التي ما زالت في إطار المعالجة، ولا يتناول المعلومات المتواجدة خارج النظام، لذلك يرى الكثيرون أن الحماية الجنائية بخصوص هذه الجريمة تظل مستمرة مع المعلومة داخل النظام أو حتى وهي في طريقها إلى المعالجة الآلية[2].

وتتجسد علة التجريم هنا في أن النظام المعلوماتي وما في حكمه من شبكة معلوماتية أو وسائل تقنية المعلومات تحمل في داخلها خصوصيات وأسرار سواء تعلقت بأفراد أو مجتمعات، وهذا بإعتبارها وسيلة أمن وأمان وما تحمله من ثقة كبيرة في نتائجها، لذا كان لزامًا على المشرع إتخاذ كل ما يلزم للمحافظة عليها وضمان أداء وظيفتها على أفضل وأحسن وجه ممكن، وهذا من خلال تجريم الإعتداء العمدي على المعطيات أو البرامج أو البيانات أو المعلومات الموجودة داخل النظام من كل أعمال العبث أو محاولة المساس بها[3].

الفرع الثاني: الركن المادي للجريمة

يقوم الركن المادي في جريمة التلاعب المعلوماتي على كل نشاط إيجابي يحدده المشرع، على أن يكون محل هذا النشاط البيانات والمعلومات المخزنة داخل النظام المعلوماتي، لذا سوف نكتفي هنا بالحديث عن السلوك المجرم (أولاً) والنتيجة الإجرامية (ثانياً).

---

[1]- أنظر في ذلك: **الملحق رقم (04).**

[2]- **عبد الفتاح بيومي حجازي:** الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص45.

[3]- **محمد علي سويلم:** المرجع السابق، ص302. - **حسني الجندي:** المرجع السابق، ص116.

أولاً- السلوك المجرَّم

بالرجوع للنصوص القانونية السالفة الذكر يمكن القول أن السلوك المجرم في هذه الجريمة يتخذ عدة صور متعددة، والمتمثلة في كل من أفعال الإدخال والإزالة والتعديل.

أ- فعل الإدخال *L'introduction*: يقصد بفعل الإدخال كل عمليات التدخل في النظام المعلوماتي من خلال إدخال معلومات وهمية أو إدراج برامج جديدة[1]، أو إضافة بيانات جديدة على الدعامة الإلكترونية الخاصة بالنظام سواء كانت هذه الدعامة خالية من البيانات أو كان يوجد عليها بيانات من قبل[2].

كما يتحقق فعل الإدخال بتغذية النظام بتعليمات لازمة لعملية المعالجة، وقد يتم إدخال هذه التعليمات الجديدة والغير المصرح بها بقصد التشويش على صحة البيانات القائمة[3]، ويتحقق أيضًا فعل الإدخال عن طريق إستخدام البرامج الخبيثة بغرض التعديل في البيانات، الأمر الذي يؤثر على صحتها أو نسبتها أو قيمتها، وقد يكون الغرض من ذلك إتلافها أو تشويشها أو تدميرها[4].

فالتدخل في المعطيات المعالجة آليًا أو المحفوظة في النظام بغرض معالجتها يؤدي مباشرة إلى المساس بها، سواء تعلق الأمر بإدخال معلومات لم تكن موجودة سابقًا بغرض التلاعب بالبيانات المخزنة، أو عن طريق التدخل في النظام المعلوماتي قصد إرباكه والتشويش عليه، وفي كلتا الصورتين وغيرهما فإن النتيجة مؤداها إما الإتلاف أو التزييف أو التزوير للحقيقة المعلوماتية[5]، وهو أمر سهل القيام به خاصة في المراحل الأولى لتشغيل النظام، وهي مرحلة إدخال المعلومات، وبالتالي يكون من السهل تغذية النظام بمعلومات مغلوطة أو زائفة لم تكن موجودة فيه من قبل، الأمر الذي يؤثر سلبًا على المعلومات والبيانات الموجودة فيه سلفًا من حيث سلامتها وقيمتها[6].

---

[1]- **زيدان زيبحة:** المرجع السابق، ص59. - **يزيد بوحليط:** المرجع السابق، ص188.

[2]- **علي عبد القادر القهوجي:** الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، لبنان، 1999، ص60.

[3]- **هدى حامد قشقوش:** المرجع السابق، ص569. - **عبد الوهاب ملياني،** المرجع السابق، ص192.

[4]- **عبد الفتاح بيومي حجازي:** مكافحة جرائم الكمبيوتر والإنترنت، المرجع السابق، ص67.

[5]- **عبد الهادي بن زيطة:** حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، (د.ت.ن)، ص88.

[6]- **عبد الفتاح بيومي حجازي:** الجريمة المعلوماتية في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي، الاسكندرية، مصر، 2008، ص96.

ويعد فعل إدخال بيانات مغلوطة وغير معتمدة في النظام المعلوماتي من أكثر الأساليب الإجرامية شيوعًا، وهي تمثل نصف إجمالي حالات الإحتيال المعلوماتي[1]، حيث يصنف الفقهاء هذا النوع من السلوك ضمن الغش المعلوماتي الذي يتم عن طريق العبث والتلاعب بالنظام بإدخال بيانات جديدة مصطنعة بغرض تغيير الحقيقة المنطقية للنظام[2]، ومن أمثلتها إدخال الفيروسات والقنابل المنطقية والزمنية والتي من شأنها إضافة معطيات جديدة أو إتلافها بالمرة[3]، فمن التطبيقات القضائية في إطار إدخال معلومات مغلوطة داخل النظام المعلوماتي ما قضت به المحكمة العليا الفرنسية عام 1994م، حين تأييدها حكم بالإدانة لأحد الأشخاص بتهمة إتلاف معلومات كانت موجودة داخل أحد الأنظمة المعلوماتية، وذلك بعد قيامه بإدخال معلومات غير مصرح بها متعلقة بالنسب الضريبية الخاصة بضريبة المبيعات[4].

كما يتميز فعل الإدخال أنه يقع في غالب الأحيان بمعرفة المسؤول عن قسم المعلومات المعالجة آليًا والموجودة داخل النظام، أو الشخص المسند إليه وظائف المحاسبتية والتعليمات المالية على أساس الوضعية المتواجد فيها والتي تؤهله للتلاعب والعبث غير المشروع بالمعلومات، فمن الصور التي يمكن للمسؤول عن المعلومات القيام بها مثلاً إدخال معلومات وهمية أو مغلوطة كأسماء وهمية في كشوف المرتبات، الأمر الذي قد يترتب عنه صرف مرتبات موظفين وهميين أو لأناس فارقوا الحياة، وبالفعل فقد قام أحد المسؤولين عن القسم المعلوماتي بإحدى الشركات الفرنسية عام 1997م من خلال إعادة ملفات المستخدمين السابقين والذين لهم حقوق مالية وإدخالها من جديد، ثم قام بتحويل هذه المبالغ إلى حسابه الخاص وإلى حسابات أخرى والتي فتحها خصيصًا لهذا الغرض، والتي بلغت حينها حوالي إثنين مليون فرنك فرنسي[5]، ومن التطبيقات أيضًا على جريمة إدخال بيانات غير مصرح بها ما قامت به المتهمة التي كانت تعمل في إحدى الشركات الفرنسية، وذلك قبل تركها للعمل في تلك الشركة، فقامت بإدخال بيانات غير صحيحة تتعلق بمعدل إحتساب الضريبة على القيم المنقولة، وقد أدى ذلك إلى إرباك العمل داخل الشركة على عكس ما كانت تنوي

---

[1]– **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، مصر، 1994، ص58.

[2]– **عبد الفتاح بيومي حجازي:** الحماية الجنائية لنظام الكمبيوتر، المرجع السابق، ص46.

[3]– **عبد الفتاح بيومي حجازي:** الجريمة المعلوماتية في عصر العولمة، المرجع السابق، ص100.

[4]– **عبد الوهاب ملياني:** المرجع السابق، ص193.

[5]– **محمد سامي الشوا:** الغش المعلوماتي كظاهرة إجرامية مستحدثة، المرجع السابق، ص546.

الشركة القيام به من أعمال المحاسبة، ومن الواضح أن قصد المتهمة كان منصرفا إلى تحقيق تلك الغاية[1].

كذلك نجد هذا السلوك في التلاعب في المعلومات كثيرًا في مجالات التعاملات المالية والمصرفية والمؤسسات البنكية كإدخال لبطاقات السحب أو الإئتمان سواء من صاحبها الشرعي أو من غيره في حالات السرقة الإلكترونية كأن يقوم بإدخال بيانات أو برامج غريبة من شأنها إضافة معطيات جديدة بغرض سحب مبلغ من النقود أكثر من الرصيد الموجود بحسابه، أو أنه يقوم بالإستخدام التعسفي لبطاقة السحب أو الإئتمان بعد إنتهاء مدة صلاحيتها أو بعد إلغاء البنك لها[2].

ولعل إصطناع المعلومات هو من الأفعال الأكثر سهولة في تنفيذ الجريمة، لاسيما في المؤسسات المالية والمصرفية والبنكية، حيث يعد المسؤول في القسم المعلوماتي في أفضل موقع يؤهله لإرتكاب هذا النمط غير المشروع من التلاعب[3]، ومن التطبيقات القضائية أيضًا ما أيدته محكمة النقض الفرنسية في قرار لها في 8 ديسمبر 1998، حيث رأت أن واقعة التعديل والإلغاء العمدي لمعطيات مخزنة في النظام المعلوماتي هي بمثابة مخالفة للوائح المطبقة خاصةً وأن هذه المخالفة قد تم إرتكابها بواسطة شخص له حق الدخول في النظام، ولا يشترط القانون هنا أن يكون هذا الشخص المخالف لديه نية الإضرار[4].

وحتى المشرع الجنائي لم يشر إلى وجوب وقوع ضرر أو حتى بقصد وقوع ضرر من هذا التغيير في المعلومات، وبالتالي فإن مجرد إدخال معلومات مغلوطة على معطيات معالجة داخل النظام يشكل السلوك الإجرامي لهذه الجريمة، كما لا يهم صحة المعلومات المدخلة من عدمه، فالعبرة بالإدخال لا بمدى صحة هذه المعلومات[5]، وبالرجوع إلى التقرير التفسيري لإتفاقية الإجرام المعلوماتي نجدها تفسر المادة الرابعة منها على أساس أنها "جريمة غش معلوماتي" تترتب على أحد الأفعال والتي من بينها فعل إدخال معلومات غير صحيحة على الحاسوب أو النظام، وكذا التلاعب

---

[1]– *Crime, 5 Janv 1994, J. C. P, 1994, P 359.*

[2]– **عصام عبد الفتاح مطر:** التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الاسكندرية، مصر، 2015، ص328.

[3]– **نبيل صقر:** جرائم الكمبيوتر والأنترنت، دار الهلال للخدمات العلمية، الجزائر، 2005، ص141.

[4]– *Crime, 8 Déc 1999, bull N° 296.*

[5]– **عبد الوهاب ملياني:** المرجع السابق، ص194.

في البرامج الموجودة فيه، وأضاف نفس التقرير أن العقوبة المقررة تطال كل تلاعب تعسفي خلال معالجة البيانات بغرض الحصول دون وجه حق على منفعة له أو للغير[1].

ومن القضايا الشهيرة أيضًا في جرائم الغش المعلوماتي، ما قضت به محكمة جنح باريس، أنه بتطبيق نص المادة (323-3) من (ق ع ف) في واقعة إنطوت على إدخال برنامج *Sniffer*، وهو البرنامج الذي يعمل على جهاز الحاسوب مع إمكانية توصيله بشبكة الإنترنت والقادر على الجمع التلقائي للمعلومات المخزنة وإرسالها إلى جهات أخرى دون التأثير على صحة المعلومات الموجودة داخل النظام، بل مهمته فقط هي تجميع المعلومات، وبناء على تفسير هذه المادة رأت المحكمة أنها تنطبق على هذه الواقعة[2].

ب- فعل الإزالة (المحو) *L'éffacement*: وهو السلوك الثاني في هذه جريمة التلاعب المعلوماتي والمنصوص عليه في المادة (394 مكرر 1) من (ق ع ج)، حيث يقصد بفعل الإزالة كل إزالة أو إلغاء أو محو أو حذف للمعلومات والمعطيات المسجلة على الدعامة الإلكترونية والموجودة داخل النظام المعلوماتي وذلك بصفة نهائية، سواء كان ذلك الحذف كليًا أو جزئيًا[3]، فالإزالة هي المحو الجزئي أو الكلي للمعلومات المتواجدة داخل النظام، أو حتى لمجرد نقل وتخزين جزء من المعلومات إلى منطقة خاصةً من الذاكرة[4]، ومثال ذلك من هذه الصورة الأخيرة أن يقوم الشخص المعتدي بعد حصوله على تصاميم وبرامج شركة ما، ثم يقوم بمحو وإزالة إسم هذه الشركة الأصلية من على الدعامة الإلكترونية وإعادة كتابة الإسم الجديد عليها وعرضه في الأسواق بتكلفة أقل من النسخة الأصلية[5].

وعلى إثر ذلك قد يكون فعل الإزالة عملية لاحقة عن عملية الإدخال للمعلومات المعالجة والمخزنة، فهي تفترض الوجود السابق لها، فمثلاً المسؤول عن عملية الحفظ يمكنه تدمير وإتلاف المعلومات المكلف بحفظها داخل النظام[6]، بحيث يستطيع أن يزيل أو يمحو بعض أو كل المعلومات المخزنة في النظام المعلوماتي، وغالبًا ما يستفيد الجاني من ربح نظير قيامه بمحو تلك المعلومات

---

[1]- **سفيان سوير:** المرجع السابق، ص94.

[2]- **رشيدة بوكر:** المرجع السابق، ص252.

[3]- **يزيد بوحليط:** المرجع السابق، ص189.

[4]- **عبد الوهاب مليايني:** المرجع نفسه، ص194. - **عبد الفتاح بيومي حجازي:** الجريمة في عصر العولمة، المرجع السابق، ص97.

[5]- **طاهر محمود أبو القاسم:** المرجع السابق، ص74.

[6]- **عبد الفتاح بيومي حجازي:** الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص47.

المهمة، وهذا ما يحدث في جرائم البنوك والشركات الكبرى والمطارات، وكمثال على ذلك في حالة رفع إسم أحد الأشخاص من قوائم الممنوعين من السفر أو في حالة ترقب وصوله[1].

وهذا يعني أن النشاط الإجرامي في فعل الإزالة إنما يرد على محل محدد وهو المعطيات والمعلومات التي تمت فعلاً "معالجتها آليًا *Traitement automatique*"، والتي يحتويها النظام وتشكل جزءًا منه، وهو ما يستخلص بوضوح من خلال نص المادة (394 مكرر 1) من (ق ع ج) والتي جاءت كما يلي: "... أو أزال بطريق الغش المعطيات التي يتضمنها"[2]، وكذلك ما جاء في نص المادة (323-3) من (ق ع ف) "*... les données qu'il contient*"[3]، وعليه يخرج من نطاق الحماية المعطيات التي لم تعالج بعد، وتلك التي لم تبدأ بعد مراحل معالجتها، وكذا تلك التي عولجت وإنفصلت عن النظام[4]، والإزالة بهذا المعنى تفترض الوجود السابق لعملية الإدخال[5].

ومن أمثلة ذلك أيضًا ما قام به بعض المسؤولين في حفظ البيانات بإحدى الشركات، حيث قاموا بنقل وتخزين المعطيات الخاصة بإحدى شركات التأمين داخل النظام المعلوماتي، وذلك بالإستيلاء على مبلغ كبير كانت قد أرسلته شركة التأمين لصالح أحد المراكز الطبية، فقام هؤلاء المسؤولين بفتح حسابات وهمية ووضعوا فيها المبلغ، وحتى تتم هذه العملية بنجاح قاموا بمحو وإزالة جزء كبير من المعلومات من سجلات الحاسب الآلي لذلك المركز الطبي، وهي كلها حسابات ومعلومات ترجع للأشخاص المتوفين، وذلك إما بجعلها غير قابلة للتحصيل وإما بحذفها من الملفات الإلكترونية الخاصة بالذاكرة[6]، وهذا كله إذا ما دل فإنما يدل على أنه يمكن للمسؤولين المكلفين بحفظ البيانات أن يعبثوا بالمعلومات المكلفين بحفظها أو نقلها أو تخزينها داخل النظام، وذلك كمحوها وإزالتها[7].

ومن القضايا أيضًا ذات الصلة بجريمة إزالة معلومات من على دعامة النظام نجد مثلاً قضية شركة التأمين الأمريكية "*T.R.W- Company Credit Data*"، والتي كانت تعمل على تزويد عملائها من البنوك والشركات والمتاجر الضخمة بمعلومات تتعلق بمراكزهم الإئتمانية نظير

---

[1]- **طاهر محمود أبو القاسم:** المرجع السابق، ص82.

[2]- أنظر في ذلك: **الملحق رقم (05).**

[3]- أنظر في ذلك: **الملحق رقم (03).**

[4]- **رشيدة بوكر:** المرجع السابق، ص104.

[5]- **محمد خليفة:** المرجع السابق، ص184.

[6]- **عبد الفتاح بيومي حجازي:** النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص49.

[7]- **خثير مسعود:** المرجع السابق، ص 124.

إشتراك مالي يدفعه المتعاملين مع هذه الشركة، بحيث كان لها ما يزيد عن خمسين مليون شخص معلوماتهم الإئتمانية موجودة لدى هذه الشركة، فإستغل أحد الموظفين بقسم علاقة المستهلكين خبرته الوظيفية وقام بالدخول إلى النظام المعلوماتي الخاص بهذه الشركة وراح يبيع مراكز إئتمانية قوية لذوي المراكز الإئتمانية الضعيفة مقابل مبلغ مالي يدفعه هؤلاء على حسابه الخاص، فعمل هذا الموظف على إزالة ومحو كل المعلومات المتعلقة بمركزيتهم الضعيفة وإستبدالها بمعلومات تحسن من مركزهم الجديد، وهذه العملية شملت صور متعددة للتلاعب بالمعلومات من إزالة ومحو وتعديل، ولم يتم كشف هذه الجريمة إلا بعد أن تقدم أحد المتعاملين مع هذه الشركة ببلاغ إلى مكتب التحقيقات الفيديرالية "*FBI*" بعدما تلقى عرضًا من الموظف بتحسين مركزه الإئتماني وخلق له مركز جديد مقابل مبلغ مالي معين[1].

وكذا فقد قضى أيضاً قسم الجنح بمحكمة وهران بالجزائر بوقوع فعل الإدخال والتعديل والإزالة والحذف بطريق الغش المعلوماتي لمعطيات مخزنة في نظام المعالجة الآلية للمعلومات في حق المتهمة المشرفة على جهاز الحاسب الآلي رقم (*X*) التابع لمصلحة التنظيم العام لولاية وهران، والتي قامت بالتلاعب بمعطيات خاصة بسيارتين، حيث أثبت التحقيق أن هاتين السيارتين موجودتين في بنك المعلومات المخزنة بجهاز الحاسوب الآلي التابع لمصلحة التنظيم العام لولاية وهران، ولكنهما غير موجودتين على جهاز مصلحة التعريفات، وأن المتهمة وحدها من كانت تملك كلمة السر للولوج على جهاز الحاسب الآلي الحاصل رقم (*X*) وأنه الجهاز الوحيد المتعلق بعملية الإزالة والحذف[2].

وعموما تشكل جريمة إزالة المعلومات وحذفها واحدة من أكثر صور التعدي علم سلامة التعاملات الإلكترونية شيوعا، وهو ما دفع العديد من التشريعات الجنائية المقارنة إلى النص عليها وتجريمها، وإن اختلفت فيا بينها في وضع المصطلحات الدالة على فعل الإزالة[3].

---

[1]– **عبد الفتاح بيومي حجازي:** النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص50.

[2]– قسم الجنح المختص التابع لمحكمة وهران بالجزائر، مجلس قضاء وهران، القطب الجزائي المختص، حكم رقم (12/00016)، المؤرخ في 2012/07/25 تحت إسم قضية جنحة المساس بأنظمة المعالجة الآلية للمعطيات (مشار إليه عند: – **رشيدة بوكر:** المرجع السابق، ص102).

[3]– فمنهم من إستخدم تعبير "الإزالة"، كما هو الشأن في التشريع الجزائري ونظيره الفرنسي، بينما إستخدم بعضها الآخر مصطلحات عديدة مثل "الإلغاء" في التشريع المصري، و"المحو" في التشريع اللبناني، و"الإتلاف" في التشريع السوري، و"الطمس" في التشريع الإماراتي، و"التدمير" و"الحجب" ذكرته كل من إتفاقية بودابست والإتفاقية العربية.

ج-فعل التعديل *Modification*: وهو سلوك يدخل كذلك في تكوين الركن المادي لجريمة التلاعب بالمعلومات داخل النظام المعلوماتي، ويقصد بالتعديل تغيير وإستبدال شكل المعلومات والمعطيات الموجودة داخل النظام وإستبدالها بمعلومات أخرى[1]، ونجد هذا السلوك يستخدمه الجاني بكثرة في هذه الجريمة بمجالاتها المختلفة بما في ذلك الإحتيال والتزوير المعلوماتي[2].

ويشير هذا المصطلح إلى قيام الغير ممن لا يملك صلاحية إحداث تغيير في المعلومات، بإحداث تعديلات عليها، وذلك بإستخدام وظائف نظام المعالجة الآلية للبيانات[3] أو إستخدام برامج غريبة في المعطيات المخزنة من أجل تعديلها سواء كليًا أو جزئيًا[4]، فقد يتم إستبدال المعلومات المخزنة عن طريق التلاعب في البرامج بإمداده بمعلومات مغايرة عن تلك التي صمم البرنامج لأجلها بواسطة برامج خبيثة[5]، بحيث يكون الهدف الرئيسي من وراء هذا التعديل عادةً هو تحقيق فائدة من ورائه[6].

ومن أمثلة ذلك قيام أحد العاملين في مجال البرمجة بإحدى الشركات الأمريكية بإعداد برنامج وإدخاله إلى جهاز الحاسب الذي يعمل عليه داخل هذه الشركة، حيث يسمح هذا البرنامج بمعرفة الحسابات التي تتضخم في فترات زمنية ببعض الإيرادات، مضمناً إياه بتعليمات بخصم بمبلغ زهيد كل شهر من رواتب ونفقات الموظفين، وذلك من خلال تعديل في إستمارة المحاسبة الضريبية الخاصة بكل موظف، وقد إستطاع من خلال هذا التعديل أن يحقق فائدة وأموال، حيث إستمرت العملية ستة سنوات من إختلاس أكثر من مليون دولار، وقد تم إكتشاف الواقعة بناءً على شكوى أحد الموظفين قدمت إلى قسم المرتبات بالشركة لعدم صحة إستمارة مرتبه المعدل في البرنامج[7].

---

[1]- لقد إستخدمت الإتفاقية العربية مصطلح "حجب المعلومات" للتعبير عن سلوك التعديل، ذلك أن حجب المعلومات دون محوها لا يمكن أن يشكل إزالة لها، فإخفاء أحد الملفات الإلكترونية مثلاً لا يترتب عليه محو له بل يؤدي فقط إلى تعديل في قائمة الملفات الموجودة على النظام، وبالتالي فإن الحجب لا يغدوا أن يكون تعديلاً للمعلومة. (- **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، المرجع السابق، ص100).

[2]- **رامي حليم:** المرجع السابق، ص17.

[3]- **نائلة عادل فريد قورة:** المرجع السابق، ص217.

[4]- **خثير مسعود:** المرجع السابق، ص125.

[5]- **علي عبد القادر القهوجي:** الحماية الجنائية لبرنامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، مصر، 2010، ص132.

[6]- **هشام محمد فريد رستم:** جرائم الفضاء الإفتراضي، مجلة أكاديمية الشرطة، القاهرة، مصر، 2013، ص11 وما بعدها.

[7]- **طاهر محمود أبو القاسم:** المرجع السابق، ص 74. - **هشام محمد فريد رستم:** جرائم الفضاء الافتراضي، المرجع نفسه، ص10.

وهناك من يرى بأن عبارة التعديل في المعلومات تدل تحديدًا عن وجود العدوان الفيروسي، إلا أننا نرى أن مصطلح التعديل وإن كان ينصرف في مدلوله إلى الفيروسات[1]، إلا أنه لا يقتصر عليها فالتعديل يمكن أن يتم عن طريق إمداد النظام بمعلومات مغايرة تؤدي إلى نتائج مغلوطة ومختلفة ومغايرة عن تلك التي صمم البرنامج لأجلها[2]، ويقال أن عبارة التعديل وردت في القانون المقارن كناية عن الإعتداء الفيروسي الذي يقوم بالتعديلات على المعطيات المعالجة والمخزنة والتي يترتب عليها نتائج سلبية منها عدم قابلية المعلومات الصحيحة للإستعمال مرة أخرى على نحو يجعلها عديمة الفائدة[3].

فتطبيقًا لذلك قضت أحد المحاكم الفرنسية بتوفير جريمة الغش المعلوماتي في حق المتهم الذي قام بتعديل الملفات الإلكترونية الخاصة بإحدى الشركات التي يعمل بها هذا المتهم لصالح شركة أخرى مقابل مبلغ من المال عن طريق بث فيروسات مصممة لمحو بعض البيانات ثم تعديلها من جديد، وقد توبع وأدين بجريمة التلاعب المعلوماتي[4]. بحكم أن المادة (323-3) من (ق ع ف) تعاقب على كل تعديل غير مشروع في البيانات المعالجة آليًا، فإن هذه الجريمة تقع حتى ولو كان الفاعل مسموحًا له بالدخول إلى النظام أصلاً، لأنه يستوي أن يكون الجاني مسموحًا له أو غير مسموح له بالدخول إلى النظام، لذا قضي بإدانة ومعاقبة هذا المتهم الذي قام بتعديل بيانات بدون وجه حق[5].

ويلاحظ أن جريمة تعديل البيانات بدون وجه حق تختلف تمامًا عن أي جريمة معلوماتية أخرى كإعاقة أو الإخلال بسير النظام المعلوماتي، على الرغم من أن هدف هذه الأخيرة يمكن معه

---

[1]– **الفيروسات:** ظهرت لأول مرة في خمسينات القرن الماضي، حين تحدث عنها عالم الرياضيات "فون نيمان *VON Neman*"، ويعتبر الفيروس كمصطلح قديم في مجال صناعة الحواسب، وهو عبارة عن برنامج يصمم ليدخل إلى الحاسب الآلي مثله كأي برنامج آخر، ولكنه لا يهدف إلى تطوير جهاز الحاسوب، كما تفعل البرامج الأخرى وإنما يهدف إلى إحداث أضرار بنظام الحاسب الآلي، كما له القدرة على ربط نفسه بالبرامج الأخرى. وعمومًا الفيروس هو برنامج يضعه شخص له معرفة واسعة أو علم كاف بعلوم الحواسيب والبرمجة، ومن أهم خصائص الفيروسات هو الإنتقال من جهاز الحاسب إلى آخر، كما لديها القدرة على أن تتكاثر وتتزايد من أجل تشويه والقضاء على برمجيات الجهاز أو النظام المعلوماتي، وهناك عدة طرق للإصابة بالفيروسات والبرامج الخبيثة ومنها زرع الفيروسات بوسائط التخزين التي تنقل الملفات والبرامج، أو عن طريق البريد الإلكتروني وما يحمله من مرفقات أو عن طريق تصفح الصفحات المشبوهة، أو تحميل برامج خبيثة من على شبكة الإنترنت، (أنظر: – **ماجد عمارة:** المسؤولية القانونية الناشئة عن إستخدام فيروس الكمبيوتر، دار النهضة العربية، القاهرة، مصر، د.ت.ن، ص74).

[2]– **رشيدة بوكر:** المرجع السابق، ص101.

[3]– **محمد علي سويلم:** المرجع السابق، ص306.

[4]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص135.

[5]– *Crim, 8 déc 1999, JCP 2000, P 395. NCP 104-E, éd. D. Paris, France, 2009, P 918.*

أن تقع تعديلات للبيانات، بيد أن ثمة فارقٌ بين الجريمتين يتمثل في أن جريمة تعديل البيانات أو إدخال بيانات كاذبة ومغلوطة ليس من شأنه أن يؤدي إلى إعاقة النظام أو الإخلال بسيره الطبيعي، ولكن العكس غير صحيح دائمًا[1].

وبناءً عليه فإن الركن المادي في جريمة تعديل بيانات قائمة على النظام يقوم على عنصر السلوك المجرم المتمثل في تعديل المحتوى المادي والمنطقي للبيانات المبرمجة، فهذا التعديل قد يتخذ صورة الإضافة أو الحذف أو التغيير للبيانات ذاتها، وقد أدخل المشرع الفرنسي هذا النوع من الجرائم إلى طائفة القواعد العامة في تزوير المحررات التي لم تكن ملائمة لمكافحة تلك الصورة من صور العبث والتلاعب بالبيانات[2]، كما أحسن المشرع الجزائري صنعًا عندما أدخل هذا النوع من التجريم لكي يحمي البيانات المبرمجة والمدخلة على النظام حتى تحل محل البيانات المكتوبة في الملفات الورقية في شكلها التقليدي، عندئذٍ يعتبر التلاعب والعبث بها عبارة عن جريمة التزوير المعلوماتي[3].

خلاصة القول:

مما سبق الكلام فيه نجد أنَّ هاته الأفعال الثلاثة الإدخال والإزالة والتعديل المكونة للسلوك الإجرامي في جريمة التلاعب المعلوماتي حسب ما ذكرته المادة (394 مكرر 1) من (ق ع ج) أنها جاءت على سبيل الحصر، وبالتالي فلا تقع تحت طائلة التجريم أي فعل آخر غيرها كنسخ المعطيات أو نقلها...، وإنما يمكن حمايتها جنائيًا عن طريق النصوص التجريمية التقليدية المقررة في قانون العقوبات أو في القوانين الخاصة المكملة له كحق الملكية الفكرية وحق الملكية الصناعية وغيرها من الحقوق الأخرى، كما لا يشترط القانون لقيام الركن المادي لجريمة التلاعب المعلوماتي أن تقع هذه الأفعال الثلاثة شاملة وجملة واحدة، بل يكفي وقوع إحداها لقيام الجريمة.

ثانيًا- النتيجة الإجرامية

تعتبر النتيجة الإجرامية العنصر الثاني بعد السلوك المجرم للركن المادي في جريمة التلاعب المعلوماتي، وهي عبارة عن ذلك الضرر الذي نتج عن السلوك الإجرامي، وهو الأثر الخارجي الذي يتولد عن السلوك، ويحدث تغييرًا يعتد به القانون طبقًا للتصور المادي للجريمة، أما

[1]- **شيماء عبد الغني محمد عطاء الله:** المرجع نفسه، ص138.

[2]- *Crim, 5 Janv 1994, Gaz-Pal, 1996, Somm, 419- 12 déc 1996 Bull, Crim N° 465.*

[3]- راجع المواد من (214 حتى 229) من قانون العقوبات الجزائري، فيما يخص جريمة تزوير المحررات الرسمية والعرفية.

التصور القانوني فهو الإعتداء على مصلحة أو حق يحميهما القانون أو يهددهما بالخطر[1]، وتعتبر جريمة التلاعب بالمعلومات الإلكترونية كغيرها من الجرائم التي يفترض لقيامها وجود النتيجة الإجرامية فيها، وإن إختلفت النتيجة الضارة في هذه الجريمة بحسب نوع الفعل المرتكب إما بالإدخال أو بالإزالة أو بالتعديل.

ففي جريمة التلاعب المعلوماتي والتي تدخل ضمن أهم الجرائم المعلوماتية، فإن النتيجة الإجرامية فيها هو تحريف الحقيقة المعلوماتية من خلال العبث والتزوير في البيانات والمعلومات الموجودة داخل النظام المعلوماتي وما في حكمه من مواقع إلكترونية وشبكات، إذ النتيجة هي ذلك الأثر المادي المترتب عن إتيان أحد الأفعال غير المشروعة السالفة الذكر والتي تمثل الإعتداء على خصوصيات الناس ومعلوماتهم بتعديلها أو حذفها أو تحريفها بما يخالف القانون.

وهكذا نجد أن النتيجة الضارة في جريمة التلاعب المعلوماتي غير المصرح به في المساس بالبيانات والمعلومات، هي وقوع ضرر فعلي على هذه البيانات والمعلومات، ويكون ذلك بإحداث تغيير في حالتها الأصلية إما بالإنقاص أو الإضافة.

ومما تقدم ذكره نستخلص أن جريمة التلاعب المعلوماتي كغيرها من الجرائم الإلكترونية الأخرى، يفترض فيها وجود النتيجة الإجرامية كأساس لقيام الركن المادي، ومع ذلك تثير النتيجة الإجرامية في هذا النوع من الجرائم مشاكل عديدة، نذكر منها على سبيل المثال النطاق المكاني والزماني في تحقق النتيجة، فمثلاً لو قام أحد المجرمين في دولة ما بإختراق النظام المعلوماتي الخاص بأحد البنوك التابع لدولة أخرى، وراح يعبث بالبيانات الموجودة على هذا النظام، فهنا يثير إشكالاً بالنسبة إلى مكان ووقت حدوث النتيجة، بالإضافة إلى مسألة القانون الواجب التطبيق في هذا الشأن، وهي من الصعوبات التي تواجه الفكر القانوني المعاصر فيما يتعلق بالنتيجة الإجرامية ذات البعد الدولي[2].

الفرع الثالث: الركن المعنوي للجريمة

ذكرنا سابقًا وفي موضع شبيه من هذا أن الركن المعنوي للجريمة المعلوماتية عمومًا يتكون من صورتين هما "القصد الجنائي العام أو الخاص"، وكذا "الخطأ غير العمدي"، ولو نظرنا إلى كل

[1]– **لورنس سعيد الحوامدة:** الجرائم المعلوماتية أركانها وآلية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، جامعة الرياض، السعودية، 2016، ص20.

[2]– **خيرت علي محرز:** التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، الإسكندرية، مصر، 2012، ص123.

من الصورتين نجدهما يعبّران عن العلاقة النفسية التي تربط بين شخصية الجاني وماديات الجريمة، وأن كلاهما محل للوم والمساءلة من طرف القانون[1]، وأن الفرق بينهما يكمن في مقدار سيطرة الجاني على العناصر المادية للجريمة ومدى فهمه لخطورتها[2]، بمعنى أن المقارنة بين القصد الجنائي والخطأ غير العمدي هي أن الأصل في الجرائم أنها قصدية وعمدية والإستثناء أنها جرائم خطأ غير عمدية[3].

ومن هذا المنطلق يتفق الفقه الجنائي على أن جريمة التلاعب المعلوماتي تعد من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي[4]، حيث أوضحت جميع التشريعات التي تناولت تجريم التلاعب بالمعلومات أن الركن المعنوي لهذه الجريمة يتطلب فيها أن ترتكب عن طريق "الغش"، كما فعله كل من المشرع الجزائري ونظيره الفرنسي، وذكر المشرع المصري عبارة "متعمدًا وبدون وجه حق"، وهو ما يستفاد منه أن هذه الجريمة تقوم بمجرد توافر القصد الجنائي العام بعنصريه العلم والإرادة.

فعنصر العلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي الذي يقدم عليه، أي أن يعلم أنه يقوم بإتيان سلوك إيجابي يتمثل في إدخال أو إزالة أو تعديل غير مصرح له القيام به على معلومات مخزنة داخل نظام المعالجة الآلية للمعطيات[5]، أما إذا تم ذلك برضاء من صاحب النظام وتحت علمه أو عن طريق الخطأ غير المقصود، فهنا تنتفي المسؤولية الجنائية[6]، كما يتعين على الجاني أن

---

[1]– **مروان بن مرزوق الروقي:**القصد الجنائي في الجرائم المعلوماتية، مكتبة القانون والإقتصاد، الرياض، السعودية، 2013، ص38.

[2]– **صالح نبيه صالح:** النظرية العامة للقصد الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص 20.

[3]– أنظر كل من: (– **رمسيس بهنام:** شرح قانون العقوبات العام، منشأة المعارف، الإسكندرية، مصر، 1971. – **عوض محمد عوض:** قانون العقوبات، القسم العام، منشأة المعارف، الاسكندرية، مصر، 2000. – **جلال ثروت:** النظرية العامة لقانون العقوبات، مؤسسة الثقافة الجامعية، الإسكندرية، مصر، د.ت.ن. – **مأمون محمد سلامة:** قانون العقوبات، القسم العام، دار الفكر العربي، القاهرة، مصر، د.ت.ن. – **أمين مصطفى محمد السيد:** شرح قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011).

[4]– **محمد علي سويلم:** المرجع السابق، ص309.

[5]– **رشيدة بوكر:** المرجع السابق، ص105.

[6]– تطبيقًا لذلك قضت أحد المحاكم الفرنسية ببراءة المتهم الذي قام ببيع مجلة ملحقة بقرص ممغنط يحمل بداخله فيروسات إلى أحد مندوبي شركة تجارية، مما أدى إلى تدمير الكثير من البيانات المخزنة داخل النظام المعلوماتي لهذه الشركة، كما أن محكمة الإستئناف في نفس القضية إستندت في قرار التبرئة على أساس أن المتهم لم يكن ليعلم بوجود هذه الفيروسات داخل القرص المرفق مع المجلة، أي عدم توافر نية الغش لديه، كما رأت محكمة النقض في ذات القضية أن نية الغش يمكن إستخلاصها من واقعة الإدخال كإستعمال قنبلة معلوماتية أو فيروس خبيث يدل على نية الغش لدى المتهم بشرط أنه يعلم بذلك مسبقًا. (أنظر: – **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص138).

يعلم بخطورة فعله على محل الجريمة الذي يناله هذا المساس والإعتداء، وأن من شأن أفعاله هذه أن تؤدي إلى نتيجة جد خطيرة وهي تغيير الحقيقة المعلوماتية[1].

كما ينبغي أن تتجه إرادته إلى إرتكاب أحد هذه الأفعال التبادلية الواردة بالنص، فإذا إنتفت هذه الإرادة إنتفى معها القصد الجنائي، كما لو حدث الفعل نتيجة الإصطدام في تشابه المعلومات المراد تعديلها أو إزالتها مما أدى إلى تغيير حقيقتها، أو حدث ذلك نتيجة الإكراه الذي يعدم الإرادة[2]، ولا أهمية هنا للباعث على السلوك الإجرامي، إذ لا يعتد القانون بأي منها[3].

أما بالنسبة للقصد الجنائي الخاص فإننا من خلال قراءتنا للنصوص التشريعية السابقة يتضح أنها لم تستخدم أية عبارات تدل على تطلب المشرع للقصد الجنائي الخاص، أو أية نية خاصة كنية الإنتقام[4] أو مجرد اللهو والتسلية، وهو الأمر الذي يستفاد منه أن هذه الجريمة تقوم بمجرد توافر القصد الجنائي العام، وهذا ما إستقر عليه القضاء الفرنسي وأكده في عدة أحكام له مستخدمًا في ذلك عبارة "سوء النية"[5]، وبالتالي لا يشترط لقيامها توافر نية الإضرار بالشخص صاحب النظام، وإن كان الضرر قد يتحقق في الواقع وفي كل الأحوال نتيجة إتيان النشاط الإجرامي، إلا أنه ليس عنصرًا في قيام الجريمة[6].

المطلب الثاني: العقوبات المقررة لجريمة التلاعب المعلوماتي

يبدو أن المشرع الجنائي سواءً الجزائري أو المقارن، لكي يعطي مفهومًا واسعًا لفكرة الحماية الجنائية للمنظومة المعلوماتية تدرج في وضع سياج متكامل ومترابط بتصور السلوكيات التي تنطوي على أفعال محددة قد يقدم عليها الجناة وتشكل خرقًا أو مساسًا بقدسية الحياة الخاصة للأفراد أو لمؤسسات الدولة والموجودة داخل النظم المعلوماتية من بيانات ومعلومات وبرامج وكل ما يتبعها من نتاج فكري، ذلك أنه وإن إعتبر المشرع أن مجرد الدخول إلى المنظومة المعلوماتية أو في جزء منها أو حتى في البقاء داخلها بطرق تدليسية يشكل جريمة في حد ذاته، ودون إقترانه بأي تصرف آخر.

---

[1]– **حسني الجندي:** التشريعات الجنائية الخاصة، المرجع السابق، ص123.

[2]– **محمد خليفة الملط:** الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص549. – **مدحت رمضان عبد الحليم:** المرجع السابق، ص61.

[3]– **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي، المرجع السابق، ص222.

[4]– **رشيدة بوكر:** المرجع السابق، ص106.

[5]– *Cass. Crim, 8 décembre 1999. Cass, Crim, 5 Janvier 1994.*

[6]– **خثير مسعود:** المرجع السابق، ص125.

كما تفطن المشرع إلى تصور ما قد يترتب عن فعل الدخول أو البقاء من المساس بالمعطيات أو البيانات المخزنة من خلال التجوال في النظام، وما قد يترتب على ذلك من إدخال أو إزالة أو تعديل لهذه المعلومات، سواءً كان هذا المساس عن عمد أو عن غير عمد[1].

من هذا المنطلق بادر المشرع الجنائي بتقرير عقوبات أصلية (فرع أول) وأخرى تكميلية (فرع ثاني) متى توافرت أركان هذه الجريمة على النحو السابق بيانه.

الفرع الأول: بالنسبة للعقوبات الأصلية

يعاقب المشرع الجزائري على هذه الجريمة بعقوبة الجنحة، مسايرًا في ذلك ما ذهب إليه نظرائه من المشرعين الفرنسي والمصري.

فنجد نص المادة (394 مكرر 1) من (ق ع ج) والتي تعاقب على هذه الجريمة بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة مالية من 500000 دج إلى 4000000 دج[2].

أما المشرع الفرنسي فيعاقب على هذه الجريمة بموجب نص المادة (323-3) من (ق ع ف) والتي تعاقب عليها بالحبس لمدة خمسة (5) سنوات وبغرامة قدرها 150000 يورو، وفي حالة ما إذا أُرتكبت هذه الجريمة ضد نظام معالجة البيانات ذات الطابع الشخصي التي تنفذها الدولة، فهنا تشدد عقوبة الحبس بسبعة (7) سنوات وغرامة مالية قدرها 300000 يورو[3].

كما عاقب المشرع المصري بموجب نص المادة (17) من القانون رقم (175 لسنة 2018) على هذه الجريمة بالحبس مدة لا تقل عن سنتين (2)، وبغرامة لا تقل عن مائة ألف 100.000 جنيه ولا تجاوز خمسمائة ألف 500.000 جنيه، أو بإحدى هاتين العقوبتين[4].

مع العلم هنا أن المشرع الجزائري يشدد من عقوبة هذه الجريمة متى أُرتكبت الأفعال الماسة بالمعلومات المعالجة آليًا والمخزنة داخل النظام التابع لمؤسسات الدولة، وهذا حسب ما جاء في سياق نص المادة (394 مكرر 3) من (ق ع ج) بقولها: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا أُستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد"[5].

---

[1]- **زيدان زيبحة:** المرجع السابق، ص53.

[2]- أنظر في ذلك: **الملحق رقم (05).**

[3]- أنظر في ذلك: **الملحق رقم (03).**

[4]- أنظر في ذلك: **الملحق رقم (04).**

[5]- أنظر في ذلك: **الملحق رقم (05).**

ومع ذلك نجد أن المشرع الجزائري من خلال هذه المادة على الرغم من إشارته إلى مضاعفة العقوبة بالتشديد، إلا أنه لم يحدد مقدارها، على عكس ما فعله المشرع الفرنسي حينما شدد العقوبة وحدد مقدارها سواءً العقوبة السالبة للحرية أو العقوبة المالية، وعليه يفهم أن المشرع الجزائري ترك مقدار مسألة تشديد العقوبة خاضع للسلطة التقديرية لقاضي الموضوع.

دون أن ننسى الإشارة هنا أن هذه العقوبات مقررة للشخص الطبيعي، أما الشخص المعنوي فيعاقب وفق القواعد المقررة في قانون العقوبات، وكذا حسب ما نصت عليه المادة (394 مكرر 4) من (ق ع ج) بقولها: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"[1].

إضافة إلى معاقـــب الشريك في هذه الجريمة بموجـــب نص المادة (394 مكرر 5) مـــن (ق ع ج) بقولها: "كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"[2].

كما تشمل السياسة العقابية في هذه الجريمة كل محاولة أو شروع في إرتكاب التلاعب بالمعلومات المخزنة داخل النظام، وهذا حسب نص المادة (394 مكرر 7) من (ق ع ج) بقولها: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"[3].

الفرع الثاني: بالنسبة للعقوبات التكميلية

علاوة على العقوبات السابق الإشارة إليها، يمكن للقاضي توقيع عقوبات أخرى تكميلية على مرتكب جريمة التلاعب المعلوماتي، وذلك حسب نص المادة (394 مكرر 6) من (ق ع ج) بقولها: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقًا لهذا القسم، علاوةً على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أُرتكبت بعلم مالكها"[4].

[1]– أنظر في ذلك: **الملحق رقم (05)**.
[2]– أنظر في ذلك: **الملحق رقم (05)**.
[3]– أنظر في ذلك: **الملحق رقم (05)**.
[4]– أنظر في ذلك: **الملحق رقم (05)**.

رأي الباحث:

يتضح من العرض السابق لصور التلاعب المعلوماتي من إدخال وتعديل وإزالة، أن موقف كل من المشرع الجزائري والتشريعات المقارنة حيالها إتسم بالبساطة، إذ لم تتعمق جميعها في تفاصيل هذه الجريمة، كأن تحدد مثلاً الجهة التي يتبع لها النظام محل الجريمة، ضف إلى ذلك أن تلك الصور التي أوردها المشرع الجزائري في نص المادة (394 مكرر 1) جاءت على سبيل الحصر، وهو الأمر الذي يضيق من نطاق التجريم، فكان الأولى بالمشرع الجنائي أن يضع معيارًا عامًا يجرم به كل ما من شأنه أن يمس بسلامة وتكامل المعلومات المعالجة آليًا.

كذلك نريد أن نوضح شيء مهم هنا وهو أن الأفعال السالفة الذكر والتي تشمل جريمة التلاعب المعلوماتي لا يتم المعاقب عليها إلا إذا أُرتكبت بدون تصريح مسبق، ولا يهم في ذلك إذا كان للشخص المرتكب للجريمة له تصريح بالدخول أو البقاء أولاً، بمعنى أن النشاط الإجرامي في هذه الجريمة يمكن أن يرتكبه شخص له الحق في الدخول إلى النظام، كما يمكن أن يرتكب بواسطة شخص ليس له أصلاً حق الدخول إلى النظام.

كما سبق أيضاً وأن أوضحنا أن المجرم المعلوماتي على خلاف حال الدخول إلى النظام أو البقاء فيه عن طريق الخطأ أو القصد، قد يأتي على مرحلة لاحقة لذلك، وهو قيامه بإدخال معطيات أو برامج جديدة أو معلومات وهمية أو مغلوطة من شأنها إرباك الكيان المنطقي للنظام، وبالتالي تغيير الحقيقة المعلوماتية التي يحتويها بداخله، فالمجرم المعلوماتي يأتي هنا على أخطر المراحل في الجريمة الإلكترونية، فهي التي تمهد لمرحلة أخطر منها وهي مرحلة إستغلال المعلومات المزيفة والتي من شأنها إلحاق الأذى والضرر بالغير.

وما يمكن إستخلاصه هنا أن المشرع الجزائري ساير نظيره المشرع الفرنسي فيما إنتهجه من تصور وفهم لجريمة التلاعب المعلوماتي مبرزًا مراحلها ومدى خطورتها، وفرضه عقوبات حسب خطورة تلك الأفعال، وإن كان هناك إختلاف بسيط بينهما في مقدار العقوبة السالبة للحرية، وفي قيمة الغرامة المالية.

كما يتضح لنا من نص المادة (394 مكرر 1) أن المشرع الجزائري لم يتوسع كثيرًا في تجريم الأفعال الواقعة على المعطيات الموجودة داخل النظام المعلوماتي، وحصرها فقط في ثلاثة أفعال سواء بالإدخال أو المحو أو التعديل، على الرغم من أن الواقع العملي كشف عن أفعال إجرامية عديدة إزدادت إستعمالاتها كثيرًا في الآونة الأخيرة في ظل إنتشار تقنية المعلومات.

وقد أحسن ما فعله المشرع الجزائري حين إعتبر هذه الجرائم من جرائم الخطر بغض النظر عن تحقيق نتيجة مادية محسوسة، لأن الجاني يقوم بالعدوان المحتمل والتهديد بالخطر في سرية المعلومات وسلامتها، كما تتحقق هذه الجريمة بإرتكاب واحد من هذه الأفعال ولا يشترط توافرها مجتمعة، إضافة إلى أن الحماية الجنائية للمعطيات والمعلومات حسب نص المادة (394 مكرر 1) أعلاه، تتحقق فقط للمعطيات والمعلومات الموجودة داخل النظام، وبالتالي لا تشمل هذه الحماية المعطيات والمعلومات الموجودة خارج النظام والتي تمت حمايتها بنص المادة (394 مكرر 2) كما سنراه لاحقًا في الفصل الموالي من هذا الباب.

الفَصل الثّانِي

جريمة الإعتداء على المعطيات الموجودة خارج النظام المعلوماتي

الفصل الثاني: جريمة الإعتداء على المعطيات الموجودة خارج النظام المعلوماتي

تمهيد وتقسيم:

لم يكتفي المشرع الجنائي الوطني وحتى المقارن بحماية المعطيات الموجودة داخل النظم المعلوماتية، بل تعداها إلى بسط حماية للمعطيات الموجودة خارجها، وذلك من خلال تجريم كل أفعال التعامل غير المشروع مع هذه المعطيات والمعلومات الناتجة عن إحدى الجرائم المنصوص عليها كما سبق الإشارة إليها سلفاً، والهدف الرئيسي من ذلك هو الوقاية قدر المستطاع من هذه الجرائم والتخفيف من آثارها لما تمثله من خطورة بالغة على الحقوق والمصالح المعلوماتية المحمية قانوناً.

فكان لزامًا في ظل الإعتداءات والإنتهاكات المتكررة والواقعة على الأشخاص والأموال في الفضاء الإلكتروني أن تظهر مقاومة تشريعية، وهذا من خلال إصدار العديد من النصوص القانونية التي تجرم كل الأفعال الماسة بالبيانات والمعلومات الخاصة بالأشخاص والأموال والتي توجد خارج المنظومة المعلوماتية.

وعليه فإنه من خلال هذا الفصل سوف نتكلم عن جريمتين في غاية الأهمية حسب ما ذكره المشرع الجزائري في القسم السابع مكرر من قانون العقوبات، مع تبيان رأي القانون المقارن في هاتين الجريمتين، وذلك من خلال مبحثين إثنين على التوالي:

المبحث الأول: جريمة التعامل غير المشروع في معطيات النظام المعلوماتي.

المبحث الثاني: جريمة الإيواء المعلوماتي عبر خدمات شبكة الإنترنت.

المبحث الأول: جريمة التعامل غير المشروع في معطيات النظام المعلوماتي

تمهيد وتقسيم:

ما يبرر مسلك المشرع الجنائي حين تجريمه التعامل غير المشروع في معطيات النظام المعلوماتي، هو أن المعطيات محل هذه الجريمة قد لا تكون مخزنة داخل نظم المعالجة الآلية لهذه المعطيات، وإنما تكون موجودة خارجها على وسائط إلكترونية أخرى سواءً كانت ثابتة عليها أو متحركة، أي مرسلة بين نظم المعلومات وأجهزتها، والغرض من ذلك هو أن تمتد الحماية الجنائية لمختلف المعطيات الصالحة لإرتكاب جريمة أو المتحصلة من إرتكاب إحدى الجرائم المعلوماتية[1].

ولقد جرم المشرع الجزائري والمقارن جملة من الأفعال الصالحة للتعامل في المعطيات بطريقة غير مشروعة، ولم يكتفي المشرع بهذه الأفعال فقط بل جرم كذلك التعامل في معطيات محصلة من إحدى الجرائم المنصوص عليها قانونًا.

وهذا ما سوف نعالجه من خلال هذا المبحث، وذلك بتحديد أهم أركان هذه الجريمة، ثم تبيان أهم العقوبات المقررة لها، وهذا وفق مطلبين إثنين هما على التوالي:

المطلب الأول: أركان جريمة التعامل غير المشروع في معطيات النظام المعلوماتي

المطلب الثاني: العقوبات المقررة لجريمة التعامل غير المشروع في معطيات النظام المعلوماتي

[1]– **غنية باطلي:** المرجع السابق، ص184. – **يزيد بوحليط:** المرجع السابق، ص191. – **لينا محمد الأسدي:** المرجع السابق، ص63.

المطلب الأول: أركان جريمة التعامل غير المشروع في معطيات النظام المعلوماتي

سوف نتطرق إلى أركان هذه الجريمة بداية بالركن الشرعي (فرع أول)، ثم الركن المادي (فرع ثاني) وأخيرًا الركن المعنوي (فرع ثالث).

الفرع الأول: الركن الشرعي للجريمة

للحديث عن الركن الشرعي لجريمة التعامل غير المشروع في معطيات النظام المعلوماتي سواءً الصالحة منها لإرتكاب جريمة أو المتحصلة من إرتكاب جريمة، كما سوف نراه لاحقاً في الركن المادي لهذه الجريمة، لابد لنا هنا أن نتطرق إلى كل من نص التجريم (أولاً)، ثم الحديث عن علة هذا التجريم (ثانياً).

أولاً- بالنسبة لنص التجريم

لقد أشارت المذكرة التفسيرية لإتفاقية بودابست في المادة السادسة من (إ.أ.م.إ.م) على أن: "جريمة التعامل غير المشروع في معطيات النظام يتطلب لإرتكابها حيازة وسائل الولوج كأدوات القرصنة أو أي أدوات أخرى، وأن هناك دفعًا قويًا للحصول على هذه الوسائل لأغراض إجرامية، مما قد يؤدي إلى خلق نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات، ومن أجل وقاية أكثر فعالية من هذه المخاطر فإنه يجب على قانون العقوبات أن يحظر هذه الأفعال الراجحة الخطورة من المنبع قبل إرتكاب الجرائم المشار إليها في المواد من (02) إلى (05)"[1]، وهذا المسلك إتبعته العديد من التشريعات الجنائية الوطنية الداخلية.

كما ذكرت المادة التاسعة من الإتفاقية العربية (إ.ع.م.ج.ت.م) تحت عنوان "جريمة إساءة إستخدام وسائل تقنية المعلومات"، حيث نصت هذه المادة على أن: "إنتاج أو بيع أو شراء أو إستيراد أو توزيع أو توفير أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة، حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد إستخدامها لغايات إرتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة"[2]. وهو نفس المسلك الذي إتبعته العديد من التشريعات الجنائية المقارنة[3].

---

[1]- *Rapport explicatif de la convention sur la cybercriminalité, Op. Cit, P 14.*

[2]- أنظر في ذلك: **الملحق رقم (02)**.

[3]- فنجد على سبيل المثال: نص المادة (6) من القانون البحريني رقم (60 لسنة 2014) بشأن جرائم تقنية المعلومات، وكذا نص المادة (14) من القانون الإماراتي رقم (5 لسنة 2012) بشأن مكافحة جرائم تقنية المعلومات.

فنجد المشرع الفرنسي قد نص هو الآخر على مجموعة من الأفعال يؤدي إتيانها إلى إرتكاب جريمة التعامل غير المشروع في معطيات النظام سواءً كانت معلومات صالحة لأن ترتكب بها إحدى الجرائم أو أنها متحصلة من هذه الجرائم، والتي تمس بسرية المعلومات أو سلامتها أو إتاحتها ووفرتها وذلك بموجب المادة (323-3-1) من (ق ع ف)[1]، والتي جاء نصها كما يلي: "كل من يقوم بدون مبرر قانوني بإستيراد أو حيازة أو توفير أو وضع تحت التصرف تجهيزات أو أدوات أو برنامج معلوماتي أو كل معطيات مصممة أو معدة لإرتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد (323-1) إلى (323-3) يعاقب...".

كما نص المشرع المصري من جهته في المادة (22) من القانون رقم (175 لسنة 2018) في شأن جرائم تقنية المعلومات[2] على أنه: "يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو إستورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض إستخدام أي منها في إرتكاب أو تسهيل إرتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الإستخدام أو التسهيل أو الإخفاء"[3].

وإلى جانب هؤلاء المشرعين نجد كذلك المشرع الجزائري الذي نص على نفس الأفعال وبنفس المعنى تقريبًا، وذلك بموجب نص المادة (394 مكرر 2) من (ق ع ج) بقولها: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج كل من يقوم عمدًا وعن طريق الغش بما يأتي:

---

[1]– ***Article (323-3-1) : Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25***

- « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

[2]– يطلق المشرع المصري على هذا النوع من الجرائم مصطلح "الجرائم المرتكبة بواسطة البرامج والأجهزة والمعدات المستخدمة في إرتكاب إحدى جرائم تقنية المعلومات".

[3]– أنظر في ذلك: **الملحق رقم (04).**

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[1].

ثانيًا– بالسنبة لعلة التجريم

تتجسد علة التجريم بوضوح في هذه النصوص السالفة الذكر، وذلك من ناحيتين إثنتين هما:

أ– الناحية الأولى: هو إرتباط تجريم عديد الأفعال والسلوكيات المتعلقة بالتعامل غير المشروع في معطيات النظام، والتي يمكن أن ترتكب بها إحدى الجرائم المعلوماتية، حيث نلمس أن المشرع الجزائري والمقارن مراده حماية المعطيات المعالجة وهي خارج النظام المعلوماتي[2]، فهو لم يشترط أن تكون هذه المعطيات داخل النظام، وعليه فإن علة التجريم هنا شملت المعطيات في أي شكل كانت عليه[3].

ب– الناحية الثانية: فلها دور وقائي أكثر منه علاجي، وذلك من خلال النص بمنع إستخدام أي من هذه المعطيات في إرتكاب أو تسهيل إرتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون أو إخفاء آثارها أو أدلتها، أو ثبت ذلك الإستخدام أو التسهيل أو الإخفاء[4].

والعلة من تجريم هذه التعاملات غير المشروعة والماسة بالمعطيات المعالجة آلياً والموجودة خارج النظام المعلوماتي، هي أنها جرائم خطر يهدف المشرع من ورائها إلى تفادي وقوع ضرر بمعنى أن المشرع يهدف من خلال تجريمه هذه الأفعال هو القضاء قدر الإمكان على آثار جريمة الدخول أو البقاء غير المشروع، وكذا جريمة التلاعب بالمعلومات – كما سبق بيانه – حيث قد تسفر هاتين الجريمتين عن إكتشاف معطيات ومعلومات معينة يكون من الخطر الحصول عليها أو تواجدها في حوزة غير صاحبها، أو إستعمالها أو إفشائها أو حتى نشرها، فأراد المشرع من كل ذلك أن يضيق الخناق إلى أكبر حد ممكن من دائرة الأشخاص الذين يمكنهم التعامل في هذه المعطيات بطريقة غير مشروعة حفاظًا على سريتها وخصوصيتها[5].

---

[1]– أنظر في ذلك: **الملحق رقم (05).**

[2]– أنظر في ذلك نص المادة (4) من القانون رقم (09-04). **الملحق رقم (06)**

[3]– **نائلة عادل محمد قورة:** المرجع السابق، ص285.

[4]– **محمد علي سويلم:** المرجع السابق، ص346.

[5]– **محمد خليفة:** المرجع السابق، ص194.

الفرع الثاني: الركن المادي للجريمة

إنَّ المحل في هذه الجريمة وكما أشارت إليه المادة (394 مكرر 2) من (ق ع ج) هو المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية والتي يمكن أن ترتكب بها جرائم معلوماتية أخرى، وإن كان المشرع الجزائري قد قصر المحل على المعطيات فقط ككيان معنوي، فنجد في المقابل أن المشرع الفرنسي كان أكثر توسعًا منه بموجب المادة (323-3-1) أن الأفعال المجرمة يمكن أن تقع على الكيان المادي من تجهيزات أو أدوات حاسوباتية، أو كيانها المعنوي من برامج ومعطيات مصممة أو معدة لإرتكاب واحدة أو أكثر من الجرائم السابقة الذكر[1] والمشرع الفرنسي أراد بهذا الأمر التوسع ليشمل كل الوسائل التي يمكن إستخدامها في إرتكاب هذه الجريمة، فإستعمل مصطلح "تجهيزات وأدوات"، والتي يقصد بها الوسائل المادية، أما مصطلح إلى البرامج والمعطيات، فيقصد بها الوسائل غير المادية أي المعنوية أو المنطقية.

فالعنصر المادي أو الركن المادي يتحقق بقيام المجرم المعلوماتي بإرتكاب نشاط إجرامي مادي من مجموع الأفعال الخطيرة التي نصت عليها المادة (394 مكرر 2) وهذه الأفعال تشمل مختلف أشكال التعامل الواقعة على معطيات النظام، والتي قد تكون بإستعمال وإستخدام هذه المعطيات في إرتكاب إحدى الجرائم، أو أنها معطيات محصلة من جرائم أخرى.

وعليه نميز هنا في هذا الفرع بين صورتين إثنتين وهما: التعامل في معطيات صالحة لإرتكاب جريمة ماسة بنظام المعلومات (أولاً) والتعامل في معطيات متحصلة من جريمة ماسة بنظام المعلومات (ثانياً).

أولاً: التعامل في معطيات صالحة لإرتكاب جريمة ماسة بنظام المعلومات

تتحقق هذه الصورة حسب ما ذكرته الفقرة الأولى من المادة (394 مكرر 2) من (ق ع ج) بأفعال وسلوكيات مختلفة، وهي أفعال على قدم المساواة في تحقيق النشاط الإجرامي المكون للركن المادي لهذه الجريمة[2]، ولا يشترط المشرع أن تقع كل هذه الأفعال مجتمعة بل يكفي أن يقع منها فعل واحد على الأقل للقول بتوافر السلوك الإجرامي الذي يكشف عن وجود صلة بين الجاني وتعامله غير المشروع بمعطيات النظام[3].

---

[1]- **غنية باطلي:** المرجع السابق، ص185.

[2]- **رشيدة بوكر:** المرجع السابق، ص108.

[3]- **غنية باطلي:** المرجع نفسه، ص187.

فهذه المعطيات وإن كانت صالحة لإرتكاب جريمة من الجرائم المعلوماتية المنصوص عليها فإنها قبل ذلك تمر بعدة مراحل حتى تصل ليد الفاعل فيرتكب بها جريمة، وتبدأ هذه المراحل إما بأعمال التصميم أو البحث فيها أو تجميعها وصولاً إلى جعلها تحت تصرف الغير وذلك بتوفيرها أو نشرها أو الإتجار فيها[1].

أ- التصميم *La Comception*: التصميم هو عملية إبداعية لإيجاد حل للمشكلة، ومصطلح "تصميم" يطلق تحديدًا على المرحلة السابقة في التعرف على تفاصيل المشكلة، ثم يبدأ بعد ذلك في جمع هذه المتطلبات والمواصفات التي حددتها مرحلة التصميم، ولا يقصد بهذه المرحلة تصميم الشكل المظهري للبرنامج فقط، بل تصميم البرنامج كبنية وإنشاء المخطط التفصيلي لمتطلبات النظام الذي يوافق ما تم تحليله وتحضيره في مرحلة تحليل النظام *Analysis System*[2].

ويتمثل هذا الفعل في تصميم وإعداد معطيات وبرامج صالحة لإرتكاب الجريمة، وهو عمل يقوم به في الأغلب المتخصصون في مجال تقنية المعلومات والمختصون في مجال البرمجيات وهم المبرمجون أو مصممي البرامج[3]، أي الذين لديهم قدرات ومهارات فنية عالية في تصميم برامج من أجل الوصول إلى نظم المعالجة الآلية كتصميم البرامج الخبيثة *Les programmes virus* لأهداف تخريبية مثل البرامج الفيروسية والقنابل المنطقية والموقوتة[4]، أو تصميم برامج الإختراق أو إنشاء مواقع وهمية لإستعمالها في القرصنة الإلكترونية[5]، أو تغيير تصاميم موقع إلكتروني[6] خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

---

[1]- **زيدان زيبحة:** المرجع السابق، ص59.

[2]- **جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي:** مرجع سابق، ص148.

[3]- **ملياني عبد الوهاب،** مرجع سابق، ص197.

[4]- **القنابل المنطقية *Bombe logique*:** عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام المعلوماتي وكيانه المنطقي بغرض تسهيل عمل معلوماتي غير مشروع.
- **أما القنابل الموقوتة (الزمنية) *Bombe à retardement*:** فهي عكس القنبلة المنطقية، فهي تثير حدثًا ما في لحظة زمنية محددة بالساعة واليوم والسنة، ويتم إدخالها في برنامج مصمم وتنفذ في أجزاء من الثانية أو ثواني أو دقائق وفقًا للتاريخ المحدد سلفًا، وبمعنى آخر أنه يمكن لأي خبير في تصميم وصناعة البرمجيات أن يقوم بزراعة القنبلة إذا كان يضمر شرًا للنظام المستهدف. (أنظر أكثر: - **محمد سامي الشوا:** ثورة المعلومات، المرجع السابق، ص 195. - **محمد علي العريان:** الجرائم المعلوماتية، المرجع السابق، ص120).

[5]- **محمد خليفة:** المرجع السابق، ص200. - **يزيد بوحليط:** المرجع السابق، ص192. - **غنية باطلي:** المرجع السابق، ص187.

[6]- تغيير تصاميم موقع إلكتروني يقصد به تغيير شكل أو حالة الموقع الإلكتروني، أو إحداث تعديل في تصاميم هذا الموقع، والذي يكون تابع لإحدى الشركات أو المؤسسات أو حتى الأشخاص الطبيعية (أنظر نص المادة (19) من القانون المصري رقم (175 لسنة 2018). أنظر في ذلك: **الملحق رقم (04).**

ومن مرادفات مصطلح التصميم نجد الإصطناع أو الصنع، وكذا التقليد والإستنساخ وغيرها كثير، ونحن هنا سوف نركز على بعض هذه المرادفات بشيء من الشرح، ونذكر منها على سبيل المثال لا الحصر بعض مرادفات التصميم ومنها:

1. إصطناع البرامج *Logiciel artificiel*: ومعناه البرامج المصطنعة وهو عبارة عن عملية تحويل مادة أولية إلى شيء صالح للإستعمال، أي عملية مزج عدة مواد للحصول على الجهاز أو البرامج وغيرها، وهو يدخل بصفة عامة في عملية الإنتاج[1]، ويقصد بالإنتاج أي إستخراج الأجهزة أو البرامج وغيرها من الأدوات الإلكترونية كبطاقات التأمين أو أكواد المرور أو الشفرات[2] أو أي بيانات مماثلة أو أي جزء منها مما يسمح بإكثارها، ويعني ذلك إستحداث وتصميم هذه الأدوات، أي إيجاد مادة لم تكن موجودة من قبل[3].

فالإصطناع معناه إنشاء شيء بأية وسيلة على نحو يجعل من يطلع عليه يعتقد أنه حقيقي وأنه قد صدر ممن ينسب إليه هذا الشيء[4]، ومنه صنع أو خلق المعطيات أو البرامج ونسبتها إلى غير صاحبها[5]، وبذلك هو يختلف عن التقليد، حيث أن هذا الأخير يرد على برنامج موجود من قبل يكاد يشبهه، فالتقليد صورة من صور الإصطناع[6]، بينما الإصطناع هو صنع شيء لم يكون موجودًا من قبل بنية الخداع والإستدراج[7].

وهكذا نفهم أن إصطناع البرامج وغيرها يعني إمكانية قيام بعض الأشخاص المحترفين أم غير المحترفين في المجال المعلوماتي بتصنيع وتشكيل برامج معينة، وذلك من أجل إستخدامها في

---

[1]– **محمد علي سويلم:** المرجع السابق، ص351.

[2]– **التشفير:** عبارة عن عملية تحويل المعلومات أو نظم أو وسائل تقنية المعلومات أو الإتصالات إلى رموز غير مفهومة أو مبعثرة، بحيث يصعب قراءتها أو معرفتها دون إعادتها إلى هيئتها الأصلية بإستخدام أكواد أو كلمات سرية معينة أو أداة التشفير المستخدمة. (أنظر نص المادة الأولى منى القانون البحريني رقم (60 لسنة 2014) بشأن جرائم تقنية المعلومات).

[3]– **سميحة القليوبي:** الملكية الصناعية وفقا لأحكام القانون المصري لحماية الملكية الفكرية رقم (82 لسنة 2002)، دار النهضة العربية، القاهرة، مصر، 2009، ص258.

[4]– **محمد حسين علي محمود:** التزوير بإستخدام الوسائل الإلكترونية، دار النهضة العربية، القاهرة، مصر، 2017، ص47.

[5]– **الإصطناع:** عرفته المادة (291) من قانون العقوبات العراقي بقولها: "الإصطناع إنشاء محرر لم يكن له وجود من قبل ونسبته إلى غير محرره دونما ضرورة لتعمد تقليد محرر بالذات".

[6]– **هشام محمد فريد رستم:** المرجع السابق، ص112.

[7]– وهذا ما جاء في سياق نص المادة (24) من القانون المصري رقم (175 لسنة 2018) في الفصل الثاني منه، تحت عنوان "الجرائم المتعلقة بإصطناع المواقع والحسابات الخاصة والبريد الإلكتروني" بقولها: "يعاقب ... كل من إصطنع بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعي أو إعتباري، فإذا إستخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى ما نسب إليه، تكون العقوبة ... وإذا وقعت الجريمة على أحد الأشخاص الإعتبارية العامة، تكون العقوبة ...". وهذا يدل على الغاية الحقيقية من أسلوب الإصطناع وهو الخداع والإستدراج. أنظر في ذلك: **الملحق رقم (04)**

التخطيط للجريمة ومراقبتها وتنفيذها والإنتهاء منها، كإستعمال أسلوب الفيروس في الإعتداء، فالفيروس عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تعطيه القدرة على ربط نفسه ذاتيًا ببرامج أخرى أو بالنظام المعلوماتي حتى يحقق الأهداف التي يتوخاها الجاني[1].

فصناعة الفيروسات ونشرها هي وسيلة تستخدم لتدمير المعلومات والبيانات أو البرامج أو تعطيل شبكة المعلومات[2]، أو إمكانية قيامه بتغيير وتعديل وحذف البيانات أو محوها، والتي تعد من أخطر الأساليب المستعملة في جريمة التلاعب المعلوماتي[3]، ويشهد هذا النوع من الصناعة والتصميم في إعتدائه على المعطيات تزايدًا مستمرًا نظرًا لوجود وسائل التقنية المعلوماتية العالية بوفرة في المتاجر والأسواق، والتي يتم إقتنائها بسهولة ثم إستخدامها من طرف الكثيرين في النواحي السلبية للبيئة الإلكترونية[4].

2. تقليد البرامج *Logiciel traditionnel*: التقليد هو صنع شيء كاذب يشبه شيئًا صحيحًا، إذن هو صنع برامج كاذبة شبيهة ببرامج صحيحة لنظام آخر، ولا يشترط أن يكون التقليد متقنًا[5]، فقد ينصب التقليد على بعض أجزاء المعطيات أو البرامج بخلاف الإصطناع الذي ينصب على هذه المعطيات والبرامج بأكملها. ويقترن أسلوب التقليد كثيرًا بإحدى طرق التزوير المعلوماتي الأخرى كتقليد إمضاء أو ختم مزور أو تقليد التوقيع الإلكتروني أو البصمة وغيرها[6].

---

[1]– **فضيلة عاقلي:** الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مقال منشور بأعمال المؤتمر الدولي الرابع عشر، تحت عنوان "الجرائم الإلكترونية"، طرابلس، لبنان، في الفترة من 24-25 مارس 2017.

[2]– من أشهرها قضيت **(دودة موريس)**، وقعت أحداثها سنة 1988، حيث تعتبر من الهجمات الكبيرة والخطيرة في بيئة شبكة الإنترنت، حيث تمكن طالب يبلغ من العمر حينها 23 عامًا ويدعى (*Robert Morris*) من إطلاق فيروس عرف بإسمه عبر شبكة الإنترنت، أدى إلى إصابة ستة (6) آلاف جهاز يرتبط مع الشبكة بما يعادل حوالي 60.000 نظام معلوماتي عبر شبكة الإنترنت، من ضمنها العديد من أنظمة المؤسسات والدوائر الحكومية، وقد قدرت الخسائر وقتها لإعادة إصلاح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار أمريكي، إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على هذا الطالب بالسجن لمدة ثلاثة أعوام وغرامة مالية قدرها عشرة آلاف دولار أمريكي. (أنظر: – **يوسف حسن يوسف:** المرجع السابق، ص51. – **يزيد بوحليط:** المرجع السابق، ص177).

[3]– **هلال أحمد:** حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 1999، ص117.

[4]– **محمد علي العريان:** المرجع السابق، ص99.

[5]– **أحمد كيلان عبد الله صكر:** حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي، دكتوراه، كلية الحقوق، جامعة بغداد، العراق، 2007، ص89.

[6]– **مشتاق طالب وهيب النعيمي:** المرجع السابق، ص252.

ومنه تقليد البرامج الإلكترونية، وهو القيام بعمل لا يقوم به سوى صاحب البرنامج أو من يرخص له بذلك، أو هو نقل مصنف لم يسقط في الملك العام من غير إذن من مصممه أو مؤلفه[1]، وهو ما ذهب إليه المشرع الجزائري من خلال تعددات الأفعال والسلوكيات التي تعد من قبيل التصميم، وذلك بموجب المادة (151) من الأمر رقم (03-05) والمتعلق بحق المؤلف والحقوق المجاورة بقوله: "يعد مرتكبًا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة المصنف.
- إستنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة"[2].

ويراد بالتقليد هنا إعداد معطيات أو برامج تشابه معطيات وبرامج نظام آخر ونسبة البيانات التي تضمنها هذا البرنامج المقلد إلى ذلك النظام، ولا يشترط أن يكون التقليد دقيق في صنعه أو متقنًا بل يكفي أن يكون من شأنه أن ينخدع به المتعامل مع هذا النظام أي الشخص العادي[3].

3. إستنساخ البرامج *Clonage de logiciel*: يعد هذا السلوك الإجرامي من أخطر عمليات التصميم في مجال الجرائم المعلوماتية، وذلك لسهولة القيام بها وقلة تكاليفها وإرتفاع مداخيلها، وإستنساخ البرامج أو البرمجيات قد يتم في عدة أشكال وصور بإختلاف شكل ونوع الدعامة الإلكترونية بإعتبارها المصدر المتواجدة فيه هذه البرمجيات[4].

والإستنساخ المقصود هنا يتمثل فقط في إجراء نسخة طبق الأصل للبرامج أو أي وسيلة أو أداة إلكترونية مشابهة، كنسخ القرص المضغوط أو القرص المرن أو القرص الثابت على الجهاز أو أية وسيلة تخزين أخرى، بحيث يدخل في حكم الإستنساخ تثبيت البرمجية *L'installation* على القرص الصلب *Disque Dur* للحاسوب أو النظام، بإعتبار أن عملية التثبيت تستدعي بالضرورة نقل الملفات الموجودة في المصدر الأصلي للبرمجية إلى جهاز آخر غير مرخص به للتثبيت في حكم الإستنساخ غير المشروع[5].

---

[1]- **خثير مسعود:** المرجع السابق، ص88.

[2]- الأمر رقم (03-05) المؤرخ في 19 يوليو 2003، والمتعلق بحقوق المؤلف والحقوق المجاورة، المعدل والمتمم للأمر رقم (73-14) ج ر العدد 44، المؤرخ في 23 يوليو 2003.

[3]- **محمد حسين علي حمودة:** المرجع السابق، ص46.

[4]- **دعامة إلكترونية معناه:** أي وسيط إلكتروني مادي لحفظ وتداول البيانات والمعلومات الإلكترونية، ومنها الأقراص المدمجة، والأقراص الضوئية والذاكرة الإلكترونية وكل ما في حكمها.

[5]- **عمار عباس الحسيني:** المرجع السابق، ص120.

وعمومًا أن المقصود من الإستنساخ هو كل عملية الهدف منها الإعتداء على البرامج محل الحماية بأي طريقة كانت، هذا وغالبًا ما تحدد إتفاقية الترخيص[1] التي ترافق معظم البرمجيات المصنفة ذات الإنتشار العالمي، شروط الإستخدام ما يعد مشروعًا وما لا يعد مشروعًا بالنسبة لإستنساخ البرامج المصنفة، وإعتبرت هذه الإتفاقية أن النسخ يكون غير مشروع إذا تم دون إذن صاحبه أو مالك الحقوق[2].

وإستثناءًا يحق لصاحب البرنامج التنازل عن برنامجه أو عن حق من الحقوق المادية المخولة له، بشرط أن تتعلق هذه الإستثناءات بأغراض تعليمية أو إعلامية غير هادفة لتحقيق الربح، ومن ذلك نورد الإستثناء الصريح الذي نصت عليه المادة (52) من الأمر رقم (03-05) السالف الذكر بأنه: "يعد عملاً مشروعًا بدون ترخيص من المؤلف أو من أي مالك آخر للحقوق، قيام المالك الشرعي لبرنامج الحاسوب بإستنساخ نسخة واحدة من هذا البرنامج أو إقتباسه شريطة أن يكون كل من النسخة أو الإقتباس ضروريًا لما يلي:

- إستعمال برنامج الحاسوب للغرض الذي أُكتسب من أجله ووفقًا للشروط التي كانت قائمة عند إكتسابه.

- تعويض نسخة مشروعية الحيازة من برنامج الحاسوب لغرض التوثيق في حالة ضياعه أو تلفه أو عدم صلاحيته للإستعمال.

كما نصت المادة (53) من نفس القانون على أنه: "ينبغي أن تقتصر الإستعمالات على إستنساخ نسخة واحدة من برنامج الحاسوب أو إقتباسه على الأوجه المنصوص عليها في المادة (52) أعلاه، يجب تدمير كل نسخة مستنسخة من برنامج الحاسوب أو مقتبسة منه عند إنقضاء مشروعية حيازتها[3].

---

[1]- **إتفاقية ترخيص البرامج:** هي العقد القانوني بين المرخص (المؤلف) ومشتري قطعة البرنامج، وهذه الإتفاقية تحدد حقوق المشتري كيف ومتى يمكنه إستخدام البرنامج، كما تقوم بتوفير أي قيود مفروضة على هذا البرنامج، ومعظم إتفاقيات ترخيص البرامج هي في شكل رقمي ولا يتم تقديمها إلى المشتري حتى إكتمال عملية الشراء، ومع ذلك يمكن للمشتري رفض هذه الإتفاقية، وبالتالي التخلي عن حقه في إستخدام البرنامج. (للمزيد حول هذا الموضوع يراجع في ذلك الموقع الإلكتروني: ***ar.theastrologypage.com*** تاريخ التصفح 2019/05/19).

[2]- وهنا إشترط المشرع الجزائري ضرورة وجود إذن كتابي من صاحب البرنامج المصنف يتنازل به عن حقوقه المادية، وبالتالي فالكتابة هنا تعتبر شرط وجود لا شرط إثبات، كما أن الإذن اللاحق لا يمكن أن يأخذ حكم الإذن السابق، لأن موافقة صاحب المصنف بعد تمام جريمة الإستنساخ لا يحول دون متابعة جزائية لمستنسخ البرنامج، أنظر نص المادة (62) من الأمر رقم (03-05) المتعلق بحق المؤلف والحقوق المجاورة، والمشار إليه سلفاً.

[3]- أنظر نص المادتين (52) و (53) من الأمر رقم (03-05) المشار إليه سلفاً.

وبهذا نجد أن المشرع الجزائري قد فصل جيدًا في مسألة التصميم والإستنساخ بالنسبة للبرمجيات وحددها في حالات إستثنائية معينة بموافقة صاحب البرنامج المصنف، حيث أن هذا الإذن أو الترخيص يعد بمثابة عنصر أساسي لقيام الجريمة أو إنتفاؤها[1]، مما يعني أن رضاء أو إذن صاحب البرنامج يعد سببًا من أسباب الإباحة، وبذلك يعتبر عدم رضاء صاحب البرنامج بإستغلال برنامجه عنصرًا في الركن المادي لجريمة التصميم أو الإصطناع أو التقليد أو الإستنساخ[2].

ب- البحث *La Recherche*: على خلاف التشريعات المقارنة والمشار إليها سلفًا، نص المشرع الجزائري في الفقرة الأولى من المادة (394 مكرر 2) من (ق ع ج) على عبارة "... أو بحث... في معطيات... يمكن أن ترتكب بها الجرائم..."، فلم يتبين ما المقصود من مصطلح "البحث" في مفهوم هذه المادة، هل المقصود به البحث عن المعطيات التي يمكن أن ترتكب بها الجريمة، أم البحث في كيفية تصميم البرامج والمعطيات وإعدادها لأن ترتكب بها الجرائم[3].

فالبحث في إطار الخدمات الإلكترونية المقدمة بواسطة الشبكة العنكبوتية وهو ما يسمى ب "محركات البحث *Moteurs de Recherche*"[4]، تعطي للباحث هدف محدد من خلال بحثه، فمحرك البحث يساعده لبلوغ هدفه المنشود من خلال تزويده بالمواقع الإلكترونية المتخصصة ذات الصلة بموضوع بحثه، ومن هنا يظهر لنا أن البحث بهذه الكيفية يتعلق بحق الأفراد في الحصول على المعلومة[5]، وعليه فإنه من منظور الكثير من الفقهاء أن ذلك لا يدخل في إطار المعنى المقصود في المادة (394 مكرر 2)، وبالتالي فالبحث المقصود هو البحث عن كيفية تصميم المعطيات والبرامج وغيرها من الأدوات وإعدادها لإرتكاب الجرائم.

ومن هذا المنطلق فهل كل شخص يشغل أحد محركات البحث الموجودة على شبكة الإنترنت لتقوم بالبحث عن مواقع كيفية صناعة وتصميم الفيروسات وبرامج إختراق أجهزة

---

[1]- **خثير مسعود:** المرجع السابق، ص95.

[2]- **عبد القادر القهوجي:** الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة، الإسكندرية، مصر، 1997، ص28.

[3]- **رشيدة بوكر:** المرجع السابق، ص109.

[4]- **محركات البحث:** عبارة عن برامج مساعدة للحصول على المعلومة بإستخدام الإنترنت، بها كم هائل ومعتبر جدًا من المعلومات، وعندما يأتي في ذهنك عبارة "محركات البحث" يأتي في عقلك موقع "جوجل *google*"، فأصبح جوجل شيء ضروري إستخدامه عندما تقوم بعملية البحث عن المعلومات والمصادر، لذلك قد نجد أن في اللغة الإنجليزية يقال: " *Google.it*" والتي تعني "إبحث عنه في جوجل"، وهذا دليل على أنه شيء أساسي في حياتنا اليومية، ولعل من أشهر محركات البحث العالمية غير جوجل نجد على سبيل المثال: (*Indeed- Aol- Yandex - Bing - Youtube- Mawdoo3*).

[5]- **عبد الوهاب مليانى:** المرجع السابق، ص197.

الحواسيب والنظم المعلوماتية، فهل يعتبر سلوكه هذا فعل مجرم، لذلك لا يمكننا التوسع في فهم وتفسير عبارة "البحث" لأن الأصل أن مسألة البحث عن وسائل إرتكاب الجرائم لا يشكل جريمة في حد ذاتها[1].

وعلى هذا يمكن القول أنى الراجح من قصد المشرع الجزائري بمصطلح "البحث" في معناه هو البحث عن كيفية تصميم المعطيات وإعدادها، وليس مجرد البحث عن هذه المعطيات، لذا جاءت عبارة "البحث" بعد عبارة "التصميم" مباشرة، وإن كان النص قد جاء عامًّا[2].

ج- التجميع *Le Rassemblement*: لا يوجد تعبير أو مصطلح موحد بين التشريعات الجنائية المقارنة للدلالة على معنى هذا الفعل، ففي حين آثر المشرع الجزائري مصطلح "التجميع"، إستعملت تشريعات أخرى مثلاً مصطلح "الحصول" كما فعل ذلك المشرع الفرنسي متأثرًا بإتفاقية بودابست، إلا أن المصطلح المعتمد من طرف المشرع الجزائري نراه أكثر دقة على أساس أن التجميع يقتضي الحصول على أكبر قدر ممكن من المعلومات دون وجود نية إستخدامها، فبمجرد توافرها لدى الجاني أو حيازته لها يكون قد إرتكب الجريمة المعاقب عليها بالمادة (394 مكرر 2) من (ق ع ج).

والتجميع في معناه هو القيام بجمع عدد من المعطيات والمعلومات الحساسة والخطيرة والحصول عليها والإلمام بها، والتي من الممكن أن تستعمل في إرتكاب الجرائم، كما أن المشرع الجزائري إستعمل لفظ "الجمع" بسبب أن تعدد المعلومات بتجميعها يرفع من درجة الخطورة[3]، فما من شك أن الذي يحوز معلومة واحدة لا يشكل خطرًا بقدر ما يشكله من يقوم بتجميع عدد كبير من المعطيات والمعلومات، إذ التجميع حسب نص المادة أعلاه يعكس خطورة الفاعل ومدى قدرته على إرتكاب الجريمة المعلوماتية وسهولة تنفيذها[4].

ومن ذلك تجميع برامج تسمح بتجاوز إجراءات الحماية الأمنية للنظام، والتجميع بهذا المعنى يقتضي بدايةً "حيازة المعلومات، لأن "الحيازة" كمصطلح تندرج ضمن مصطلح "التجميع"، وهذا الأخير أوسع نطاقًا منها، ضف إلى ذلك أن التجميع هو ما يتطلبه النص الجنائي دونما ضرورة لتوافر نية لدى الفاعل بإستعمالها[5].

---

[1]- **غنية باطلي**، المرجع السابق، ص188.

[2]- **محمد خليفة:** المرجع السابق، ص201.

[3]- **يزيد بوحليط:** المرجع السابق، ص192. - **مليانى عبد الوهاب:** مرجع سابق، ص198.

[4]- **غنية باطلي:** مرجع سابق، ص188.

[5]- **رشيدة بوكر:** مرجع سابق، ص110.

فقد إعتبر المشرع الجزائري عملية تجميع أو إلتقاط البيانات بطريقة غير مشروعة بغية إستعمالها لأي غرض كان، بأنه عمل غير قانوني وغير مشروع، سواءً تم جمع هذه البيانات عن طريق أخذها مباشرة من قاعدة التخزين الموجودة على النظام أو عن طريق إلتقاطها ورصدها أثناء تبادلها عبر شبكة الإنترنت أو عن طريق رفعها من على أي وسيط إلكتروني آخر[1].

د- التوفير *Metter à disposition*: يقابل مصطلح "التوفير" مصطلح آخر قريب له في المعنى وهو "الوضع تحت التصرف *Metter à disposition*"، وهو نفس المصطلح الذي إستعملته إتفاقية بودابست في المادة السادسة من (إ.أ.م.إ.م) في عبارة "أي أشكال للوضع تحت التصرف"[2]، وفي نفس السياق نجد المشرع الفرنسي في المادة (323-3-1) من (ق ع ف) نص على مصطلح "التوفير" أو "الوضع تحت التصرف"[3].

كما أن مصطلح "التوفير" يشير إلى مصطلح آخر دقيق في معناه وهو "التزويد *Approvisionnement*"، أي عرض المعلومات وإتاحتها وجعلها في متناول الغير، بل وتحت تصرفه وحيازته، ومنه تهيئة وتيسير وتقديم الأجهزة أو المعدات أو البرامج وكل المعطيات والمعلومات غير المشروعة وجعلها في متناول الغير، والتي تمكنه من إرتكاب جريمة من الجرائم المعلوماتية.

ومن قبيل ذلك توفير كلمات المرور أو الشفرات أو الأكواد أو أي بيانات أخرى تسمح بالدخول لكل أو لجزء من النظام المعلوماتي دون إذن مسبق، ويدخل في إطارها كذلك وضع أجهزة على الخط ليتم إستخدامها بواسطة الغير في تجميع الروابط بين الخطوط المتشعبة من أجل تسهيل عملية الوصول إلى المعلومات والكشف عنها داخل الجهاز[4]، بل إن القضاء الفرنسي قد توسع في تفسيره لمدلول مصطلح "التوفير" ليشمل كل أشكال الكشف والإفشاء العلني للثغرات الأمنية من

---

[1]- لم يشترط المشرع في المعطيات والمعلومات المحصلة من إحدى الجرائم المنصوص عليها بأن تكون مخزنة داخل النظام المعلوماتي نفسه، مما يعني أن الحماية القانونية تشمل كذلك المعلومات والمعطيات المعالجة آليًا والموجودة على أية وسائط إلكترونية خارج النظام كالأشرطة والأقراص والفلاشات والديسك وغيرها، ويستوي في ذلك أن يتم إلتقاط هذه المعلومات والوصول إليها عن طريق التجسس المعلوماتي أو بطرق الإحتيال أو حتى عن طريق السرقة للمال المعلوماتي، وتكتسي هذه الحالة الأخيرة خطورة كبيرة سيما حال إستهدافها بيانات سرية للغاية تجارية أو إقتصادية أو عسكرية أو أمنية، والتي تعتبر ظرفا مشددًا في نظر المشرع الجزائري (- **زيبحة زيدان:** المرجع السابق، ص63).

[2]- ***Rapport :*** *explicatif de la convention sur la cybercriminalité, Op. Cit, P13.*

[3]- أنظر في ذلك: **الملحق رقم (03).**

[4]- **رشيدة بوكر:** المرجع السابق، ص111.

خلال كسر الحواجز الأمنية في النظم أو المواقع وجعلها مفتوحة وفي متناول الجميع، وهذا من خلال برامج مصممة لذلك[1].

أما عن الفرق بين مصطلح "التوفير" ومصطلح "التجميع" كون أن هذا الأخير لا تتعدى فيه عملية حيازة المعطيات والمعلومات والتصرف فيها إلاَّ على من يقوم بذلك، أي أنها محصورة في شخص واحد، فهو من قام بتجميعها والحصول عليها بمعرفته الخاصة حتى وإن تعدد الأشخاص، بينما التوفير فيتسع معه نطاق دائرة الأشخاص الذين يمكنهم الحصول على هذه المعلومات والتصرف فيها، فهي متوفرة للجميع مما تزيد معه درجة الخطورة بإزدياد هؤلاء الأشخاص، ومن هنا نلمس خطورة التوفير وفق المعنى السابق عن التجميع كون أن الذي يقوم بالتجميع هو المستفيد من ما جمع، بينما في التوفير فالمستفيدون كثر وعددهم كبير، وكلما إتسعت دائرتهم كانت الخطورة أكبر[2].

هـــ- النشر *La Diffusion*: نص على هذا الفعل كل من التشريع الجزائري وكذا إتفاقية بودابست، في حين لم نجد له ذكرًا لا في التشريع الفرنسي ولا في الإتفاقية العربية ولا حتى في التشريع المصري كما أنه لا يوجد تعريف في كل نصوص القانون الوطني والمقارن تعرف مصطلح "النشر" أو تعرف "جرائم النشر الإلكتروني"، وبالتالي يترك سلطة تقديرية واسعة في تحديد المراد بالنشر الإلكتروني، إلا أنه قريب من التعريف ما تم وضعه في التقرير الصادر عن الجمعية الوطنية الفرنسية للناشرين، حيث تم تعريف هؤلاء بأنهم: "الأشخاص الذين يقومون بصياغة المعلومات أو تحريرها أو نشرها أو إعادة نشرها أو وضعها على مواقع التواصل الإجتماعي"[3].

فالناشر الإلكتروني هو كل شخص طبيعي أو إعتباري قام بإنشاء مواقع على الشبكة العنكبوتية، وسمح فيها بإضافة أشخاص وتلقى منهم البرامج والمعلومات المتحصلة من جريمة، أو أنه قام بإرسال هذه البرامج والمعلومات أو وضعها على الموقع الإلكتروني أو إحدى وسائل تقنية المعلومات، مما جعلها منشورة ومتاحة لمستخدمي الإنترنت[4].

---

[1]- *Cass, Crim 27 Octobre 2009. - Cass, Crim 22 Décember 2009.*

[2]- **محمد خليفة:** المرجع السابق، ص203. - **يزيد بوحليط:** المرجع السابق، ص192. - **عبد الوهاب ملياني:** مرجع سابق، ص198.

[3]- ***Rapport :*** *d'information de l'assemblée Nationale sur la mise en application de la loi N°: (2004-575) du 21 juin 2004, pour la confiance dans l'économie numérique.*
(ce rapport est disponible sur sur le site web: ***http://www.assemblée-nationale.fr****)*. تاريخ التصفح (2019/12/03).

[4]- **دينا عبد العزيز فهمي:** الحماية الجنائية من إساءة إستخدام مواقع التواصل الإجتماعي، دار النهضة العربية، القاهرة، مصر، 2018، ص89.

ولقد نص على هذا المصطلح الدستور الجزائري لعام 2020 بموجب نص المادة (54) منه في فقرتها السادسة بأن "الحق في نشر الأخبار والأفكار والصور والآراء في إطار القانون ..."، وجاءت الفقرة السابعة من نفس المادة تنص على أنه: "يحظر نشر خطاب التمييز والكراهية".

وهكذا يقصد بالنشر في هذا الإطار إعلام وإذاعة المعطيات والمعلومات محل الجريمة وتمكين الغير من الإطلاع عليها، بما ينبغي أن يمتد نشره ليشمل كل نشاط من شأنه نقل معلومات إلى الآخرين[1]، وهذا الفعل من أخطر الأفعال السابقة، حيث أن النشر كفيل بأن ينقل هذه المعلومات والمعطيات غير المشروعة إلى أكبر عدد ممكن من الأشخاص مما يجعل إحتمال إستعمالها في الجرائم أكبر[2]، لاسيما في جرائم "الإبتزاز الإلكتروني" ضد الضحايا أصحاب هذه المعلومات وذلك بطلب مبالغ مالية طائلة مقابل عدم نشر هذه المعلومات، أو مثلاً في "جريمة سرقة الأسرار المعلوماتية" وإعادة بيعها إلى شركات منافسة، وغيرها الكثير من الجرائم المعلوماتية المشابهة[3].

كما قد تقع جرائم نشر البيانات أو المعلومات أو إعادة نشرها من المستفيدين لمواقع التواصل الإجتماعي أو من شخص يقوم بالنشر أو إعادة النشر بسبب تأديته لعمله وبحكم وظيفته، كأن يستغل هذا الأخير شبكة الإنترنت في الجهة التي يعمل بها بعد حصوله على معلومات سرية وخاصة للغاية ويقوم بإذاعة هذه المعلومات والتي مهما كان نوعها أو طبيعتها، فيقوم بنشرها أو إعادة نشرها وتمكين الغير من الإطلاع عليها، وسواء كانت هناك صلة بين هذه المعلومات والجهة التي يعمل بها أم لا[4].

و- الإتجار *La Commercialisation*: الإتجار المقصود في نص المادة (394 مكرر 2) من **(ق ع ج)** ليس هو ذلك المقصود في القانون التجاري، بل يشمل كافة التصرفات التي تكون بمقابل سواءً كان عينيًا أو نقديًا، حتى ولو لم ينص عليها القانون التجاري في إطار الأعمال التجارية المنظمة من خلاله[5]، ووفق هذا فإن الإتجار يختلف عن التوفير على أساس أن هذا الأخير قد يكون بدون مقابل يذكر، لهذا فالإتجار قد يكون جزء من التوفير لأنه يشمل تقديم المعلومات بمقابل أو بدون مقابل.

---

[1]- ***Rapport :*** *explicatif de la convention sur la cybercriminalité, Op. Cit, P 14.*

[2]- **محمد خليفة:** المرجع السابق، ص204. - **يزيد بوحليط:** المرجع السابق، ص193.

[3]- **رشيدة بوبكر:** المرجع السابق، ص111. - **غنية باطلي:** المرجع السابق، ص188.

[4]- هنا إشترط المشرع الإماراتي وفقًا لنص المادة (الثالثة من القانون رقم (5 لسنة 2012) في شأن مكافحة جرائم تقنية المعلومات، أن يكون عمل الشخص في تلك الجهة قد سهل له نشر بيانات أو معلومات أو إعادة نشرها، فالمصلحة المحمية جنائيًا هي عدم إستغلال تلك الجهة أو الوظيفة في نشر بيانات أو معلومات متحصلة من الجريمة. (أنظر: - **دينا عبد العزيز فهمي:** المرجع السابق، ص90).

[5]- **عبد الوهاب ملياني:** المرجع السابق، ص199.

إلا أننا نجد أن المشرع الفرنسي لم ينص على مصطلح "الإتجار" وإنما إستعمل مصطلح آخر وهو "الإستيراد"، في حين إستخدمت إتفاقية بودابست مصطلح "البيع والإستيراد"، وكذلك فعلت الإتفاقية العربية، بينما آثر المشرع الجزائري إستخدام مصطلح "الإتجار"، فهو أوسع من مفهوم البيع والإستيراد، إذ يسمح مصطلح "الإتجار" بإستيعاب مختلف التعاملات التجارية التي تصور وقوعها على المعلومات من بيع وشراء وإستيراد وتداول وغيرها[1]، لهذا نقول أن المشرع الجزائري يتجه نحو التوسع في تجريم كافة التعاملات غير المشروعة التي يمكن أن ترتكب بها الجرائم موضوع دراستنا، وهذا رغبة منه في الوقاية المسبقة والقبلية للحد من هذه الجرائم وضمان لغياب النص التشريعي الذي قد يستفيد منه المجرم المعلوماتي وإفلاته من العقاب.

وحتى نعطي مفهومًا واسعًا لمصطلح "الإتجار" سوف نذكر هنا بعض المصطلحات التي إعتمدها بعض المشرعين ونقوم بشرحها، حسب ما ذكره بعض الفقه ومنها على سبيل المثال:

1. الجلب والإستيراد *Importer*: الجلب أو الإستيراد[2] معناه إدخال الأجهزة أو المعدات أو البرامج إلى أرض الوطن إما عينيًا بدخولها مع الشخص المستورد لها، وإما عن طريق شحنها وتحويلها من الخارج إلى الداخل، ولا تقع الجريمة هنا إلا إذا إجتازت هذه الأشياء الممنوعة للحدود السياسية للبلاد إجتيازًا ماديًا أو حقيقيًا بقصد طرحها في التداول، بحيث لا تتم الجريمة إلا بدخول الأجهزة أو البرامج من الحدود البرية للدولة أو من مياهها الإقليمية، أي أن مناط المسؤولية الجنائية في حالة جلب أو إستيراد تلك الأجهزة والمعدات غير المشروعة هو ثبوت إتصال الجاني بها إتصالاً مباشراً أو بالوساطة مع بسط سلطانه عليها بأية صورة من علم وإرادة حتى ولو لم يتحقق له الحيازة الفعلية والمادية[3]، ومن ثم إذا ضبطت تلك الأجهزة قبل ذلك وقفت الجريمة عند حد المحاولة والشروع المعاقب عليه[4].

---

[1]– **رشيدة بوبكر:** المرجع السابق، ص112. – **غنية باطلي:** المرجع السابق، ص189.

[2]– كل من الجلب والإستيراد وإن كانا يتفقان في عملية إدخال الأشياء إلى البلاد، إلا أنهما يفترقان من حيث المبدأ، إذ أن الإستيراد عملية قانونية ومشروعة يحميها القانون وتتطلب إجراءات قانونية وإدارية معينة، أما الجلب فهو إدخال تحت إسم الإستيراد أو غيره، ولكنه لا يتم بطرق مشروعة، وتطبيقًا لذلك قضت محكمة النقض المصرية في إحـدى القضايا أن: "الجلب معناه إستيراد الشيء، وهو معنى لا يتحقق إلا إذا كان الشيء المجلوب يفيض عن حاجة الشخص وإستـعماله الشخصي له، أو طرحه وتداوله بين الناس فـي الداخل...". أنظـر في ذلك: – الطعن رقم (21609)، س.ق 62، جلسة بتاريخ 10 ديسمبر 1995، مجموعة أحكام النقض، س 46، ج1، ص5.

[3]– **محمد علي سويلم:** المرجع السابق، ص350.

[4]– وتطبيقًا لذلك قضت محكمة النقض المصرية أن النص في المادة (121) من قانون الجمارك والتي جاء فيها: "يعتبر تهريبًا إدخال البضائع من أي نوع إلى أراضي الجمهورية أو إخراجها منها بطرق غير مشروعة، وبدون أداء الضرائب الجمركية كلها أو بعضها أو بالمخالفة للنظم المعمول بها". أنظر في ذلك أيضاً: – الطعن رقم (2534 س.ق 59) جلسة بتاريخ 6 فبراير 1990 مج. أ.ن، س 41، ج1، ص275. – وكذا الطعن رقم (2358 س.ق 54) جلسة بتاريخ 24 مايو 1985 مج. أ.ن، س 36، ج1، ص117.

وفي حكمه أيضًا التصدير وهو عكس الإستيراد، ويعني إخراج الأجهزة أو المعدات أو البرامج المصممة أو المطورة أو المحورة أو أي بيانات أخرى مماثلة من أراضي الدولة، بصرف النظر عمَّا إذا كان يقصد منه إدخالها إلى دولة أخرى أو مجرد التخلص منها، إذ أنه باعث على الجريمة لا أثر له في قيامها، ويستوي في التصدير أو الإستيراد أن يكون الجهاز أو البرامج أو المعدات في حوزة الجاني أو في غير حوزته[1].

كما يستوي أن يكون الجاني وقت التصدير أو الإستيراد خارج الدولة أو داخلها، ويستوي أيضًا أن يكون الجاني قد إستورد الأجهزة أو المعدات أو البرامج لحساب نفسه أم لحساب غيره[2].

2. البيع *Vendre*: البيع يقابله في اللغة الشراء، كما يطلق كل منهما على الآخر، والبيع هو المعاملة التي تجري بين البائع والمشتري، فهو عملية تبادل المنتجات والسلع والخدمات مقابل النقود، أما الشراء فهو العملية المقابلة للبيع، وهي مجموعة من الإجراءات التي يقوم بها المشتري في تحديد نوع المنتج أو السلعة أو الخدمة التي يريد الحصول عليها، بمعنى آخر يقصد بعملية البيع أنها عبارة عن تصريف المنتجات للمستهلكين والتركيز على نشاط مبادلة الشيء المبيع بالنقود، أما عملية الشراء فهي قبول المبيع ودفع ثمنه، حيث نستنتج من ذلك أن كل من البيع والشراء عبارة عن عملية إتصال بين شخصين أو أكثر بائع ومشتري، والهدف منهما تحقيق الرضا وتحقيق الربح، وهذه العملية موجودة منذ القدم، فهي تعد من أقدم العلاقات التجارية والإقتصادية في تاريخ الإنسان.

وعليه فالبيع هنا هو إتفاق إرادتين أو أكثر على نقل ملكية الشيء المبيع[3] من الأجهزة أو المعدات أو الأدوات أو البرامج المصممة أو أي بيانات مماثلة بدون تصريح مسبق أو مسوغ من الواقع أو القانون[4]، وسواء حقق البائع أرباحًا من هذا البيع أم لم يحقق، وسواء تم البيع بسعر أقل من سعر السوق المقرر أم أكثر، وسواء كانت تلك الأجهزة المباعة مصنوعة بالداخل أم بالخارج، وسواء يراد بيعها داخل الوطن أم تصديرها لبيعها بالخارج، وسواء تم البيع مرة واحدة أم تكرر

---

[1]– **محمد علي سويلم:** المرجع السابق، ص348.

[2]– **فوزية عبد الستار:** شرح قانون مكافحة المخدرات، دار النهضة العربية، القاهرة، مصر، 1990، ص24.

[3]– عرفت المادة (351) من القانون المدني الجزائري "عقد البيع" بقولها: "البيع عقد يلتزم بمقتضاه البائع أن ينقل للمشتري ملكية شيء أو حقًا ماليا آخر في مقابل ثمن نقدي"، (ق م ج)، صادر بالأمر رقم (75–58) المؤرخ في 26 سبتمبر 1975 المعدل والمتمم بآخر تعديل له بالقانون رقم (07–05) المؤرخ في 13 مايو 2007.

[4]– **محمد علي سويلم:** المرجع نفسه، ص351.

عدة مرات، وفي هذه الحالة الأخيرة تعتبر جميع الأفعال المتكررة جريمة واحدة مستمرة، لأنها ترتكب جميعها بقصد جنائي واحد[1].

وعليه فإن مصطلح "الإتجار" حسب الفقرة الأولى من نص المادة (394 مكرر 2) جاء ليشمل أيضًا كل من عملتي البيع والشراء، فهو مصطلح واسع ومفتوح، وذلك حتى لا يفلت مجرم من مسطرة العدالة والمساءلة والعقاب.

3. التداول *Commerce*: يقصد بالتداول طرح الأجهزة أو البرامج للتعامل أو للتصرف، ولا يشترط فيه البيع بمقابل نقدي كما لو أنه يتم عن طريق المقايضة أو بدون مقابل في سبيل الإعلان عنها.

وقد إشترط المشرع في هذه الأفعال التبادلية شرطان أساسيان:

– الشرط الأول: أن يكون النشاط الإجرامي بدون تصريح مسبق من صاحب الجهاز أو مسوغ من الواقع أو القانون.

– الشرط الثاني: أن يثبت أن ذلك السلوك كان بغرض إستخدام أي منها في إرتكاب أو تسهيل إرتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها، أو ثبت ذلك الإستخدام أو التسهيل أو الإخفاء[2].

وعمومًا يشير مصطلح "الإتجار" حسب نص المادة (394 مكرر 2) من (ق ع ج) على عملية الإتجار بالمعلومات أو المعطيات أو البرامج أو الأجهزة بتقديمها إلى الغير بمقابل، ولا يهم نوع ومقدار هذا المقابل، إذ يستوي أن يكون مال أو مجرد خدمات أو غير ذلك[3]، والإتجار كمصطلح أراد به المشرع الجزائري أن يجرم كل أفعال التعامل في المعطيات والمعلومات بطريقة غير مشروعة، سواءً كان ذلك بمقابل أو بغير مقابل، والتي ترتكب بها إحدى الجرائم المعلوماتية[4].

ثانيًا– التعامل غير المشروع في معطيات متحصلة من الجريمة

هذه الصورة من التعامل غير المشروع إنفرد بها المشرع الجزائري، إذ لا نجد لها ذكراً في التشريعات الجنائية المقارنة ما عدا بعض الحالات المشابهة، ولعل ذلك يَنُمُّ عن سياسة المشرع

---

[1]– والملاحظ أن البيع هنا لفظ واسع ومطلق، فهو يشمل جميع صور البيع أيًّا كانت طبيعتها، سواء كانت بالمزاد العلني أم كان بيعًا رضائياً، ويستوي أن يكون بين شركة وأحد أعضائها أو مع الغير، أو بين شخصين طبيعيين (أنظر: – **سميحة القليوبي:** المرجع السابق، ص353).

[2]– **محمد علي سويلم:** المرجع السابق، ص353.

[3]– **محمد خليفة:** المرجع السابق، ص204.

[4]– **هلالي عبد الإله أحمد:** الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2003، ص97.

الجزائري في وضع حماية أكثر للمعلومات الإلكترونية[1]، لاسيما الموجودة منها خارج النظام المعلوماتي والمتحصلة من إرتكاب إحدى الجرائم المعلوماتية، حيث ضيَّق المشرع من نطاق التعامل أو الإستخدام غير المشروع لمعطيات النظام، بما فيها المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القانون، كما ضيَّق أيضًا من نطاق الأشخاص الذين يمكن أن يتعاملوا في هذه المعطيات المتحصلة من جرائم الإعتداء على نظام المعالجة الآلية للبيانات، وهذا كله للحفاظ على ما تبقى من سرية وخصوصية هذه المعطيات وغيرها[2].

ويقوم الركن المادي لهذه الصورة من الجرائم بإتيان الأفعال التي نصت عليها الفقرة الثانية من المادة (394 مكرر 2) من (ق ع ج)، بل يكفي تحقق واحد منها فقط لكي يقوم السلوك الإجرامي لها، أي لا يشترط إجتماع كل هذه الأفعال مع بعض، وهذه الأفعال هي: "الحيازة، الإفشاء، النشر، الإستعمال" وهي أفعال على قدم المساواة في قيام هذه الجريمة، لذا سنتعرض لكل فعل على حدة من هذه الأفعال كما يلي:

أ- الحيازة *La possession*: يقصد بالحيازة هنا السيطرة الفعلية والإرادية لشخص الحائز على شيء منقول تخوله مكنة الإنتفاع به، فهي بمثابة سلطة فعلية لممارسة الشخص الحائز على شيء ما تظهره بمظهر صاحب الحق، فالحيازة ليست حقًا وإنما مركز واقعي، والأصل فيها أن تكون مشروعة وأن تستند إلى سند صحيح أو مسوغ من الواقع والقانون[3]، فالحيازة هي رابطة واقعية بين شخص الحائز والمال المنقول، تتيح للأول سيطرة على الثاني سيطرة مستقلة مقترنة بنية التملك[4]، وتكون السيطرة مستقلة إذا كان يمكن للشخص الحائز أن يمارس أي عمل مادي على الشيء بدون رقابة من شخص آخر[5].

---

[1]- **غنية باطلي:** المرجع السابق، ص191.

[2]- **رشيدة بوكر:** المرجع السابق، ص113.

[3]- وهذا ما ذكره القانون المدني الجزائري في القسم السادس تحت عنوان "الحيازة"، وذلك بذكره جملة من القواعد والأحكام المنظمة لها من المادة (808) حتى (843) منه، فنذكر هنا على سبيل المثال نص المادة (823) بقولها: "الحائز لحق يفرض أنه صاحب لهذا الحق حتى يتبين خلاف ذلك".

[4]- وهذا ما نصت عليه المادة (835) من (ق م ج) بقولها: "من حاز بسند صحيح منقولاً أو حقًا عينيًا على المنقول أو سنداً لحامله، فإنه يصبح ملكًا له إذا كان حسن النية وقت حيازته ... والحيازة في ذاتها قرينة على وجود السند الصحيح وحسن النية، ما لم يقم دليل على خلاف ذلك".

[5]- **غنية باطلي:** المرجع السابق، ص191.

والحيازة في نطاق القانون الجنائي قد تكون مشروعة، كما قد تكون غير مشروعة، ففيما يتعلق بهذه الجريمة التي نحن بصدد دراستها يجب أن تكون الحيازة غير مشروعة، أي أن المعطيات يجب أن تكون محصل عليها من إحدى جرائم الإعتداء على نظم المعالجة الآلية فتم حيازتها[1].

والحيازة على النحو السالف بيانه تقوم على عنصرين إثنين "مادي ومعنوي"[2]، أما العنصر المادي أي "فعل الإحراز" فهو وضع اليد على الشيء والسيطرة عليه سيطرة مادية[3]، أي أنه يحوزها حيازة مادية أو معنوية[4]، كالإستيلاء على تلك المعلومات أو الأجهزة[5] أو المعدات أو البرامج المصممة أو أي بيانات مماثلة[6] لأي غرض كان، وذلك بالتأثير عليها تأثيرًا يتفاوت حجمه تبعًا لنوع الحيازة، وصور هذا التأثير متنوعة وأبرزها إتلاف هذه المعطيات أو التعديل منها أو توجيهها في إستعمال معين، أو نقلها للجهة التي يريدها أو إخفائها عن الأعين أو الإنتفاع بها إلى غير ذلك من الأغراض، ولا يتأتى ذلك إلا إذا كان للحائز السلطة التي تخوله القيام بالأعمال المادية كالتي يستطيع مباشرتها من له حق على الشيء قبل زواله[7].

---

[1]– **محمد خليفة:** المرجع السابق، ص206.

[2]– **محمود نجيب حسني:** شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1992، ص834.

– **فتوح عبد الله الشاذلي:** شرح قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، مصر، 2001، ص452.

[3]– **محمد علي سويلم:** المرجع السابق، ص347.

[4]– تعد الحيازة معنوية كلما كانت ذات طابع رقمي تتمثل في المعرفة بمجموعة البيانات والمعطيات الرقمية التي تتخذ شكل أرقام أو حروف أو شفرات أو بصمات وفق اللغة التي يتعامل بها المشترك أو الحائز مع النظام، ويمكن أن تكون هذه الحيازة المعنوية في متناول أي شخص ولو مصادفة، وهو أمر يستوجب ممارسة الدخول إلى النظام المعلوماتي مرة واحدة أو عدة مرات متكررة دون إذن مسبق من صاحبه، فلا يكفي مجرد حيازة هذه المعطيات من الأرقام وكلمات المرور، وإنما يلزم إستعمالها إستعمال غير مشروع. (أنظر: – **محمد علي سويلم**، المرجع نفسه، ص267).

[5]– كالجهاز القومي لتنظيم الإتصالات (أنظر في ذلك: – نص المادة الأولى من القانون المصري رقم (175 لسنة 2018) بشأن مكافحة جرائم تقنية المعلومات.

[6]– **كيانات المرور:** وهي بيانات أو معلومات إلكترونية تنشأ عن طريق إحدى وسائل تقنية المعلومات من شأنها أن توضح مصدر الإتصال والوجهة المرسلة إليها والطريق الذي تسلكه، ووقت وتاريخ وحجم ومدة ونوع الخدمة (أنظر: – نص المادة الأولى من القانون القطري رقم (14 لسنة 2014) بشأن مكافحة الجرائم الإلكترونية، والتي تقابلها نفس المادة الأولى من القانون المصري رقم (175 لسنة 2018).

[7]– ذكرت هنا كل من المادتين:

– المادة (815) من (ق م ج) أنه: "تزول الحيازة إذا تخلى الحائز عن سيطرته الفعلية على الحق أو إذا فقد هذه السيطرة بأية طريقة أخرى".

– المادة (816) من (ق م ج) أنه: "لا تزول الحيازة إلا إذا حال مانع وقتي دون مباشرة الحائز للسيطرة الفعلية على الحق".

وتجدر التفرقة بين الحيازة الضرورية والحيازة العارضة أو الطارئة، فالحيازة الضرورية هي التي تكون في يد المتدخل إلى النظام بحكم وظيفته أو عمله أو بسببهما، فالمتدخل في شبكة النظام يكون حائزًا لكلمة المرور أو كود الدخول بالضرورة أثناء عمله، ومن ثمة فالحيازة واقعة بحكم عمله أو وظيفته، في حين أن الحيازة العارضة هي التي تتوافر حال قيام المهني على سبيل المثال بالدخول إلى الحاسوب أو النظام من أجل إصلاح عطب أو خلل بداخله بحكم مهنته ومعرفته بطرق التصليح فيضطر إلى حيازة كود الدخول لكي يمكنه من مباشرة عمله، ففي هذه الحالة تكون الحيازة عارضة والحيازة بنوعيها –الضرورية والعرضية– لا تمنح الحائز الحق في تجاوز إستخدام كلمات المرور في أغراض غير تلك التي تتناسب مع طبيعة العمل ومستلزماته.

وتعد حيازة أو إكتساب كلمات أو أرقام المرور مثلها مثل أية حيازة مادية لا تؤدي إلى خسارة مادية لصاحب النظام، وإنما تعني عدواناً يتخذ شكل المشاركة فيما يحوزه دون أن يكون هناك أحقية للغير فيها، ومن ثم لا يفقد صاحب النظام حيازته الشرعية نتيجة إستلاء الغير عليها، وإنما تبقى له الحيازة قائمة[1]، ومن ثم ليس هناك ملكية على كلمات أو أرقام المرور ما دام صاحبها الأصلي يملك صلاحية سحبها وتغييرها، وهذا بحكم أنها ليست جامدة، بل إنها على درجة عالية من المرونة، بحيث يمكن تغييرها وتعديلها بإستمرار[2].

ولا فرق بين أن يكون الإحراز عرضيًا طارئًا أو أصليًا ثابتاً، طويل الأمد أو قصيره، كلما وجد إحراز مادي لتلك الأجهزة أو المعدات أو البرامج وثبت القصد الجنائي فقد إستوفت الجريمة هذا العنصر وبالتالي حق العقاب، ولا يلزم لتوافر ركن الإحراز أن تضبط الأجهزة مع المتهم، بل يكفي أن يثبت أنها كانت معه بأي دليل من شأنه أن يؤدي إلى ذلك، ويعتبر الإحراز في مثل هذه الحالة جريمة مستمرة، ومن ثم لا يبدأ سقوط الدعوى الجنائية إلا من يوم خروج الأجهزة أو المعدات أو البرامج من حيازة الجاني، فطالما كانت الحيازة أو الإحراز قائمًا فإن إرتكاب الجريمة يتجدد بإستمرار تلك الحيازة أو الإحراز[3].

والقول بحيازة المعطيات هو إمكانية الحائز من التأثير عليها تأثيرًا يتفاوت تبعًا لنوع الحيازة فقد تكون الحيازة مطلقةٌ حيث يكون للحائز من خلال سيطرته المطلقة أن يفشي المعطيات

[1]– محمد علي سويلم: المرجع السابق، ص268.

[2]– عمر محمد أبو بكر بن يونس: المرجع السابق، ص328.

[3]– محمد علي سويلم: المرجع نفسه، ص348.

أو يعدل فيها أو يستعملها، كما قد تكون هذه السيطرة نسبية أي محدودية، بحيث تمكنه فقط من الإنتفاع بها لوحده أو إستعمالها على وجه الخصوص أو على وجه معين، وتكفي هنا السيطرة المحدودة لقيام هذه الجريمة[1].

وأما العنصر المعنوي أي "نية التملك" فقوامه هو نية وإرادة الشخص الحائز في السيطرة على المعلومات المتحصلة من الجريمة، أي أن ما يأتيه الحائز من أفعال ليست أمراً عارضًا أوجدته المصادفة أو عن طريق الخطأ، وإنما كان ذلك بسوء نية[2]. فهي ليست عارضة بل صادرة عن إرادة الإحتفاظ بهذه المعلومات وإستبقاء السيطرة عليها إما على الدوام أو لمدة معينة.

وتفترض هذه الإرادة العلم بمضمون المعلومات المحروزة كونها متحصلة من جريمة ودخولها في نطاق السيطرة عليها بنية التملك[3]، وتطبيقًا لذلك فإن من يخزن كلمة مرور أو شيفرة أو برامج تحصل عليها من إختراق موقع إلكتروني من على النظام أو أي جريمة معلوماتية أخرى، وهو يعلم أنها متحصلة من إحدى هذه الجرائم وقبوله أن تدخل تحت سيطرته، فهنا تقوم الحيازة ومنه تقوم معها الجريمة المعلوماتية[4].

ب- الإفشاء *La Révelation*: ولقد جرم المشرع الجزائري فعل "الإفشاء" بموجب الفقرة الثانية من المادة (394 مكرر 2) من (ق ع ج)، وهذا على خلاف المشرع الفرنسي الذي لم يشر إلى هذا المصطلح، وكذلك الأمر بالنسبة لكل من الإتفاقيتين الأوروبية والعربية السالف ذكرهما.

ونفس المسلك إنتهجه المشرع الأمريكي بموجب القانون الفيدرالي لجرائم الحاسبات الآلية لعام 1984، حيث تعاقب المادة (1030-1-3) منه: "كل من يقوم بالدخول غير المصرح به إلى نظام الحاسب الآلي متى كان هذا الدخول من شأنه القيام بإفشاء معلومات مخزنة داخل هذا النظام"[5]، وهذا قريب جدًا إلى ما نصت عليه المادة (353 مكرر 1) من (ق ع ج) بقولها: "يعاقب بالعقوبات

---

[1]- **غنية باطلي:** المرجع السابق، ص192.

[2]- وهذا ما يفهم من نص المادتين:

- المادة (824) من (ق م ج) بقولها: "يفرض حسن النية لمن يحوز حقًا وهو يجهل أنه يعتدي على حق الغير، إلا إذا كان هذا الجهل ناشئًا عن خطأ جسيم، وإذا كان الحائز شخصًا معنويًا، فالعبرة بنية من يمثله، ويفترض حسن النية دائمًا حتى يقوم الدليل على العكس".

- المادة (825) من (ق م ج) بقولها: "لا تزول صفة حسن النية من الحائز إلا من الوقت الذي يعلم فيه أن حيازته إعتداء على حق الغير، ويزول حسن النية من وقت إعلان الحائز بعيوب حيازته ... ويعد سيء النية من إغتصب حيازة الغير بالإكراه".

[3]- **رشيدة بوكر:** المرجع السابق، ص114.

[4]- **غنية باطلي:** المرجع السابق، ص192.

[5]- مشار إليه لدى: - **شرين دبابنة:** المرجع السابق، ص115.

المنصوص عليها في المادة السابقة كل من إحتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو إستخدام بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 353 مكرر من هذا القانون. عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة، تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة لتحديد الأشخاص المسؤولين ...".

لذا تعتبر الحياة الخاصة للأشخاص– طبيعية كانت أم معنوية – من الأمور التي عنت بها معظم دساتير العالم وقوانين الدولة المعمول بها[1]، وبما أن الحاسبات الآلية وما في حكمها من وسائط التخزين الإلكتروني والنظم المعلوماتية تتمتع بقدرة فائقة في تخزين كم هائل من المعلومات، سواءً كانت هذه المعلومات تتعلق بمصالح الدولة ومؤسساتها أو أنها تتعلق بمصالح الأفراد الإقتصادية والإجتماعية والعلمية...، ونظراً لإزدياد أهمية المعلومات الإلكترونية وكثرة الإعتماد عليها فيما يسمى "بالأرشيف الإلكتروني *Archives éléctronique*"، إزدادت المخاوف من الحصول عليها بطرق غير مشروعة سواءً بالمساس بها أو بالإعتداء عليها وإفشائها للغير بغية تحقيق مصلحة أو هدف معين[2].

ويقصد بالإفشاء البوح أو كشف السر وإطلاع الغير عليه بأية طريقة، وقد عبر عنه الفقه الفرنسي بإصطلاح "*Reveler*" وفيها كشف لما خفي ونشر لما طوي، أو أنه كل عمل ينقل الواقعة المفشاة من واقعة سرية إلى واقعة معروفة، فلا يكون هناك إفشاء إذا إنصب على واقعة عرفت من قبل[3]، بحيث يفرق البعض بين الإفشاء والإذاعة للسر، فإذاعة السر هي الكشف عنه للجمهور دون تمييز فيتحقق بمجرد إطلاع شخص غير معين بالذات على مضمونه، ولا يشترط حصول الإطلاع لعدد من الناس أو إذاعته لشخص واحد.

أما المفشي إليه فإنه يجب أن يكون شخصاً معيناً بالذات حتى وإن تعدد هؤلاء الأشخاص المهم أنهم معينين بالإفشاء إليهم، وإلا إختلط مدلول الإفشاء مع الإذاعة، والسبب في ذلك أنه وإن

---

[1]– وهذا ما جاء في سياق نص المواد (47) و (55) من الدستور الجزائري لعام 2020 بقولهما:

– المادة (47): "لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته وإتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة... إلا بأمر معلل من السلطة القضائية".

– المادة (55): "يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات والحصول عليها وتداولها، لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم وبالمصالح المشروعة للمؤسسات، وبمقتضيات الأمن الوطني ...".

[2]– **غنية باطلي:** المرجع السابق، ص192.

[3]– **أحمد كامل سلامة:** الحماية الجنائية لأسرار المهنة، دراسة مقارنة، (د د ن)، 1982، ص60.

كانت كل إذاعة للسر تتضمن إفشاء له، إلا أن إفشاء الأسرار لا يتضمن بالضرورة إذاعتها، وأن القول بترادف معنى الإفشاء والإذاعة يؤدي إلى الخلط بين مفاهيم القانون وإزالة جدوى التمييز بينهما[1].

ويفرق البعض الآخر بين فعل الإفشاء وفعل البلاغ، فإفشاء السر هو كشف له وبوح به، ولا يمكن أن يكون إلا من شخص يعلم السر ويجهر به كما علمه، أما إبلاغ السر أو نقله فقد يقع من شخص رآه أو سمع به ولا يقتضي الإبلاغ أن يكون الشخص المبلغ عالمًا بتفاصيل ما يبلغ عنه، وإنما يكفي أن يكون عالمًا بأن ما يقوم بنقله أو إبلاغه هو سِرٌّ من الأسرار الواجب كتمانها، كما أن الفاعل في فعل الإبلاغ يستهدف شخصًا معيناً، أما في فعل الإفشاء فإنه قد يقع ولو لم يقصد الفاعل بها جهة معينة أو شخصًا بعينه[2].

ويفترض في فعل الإفشاء –مثله في ذلك مثل فعل النشر– إنتقال المعلومات من حيازة الجاني الذي حصل عليها من إحدى الجرائم إلى غيره من الأشخاص، وهذا هو الفرق بين الإفشاء والحيازة، حيث أن هذه الأخيرة ينحصر فيها وجود المعلومات لدى الحائز دون تقديمها لشخص آخر، في حين أن في فعل الإفشاء نجد أن المعلومات يتم إنتقالها من يد الحائز لها إلى الغير ولا يشترط أن يكون هذا الغير شخص بعينه أو فئة معينة[3].

ولم يتطلب المشرع الجزائري حدوث أية نتيجة معينة من وراء فعل الإفشاء، فهو فعل مجرم لذاته[4]، كما لا ينبغي أن يفهم فعل الإفشاء على أنه محصور في شخص معين، بل يمكن أن يكون القائم على إتيانه شخص ملزم بموجب وظيفة معينة أو عقد أو إتفاق يلزمه بكتمان سرية هذه المعلومات وعدم إفشائها[5]، أو أن يرتكبه أي شخص آخر طالما تحصل على هذه المعلومات بطريقة

---

[1]– **أحمد فتحي سرور:** الوسيط في قانون العقوبات، القسم الخاص، ط4، دار النهضة العربية، القاهرة، مصر، 1991، ص779.

[2]– **محمد علي سويلم:** المرجع السابق، ص464–465.

[3]– **محمود كبيش:** الحماية الجنائية لسرية الحاسبات البنكية في القانون المصري، دار النهضة العربية، القاهرة، مصر، 1996، ص12.

[4]– **رشيدة بوكر:** المرجع السابق، ص114. – **يزيد بوحليط:** المرجع السابق، ص194. – **زيدان زيبحة:** المرجع السابق، ص65.
– **غنية باطلي:** المرجع السابق، ص192. – **محمد خليفة:** المرجع السابق، ص209.

[5]– في الحقيقة هناك بعض الصعوبة في تحديد ما هو المقصود بالسر أو السرية؟ حيث عرّف جانب من الفقه الفرنسي السر بأنه: "كل ما يضر إفشاؤه بسمعة مودعه وكرامته، ومع ذلك فإن السر قد يكون على عكس من ذلك أمرًا مشرفًا لصاحبه غير ضار بسمعته أو كرامته، ومع ذلك يعتبره سرًا ويحرص على كتمانه"، وبالتالي يجب عدم إفشاء السر خاصة بمن هو ملزم بكتمانه بشرط أن يترتب عليه ضررًا بالمجني عليه ويستوي أن يكون الضرر مادي أو معنوي، فالسر هو الذي يترتب على إفشاءه مساس بما يؤثر بشخص المجني عليه وبما يؤثر في قدرته على الإحتفاظ بهذا السر دون أن يطلع عليه أحد سوى من إئتمنه عليه، في حين نجد البعض الآخر يشير إلى أن حتى النبأ أو الخبر أو المعلومة تصح أن تكون سرًا طالما أنه يمس بخصوصية صاحبها حتى ولو كانت غير مشينة وغير ماسة بالكرامة أو السمعة. (أنظر: – **بلال أمين زين الدين:** المرجع السابق، ص 286. – **محمد علي سويلم:** المرجع السابق، ص459).

غير مشروعة، وهو ما يستفاد من الصيغة المطلقة التي جاءت بها الفقرة الثانية من المادة (394 مكرر 2) من (ق ع ج)، إذ أراد المشرع من ذلك أن يمنع إفشاء المعلومات المتحصلة من جرائم الإعتداء على النظام المعلوماتي.

ج- النشر *La Diffusion*: يعتبر فعل "النشر" حسب الفقرة الثانية من المادة (394 مكرر 2) فعل مشترك بين صورتي جريمة التعامل غير المشروع في معطيات النظام، وقد بينا في الصورة الأولى من جريمة التعامل غير المشروع في معطيات صالحة لإرتكاب الجريمة المقصود من فعل "النشر"، لكن الغريب في الأمر أن نفس المصطلح ذكره المشرع في الصورة الثانية من جريمة التعامل غير المشروع في معطيات متحصلة من الجريمة، وهنا نتساءل هل هذا التكرار لمصطلح "النشر" كان مقصودًا من المشرع، أم أن هذه العبارة وقعت سهواً حين صياغتها، إذ ذكرت في كل من الفقرة الأولى والثانية على التوالي من المادة (394 مكرر 2) إذ لا يمكن أن يتضمن نص المادة نفس العبارة في كل من الفقرتين بنفس المعنى.

وعمومًا فإنه يقصد بهذا الفعل نشر المعطيات والمعلومات المتحصل عليها من إحدى الجرائم المعلوماتية بطريقة غير مشروعة، وذلك بإطلاع شخص أو عدد أكبر من الأشخاص عليها[1]، وهو الفعل الذي يقوم به عادةً "المخترقون للمواقع الإلكترونية – الهاكرز والكراكرز- وهم أشخاص يتميزون بسعة الخبرة الفنية والإدراك الواسع للمهارات التقنية، فيقومون بالتسلل إلى هذه المواقع والنظم قصد الإطلاع على ما تحتويه من بيانات مخزنة بداخلها، وذلك من أجل سرقتها أو العبث والتلاعب بها أو نشرها للجميع إضرارًا بأصحابها وإنتقامًا منهم من أجل التشهير وتشويه السمعة[2]، أو حتى من أجل التحدي وإظهار مقدرتهم على قهر النظام المعلوماتي[3].

والمشرع الجزائري لم يشترط في فعل النشر الإلكتروني أن يتكرر لأكثر من مرة، بل يكفي لقيام الجريمة إرتكابه مرة واحدة فقط، سواء كان النشر بمقابل أو بدونه، فالفعل يتحقق في

---

[1]- **يزيد بوحليط:** المرجع السابق، ص194.

[2]- **جريمة التشهير وتشويه السمعة:** هي من أخطر الجرائم التي ترتكب بواسطة الفضاء الإلكتروني باستخدام شبكة الإنترنت، حيث تعتبر هذه الأخيرة مسرحًا غير محدود في تلقي كل ما يدرج عليها دون قيد أو رقابة، لذلك تشكل بعض حالات النشر السلبي جرائم تؤذي البعض خاصة إذا تم التشهير بهم عبر إيراد معلومات خاصة بهم صحيحة كانت أم مغلوطة، حيث تتيح شبكة الإنترنت الفرصة للمجرمين وذوي النفوس المريضة بالقيام بنشر معلومات قد تكون سرية أو مظللة أو حتى مغلوطة تضر بالضحية سواء كان فردًا أو أسرةً أو مجتمعًا أو دينًا أو مؤسسةً. (أنظر: - **نبيل صقر:** الوسيط في شرح جرائم الأموال، المرجع السابق، ص203).

[3]- **غنية باطلي:** المرجع السابق، ص193. - **رشيدة بوكر:** المرجع السابق، ص 115.

كلتا الحالتين[1]، هذا ولم يحدد أيضًا المشرع الجزائري وسيلة معينة يتم بها فعل النشر، وعلى إثر ذلك يستوي إستعمال كل الوسائل سواء عن طريق الوسائل التقليدية كالكتابة على الورق أو الصحف وغيرها، أو عن طريق نشرها بإستعمال الوسائل التقنية الحديثة كالكتابة على الصفحات الإلكترونية أو على الأقراص المضغوطة أو الممغنطة أو المدمجة...[2].

ولعل أبرز وسائل إرتكاب هذه الجريمة هو إنشاء مواقع على الشبكة تحتوي على المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر البريد الإلكتروني أو عن طريق وسائل التواصل الإجتماعي إلى أكبر عدد ممكن من المستخدمين للشبكة، والأمثلة من الواقع كثيرة عن هذه الجرائم كنشر صورة مركبة لإحدى الشخصيات أو لإحدى الفنانات أو من عامة الناس وهي مثلاً عارية أو في وضع مشين ومستنكر، أو مثلاً نشر معلومات غير صحيحة بالمرة عنهم ...الخ[3].

د- الإستعمال *Faire un Usage*: يعتبر فعل "الإستعمال" أخطر سلوك يمكن أن يقع على المعلومات المتحصل عليها من جريمة، ذلك أنه إذا كانت حيازة المعلومات غير المشروعة وإفشاؤها ونشرها أمورًا خطيرةً، فإن الأخطر من ذلك كله هو القيام بإستعمال هذه المعطيات[4].

وعنصر الإستعمال عنصرًا واسعًا وفضفاضًا، فالمشرع يرمي إلى تجريم الإستعمال مهما كانت كيفيته أو غرضه، بمعنى أنه وإن كان فعل الإستعمال يختلف عن الأفعال السالف ذكرها، إلا أنه لا يمكن تصور حالات يتم فيها الإستعمال غير المشروع للمعطيات دون حيازتها أو إعلام الغير بها أي دون نشرها وإفشائها[5].

وعليه لم يخفى على المشرع الجزائري أن يجرم فعل الإستعمال في حد ذاته بصفته أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من إحدى الجرائم المعلوماتية، كأن يستعمل شخص ما معطيات أو معلومات عن شخص آخر منافس له تم الحصول عليها بطريقة غير مشروعة أو أن تستعمل شركة ما معطيات شركة منافسة لها[6]، ومن قبيل ذلك أيضًا جريمة التزوير المعلوماتي ثم إستعمال هذا المزور[7]، ويشمل هذا التجريم كل إستعمال في معالجة معطيات شخصية للغير لربطها

---

[1]- **دينا عبد العزيز فهمي:** المرجع السابق، ص145.

[2]- **مصطفى محمد موسى:** أساليب إجرامية بالتقنية الرقمية، ما هيتها ومكافحتها، دار الكتب القومية، القاهرة، مصر، 2005، ص16.

[3]- **نبيل صقر:** الوسيط في شرح جرائم الأموال، المرجع السابق، ص203.

[4]- **محمد علي سويلم:** المرجع السابق، ص413.

[5]- **غنية باطلي:** المرجع السابق، ص193. - **يزيد بوحليط:** المرجع السابق، ص195.

[6]- **محمد خليفة:** المرجع السابق، ص110. - **رشيدة بوكر:** المرجع السابق، ص115.

[7]- أنظر في ذلك الفصل السابع من قانون العقوبات الجزائري، تحت عنوان "التزوير" بموجب المواد من (197 حتى 229) منه.

بمحتوى مناف للأخلاق والآداب العامة، أو لإظهارها بطريقة من شأنها المساس بإعتباره أو شرفه، بحيث يشمل هذا التجريم كل إستعمال مهما كان نوعه أو الغاية منه، وهذا ما يفهم من خلال عبارة "...أو أي إستعمال لأي غرض كان..."[1].

ويستفاد من نص المادة المطلق أن فعل الإستعمال ولو لمرة واحدة تقوم به الجريمة لأنه لم يرد تحديدًا لعدد المرات اللازمة لقيامها، بمعنى تتحقق هذه الجريمة بفعل الإستعمال حتى ولو وقع هذا الإستعمال لمرة واحدة فقط[2]، كما لم يتطلب المشرع الجزائري حدوث نتيجة إجرامية معينة جراء هذا الفعل، ولا يتطلب أيضًا أن يتحقق ضرر فعلي وحال يقع على المعطيات، فهو إذ يجرمها بوصفها أفعالاً خطرةً يمكن أن تؤدي إلى ضرر فعلي مادي كان أو معنوي[3].

وفي الأخير يجدر بنا التنويه هنا إلى أن هذه الجريمة الواردة في نص المادة (394 مكرر 2) هي من الجرائم الشكلية، أي أنها تقع وتكتمل بمجرد وقوع الفعل المكون لها، أي الحصول على المعطيات بطريقة غير مشروعة دون أن يتطلب المشرع في نموذجها القانوني أية نتيجة إجرامية تترتب على هذا الفعل وكل الأفعال الأخرى، فهذا النوع من الإجرام يكفي فيه مجرد إتيان النشاط المادي تحديدًا وليس الركن المادي كليةً والذي يكشف به الجاني عما يجول في خاطره ويهدد به[4]، بمعنى أنه يقرر المشرع في إرتكاب الجريمة تامة بمجرد إرتكاب السلوك دون النظر إلى الآثار التي يرتبها هذا السلوك[5].

الفرع الثالث: الركن المعنوي للجريمة

تعتبر جريمة التعامل غير المشروع في معطيات النظام بصورتيها الأولى والثانية كما سبق بيانه من الجرائم العمدية، وهو ما يستفاد من عبارة نص المادة (394 مكرر 2) بقولها: "... كل من يقوم عمدًا وعن طريق الغش ..."، وكذا عبارة "... وبدون مبرر شرعي..." التي وظفها المشرع الفرنسي في المادة (323-3-1) هي نفس العبارة التي إعتمدها المشرع المصري في المادة (22)

---

[1]– أنظر الفقرة الثانية من نص المادة (394 مكرر 2) من (ق ع ج). **الملحق رقم (05).**

[2]– **محمد محمد صالح الألفي:** المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2011، ص64-65.

[3]– **غنية باطلي:** المرجع السابق، ص193.

– **رشيدة بوكر:** المرجع السابق، ص116.

[4]– **عمر سالم:** شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، مصر، 2010، ص325.

[5]– ***TASRPALAS (A) :*** *Le moment et la duree de les infractions pénales, Ed, D, Paris, France, 1996, P128.*

بقوله: "وبدون مسوغ من الواقع أو القانون ..."، وهذا ما يجعلها جريمة مقصودة يتطلب لقيامها توافر القصد الجنائي بنوعيه العام والخاص[1].

فالقصد الجنائي العام على النحو السالف بيانه يتألف من عنصرين "العلم والإرادة"، فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي الذي يأتيه ويقوم به، من تصميم أو بحث أو تجميع أو توفير أو نشر أو إتجار أو حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان في المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[2]، كما يتعين أن يعلم الجاني بخطورة هذه الأفعال على محل الجريمة[3] الذي يناله الإعتداء.

كما يلزم توافر إرادة النشاط سواء كانت الجريمة من جرائم النتيجة أم من جرائم السلوك المجرد أو المحض، ومثال هذه الأخيرة جريمة حيازة معطيات غير مشروعة، أي أن تتجه إرادة الجاني إلى أحد الأفعال التبادلية الواردة في نص القانون، وبالتالي ينبغي أن يكون مثل هذا السلوك إراديًا ولو لم يسفر عن وقوع نتيجة معينة[4]، وعليه إذا إنتفت هذه الإرادة إنتفى معها القصد الجنائي، كما لو ثبت أن هذه الإرادة معدومة أو بها عيب من العيوب[5].

وفي هذه الصورة من الجرائم لا يكفي توفر القصد الجنائي العام، بل لابد من توافر القصد الجنائي الخاص، وهو إتجاه نية الجاني في التعامل بهذه المعلومات غير المشروعة إلى الإعداد والتمهيد لإستعمالها في إرتكاب جريمة من جرائم الإعتداء على نظام المعالجة الآلية للمعطيات عن طريق الغش المعلوماتي[6].

---

[1]– **غنية باطلي:** المرجع السابق، ص194.

[2]– **رشيدة بوكر:** المرجع السابق، ص117. – **يزيد بوحليط:** المرجع السابق، ص196.

[3]– محل الجريمة هنا يكمن في المعلومات والمعطيات المعالجة آليًا والموجودة خارج النظام المعلوماتي، والتي يمكن أن تكون مخزنة على أشرطة ممغنطة أو على السيديهات أو على الفلاش ديسك أو على البطاقات الإئتمانية وغيرها، كما يشكل محل الجريمة هنا كل الأجهزة والأدوات والبرامج المصممة والمعدة خصيصًا لإرتكاب واحدة أو أكثر من جرائم الإعتداء على نظم المعالجة الآلية، وعليه فإن محل هذه الجريمة مزدوج، فمن جهة فإن الأفعال المعاقب عليها من حيازة أو توفير أو تصميم... وغيرها، ومن جهة أخرى إعدادها من أجل إرتكاب جريمة أخرى من جرائم الإعتداء على نظم المعالجة.

[4]– **سليمان عبد المنعم:** المرجع سابق، ص438.

[5]– لا يكفي لقيام المسؤولية الجنائية أو ما يعرف أحيانًا بأهمية الإسناد هو توافر الإرادة الواعية أو التمييز لدى مرتكب الجريمة، بل يجب أن يكون متمتعًا بحرية الإختيار، لأن الجاني أحيانا قد يكون مميزًا وواعيًا لحقيقة ودلالات أفعاله، لكنه قد يتجرد في نفس الوقت من إرادته، كما في حالة "الإكراه المادي"، وقد ينتقص من إرادته فحسب على نحو يجعلها إرادة معيبة غير حرة "كالإكراه المعنوي وحالة الضرورة".
(أنظر: – **محمود نجيب حسني:** المرجع السابق، ص550، – **عوض محمد عوض:** المرجع السابق، ص510. – **جلال ثروت:** المرجع السابق، ص406).

[6]– **عبد الوهاب مليايني:** المرجع السابق، ص 202.

المطلب الثاني: العقوبات المقررة لجريمة التعامل غير المشروع في معطيات النظام

من أهم الأحكام الخاصة بهذه الجريمة والتي جاء بها المشرع الجنائي عمومًا والمشرع الجزائري على وجه الخصوص هو تقرير نظام عقابي صارم لها، سواءً من حيث العقوبات الأصلية (فرع أول) أو من حيث العقوبات التكميلية (فرع ثاني).

الفرع الأول: بالنسبة للعقوبات الأصلية

لابد علينا هنا أن نفرق بين العقوبات المقررة والمطبقة على الشخص الطبيعي (أولاً) والعقوبات المقررة على الشخص المعنوي (ثانياً) بالإضافة إلى كل من عقوبة الإشتراك والشروع في الجريمة (ثالثاً).

أولاً: العقوبات المقررة للشخص الطبيعي

وهنا أيضًا سوف نتكلم عن عقوبات هذه الجريمة في حالتها البسيطة، ثم يليها بعد ذلك عقوبات هذه الجريمة في حالاتها المشددة.

أ- العقوبة البسيطة للجريمة: بالنسبة للمشرع الفرنسي لم يذكر عقوبة محددة بعينها بالنسبة لهذه الجريمة والمنصوص عليها في المادة (323-3-1) من (ق ع ف)، وإنما قام بإحالة مسألة مقدار العقوبة هنا على نص المواد من (323-1) إلى (323-3) من نفس القانون، كما سبق لنا وأن بيَّناه في الجرائم السالف ذكرها[1].

ذلك أن نص المادة (323-3-1) من (ق ع ف)[2] والتي جاء نصها: "كل من يقوم بحيازة أو توفير تجهيزات أو أدوات برنامج معلوماتي أو كل معطيات مصممة أو معدة لإرتكاب الجرائم المنصوص عليها في المواد (323-1) إلى (323-3) يعاقب بالعقوبات المقررة للجريمة نفسها أو بعقوبة الجريمة الأشد".

[1]- أنظر نص المواد من (323-1) حتى (323-3) من (ق ع ف). **الملحق رقم (03)**

[2]- ***Article 323-1 : Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4***

« - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

بينما عاقب المشرع المصري على هذه الجريمة بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة 300.000 ألف جنيه ولا تجاوز خمسمائة ألف 500.000 جنيه[1].

أما عن المشرع الجزائري فقد عاقب على هذه الجريمة بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج، وما يلاحظ هنا أن المشرع الجزائري خفض من الحد الأدنى للعقوبة السالبة للحرية، ورفع من مقدار العقوبة المالية برفع حديها الأدنى والأقصى معا، وهذا مقارنة بالعقوبات المقررة في جريمة التلاعب المعلوماتي المرتكبة بمفهوم نص المادة (394 مكرر 1) وذلك بسبب عنصر العمد والخطورة.

ب- العقوبة المشددة للجريمة: لم يكتفي المشرع الجزائري بالعقوبات البسيطة المقررة لجريمة التعامل غير المشروع في المعطيات حسب نص المادة (394 مكرر 2)، وإنما نص أيضًا على تشديد عقوبة هذه الجريمة بجعلها مضاعفة، وهذا ما ذكرته المادة (394 مكرر 3) من نفس القانون بقولها: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".

وحسن فعل المشرع الجزائري في ذلك، حيث إعتبر هذه الجريمة وكل الجرائم المعلوماتية التي تستهدف مؤسسات الأمن والدفاع الوطني أو أي من المؤسسات الرسمية التابعة للدولة، يتم تشديد العقاب فيها، أي أن العقوبة المشددة تنصرف على جميع الجرائم المنصوص عليها في المواد من (394 مكرر) حتى (394 مكرر 8). ويبدو هنا أن المشرع حرص على ضمان حماية مطلقة لهيئات الدفاع الوطني وكل مؤسسات الدولة الجزائرية، ولا غرابة في ذلك طالما أن هذه المؤسسات وخاصة مؤسسة الدفاع الوطني، إذ تكتسي طابع خاص وحساس بما تحتويه أجهزتها الإلكترونية وحواسيبها من معلومات ومعطيات ذات أهمية بمكان، بحكم أن نظمها المعلوماتية ذات طابع خاص وحساس وأن معلوماتها غاية في السرية، وأن المساس بها يمس بسلامة الدولة وإقتصادها وأمنها، وهي مستهدفة بالدرجة الأولى من طرف قراصنة ومجرمي الإنترنت باللجوء إلى إستخدام أساليب الإحتيال لإختراق المواقع الإلكترونية والحصول على المعلومات بشكل غير مشروع[2].

ويمكن إدراج هذه الجرائم بما يطلق عليه اليوم "بجرائم تعطيل الأعمال الحكومية *Crimes de perturbation des affaires du gouvernement*" والمهددة للأمن القومي، سيما إذا أخذنا بعين

[1]- أنظر نص المادة (22) من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

[2]- **زيدان زبيحة:** المرجع السابق، ص100.

الإعتبار الظاهرة الجديدة المسماة في فقه القانون الجنائي الحديث "بالإرهاب الإلكتروني *Cyber terrorisme*" وعلاقته بالجريمة المنظمة والعابرة للحدود الوطنية[1]، ويتضح تفصيل ذلك من خلال ما شرحناه سابقًا في تعريف وتوضيح أحكام جرائم الدخول أو البقاء غير المشروع عن طريق الغش في منظومة البيانات المعالجة آليًا أو إعتراض سير هذه البيانات المرسلة عن طريق منظومة معلوماتية.

والحال أن هاجس الأمن المعلوماتي بات يؤرق جميع الأوساط الحكومية في العالم، طالما أضحت هذه الجرائم المعلوماتية تشكل تهديدًا متزايدًا وظاهرة إجرامية خطيرة وفي تصاعد مستمر، وقد تصدت مختلف التشريعات العالمية ومنها المشرع الجزائري إلى اللجوء لسياسة التشديد في العقاب على إعتبار أنها من أخطر أنواع الجرائم في الوقت الراهن[2].

إذ يستخلص من نص المادة (394 مكرر 3) بإمكانية تطبيق عقوبات أشد، وهذا ما جاء صراحةً في عبارة "... دون الإخلال بتطبيق عقوبات أشد" وهي المنصوص عليها أيضًا في المواد من (61) إلى (87 مكرر 12) من (ق ع ج) تحت عنوان "الجنايات والجنح ضد أمن الدولة"، وكل ما يندرج فيها على الأخص في خانة الجرائم الماسة بأمن الدولة وبمؤسساتها أو الوحدة الوطنية والسلامة الترابية[3]، لذا يمكن للقاضي الجنائي هنا اللجوء إلى تطبيق عقوبات أشد على مرتكب إحدى الجرائم المنصوص عليها في المادة (394 مكرر 2)، وذلك إذا ما أدت هذه الجرائم إلى المساس بأمن الدولة ومؤسساتها ووحدتها، وبالتالي فإنه بإمكان جريمة إختراق أو تجسس إلكتروني أن توصل صاحبها إلا ما لا يحمد عقباه.

---

[1]– هذه الجريمة الخطيرة تصدت لها مختلف التشريعات الجنائية المقارنة وفي مقدمتها إتفاقية الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية، والمعتمدة من طرف الجمعية العامة بتاريخ 2001/05/31، والتي صادقت عليها الجزائر على الإنضمام إليها بتحفظ بموجب المرسوم الرئاسي رقم (04-165) والمؤرخ في 2004/06/08، ومن الملاحظ هنا أن المشرع الجزائري يلتزم دائمًا في الإنسجام مع الإتفاقيات الدولية التي إنضمت إليها، وخاصةً ما يتعلق منها بالجرائم المعلوماتية والإرهاب والجريمة المنظمة والعابرة للحدود، ونصت بذلك على ملاحقة كل جزائري ينشط أو ينخرط في الخارج في جمعية أو جماعة أو منظمة إرهابية أو تخريبية مهما كان شكلها أو تسميتها حتى وإن كانت أفعالها غير موجهة ضد الجزائر. أنظر في ذلك: نص المادة (87 مكرر 6) من (ق ع ج).

[2]– **زيدان زبيحة:** المرجع السابق، ص101.

[3]– أنظر في ذلك المواد من (61) حتى (87 مكرر 12) من (ق ع ج) والمتعلقة بالجنايات والجنح ضد أمن الدولة، والمستحدثة بالقانون رقم (06-23) المؤرخ في 20 ديسمبر 2006، وكذا القانون رقم (14-01) والمؤرخ في 4 فبراير 2014، والقانون رقم (16-02) والمؤرخ في 19 يونيو 2016، وكلها قوانين تعدل وتتمم قانون العقوبات.

ثانيا: بالنسبة للعقوبات المقررة للشخص المعنوي

كما ننوه هنا أيضًا بأن المشرع الجزائري إنتهج نفس الموقف في تحميل الشخص المعنوي المسؤولية الجنائية، ومن ثم معاقبته مثلما فعله مع كل الجرائم السالف ذكرها، وهذا بموجب نص المادة (394 مكرر 4) بقولها: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"[1].

ثالثا: بالنسبة لعقوبة الإشتراك في الجريمة والشروع فيها

وهنا أيضًا حتى لا نقع في فخ التكرار لما سبق الحديث عنه في مسألة معاقبة الشريك في الجريمة، وكذا العقاب على الشروع في الجريمة، فهنا نجد أن قانون العقوبات الجزائري فصل ووضح هذه العقوبات كما يلي:

أ- بالنسبة لعقوبة الإشتراك: أما عن العقوبات التي تلحق الشخص الشريك جاء ذكرها في نص المادة (394 مكرر 5) بقولها: "كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

ب- بالنسبة لعقوبة الشروع: وكذلك الأمر فيما يخص مسألة الشروع في إرتكاب هذه الجريمة ذات الوصف الجنحي، فإن المشرع يعاقب على الشروع متى كان منصوص عليه صراحةً، حيث جاء في نص المادة (394 مكرر 7) أنه: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

---

[1]- وهذا ما جاء في الباب الأول مكرر من قانون العقوبات تحت عنوان "العقوبات المطبقة على الأشخاص المعنوية" والمستحدة بالقانون رقم (04-15) المؤرخ في 10 نوفمبر 2004، والمعدل والمتمم بالقانون رقم (06-23) المؤرخ في 20 ديسمبر 2006، حيث نصت كل من:

- المادة (18 مكرر): "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي: - الغرامة التي تساوي من مرة (1) إلى خمسة (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة ...".

- المادة (18 مكرر 2): "عندما لا ينص القانون على عقوبة الغرامة بالنسبة للأشخاص الطبيعيين سواء في الجنايات أو الجنح، وقامت المسؤولية الجزائية للشخص المعنوي طبقاً لأحكام المادة (51 مكرر) فإن الحد الأقصى للغرامة المحتسب لتطبيق النسبة القانونية المقررة للعقوبة فيما يخص الشخص المعنوي يكون كالآتي:

- 2.000.000 دج عندما تكون الجناية معاقباً عليها بالإعدام أو بالسجن المؤبد.

- 1.000.000 دج عندما تكون الجناية معاقباً عليها بالسجن المؤقت.

- 500.000 دج بالنسبة للجنح".

الفرع الثاني: بالنسبة للعقوبات التكميلية

يمكننا أن نشير هنا أنه علاوةً على العقوبات الأصلية السالف الإشارة إليها، ونظرًا لوعي المشرع بخطورة المساس بنظم المعالجة الآلية التي تقوم عليها جل التعاملات الإلكترونية، وما يترتب عن ذلك من تهديد جدي للمصالح المرتبطة بها، فقد أورد المشرع الجزائري عقوبات تكميلية، وذلك حسب ما جاء في سياق نص المادة (394 مكرر 6) بقولها: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقًا لهذا القسم، علاوةً على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد اُرتكبت بعلم مالكها".

وعليه إستثنت المادة نفسها الغير حسن النية بحفظ حقوقه ونصت على مصادرة الأجهزة المستعملة والبرامج والوسائل المستعملة مع إلحاق ذلك بغلق المواقع، وكذا أماكن الإستغلال شريطة أن تكون الجريمة قد أُرتكبت بعلم صاحب أو مالك تلك المحلات، ومن الواضح أن تطبيق هذا النص يثير إشكالات عديدة في الحياة العملية سيما بخصوص إجراءات وطرق التفتيش والتحري عن جريمة من هذا النوع نظرًا لطابعها الفني والتقني.

ذلك أن العقوبات المنصوص عليها هنا وإن كانت تبدو قابلة للتطبيق فيما يتعلق بمصادرة الأجهزة من حواسيب وملحقاتها وكذا البرامج، فكل ذلك لا يثير أية إشكاليات أو عوائق، لكن الصعوبة قد تكمن في إغلاق هذه المواقع الإلكترونية، سيما إذا كانت هذه الأخيرة لا تقع تحت نطاق الإختصاص المحلي للإقليم الوطني[1]، وهنا حاول المشرع الجزائري فعلاً تداركه لهذا الوضع بإصداره للقانون رقم (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[2].

رأينا الخاص:

يتضح لنا من جريمة الإعتداء والتعامل غير المشروع في المعطيات والموجودة خارج النظام المعلوماتي بصورتيها الأولى والثانية كما تم توضيحه في الفصل الأول من هذا الباب، أن المشرع الجزائري إتجه نحو سياسة جنائية جديدة، وهو التوسع في تجريم جملة من أشكال التعامل غير المشروع في المعطيات والتي يمكن أنها تستعمل في إرتكاب الجرائم الماسة بأنظمة المعالجة

[1]- زيدان زبيحة: المرجع السابق، ص106.

[2]- أنظر في ذلك: الملحق رقم (06).

الآلية للمعطيات، إذ لا يقتصر الأمر على المعطيات المخزنة داخل النظام المعلوماتي فقط، وإنما أيضًا على المعطيات الموجودة خارج المنظومة المعلوماتية.

كما إنفرد المشرع الجزائري عن باقي نظرائه من المشرعين – وأخص بالذكر الفرنسي والمصري – في تجريمه التعامل في معطيات متحصلة من جريمة بنص صريح بموجب الفقرة الثانية من المادة (394 مكرر 2)، وهو مسلك حسن الهدف من ورائه الوقاية من هذه الأفعال التي تشكل عدوان حقيقي على النظم المعلوماتية، وكذا ضمان عدم إفلات المجرم المعلوماتي من المساءلة الجنائية، وهذا إتجاه حسن يساير فعلاً الأنظمة التشريعية الحديثة في مجال حماية المعطيات ذات الطابع الشخصي والسري والمؤسساتي خاصةً في ظل توجه الجزائر نحو عصرنة قطاعاتها الإدارية والقضائية وكل منظوماتها بإستخدام تكنولوجيات الإعلام والإتصال إستجابة لمتطلبات عولمة الحكومة الإلكترونية.

المبحث الثاني: جرائم مقدمي خدمة الإنترنت

تمهيد وتقسيم:

تتمتع شبكة الإنترنت وما تحتويه من مواقع إلكترونية بطابع خاص يميزها عن غيرها من وسائل الإتصال التقليدية، فكان من الضروري أن يحكمها نظام خاص بها، ينبثق من النظرة التشريعية المتطورة بشأن تحديد المسؤولية الجنائية عن الجرائم المرتكبة عبر الشبكة وهذه المواقع، على نحو يحول دون إفلات مرتكبي هذه الجرائم عبرها من العقاب، وبما لا يعوق الطبيعة الفنية الخاصة لهذه التقنية، حيث أوصى المجلس الأعلى للوسائل السمعية والبصرية بإتحاد الدول الناطقة بالفرنسية، والمنعقد ببلجيكا في شهر مارس من سنة 1998، بأن يراعي في المسؤولية الجنائية عبر شبكات المعلومات والمواقع الإلكترونية تطبيق صارم لقانون العقوبات والقوانين المكملة له، بما يتماشى مع خصوصية الإنتهاكات التي تقع عبرها[1].

وبما أن التعامل الإلكتروني يتطلب تشغيل الوسائل الإلكترونية وعلى رأسها شبكة الإنترنت، ولما كانت هذه الأخيرة عبارة عن أنشطة متعددة تشارك كل واحدة منها في عملية تشغيل أجهزة تخزين المعلومات وبثّها وعرضها، فإنها تتطلب في المقابل وجود أشخاص قائمين على هذا التشغيل يطلق عليهم "الوسطاء في خدمة الإنترنت"، أو كما تسميهم بعض التشريعات المقارنة "بمقدمي خدمة الإنترنت"[2].

ومع التطور الهائل الذي شهدته تقنية الإنترنت في السنوات الأخيرة وما تضمنته من محتوى إلكرتوني في شتى التعاملات، إتسع معها الجدل حول نوع المسؤولية الملقاة على عاتق مقدمي الخدمات الخاصة عن المعلومات الوارة في ذلك المحتوى إذا ما تضمنت الإساءة للمتعاملين في مواقع التعاملات الإلكترونية أو حتى نشر وقائع تشكل جريمة.

ومما لا شك فيه أن من شأن تحديد المسؤولية الجنائية لمقدمي الخدمات في شبكة الإنترنت يؤدي بالضرورة إلى نوع من الحماية الجزائية للتعاملات الإلكترونية هذا من جهة، ومن جهة أخرى يساهم في تأمينها، مما يشجع المتعاملين على الإقدام على التعامل بواسطة الإنترنت[3].

---

[1]– **محمد محمد صالح الألفي:** المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، المكتب المصري الحديث، ط1، الإسكندرية، مصر، 2005، ص77.

[2]– **عبد الرحمن عبد الله السند:** الأحكام الفقهية للتعاملات الإلكترونية، ط3، دار الوراق، الرياض، السعودية، 2006، ص87.

[3]– **رشيدة بوكر:** المرجع السابق، ص123.

ولبيان الأحكام التي تقوم عليها جرائم مقدمي خدمات الإنترنت سوف سوف نتطرق إلى كل مفهوم مقدمي خدمات الإنترنت، ثم نعرج بعدها إلى جدلية المسؤولية الجنائية لمقدمي خدمات الإنترنت، وأخيرًا الحديث عن تقرير المسؤولية الجنائية لمقدمي خدمات الإنترنت، وهذا وفق المطالب الثلاثة التالية:

المطلب الأول: مفهوم مقدمي خدمات الإنترنت

المطلب الثاني: أساس المسؤولية الجنائية لمقدمي خدمات الإنترنت

المطلب الثالث: تقرير المسؤولية الجنائية لمقدمي خدمات الإنترنت

المطلب الأول: مفهوم مقدمي خدمات الإنترنت

يعد مقدمي خدمات الإنترنت من أحد أهم المتدخلين عبر مواقع الإنترنت وأبرز مقدمي الخدمات عبرها، لما لهم من أهمية في تخزين مضامين ومعطيات المواقع الإلكترونية، فهم بمثابة الوسيط الفني وأداة الوصل وقناة الإتصال بين كافة المتعاملين الإلكترونيين على إختلاف أنواعهم ومراكزهم، فهم بمثابة المحرك الأساسي للمحتوى الإلكتروني عبر الشبكة، ويترتب على عدم تأدية الواجب المناط بهم قطع كافة قنوات الإتصال وآليات المفاوضات والإبرام بين أطراف التعامل.

وحيث أن وسطاء الخدمة بأنواعهم المختلفة ذوي علاقة بشكل أو بآخر فيما يتعلق بآلية عمل التعاملات الإلكترونية، لأن كل منهم يؤدي جزءًا من نظام "العملية المعلوماتية *Processus informationnel*" التي تتعلق بمحتوى هذه التعاملات عبر الشبكة[1]، فهم بالتالي لهم دور إيجابي في حماية النظم والمواقع التي تتعامل مع شبكة الإنترنت من كل المحتويات الإلكترونية اللامشروعة وغيرها من الأفعال المستنكرة في المجتمع واللاأخلاقية[2].

ومن أجل الوقوف أكثر على مفهوم مقدمي خدمات الإنترنت يقتضي الأمر هنا تحديد أهم التعاريف التي تناولت هؤلاء الوسطاء (فرع أول)، ثم تبيان طبيعة الوظيفة التقنية لمقدمي خدمات الإنترنت وأهم إلتزاماتهم القانونية (فرع ثاني).

الفرع الأول: تعريف مقدمي خدمات الإنترنت

تحظى التعاملات الإلكترونية بأهمية قصوى، حيث أن الهاجس الأول والأخير في هذا النوع من التعاملات هو الثقة والأمان، وهذان العنصران أهم الضمانات التي يتعين توافرها لإزدهار هذه التعاملات الإلكترونية، ولتحديد أكثر هوية هؤلاء المتعاملين كوسطاء فنيون، فقد إستلزم الأمر هنا التطرق إلى تعريفهم بدايةً بالتعريف الإصطلاحي (أولاً)، ثم التعريف الفقهي (ثانياً) وبعدها التعريف القانوني (ثالثاً).

---

[1]– **رشيدة بوكر:** المرجع السابق، ص 122.

[2]– تعبير "اللامشروعة" تعبير قانوني على عكس تعبير "اللاأخلاقية"، بحيث نجده في العديد من المعاهدات الدولية والقوانين الوطنية، فهو تعبير يرتبط بمفاهيم أخرى كالأخلاق والنظام العام والآداب العامة وغيرها من المفاهيم التي تتغير وتتطور من بلد إلى آخر، خاصةً عند تحديد مفهومه فتأخذ بعين الإعتبار الإيديولوجيات والعقائد والديانات والسياسات التي تتغير في المكان والزمان أيضًا، ويندرج في هذا المجال عدة نشاطات يمكن وضعها تحت مضمون عبارة "اللامشروعة أو غير مشروعة" منها على سبيل المثال: "الدعاية العنصرية والخلاعية، الإستغلال الجنسي للقاصرين، ترويج المخدرات عبر الإنترنت، المواقع التي تحرض على العنـــف والدعايات المبغضة وخطابـــات الكراهية". (أنظـــر: – **أودين سلوم الحايك:** مسؤولية مزودي خدمات الإنترنت التقنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2009، ص106).

أولاً: التعريف الإصطلاحي

لقد تعددت المصطلحات والتسميات التي أوردها كل من الفقه والقانون لأطراف التعامل الإلكتروني، فالبعض يصنفهم معتمدًا على كيفية مسار المعلومة، والبعض الآخر يدخل أي شخص يقوم بالإتصال بالإنترنت، والبعض يصنفهم تصنيف تقني[1]، ومن جملة المصطلحات والتسميات المعتمدة هنا نجد ما يلي:

أ- الوسيط الإلكتروني: تنحدر كلمة وسيط *Intermédiaire* من أصل لاتيني *Intermédius*، وهي تعني من يكون الوسط بين حدين، ومنه قوله تعالى: "وَكَذَلِكَ جَعَلْنَكُمْ أُمَّةً وَسَطًا"[2]، كما تدل أيضًا بمن يكون في موضع وسط بين شيئين أو بين شخصين[3] كرابط أو كنظام إنتقالي بحيث يؤمن لهما التواصل، فإذا كانت بعض التعاملات العادية تتطلب تدخل وسيط لإتمامها، فإن التعاملات الإلكترونية في حاجة أكبر لوسطاء أكثر منه في التعاملات العادية، كون هذا التعامل الإلكتروني يتم عن بعد وعبر وسائل إلكترونية مما يثير مسألة الجهالة بالطرف الآخر المتعامل معه إلكترونيًا، وهو ما يتطلب بالضرورة وجود وسيط ذو ثقة ويطمئنّان إليه[4].

ومعنى الوسيط على النحو السالف بيانه يشتمل على فئتين من الوسطاء "الوسطاء النظاميين" و"الوسطاء الفنيون"، ويسمى وسيط نظامي أو قانوني لأن له أثرًا في المركز القانوني للأطراف، فمعيار التمييز بينه وبين الوسيط الفني[5] هو تخصصه في واسطة تعامل إلكتروني قانوني وليس تعامل إلكتروني فني، ذلك أن هذا الدور الأخير منوط بالوسيط الفني، وبالرجوع لقوانين التعاملات الإلكترونية، نجد أن هناك نوعان من المتدخلين يمكن أن ينطبق عليهما معنى وسيط نظامي أو قانوني وهما "مقدم خدمة الإنترنت والوسيط الإلكتروني"[6].

---

[1]- **رشيدة بوكر:** المرجع السابق، ص124.

[2]- سورة البقرة: الآية 143.

[3]- ومنه نقول "الوسيط التجاري" أو "الوساطة القضائية" أو "وسيط الجمهورية" أو "وسطاء النقل" أو "الوسطاء الماليين كالسماسرة" ...وغيرهم.

[4]- **رشيدة بوكر:** المرجع السابق، ص128.

[5]- إن تشغيل شبكة الإنترنت يتطلب تضافر جهود الوسطاء الفنيون، فمنهم من ينقل الخدمة عن طريق خطوط الإتصال، ومنهم من يمكن المستخدم من الوصول إلى الموقع الإلكتروني الخاص به أو المراد الدخول إليه، ومنهم من يخزن المعلومات أو ينتجها أو يوردها، ولعل أهم هؤلاء الوسطاء الفنيون هم "متعهد الوصول إلى الشبكة ومعهد الإيواء الإلكتروني وناقل المعلومات" وهؤلاء تخصصهم فني وليس قانوني (أنظر أكثر: - **رشيدة بوكر:** المرجع السابق، ص133. - **محمد حسين منصور:** المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص150).

[6]- **سليمان عبد الحميد عثمان محمد:** مسؤولية مزود الخدمة المعلوماتية في القانون البحريني، بحث مقدم ضمن كتاب "المعاملات الرقمية وقانون الإنترنت"، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2006، ص168. - **فاروق محمد الأباصيري:** عقد الإشتراك في قواعد المعلومات عبر شبكة الإنترنت، دراسة لعقود التجارة الإلكترونية الدولية، دار النهضة العربية، مصر، 2003، ص12.

ولقد أدى التطور الهائل في ثورة الإتصالات والمعلومات إلى ظهور مصطلح الوسيط الإلكتروني في التعاملات الإلكترونية[1]، وقد ظهر إستخدامه لأول مرة في وثائق لجنة الأمم المتحدة للقانون التجاري الدولي "الأونسيترال"، ثم إستخدمته بعد ذلك بعض الدول العربية في قوانينها المعنية بالتعاملات الإلكترونية ومنها القانون الأردني[2]، بحيث يتمثل هذا الوسيط كطرف محايد في جهة مختصة – طبيعية أو معنوية – وظيفتها توطيد التعاملات الإلكترونية بين الأشخاص الذين يعتمدون على الوسائط الإلكترونية الموجودة على شبكة الإنترنت في إبرام تصرفاتهم، وتعمل هذه الجهة بترخيص من السلطات المختصة في الدولة وتحت إشرافها ضمن أحكام تحدد نظامها وماهية الواجبات الملقاة على عاتقها ومدى مسؤوليتها عن الأضرار التي تلحقها بالمتعاقدين أو الغير[3].

ب– متعهد الإيواء الإلكتروني: هذه التسمية هي من أكثر التسميات والمصطلحات التي تتجه إليها الأبحاث والدراسات القانونية، والتي تقابلها بعض المصطلحات التي لها ذات المعنى ومنها مثلاً "متعهد خدمة الإيواء، متعهد إيواء المواقع الإلكترونية، متعهد الإيواء عبر الشبكة ..."، وهو من يقوم بتأمين مسافة على الشبكة لنشر المحتويات والمضامين الإلكترونية والتي قد لا تكون مشروعة والمضرة بالغير[4].

وهذا على عكس "متعهد الوصول إلى الشبكة" وهو عبارة عن مركز من مراكز التوزيع التي تتألف منها شبكة الإنترنت، وهو موصول بالشبكة بإستمرار، فهو بمثابة الممر الإلزامي لوصول المستخدم إليها أي نقطة وصول وترحيل إلى الإنترنت[5]، وبصفته متعهدًا يلتزم تقنيًا بوصل المستخدمين بالشبكة من خلال أجهزة الكمبيوتر العائدة إليهم بواسطة جهاز "موديم *Modem*".

ج– مقدمي خدمة الإنترنت: مقدمي خدمة الإنترنت *Internet Service Provider (I.S.P)* ومنهم من يصطلح عليه "بمقدمي الخدمات الإلكترونية أو مزودي خدمة الإستضافة ..."، فالإستضافة هي عملية تخزين مستمرة للمعلومات على دعامات المورد المضيفة تؤدي إلى جعل المعلومات جاهزة

---

[1]– حيث عرفته المادة الأولى من القانون الإتحادي الإماراتي والمتعلق بقانون المعاملات والتجارة لعام 2006 بقولها: "الوسيط الإلكتروني عبارة عن برنامج أو نظام إلكتروني لوسيلة تقنية المعلومات التي تعمل تلقائيًا بشكل مستقل كليًا أو جزئيًا دون إشراف من أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الإستجابة له".

[2]– راجع في ذلك نص المادة (2) من القانون الأردني رقم (27 لسنة 2015) بشأن الجرائم الإلكترونية.

[3]– **رشيدة بوكر:** المرجع السابق، ص130.

[4]– **عبد الفتاح بيومي حجازي:** النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص130.

[5]– ***VALÉRIE Sédallian :*** *Droit de l'internet, réglementation, résponsabilités, contrats, Collection association des utilisateurs d'internet (Ed, Net press), Paris, France, 1997, P 123.*

للإسترجاع وبمتناول الأشخاص الذين يرغبون في الإطلاع عليها[1]، وهذا ما سعى كل من المشرع الجزائري ونظيره المصري إلى إستعماله كمصطلح قانوني، كما سوف يأتي بيانه.

ثانيًا: التعريف الفقهي

إهتم البعض من الفقه الجنائي الحديث بدراسة هذا الوسيط أو كما يسميه البعض بمتعهدي إيواء المواقع الإلكترونية أو مقدمي خدمات الإنترنت، محاولين وضع تعريف مناسب له يتلاءم مع طبيعته القانونية والفنية.

– فقد عرفه البعض على أنه: "كل شخص طبيعي أو معنوي يتولى تخزين التطبيقات والسجلات المعلوماتية لعملائه من المستخدمين للشبكة، ويمدهم بالوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى ذلك المخزون عبر شبكة الإنترنت"[2].

– وعرفهم جانب آخر من الفقه بأنهم: "مقدم خدمة التقنية هو كل شخص طبيعي أو معنوي عام أو خاص يعمل على توفير خدمات الإتصال للجمهور، أو يقوم بمعالجة أو تخزين المعلومات، ويلتزم بالإبقاء على البيانات التي تمكن من التعرف على صاحب الموقع أو المحتوى البياناتي"[3].

– وعرف أيضًا بأنه: "كل شخص طبيعي كان أو معنوي يقوم بتخزين صفحات الويب والمواقع الإلكترونية عبر أنظمته المعلوماتية بمقابل أو بالمجان، على أن يلتزم بقواعد السلامة والربط الكفيلة بحماية شبكة الإنترنت، وضمان إستمرارية النفاذ إلى هذه الصفحات والمواقع"[4].

– وقيل أيضًا بأنه: "كل شخص طبيعي أو معنوي يزود المستخدمين بخدمات الشبكة أو التواصل بواسطة تقنية المعلومات، ويشمل ذلك كل من يقوم بمعالجة أو تخزين المعلومات نيابة عن مقدم خدمة الإتصالات أو المعلومات"[5].

– وإتجه البعض إلى تعريفه أنه: "مجموعة من الموردين المعلوماتيين الذين يؤمنون تخزين المحتويات والمضامين الإلكترونية وإدارتها وإسترجاع المعلومات التي تتضمنها، والتي يرغب موردوا المضمون بجعلها في متناول الجمهور عبر شبكة الإنترنت[6].

---

[1]– **رشيدة بوكر:** المرجع السابق، ص136.

[2]– **محمد حسين منصور:** المسؤولية الإلكترونية، المرجع السابق، ص202.

[3]– **دينا عبد العزيز فهمي:** المرجع السابق، ص104.

[4]– **عادل بوزيدة:** المرجع السابق، ص26.

[5]– **مركز هردو *HRDO*:** عبارة عن مركز لدعم التعبير الرقمي حول التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، متاح على الموقع: ***www.hrdoegypt.org***، تاريخ التصفح للموقع: 2020/06/17.

[6] أودين سلوم الحايك، المرجع السابق، ص 42.

– وعرفوه أيضًا بأنه: "مزود الخدمة هو من يمكن المشتركين من الوصول إلى شبكة الإنترنت عن طريق مدهم بالوسائل الفنية اللازمة للوصول إلى الشبكة بمقتضى عقد توصيل الخدمة"[1].

– ومن جانبنا نعرف مقدمي خدمات الإنترنت بأنهم: "كل شخص طبيعي أو معنوي يمد المستخدمين للشبكة بالقدرة على الإتصال بواسطة الأنظمة المعلوماتية، ويقدمون لعملائهم خدمة تخزين المحتوى المعلوماتي عبر المواقع والصفحات الإلكترونية بمقابل أو بالمجان، أو أنهم يقومون بمعالجة البيانات وتخزينها بالنيابة عن هؤلاء المستخدمين، وذلك بتوفير مساحات معلوماتية عبر حساباتهم الخادمة لإستضافة هذا المضمون أو المحتوى، مع إمكانية إحالة أسماء مواقع الإيواء عبر محركات البحث لشبكة الإنترنت".

ثالثًا: التعريف القانوني

لقد تناولت كل من الإتفاقيات الدولية والقوانين الوطنية مسألة تعريف مقدمي خدمة الإنترنت، فنجد مثلاً:

أ– في الإتفاقيات الدولية: ونجد هنا على سبيل المثال كل من الإتفاقية الأوروبية والإتفاقية العربية على التوالي:

– عرفته المادة (3/1) من إتفاقية بودابست لعام 2001 بقولها: "يقصد بمقدم الخدمة، أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الإتصال عن طريق نظام الكمبيوتر، وأي كيان آخر يقوم بمعالجة بيانات الكمبيوتر أو تخزينها نيابة عن مزود خدمة الإتصالات أو مستخدمي هذه الخدمة"[2].

– كما عرفته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 بموجب المادة (3/2) بقولها: "مزود الخدمة أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الإتصالات أو مستخدميها"[3].

---

[1]– **محمد نصر:** المسؤولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت، المجلة الجنائية القومية، مج 59، ع 1، دار المنظومة، عمان، الأردن، 2016، ص119.

[2]– أنظر في ذلك: **الملحق رقم (01).**

[3]– أنظر في ذلك: **الملحق رقم (02).**

– وقد عرفه القانون النموذجي "للأونسيترال *UNCITRAL*"[1] بشأن التجارة الإلكترونية الدولية بموجب المادة (5/2) على أنه: "الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو إستلام أو تخزين رسالة المعلومات أو بتقديم خدمات أخرى فيما يتعلق برسالة المعلومات هذه"[2].

ب– في القوانين الوطنية: ومن أهم هذه القوانين التي عرّفت مقدمي خدمات الإنترنت نجد ما يلي:

– عرفته المادة (6–1–2) من القانون الفرنسي رقم (575–2004) والمتعلق بالثقة في الإقتصاد الرقمي بأنه: "كل شخص طبيعي أو معنوي يقدم ولو مجاناً خدمات بواسطة وسائل الإتصال عبر الشبكة، بتخزين الرموز والكتابات والصور والأصوات أو الرسائل أيًّا كانت طبيعتها لفائدة مستعملي هذه الخدمات"[3].

– كما عرف المشرع المصري بموجب المادة (8/1) من القانون رقم (175 لسنة 2018) بقوله: "مقدم الخدمة أي شخص طبيعي أو إعتباري يزود المستخدمين بخدمات تقنيات المعلومات والإتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات"[4].

– وقد عرفه المشرع الجزائري بموجب كل من المادة (19/3) من القانون رقم (07/18) والمتعلق بحماية الأشخاص الطبعيين في مجال معالجة المعطيات ذات الطابع الشخصي[5]، وكذا نص المادة (4/2) من القانون رقم (09–04) والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بقوله: "مقدمو الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"[6].

---

[1]– أنشأت الجمعية العامة لجنة الأمم المتحدة للقانون التجاري الدولي "الأونسيترال *UNCITRAL*" في عام 1966، وهي بمثابة الهيئة القانونية الرئيسية التابعة لمنظمة الأمم المتحدة في مجال القانون التجاري الدولي، وتتمثل مهمتها الأساسية في عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية، بحيث تؤدي هذه اللجنة هذا الدور من خلال إعداد الصكوك التشريعية وغير التشريعية في عدد من مجالات القانون التجاري الدولي، والتي من بينها التجارة الإلكترونية، وتشجيع إستخدام تلك الصكوك وإعتمادها في القوانين الوطنية الداخلية.

[2]– ***Article (2/5) :*** *Le terme « intermédiaire », dispose dans le cas d'un message de données particulier, la personne qui, au nom d'une autre, envoie, reçoit ou conserve le message ou fournit d'autres services afférents à celui…*

[3]– ***Article (6-1-2) :*** *du loi N° (2004-575) du 21 Juin 2004, pour la confiance dans l'économie numérique. Modifié par loi N°: (2016-444) du 13 Avril 2016.*

[4]– أنظر في ذلك: **الملحق رقم (04).**

[5]– أنظر القانون رقم (07/18) المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018، ج ر عدد 34، المؤرخة في 10 يونيو 2018. **الملحق رقم (09)**

[6]– أنظر في ذلك: **الملحق رقم (06).**

الفرع الثاني: طبيعة الوظيفة التقنية لمقدمي الخدمات وإلتزاماتهم القانونية

يتمتع مقدمو الخدمات عبر شبكة الإنترنت بوظيفة خاصة، فبدونهم لا يمكن الوصول إلى محتوى هذه الشبكة، هذا علاوةً على السلطة التي منحهم إياها القانون تجاه محتوى المواقع الإلكترونية محل الإيواء، ناهيك عن الإلتزامات القانونية التي يتوجب عليهم إحترام مضمونها، ومراعاة أحكامها وقت تنفيذها، وهذا ما سوف نفصله في هذا الفرع من خلال الحديث عن طبيعة الوظيفة التقنية لمقدمي الخدمات (أولاً) ثم بعد ذلك نتحدث عن الإلتزامات القانونية لمقدمي خدمات الإنترنت (ثانيًا).

أولاً: طبيعة الوظيفة التقنية لمقدمي الخدمات

من الثابت أن عمل مقدمي الخدمات كوسطاء معلوماتيين على شبكة الإنترنت، إنما يتمثل في تلك الوظيفة التقنية لهؤلاء، إذ يقتصر دورهم على المساهمة المادية في بث المحتوى عبر المواقع الإلكترونية من خلال تقديم المساعدة الفنية لمالكي المواقع في الإتصال بمواقعهم، فدورهم هنا دور فني بحت في توصيل العميل إلى الشبكة بمقتضى إتفاق بينهما، فهو لا يقدم المعلومة أو محتوى المواقع الإلكترونية بل تقتصر مهمته على إيصال المستخدم إلى الإنترنت عن طريق أجهزته الخاصة، وعمله على النحو السالف بيانه أقرب من عمل الموزع في الصحافة المكتوبة[1].

كما يتولى مقدمو الخدمات تخزين المواقع الإلكترونية وإستضافة معطياتها عبر شبكة الإنترنت، ويتولون كذلك إدارة المعلومات والرسائل الخاصة عبر هذه المواقع بعد أن يتيحوا للموردين المعلوماتيين *Ressource d'information*[2] فرصة نشر هذه المعلومات والمحتويات عبر مواقع الإنترنت، فتكون بذلك متاحة لكل الراغبين في الاطلاع عليها، ودورهم هذا يتجاوز حتما دورهم الفني كناقلين للمعلومات[3]، فهم يتولون من جانب إدارة النشاط المعلوماتي عبر المواقع الإلكترونية، ومن جانب آخر فإنهم يمدون موردي المحتوى المعلوماتي بالوسائل التقنية التي تمكنهم

---

[1]– **أكمل يوسف السعيد يوسف:** المسؤولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الإنترنت، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، مصر، 2011، ص32.

[2]– **المورد المعلوماتي** *Ressource d'information*: أو كما يطلق عليه بمورد المحتوى المعلوماتي *Ressource de contenu d'information* هو ذلك الشخص الذي يغذي الشبكة بالمعلومات، فهو أهم أشخاص الإنترنت على الإطلاق سواء أكان هو منتج المعلومة أو مصدرها أو مؤلفها، أم كان مجرد صاحب حق في نشرها وبثها عبر الإنترنت، فقد يكون شخصًا عاديًا وقد يكون مهنيًا متخصصًا في جمع المعلومات وتزويد الشبكات بها، فهو يتحمل عبء إنشاء وجمع المعلومات المتعلقة بموضوع معين، لذلك فهو المسؤول الأول عن تلك المعلومات التي يتم بثها بواسطة الشبكة، وهو كمحترف في إنتاج وبث المعلومات عبر الشبكة يمكن أن تثور مسؤوليته بحسب الأحوال عن تلك المعلومات المزيفة أو الناقصة أو المشينة أو الفاضحة التي يجمعها ويعدها وينشرها على موقعه الإلكتروني. (أنظر كل من: – **عايد رجا الخلايلة:** المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص58. – **رشيدة بوكر:** المرجع السابق، ص138. – **محمد حسين منصور:** المرجع السابق، ص182.

[3]– **أحمد فرج:** النظام القانوني لمقدمي خدمات الإنترنت، مجلة المنارة، المجلد 13، ع 9، 2007، ص325.

من الوصول إلى المواقع التي خزنت فيها المعلومات، فآلية عمل مقدمي خدمات الإنترنت والإمكانيات التقنية والفنية التي يتمتعون بها تساهم وبشكل فعال في تداول المضامين المعلوماتية عبر الشبكة[1].

والواقع أنه يمكن لمقدم الخدمة أن يتولى القيام بوظائف تقنية عدة، فبالإضافة إلى وظيفته الأصلية كمخزن للمعلومات ومراقب لها، فهو يمتلك أيضًا أجهزة معالجة البيانات وذلك من خلال تخزين التطبيقات والسجلات المعلوماتية الخاصة بمالكي المواقع الإلكترونية، والتي تتيح لهم أن يحذفوا أو يعدلوا وبسهولة تامة محتويات مواقع هذه الشبكة، هذا إلى جانب ما يتمتعون به من قدرات فنية تبعًا لما يحوزونه من وسائل تقنية تمكنهم من الوصول إلى هذه المحتويات أو ربط الغير وتمكينهم من الوصول إليها[2]، وهذه سلطات إستثنائية يمارسها مقدمي الخدمة والتي قد تجعلهم عرضة للمساءلة متى إتسمت هذه السلطات بعدم المشروعية[3].

وعمل المتعهد أو الوسيط أو مقدم الخدمة على النحو السالف بيانه يتشابه إلى حد كبير بعمل مدير التحرير في الصحف المكتوبة – الورقية أو الإلكترونية – الذي يخصص مساحة إعلانية لإعلانات شركة معينة مثلاً[4]، لذلك يطلق عليه بمتعهد الإيواء أو المستضيف، ويذهب البعض من الفقه إلى إعتبار العقد الرابط بين مزود المأوى الإلكتروني والمشترك فيه بمثابة عقد إيجار يسمى "بعقد الإيجار المعلوماتي"*Contrat de location à titre informatif*"[5]، حيث يقوم مزود المأوى الإلكتروني بكراء بعض الفضاءات على موزعه الإلكتروني أو على حساباته الخادمة "*Server*" معتمدًا في ذلك على البرمجة السابقة للجهاز أو النظام[6] مقابل أجر معين لكل من يرغب أو يريد تخزين المعلومات فيها أو نشرها على الشبكة[7].

---

[1]– **عادل بوزيدة:** المرجع السابق، ص24.

[2]– **أشرف جابر سيد:** مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة لمسؤولية متعهدي الإيواء، دار النهضة العربية، القاهرة، مصر، 2010، ص92 وما بعدها.

[3]– **عادل بوزيدة:** المرجع السابق، ص25.

[4]– **رشيدة بوكر:** المرجع السابق، ص136.

[5]– **عبد الرؤوف اللومي:** المسؤولية التقصيرية على شبكة الإنترنت، المجلة القانونية التونسية، مركز النشر الجامعي، تونس، 2007، ص66.

[6]– وتجدر الإشارة هنا إلى أن فكرة "البرمجة السابقة" وهي البرامج القادرة على التصرف مكان الإنسان العادي بإستخدام برامج الذكاء الإصطناعي، وهي برامج تتسم بخصائص معينة تميزها عن غيرها من البرامج العديدة والمتنوعة، بحيث يمكن أن تعمل برامج الذكاء الإصطناعي دون أن تخضع لسيطرة الإنسان وتدخله المباشر، ويتميز هذا البرنامج بالإستقلالية والقدرة الفائقة على المعالجة والتخزين والإسترجاع، كما له القدرة على التعامل مع غيره من البرامج وأجهزة الحواسيب والنظم المعلوماتية أو حتى مع الأشخاص العاديين، وكذلك له القدرة على ردّ الفعل والمبادرة. (أنظر أكثر: – **ألاء يعقوب النعيمي:** الوكيل الإلكتروني، مفهومه وطبيعته القانونية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد السابع، العدد 2، الإمارات العربية المتحدة، 2010، ص153).

[7]– **محمد نصر:** المرجع السابق، ص121.

فهو عقد بمقتضاه يضع مقدم الخدمة تحت تصرف المشترك بعض إمكانيات أجهزته أو أدواته المعلوماتية على شبكة الإنترنت من أجل إيواء صفحات معينة من الشبكة "*Web*"[1]، حيث يقوم هذا العميل وهو بمثابة المستأجر لتلك المساحات أو الصفحات بكتابة المضمون أو المحتوى الخاص عليها بطريقة مباشرة، فيقوم بتخزين المادة المعلوماتية المنشورة لكي يتمكن أي عميل آخر من الوصول إليها بسهولة وفي أي وقت[2].

خلاصة القول:

مما سبق الحديث عنه نخلص إلى أن متعهد الإيواء أو مقدم الخدمة يعتبر بمنزلة المؤجر لمكان أو مساحة على الشبكة، إذ يعرض صفحات "الواب *Web*" على حساباته "الخادمة *Server*"، ويكون للمستأجر حرية نشر ما يشاء على هذه الصفحات أو إنشاء مواقع إلكترونية عليها، مع تمكينه من الوصول إليها بواسطة الإنترنت في كل الأوقات عن طريق ما يتم توفيره من وسائل تقنية وإعلامية، كما يتولى متعهد الإيواء مهمة تخزين وإدارة المحتوى الذي قدمه له العميل المستأجر، فهو يسهم في عملية النشر دون أن يكون بإمكانه السيطرة على المعلومة أو المحتوى أو المضمون المنشور قبل عرضه على الإنترنت، فهو يساعد المستخدم في الوصول إلى موقعه الإلكتروني والتجول فيه.

ثانيًا– الإلتزامات القانونية لمقدمي خدمات الإنترنت

من بين أهم الإلتزامات الملقاة على عاتق مقدمي خدمة الإنترنت سواءً في التشريعات المقارنة أو في التشريع الجزائري نجد على سبيل المثال ما يلي:

أ– أهم الإلتزامات التي جاءت في التشريعات المقارنة:

– إلزام مقدم خدمات الإنترنت بالحصول على المعلومات الشخصية للمستخدمين وأصحاب المواقع والصفحات الإلكترونية مسبقًا عند إنشاء هذه المواقع، أو عند وضع محتوى على صفحات التواصل الإجتماعي.[3]

---

[1]– **عبد المهدي كاظم ناصر، حسين عبيد شعواط:** عقد الإيواء المعلوماتي، مجلة الكوفة للعلوم القانونية والسياسية، العدد 21، جامعة الكوفة، العراق، 2014، ص55. – **عبد الفتاح بيومي حجازي:** الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة، المرجع السابق، ص100.

[2]– **محمد حسين منصور:** المرجع السابق، ص202. – **عبد الرؤوف اللومي:** المرجع السابق، ص70. – **عبد المهدي كاظم ناصر، حسين عبيد شعواط،** المرجع نفسه، ص58.

[3]– ***BOSSAN Jérôme :*** *Le droit pénal confronté à la diversité des intermédiaires de l'internet (R S C, N°02) ed. Dalloz, Paris, France ,2013, P295.*

– يلتزم مقدمي خدمات الإنترنت بإحترام الحق في الخصوصية وسرية المراسلات، والحفاظ على حقوق الملكية الفكرية، وعدم جواز نسخ أي بيانات أو معلومات أو نقلها إلى الجمهور دون موافقة أصحاب حقوق الطبع والنشر.[1]

– يلتزم مقدمي خدمات الإنترنت بعدم جوازية إلغاء أو حذف أو تعديل أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات مهما كان نوعها، إلاَّ في حدود السلطات المخولة له.[2]

– يجب على مقدمي خدمات الإنترنت الرقابة المحكمة على المعلومات التي من شأنها أن تهدد سلامة أمن الدولة، وإبلاغ السلطات عنها، وإذا ورد بلاغ لمقدمي الخدمة عن وجود معلومات أو بيانات غير قانونية كالتشهير بأحد الأشخاص، فيتعين عليهم التدخل فورًا لسحب هذه المعلومات أو البيانات، أو الإمتناع عن تخزينها، أو جعل الدخول إليها غير ممكن.[3]

– يلتزم مقدمي خدمات الإنترنت بإبلاغ السلطات والجهات المختصة بعناوين هؤلاء الأشخاص المتعاملين أو المشتركين والبريد الإلكتروني والصفحة الشخصية الخاصة بهم، لاسيما في حالة نشر أي بيانات أو معلومات من شأنها تهديد الأمن القومي أو الإقتصاد القومي للدولة، أو نشر المواد الإباحية، أو التحريض على الإتجار بالبشر أو الأعضاء البشرية، وجميع الأنشطة غير المشروعة.[4]

– يلتزم مقدم خدمات الإنترنت عند حصوله على البيانات المتعلقة بالمستخدمين، عدم الإفصاح عنها أو توفيرها أو معالجتها، وإستثناءًا يجوز لهم ذلك لغرض منع أو كشف جريمة بناءً على طلب رسمي من الجهات المختصة، أو إذا كانت ضرورية أو مصرح بها بموجب القانون.[5]

– يلتزم مقدمي خدمات الإنترنت، بإخطار اللجنة الوطنية المعلوماتية والحريات في حالة إختراق أو قرصنة المواقع الإلكترونية والمساس بالمعلومات والبيانات الشخصية الموجودة بداخلها، وذلك ما

---

[1]– **دينا عبد العزيز فهمي:** المرجع السابق، ص107

[2]– ***BOSSAN Jérôme :*** *Le droit pénal confronté, Op Cit, P296.*

[3]– وهو نفسه ما أشار إليه المشرع الجزائري في الفقرة الثانية من المادة (394 مكرر8) من (ق ع ج) بقوله: "... بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الإطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانوناً ...".

[4]– **يقصد بكل من الأمن القومي والإقتصاد القومي أنه:**

– **"الأمن القومي:** هو كل ما يتصل بإستقلال وإستقرار وأمن الوطن ووحدته وسلامة أراضيه وأقاليمه. (أنظر في ذلك نص المادة (1–25) من القانون المصري رقم (175 لسنة 2018). **الملحق رقم (04)**

– **الإقتصاد القومي:** هو مصطلح يطلق على مجموعة من السياسات التي تؤكد على فكرة السيطرة المحلية على الإقتصاد والعمل وتكوين رأس المال، حتى لو تطلب ذلك فرض الرسوم الجمركية وغيرها من القيود على حركة العـمالة والبضـائع ورؤوس الأمـوال. (أنظر: – **سعد ماهر حمزة:** علم الإقتصاد، دار المعارف، الإسكندرية، مصر، 1967، ص07 وما بعدها).

[5]– راجع المادة (43) من المرسوم السلطاني العماني رقم (69 لسنة 2008) بشأن قانون المعاملات الإلكترونية.

نصت عليه المادة (1-17) من القانون الفرنسي رقم (2011-1012) الصادر في 24 أغسطس2011 بشأن الإتصالات الإلكترونية.[1]

- كما يلتزم مقدمي خدمات الإنترنت بتخزين البيانات والمعلومات وجعلها متاحة للمستخدمين عبر الشبكة فقط، ولا تكون له علاقة بالمضمون أو المحتوى المعلوماتي، وإنما الإبقاء عليها مخزنة مع إمكانية الرجوع إليها عند الحاجة.[2]

- كما يلتزم مقدم الخدمة عبر الإنترنت بتزويد الجهات المختصة أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، وذلك بناءً على طلب من النيابة العامة.[3]

ب- إلتزامات مقدمي خدمة الإنترنت في التشريع المصري: لقد نص أيضًا القانون المصري رقم (175 لسنة 2018) والمتعلق بمكافحة جرائم تقنية المعلومات، بموجب المادة الثانية منه، تحت عنوان "إلتزامات وواجبات مقدم الخدمة"، على أنه:

"- أولاً: عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الإتصالات الصادر بالقانون رقم (10 لسنة 2003) يلتزم مقدمو الخدمة بما يأتي:

-1- حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يومًا متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

(أ) البيانات التي تمكن من التعرف على مستخدم الخدمة.

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة.

(ت) البيانات المتعلقة بحركة الإتصال.

(ث) البيانات المتعلقة بالأجهزة الطرفية للإتصال.

(ج) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

---

[1]- ***Article :*** *(1-17). Ord N°2011-1012) du 24 aout2011, (JOR F N°197)du 26 Aout2011, P14473, (texte N° :49) relative aux communications électroniques.*

[2]- ***FRANCILLON (J) :*** *Application à la télématique et à l'internet des régles de responsabilité propres au droit de la presse et de la communication audiovisuelle (R S C N°3) ED. Dalloz, Paris, France, 1999, P607.*

[3]- راجع المادة (21) من القانون القطري رقم (14 لسنة 2014) بشأن مكافحة الجرائم الإلكترونية.

-2- المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

-3- تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم إختراقها أو تلفها.

- ثانيًا: مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:

-1- إسم مقدم الخدمة وعنوانه.

-2- معلومات الإتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الإتصال الإلكتروني.

-3- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.

-4- أي معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المختص.

- ثالثًا: مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقًا لإحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة إختصاصاتها وفقًا للقانون.

- رابعًا: يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك"[1].

ج- إلتزامات مقدمي خدمات الإنترنت في التشريع الجزائري: ولقد نص من جهته أيضًا المشرع الجزائري عن جملة من الإلتزامات الملقاة على عاتق مقدمي خدمات الإنترنت وذلك بموجب القانون رقم (09-04) السالف الذكر والواردة في الفصل الرابع من هذا القانون تحت عنوان "إلتزامات مقدمي الخدمات"، وذلك بموجب المواد (10، 11، 12) على التوالي:

- المادة (10): "مساعدة السلطات"

[1]- أنظر: الملحق رقم (04).

-1- "في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه، تحت تصرف السلطات المذكورة.

-2- ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

- المادة (11): "حفظ المعطيات المتعلقة بحركة السير"

-1- "مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ. المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب. المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

ج.الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

د. المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

ه. المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

-2- بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة (أ) من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

-3- تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداءًا من تاريخ التسجيل.

-4- دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية... تحدد كيفيات تطبيق الفقرات (1، 2، 3) من هذه المادة، عند الحاجة، عن طريق التنظيم".

- المادة (12): "الإلتزامات الخاصة بمقدمي خدمة الإنترنت"

-1- "زيادة على الإلتزامات المنصوص عليها في المادة (11) أعلاه، يتعين على مقدمي خدمات الإنترنت ما يأتي:

أ. التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب. وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها"[1].

المطلب الثاني: أساس المسؤولية الجنائية لمقدمي خدمات الإنترنت

ينطوي معنى مساءلة مقدمي خدمات الإنترنت عمومًا، على مؤاخذتهم وتحميلهم تبعة أعمالهم غير القانونية، وعلى إلزامهم بتحمل العواقب التي تترتب على سلوكاتهم التي إرتكبوها مخالفين بها أصول وقواعد وإلتزامات معينة، وسواء أكان سلوكهم إيجابيًا أم سلبيًا مخالفة لقواعد القانون لتوصف مسؤوليتهم بأنها قانونية تستتبع بالضرورة فرض جزاء قانوني تحدده السلطة المختصة ويطبقه القضاء،[2] والمسؤولية القانونية لمقدمي خدمات الإنترنت وفقًا لهذا التحديد تثير فكرتي "الخطأ والجزاء"، فتأخذ تبعًا لذلك مفهومًا مدنيًا أو مفهومًا إداريًا أو بعدًا جنائيًا.[3]

وتعد المسؤولية الجنائية لمتعهدي الإيواء ومقدمي خدمات الإنترنت، كونهم متدخلين مهنيين في تقديم الخدمات عبر شبكة الإنترنت، من أهم الموضوعات التي أثارت ولا زالت تثير نقاشات فقهية كبيرة، وتضاربات ظاهرة في أحكام القضاء أثناء نظره دعاوى مسؤولية هؤلاء المتعهدين عن الإيواء والخدمات المعلوماتية غير المشروعة، وكذلك تعتبر المسؤولية الجنائية لمقدمي خدمات الإنترنت من النظريات المستحدثة مما يرشح هذه المسؤولية لتكون محورًا أساسيًا لفلسفة "القانون الجنائي المعلوماتي" بإحتلالها مكانة مهمة في الدراسات الفقهية وأهمية بالغة في التشريعات الجنائية الحديثة الوطنية والمقارنة، وهذا على الرغم من إغفال العديد من القوانين المنظمة لهذه المسؤولية من رسم معالمها بدقة، وإكتفوا بالإشارة إلى بعض أحكامها في نصوص متفرقة، وجّل هذه الأحكام تتعلق بضوابط تقديم خدمات المعلومات عبر الشبكة، أما شروط تقرير مسؤولية هؤلاء المتعهدين والوسطاء فلم تعالج بنصوص قانونية صريحة، ليلقى على عاتق الفقه والقضاء مسألة إستنباط هذه الشروط وإكتشاف المعالم العامة لهذه المسؤولية، وهكذا إتسع الجدل الفقهي الدائر بينهما حول مسؤولية مقدمي الخدمات عبر الشبكة والخاصة بالمعلومات الواردة في ذلك المحتوى الإلكتروني.[4]

---

[1]- أنظر في ذلك: **الملحق رقم (06)**.

[2]- **عادل بوزيدة:** المرجع السابق، ص21.

[3]- وهذا ما أشار إليه المشرع الجزائري في بداية الفقرة الأولى من نص المادة (394 مكرر8) بقوله: "... دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب ...".

[4]- **عادل بوزيدة:** المرجع السابق، ص91.

وهنا يثور التساؤل حول مدى تقرير المسؤولية الجنائية بالنسبة لهؤلاء، حيث ظهر جدل فقهي تبناه إتجاهان إثنان نعرض لهما تباعًا.

الفرع الأول: الإتجاه الأول القائل بعدم مسؤولية المزود أو الوسيط أو الخادم

وقد إستند هذا الإتجاه إلى أنَّ مزود الخدمة لا يملك القدرة على التحكم في أي محتوى أو مضمون إلكتروني يبث على الشبكة، وأنَّ القول بتقرير مسؤوليته هنا يماثل القول بمساءلة مدير البريد والإتصالات الهاتفية على مدى مشروعة الخطابات والمكالمات الهاتفية التي تجرى عبر هذه الخطوط،[1] فتقرير مسؤولية مزود الخدمة يتطلب أن يكون دوره أكثر إيجابية في بث المادة المجرمة بالإضافة إلى أنه لا يملك الوسائل الفنية التي تمكنه من مراقبة كل تلك المعلومات المتدفقة بأعداد تتجاوز الملايين.[2]

وسرعان ما تتلاشى هذه المسؤولية خاصةً إذا ما علمنا أنَّ تحديد الطرف المتسبب في عملية النشر المعلوماتي غير المشروع يعتبر أمرًا صعبًا في العالم اللامادي، وأنّ مقدمي الخدمة لم يكن تدخلهم على الشبكة إلاَّ لإيصال المعلومات بشتى أنواعها إلى المستعمل[3]، كما أنَّ هناك شبه إجماع على أنّ المسؤولية عن نشر المعلومات غير المشروعة يحملها الطرف الذي قرر نشر تلك المعلومات على شبكة الإنترنت.

وعليه يرى أصحاب هذا الإتجاه ضرورة إعفاء كل من الوسيط أو مقدم الخدمة على الشبكة من المسؤولية الجنائية، كون أنّ وظيفتهم تقنية بحتة، وكذا لإستحالة مراقبة الكم الهائل من المعلومات التي لا يكونون طرفًا فيها[4]. وإنما ينحصر دورهم في تمكين المستخدم من الدخول إلى الشبكة والتجول فيها والإطلاع على ما يريد، فهؤلاء دورهم فني بحت قائم على التعاطي مع الأجهزة والبرامج وتشغيلها، وليس قائمًا على المراقبة والتصديق، ذلك أنَّ هذا الدور الأخير منوط بجهات نظامية أخرى.[5]

---

[1]– **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، مصر، 1992، ص119.

[2]– **محمد عبد الطاهر حسين:** المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص38.

[3]– ***OLIVIER Cachard :*** *Droit du commerce éléctronique, (R.D.A.I) N°3, Ed, D, Paris, France, 2004, P394.*

[4]– **أكمل يوسف السعيد يوسف:** المرجع السابق، ص45.

[5]– **عبد الرحمن عبد الله السند:** المرجع السابق، ص110.

الفرع الثاني: الإتجاه الثاني القائل بتقرير مسؤولية المزود أو الوسيط أو الخادم

إنَّ عدم تنظيم المشرع لهذه المسألة بشكل دقيق، قد جعل باب الإجتهاد مفتوحًا أمام الفقهاء ليخوض كل منهم في أغوار هذه المسألة، حيث إنقسم أنصار الإتجاه القائل بتقرير مسؤولية مقدمي الخدمة عبر الإنترنت إلى فريقين إثنين، الأول ينادي بتقرير المسؤولية الجنائية طبقًا لأحكام المسؤولية المفترضة (أولاً)، والثاني يذهب إلى تقرير المسؤولية طبقًا للأحكام العامة للمسؤولية الجنائية وإقامة مسؤوليتهم في كل الحالات (ثانياً).[1]

أولاً: مساءلة مقدمي الخدمة طبقًا لأحكام المسؤولية المفترضة

لم يقف الفقه والقضاء حين عرض هذا النوع من المسائل عليه لأول مرة مكتوف الأيدي تجاه تقرير مسؤولية مقدم الخدمة أو الوسيط الفني عبر الشبكة، وذلك بمحلوله تحديد مسؤوليته وفقًا لطبيعة الوظيفة أو العمل الذي يؤديه، وبصفة خاصة مدى الرقابة التي يمكن أن يقوم بها على المحتويات الإلكترونية غير المشروعة التي تتم عبر خدمة الإنترنت التي يقدمها.[2]

حيث ذهب رأي فقهي إلى القول بإمكانية بحث الأساس النظري لمسؤولية مقدمي خدمات الإستضافة عبر شبكة الإنترنت، وذلك بالإحتكام إلى القواعد المعمول بها في نطاق نظرية المسؤولية الجنائية عن فعل الغير، مؤسسًا توجهه هذا على طبيعة الدور الذي يلعبه مقدم الخدمة في عملية بث وتداول الأنشطة المعلوماتية المجرمة عبر مواقع الإنترنت، وخصوصية العلاقة التي تجمع هؤلاء الوسطاء بموردي الأنشطة الإلكترونية.[3]

ففي فرنسا على سبيل المثال، وقبل صدور القانون رقم (719-2000) المعدل لأحكام قانون حرية الإتصالات[4]، أثيرت مسألة إمكانية تطبيق نظام النشر الصحفي والذي يأخذ بنظام "المسؤولية

---

[1]– **عبد الفتاح بيومي حجازي:** الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2002، ص13.

– **أحمد عبد الله هلالي:** الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2006، ص160.

[2]– **رشيدة بوكر:** المرجع السابق، ص141. – **عبد الرؤوف اللومي:** المرجع السابق، ص49.

[3]– **محمد عبد الكريم حسين الداوودي:** المسؤولية الجنائية لمورد خدمة الإنترنت، منشورات الحلبي الحقوقية، ط1، لبنان، 2017، ص176.

[4]– ***Loi** N° (2000-719) du 1 Août 2000, modifiant la loi N° (1986-1067) du 30 septembre 1986, relative à la liberté de communication (JORF) N°(177) du 2 Août 2000.*

التتابعية *Responsabilité séquentielle*" أي "المسؤولـــية المفترضـــة *Responsabilité assumée*"[1] عــن الجرائم الصحفية على عمل موردي خدمات الإنترنت، أي أنه يتعين إعمال قانون الصحافة على البث الإلكتروني من هذه الشبكة، وبالتالي مساءلة مزود الخدمات بإعتباره مديرًا للتحرير مثله مثل مدير التحرير الصحفي[2]. وما دام مزود الخدمات يقوم بالنشر فهو يتماثل مع ما يقوم به مدير التحرير في الصحف من قيامه بدور النشر، وبالتالي يسري عليه قانون الصحافة والنشر[3].

حيث قضت محكمة إستئناف باريس في إحدى أحكامها بمسؤولية الشخص الذي يقوم بإيواء المواد المعلوماتية المتعلقة بالإنترنت على أساس أنّ هذه الخدمة تدخل ضمن الخدمات الصحفية السمعية والبصرية، وأقامت مسؤوليته على أساس "المسؤولية التتابعية" والتي يفترض أنها تتعلق بجرائم الصحافة[4] التي تنظمها المادة (42) من قانون الصحافة الفرنسي لسنة 1881 والتي تقضي أنَّ مدير التحرير أو الناشر هو المسؤول الأول، فإنَّ لم يوجد تقع المسؤولية على المؤلف، فإن لم يكن فالطابع، فإن لم يكن فالبائع أو الموزع أو ملصق الإعلانات بصفتهم فاعلين أصليين، وإذا كان رئيس التحرير أو الناشر معروفاً فإنه يُسأل جنائيًا كفاعل أصلي عن الجريمة، ويسأل المؤلف بإعتباره شريكًا[5].

وكذا قانون الإتصالات السمعية والبصرية رقم (652-1982) بمقتضى المادة (93-1) منه[6] والتي نقلت نظام المسؤولية بالتتابع إلى نطاق جرائم الإتصال السمعي البصري وفقًا للترتيب التالي "مدير البرنامج أو مؤلف الرسالة وأخيرًا المنتج" ونفس الأمر ينطبق بالنسبة لشبكة الإنترنت بإعتبارها نظام سمعي بصري، بشرط أن تكون الرسالة غير المشروعة التي يجرى بثُّها سابقة التخزين أي مسجلة قبل عرضها أو نشرها[7]، ذلك أنه إذا كانت مذاعة على الهواء فإنَّ رئيس التحرير لا يستطيع أن يمارس رقابة على الرسالة، فيسأل تبعًا لذلك صاحب الرسالة بإعتباره فاعلاً

---

[1]– ويطلق عليها البعض إسم "المسؤولية التوجيهية *Résponsabilité guidage*". (أنظر في ذلك: – **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، المرجع السابق، ص143).

[2]– ***AUVERT Patrick :*** *L'application du droit de la presse au réseau internet , (JCP) N°3, France, 1999, P108.*

[3]– **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص169.

[4]– *Cass. Crim, Paris, 10 Février1999.*

[5]– ***Article*** *(42) et Article (43) du loi du 29 juillet 1881 sur la liberté de la presse, modifié par ordonnance du 26 Août 1944, modifié par loi N° : (1952-336) du 25Mars1952 (JORF) du 26Mars1952.*

[6]– ***Article*** *(93-1) du loi N (1982-652) du 29 Juillet 1982 sur la communication audiovisuelle.*

[7]– **رشيدة بوكر:** المرجع السابق، ص145. – **جميل عبد الباقي الصغير:** المرجع السابق، ص129. – **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص172.

أصليًا، ومن هنا لم ترى وقتها محكمة النقض الفرنسية في المسؤولية التتابعية ما يخالف مبدأ الأصل في البراءة.[1]

نقد الإتجاه: يعد هذا النوع من المساءلة أكد المسائل إثارة للجدل، ذلك لأنها تثير إمكانية مساءلة متعهدي الإيواء الإلكتروني عن الأنشطة المجرمة التي يقترفها غيرهم من غير أن يضطلعوا إضطلاعًا مباشرًا في إتيان هذه الأفعال[2]، وهو الطرح الذي قد يتنافى مع مبادئ جنائية ثابتة ويتعارض مع أعراف فقهية مستقر عليها، غير أنَّ ذلك لم يمنع بعض الفقه من مناقشة جوانب هذه المسؤولية وتبريرها، رافضين بذلك مساءلة مزود الخدمات على أساس المسؤولية التتابعية المفترضة وهذا لمخالفتها أحكام الدستور الذي ينص على قرينة البراءة، مادام أنها تقيم قرينة قاطعة على مسؤولية رئيس التحرير وما يليه في سلم التسلسل المهني.[3]

ثانيًا: مساءلة مقدم الخدمة طبقاً للأحكام العامة للمسؤولية الجنائية

على أنقاض الإتجاه السالف الذكر والقاضي بإثارة مسؤولية متعهدي الإيواء عن سلوكات موردي المحتوى إعمالاً لنظرية فعل الغير، راح إتجاه آخر يقضي بضرورة التمسك بنظرية الخطأ الشخصي كأساس لمساءلة هؤلاء الوسطاء، وذلك على ضوء الأحكام العامة المعمول بها في قيام المسؤولية الجنائية، مع حتمية الإستقرار على الخطأ المعلوماتي واجب الإثبات،[4] وذلك بإعمال فكرة إفتراض الخطأ الشخصي من جانب هؤلاء الوسطاء.

فقد أصدر لأول مرة قسم التقارير والدراسات بمجلس الدولة الفرنسي تقريرًا في شأن الإنترنت والخطوط الرقمية الذي وافقت عليه الجمعية العامة للمجلس في عام 1998، ومن بين ما تعرض له تقرير المسؤولية الجنائية القائمة على أساس الخطأ المفترض لمقدمي الخدمات الوسيطية بالإنترنت، ومن ثم أُستبعد تطبيق المسؤولية التتابعية عليهم كون الإنترنت يتسم بالتعقيد ولا يسمح بتطبيق أحكام هذا النوع من المسؤولية، مع تأكيده على تطبيق الأحكام العامة للقانون الجنائي بشأن الأعمال الوسيطية الخاصة بالإنترنت، مع الأخذ بعين الإعتبار معرفة المحتوى والمضمون غير

---

[1]– *Crim du 23Fév2000, Rev, Sec,crim 2000, P642.*

[2]– **نسيمة درار:** واقع المسؤولية المدنية في المعاملات الإلكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2012، ص149.

[3]– *Crim 17 Déc 1991, Bull, crim, N°481, Rev, sc, crim1993, P88.*

[4]– **عادل بوزيدة:** المرجع السابق، ص63.

المشروع وكذا توافر القصد الجنائي وإحترام الإجراءات المتخذة لمراقبة النشاط الإلكتروني والقدرة على المراقبة.[1]

وإدراكاً من المشرع الفرنسي لخصوصية عمل الوسيط أو مقدم خدمة الإنترنت، تدخل بموجب القانون رقم (719-2000) والمتعلق بحرية الإتصالات[2]، حيث أقرت المادة (43-8) منه بقولها: "لا تقوم المسؤولية المدنية أو الجزائية للأشخاص المعنوية أو الطبيعية التي تقوم بدون مقابل أو بمقابل بالتخزين المباشر والدائم لتضع تحت تصرف الجمهور نشاطات إلكترونية كيفما كانت طبيعتها عن محتوى هذه الخدمات، إلاّ في حالتين، الأولى في حالة عدم تنفيذ الأمر القضائي الصادر بإلزامه بمنع الوصول إلى هذا المضمون، والثانية هي حالة ما إذا قدر الغير وجود مضمون غير مشروع أو من شأنه الإضرار بحقوقه، وعدم إتخاذ الإجراءات اللازمة لمنع بث هذا المضمون رغم التنبيه عليه بذلك"[3].

لكن سرعان ما تراجع المشرع الفرنسي عن موقفه هذا، ليقوم عام 2004 بتبني ضوابط قانونية خاصة وجديدة ومتوازنة أرسى فيها النظام القانوني لمقدمي خدمات الإنترنت، لاسيما من حيث تحديد طبيعة عملهم وكذا إلتزاماتهم الواجب عليهم إتباعها، ومسؤولية كل منهم في مواجهة السلسلة المعلوماتية المتواصلة عبر الشبكة، وذلك من خلال إصدار المشرع الفرنسي القانون رقم (575-2004) والمتعلق بالثقة في الإقتصاد الرقمي[4]، والذي أنشأ ولأول مرة مسؤولية جنائية مستقلة لمزودي خدمات الإنترنت بموجب المواد من (05) إلى المادة (09) منه، وإعتبارًا من هذا التاريخ أصبح لمقدمي خدمات الإنترنت في فرنسا نظامهم القانوني الخاص.[5]

نقد الإتجاه: بالرغم من الإستقرار الذي تعرفه اليوم قاعدة شخصية المسؤولية الجنائية وذيوعها بشكل مقنن في التطبيقات الجنائية المعاصرة، وهذا لإستنادها إلى المبدأ الدستوري القاضي بشخصية العقوبة، إلاَّ أن البعض من الفقه يتجه إلى القول بخروج المشرع عن هذه القواعد في بعض المناسبات ومنها إثبات المسؤولية الجنائية لمتعهدي الإيواء المعلوماتي، بحيث يفترض

---

[1]- ***Conseil détat :*** *« Internet et les réseaux numériques » étude adoptée par l'assemblée générale du conseil d'état, section du rapport et des études, le 2juillet1998, (la documentation française) Paris, France,1998, P266.*

[2]- القانون الفرنسي رقم (719-2000) المؤرخ في 01 أوت 2000 المعدل للقانون رقم (1067-1986) المؤرخ في 30 سبتمبر1986 والمتعلق بحرية الإتصالات.

[3]- مشار إليه لدى كل من: (- **رشيدة بوكر:** المرجع السابق، ص146. - **شيماء عبد الغني محمد عطاء الله:** المرجع السابق، ص173).

[4]- القانون رقم (575-2004) والمتعلق باثقة في الإقتصاد الرقمي والمؤرخ في 21 جوان 2004.

[5]- **أحمد قاسم فرح:** النظام القانوني لمقدمي خدمات الإنترنت، دراسة مقارنة، مجلة المنارة، المجلد13، العدد09، 2007، ص322.

المنطق والعقل وجود خطأ شخصي في جانب هؤلاء الوسطاء حتى يمكن مساءلتهم ثم معاقبتهم مع ضرورة بحث توافر القصد الجنائي لديهم من عدمه.[1]

الفرع الثالث: موقف المشرع الجزائري من هذه المسالة

بنفس النهج الذي ذهبت إليه العديد من الأنظمة القانونية المقارنة والتي إستحدثت تشريعات جنائية خاصة تنظم خدمات الإيواء المعلوماتي، فقد تعرض المشرع الجزائري لتنظيم مساءلة مقدمي خدمات الإنترنت بصورة صريحة، سواءً كان ذلك في ضوء الأحكام العامة لقانون العقوبات أو في قوانين خاصة مكملة له.

ففي البداية جاء القانون رقم (04-15) المعدل والمتمم لقانون العقوبات، خاليًا تمامًامن أي نص صريح يعالج مسألة تقرير مسؤولية مقدمي الخدمة عبر شبكة الإنترنت، وإنما إكتفى بالنص على بعض جرائم المساس بنظام المعالجة الآلية للمعطيات وذلك بموجب المواد من (394 مكرر) إلى (394 مكرر7)، ولربما أنه عند إصدار هذه المواد أراد مشرعنا التريث في تقنين مسؤولية مقدمي الخدمة لحين إستقرار الحلول والجدل الذي كان قائمًا وقتها وإنتظار وضوح الرؤية في تقرير المسؤولية الجنائية لهؤلاء الوسطاء.

ومع إتضاح الرؤية وتحديد الأدوار وفي ظل ظهور العديد من التشريعات الجنائية المقارنة التي عالجت هذه المسألة بشكل جدي، تدخل المشرع الجزائري بسن قانون يكرس مسؤولية هؤلاء الوسطاء، وذلك بموجب القانون رقم (16-02) المعدل والمتمم لقانون العقوبات،[2] مستحدثًا بذلك نص مادة جديدة وهي المادة (394 مكرر 8). وكذا إصداره تشريع خاص ومستقل ينظم أحكام وإلتزامات مقدمي الخدمات عبر الإنترنت، ويحدد القواعد العامة في مساءلة وسطائها في كل من القانون رقم (09-04) والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،[3] وكذا القانون رقم (12-05) والمتعلق بالإعلام.[4]

---

[1]- **رضا متولي وهدان:** الخطأ المفترض في المسؤولية عن أضرار الحاسبات الآلية، الأساس والضوابط، دار الفكر والقانون، الإسكندرية، مصر، 2009، ص25. - **محمد حماد الهيتي:** الخطأ المفترض في المسؤولية الجنائية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2005، ص110.

[2]- قانون رقم (16-02) مؤرخ في 19 يونيو2016، المعدل والمتمم للأمر رقم (66-156) المتضمن قانون العقوبات، الجريدة الرسمية، العدد37، المؤرخة في 22 يونيو2016.

[3]- راجع في ذلك: **الملحق رقم (06).**

[4]- القانون العضوي رقم (12-05) المؤرخ في 12 يناير 2012 والمتعلق بقانون الإعلام، الجريدة الرسمية، العدد 02 في 15 يناير2012.

ليرسي بذلك المشرع الجزائري بيئة تشريعية خاصة ومتوازنة إيماناً منه لخصوصية تقديم خدمات الوساطة على الإنترنت، والتي يمكن أن تكون أساسًا متين يستند إليه القضاء في شأن مساءلة هؤلاء الوسطاء طبيعيين كانوا أو معنويين، متبنيًا في ذلك الإتجاه الذي ذهب إليه المشرع الفرنسي في مساءلة مقدمي خدمات الإنترنت سواءً جنائيًا أو مدنيًا أو إداريًا، والتي يجب أن تقوم وفق القواعد العامة للقانون الجنائي والمبادئ الدستورية الخاصة كمبدأ المسؤولية الشخصية ومبدأ الشرعية والمساواة بين المواطنين أمام القانون والقضاء.

رأي الباحث:

على أنقاض الجدلية القائمة لدى فقهاء القانون الجنائي وأجهزة القضاء الوطني والمقارن حول مدى إمكانية مساءلة متعهدي الإيواء عبر شبكة الإنترنت، والتي أثارتها طبيعة الخدمات المقدمة من طرفهم يمكن القول بوجود إجماع شبه تام على إمكانية مساءلة هؤلاء الوسطاء.

ونحن من جانبنا إذا ما أردنا ترجيح أحد هذه الإتجاهات فسوف نجد أنفسنا نوافق الإتجاه الأول في جزئية البراءة المفترضة إستنادًا إلى مبدأ الأصل في الإنسان البراءة، والذي يحتم على النيابة العامة أن تقوم بإثبات العكس في جانب المتهم حتى تقوم مسؤوليته، ولا يكلف المتهم بإثبات براءته، فضلاً على ذلك لا يصلح تشبيه سلسلة المتدخلين في مجال الإنترنت مع تلك المتوفرة في مجال الإعلام والصحافة فالطبيعة الفنية المعقدة لتقديم الخدمات عبر الإنترنت تفصل لها الإعتبارات الفنية، وعليه فإنَّ أحكام المسؤولية المتتابعة والمفترضة لا يمكن تطبيقها في هذا المجال وهذا لإعتبار أن أحكام هذه المسؤولية إستثناء من الأصل العام لا يجوز التوسع فيه.

أما إذا أردنا ترجيح الإتجاه الثاني نرى أنه يجب أن تقرر المسؤولية الجنائية بنص صريح ودقيق، لأنه كلما تشدد المشرع في إقامة مسؤولية مزودي ووسطاء الخدمة عبر الإنترنت زاد حرصهم على عدم مخالفة الوقوع في الخطأ، ومنه حرصهم على الرقابة الذاتية على المعلومات لدرء المسؤولية عنهم، لأنه إذا ما تم تجاهل مسؤولية هؤلاء أدى ذلك حتمًا إلى وجود عدد كبير من المعلومات غير المشروعة على الشبكة، ويزداد تبعًا لذلك التدفق لواسع لهذه المعلومات مما قد يؤدي ذلك إلى تقاعس المزودين عن إستخدام الوسائل اللازمة للحد أو لمنع إنتشار هذه المعلومات غير المشروعة، وبالتالي تتفشى الجريمة المعلوماتية ويفلت المجرم المعلوماتي من المساءلة والعقاب.

المطلب الثالث: تقرير المسؤولية الجنائية لمقدمي خدمات الإنترنت

لم تتعرض كثير من التشريعات الجنائية المقارنة لموضوع تقرير المسؤولية الجنائية لمقدمي الخدمة والمتدخلين في الإنترنت بشكل دقيق، لاسيما الدول العربية منها، فنجد بعض الدول عالجت هذه المسألة من وقت قريب، ونذكر هنا على سبيل المثال التشريع الجزائري والذي تطرق لهذه المسألة في عام 2016 وكذا التشريع المصري في عام 2018.

ولعل أهم جريمة هي إخلال مقدمي خدمات الإنترنت بالإلتزامات القانونية الملقاة على عاتقهم بموجب نصوص القانون، وهو ما يطلق عليه "بالجرائم المرتبطة بالإيواء المعلوماتي للمواقع الإلكترونية" وللحديث أكثر عن هذه الجريمة وما يترتب عن إرتكابها من تقرير للمساءلة الجنائية، لابد من التطرق إلى أركان هذه الجريمة (فرع أول) ثم ذكر أهم العقوبات المقررة لها (فرع ثاني).

الفرع الأول: أركان جريمة الإيواء المعلوماتي

إنَّ الأركان العامة لجرائم الإيواء المعلوماتي هي تلك العناصر القانونية الواجب تحققها في واقعة الإيواء غير المشروع، ليصح وصفها بالجريمة، وهي كل ما يتصل بالتكييف القانوني لهذه الواقعة، سواء ما يتصل بجوانبها المادية أو المعنوية، ومعنى ذلك أنّ القول بمسؤولية مقدم الخدمة يتمثل في عدم مشروعية خدمة الإيواء في شقِّها الجزائي، علاوةً على عدم إحترام الواجبات والإلتزامات الملقاة على عاتقه في إقتراف هذه الجريمة بصورة أصلية أو بالإشتراك مع الغير، مع حتمية وجود إرادة آثمة لحظة البث غير المشروع أو حتى الشروع فيه، بشرط وجود النص المجرم.

أولاً: الركن الشرعي لجريمة الإيواء المعلوماتي

وللحديث عن الركن الشرعي في الجريمة المرتبطة بالإيواء المعلوماتي، أو كما يسميها البعض "بجرائم مقدمي خدمات الإنترنت"، لابد من ذكر النص القانوني لهذه الجريمة، ثم نتكلم بعد ذلك عن علة التجريم.

أ- بالنسبة لنص التجريم: وهنا نذكر بعض النصوص القانونية المجرمة لهذه الوقائع، والواردة في كل من التشريع الفرنسي ثم التشريع المصري ثم التشريع الجزائري تباعًا.

1. في التشريع الفرنسي: إدراكًا من المشرع الفرنسي لخصوصية عمل مقدم خدمة الإنترنت كـوسيط فنـي وتقني في مجال المعلوماتية تدخل بموجب القانون رقم (719-2000) والمؤرخ في 1 أوت 2000 والمعدل للقانـون رقم (1067-1986) المؤرخ في 30 سبتمبر1986 والمتعلق بحرية الإتصالات، حيث أضاف المادة (43-8)، والتي قررت ما يلي: "عدم قيام المسؤولية المدنية أو

الجزائية للأشخاص المعنوية أو الطبيعية التي تقوم بدون مقابل أو بمقابل بالتخزين المباشر والدائم لتضع تحت تصرف الجمهور إشارات أو كتابات أو صور أو أصوات أو رسائل كيفما كانت طبيعتها عن محتوى هذه الخدمات، إلاّ في حالتين هما:

- حالة عدم تنفيذ الأمر القضائي الصادر بإلزامه بمنع الوصول إلى هذا المضمون.
- وحالة ما إذا قدر الغير وجود مضمون غير مشروع أو من شأنه الإضرار بحقوقه، وعدم إتخاذ الإجراءات اللازمة لمنع بث هذا المضمون رغم التنبيه عليه بذلك"[1].

وما نلاحظه على هذا النص أنه جعل الأصل هو عدم مسؤولية الوسيط الفني، وإستثنى منه الحالتين سالفتي الذكر، وهو ما يمكن القول معه انّ المشرع الفرنسي تبنى مسؤولية مخففة، كما أنّ النص جاء عامًّا فلم يميز بين المسؤولية المدنية والمسؤولية الجزائية[2]، ضف إلى ذلك أنّ صياغة النص على النحو السالف بيانه خولت الأفراد – الغير– سلطة تقدير ما يعد مشروعًا وما لا يعد كذلك، وهو ما يخالف صراحةً مبدأ الشرعية، الأمر الذي إستدعى المجلس الدستوري الفرنسي إلى القضاء بعد دستورية الحالة الثانية.[3]

ليقرر بعدها المشرع الفرنسي عام 2004 بتبني ضوابط قانونية جديدة ومتوازنة أرسى فيها النظام القانوني الخاص بمقدمي خدمات الإنترنت، منتهجًا في ذلك نفس نهج توجه البرلمان الأوروبي وذلك بموجب القانون رقم (31–2000)،[4] من حيث تحديد طبيعة عمل هؤلاء الوسطاء وإلتزاماتهم الوظيفية، ومسؤولية كل منهم في مواجهة الجرائم المعلوماتية المتواصلة عبر الشبكة، فأصدر قانون "الثقة في الإقتصاد الرقمي *La confiance dans l'économie numérique* رقم (575–2004) والمؤرخ في 21 جوان 2004. والذي عدل بموجب القانون رقم (444–2016) بشأن الثقة في

---

[1]– ***Article : (43-8) du loi N° (2000-719) du 1er Août 2000.***

« dispose que les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsables du fait du contenu de ces services que :

- Si ayant été saisies par une autorité judiciaire, elles n'ont pas agipromptement pour empêcher l'accès à ce contenu.

- Ayant été saisies par un tiers estimant que le contenu qu'elles hébergent est illicite ou lui cause un préjudice, elles n'ont pas procédé aux diligences appropriées ».

[2]– **رشيدة بوكر:** المرجع السابق، ص147.

[3]– ***Voir plus :*** *La décision du conseil constitutionnel N° (2000-433) D.C – en date du27 Juillet 2000, (JORF) N°177 du 2 Août 2000.*

[4]– *Directive (2000-31) CE, du parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques, journal officiel N° (L.178) du 17/07/2000. P 0001-0016.*

الإقتصاد الرقمي،[1] والمؤرخ في 13 أفريل 2016، والذي وضع نظام مستقل بمسؤولية مزودي خدمات الإنترنت بموجب المواد من (5) إلى (9) منه، وإعتبارًا من هذا التاريخ أصبح لهؤلاء الوسطاء في فرنسا نظامهم القانوني الخاص.[2]

حيث نصت المادة (6-1-3) من القانون الفرنسي المتعلق بالثقة في الإقتصاد الرقمي، والتي جاء فيها: "أنَّ أفعال مقدمي خدمات الإنترنت الخاطئة لا يمكن أن تدخل في نطاق التجريم إلاَّ إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه"[3]. وهو بهذا النص جاء متفقًا مع الإتجاه العام لتوجيهات البرلمان الأوروبي، حيث وضع التوجيه مبدأ عام هو عدم مسؤولية مقدم الخدمة إلاَّ في أحوال معينة وبشروط خاصة، ولذلك يوصف نظام المسؤولية الذي تبناه المشرع الفرنسي بنظام "المسؤولية المشروطة *Responsabilité conditionnelle*"[4]. كما أضافت المادة (6-1-8) من نفس القانون على أنه: "للقضاء أن يصدر أمرًا على عريضة في مواجهة متعهد الوصول أو الإيواء، بإلزام أي منهما بإتخاذ التدابير اللازمة لتفادي الضرر أو وقفه حال حدوثه، وأنَّ عدم تقييده بهذا الأمر يمكن حينها إدانته ..."[5].

2. في التشريع المصري: في السابق لم يتعرض المشرع المصري لمسألة مسؤولية مقدمي خدمات الإنترنت لا في قانون العقوبات، ولا حتى في قانون التوقيع الإلكتروني رقم (15 لسنة 2004)، ولكن بعدها أصدر المشرع المصري القانون رقم (175 لسنة 2018) في شأن مكافحة جرائم تقنية المعلومات وتكلم من خلاله عن هذه المسألة، وذلك بموجب الفصل الخامس منه تحت عنوان "المسؤولية الجنائية لمقدمي الخدمة" بالمواد من (30) إلى (34) من هذا القانون.

حيث نصت المادة (30) على أنه: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة إمتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى

---

[1]– ***Loi*** *N° (2004-575) du 21 juin 2004 pour la confiance dans l'économie numérique. Modifié par loi N° (2016-444° du 13 avril 2016, visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées.*

[2]– **أحمد قاسم فرح:** المرجع السابق، ص322.

[3]– ***Article (6-1-3) :*** *du (LCEN) Modifié par loi N° (2016-444) du 13 Avril 2016.*

[4]– **أشرف جابر السيد:** مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة لمسؤولية متعهدي الإيواء، دار النهضة العربية، القاهرة، مصر، 2010، ص78.

[5]– ***Article (6-1-8) :*** *du (LCEN) modifié par loi N° (2016-444) du 13 Avril 2016.*

المشار إليه في الفقرة الأولى من المادة (7) من هذا القانون. فإذا ترتب على الإمتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومي تكون العقوبة السجن المشدد، والغرامة التي لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضي المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط"[1].

3. في التشريع الجزائري: أما في التشريع الجزائري فإنّ النصوص التي تشير إلى مسؤولية مقدمي خدمات الإنترنت كانت عامة وقليلة جدًا، والسبب في ذلك هو أنه لم يكن هناك تصور واضح في وضع مبادئ قانونية لهؤلاء الوسطاء ما لم تكن هناك إلتزامات واضحة ومحددة تقوم عليها مسؤولية على عاتقهم حيث كان في السابق يتم الإستناد إلى المرسوم التنفيذي رقم (98-257) والمؤرخ في 25 غشت 1998 والمتعلق بضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، والمعدل بالمرسوم التنفيذي رقم (2000- 307) والمؤرخ في 14 أكتوبر 2000[2]، وكذا القانون رقم (09-04) المتعلق بجرائم تكنولوجيات الإعلام والإتصال،[3] والمشار إليه سلفًا.

حيث نص المرسوم التنفيذي رقم (98-257) في مادته (14) على جملة من الإلتزامات العامة تقع على عاتق الوسيط الفني، إلاَّ أنها لم تفرض جَزاءًا عن الإخلال بهذه الإلتزامات ولو بفرض الغرامة[4]، أما القانون رقم (09-04) فقد أوجبت المادة (12) منه على الوسيط الفني أهم إلتزامين، تم التطرق إليهما سلفًا.

---

[1]- أنظر في ذلك: **الملحق رقم (04)**.

[2]- المرسوم التنفيذي رقم (98-257) مؤرخ في 25 غشت 1998 والمتعلق بضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، الجريدة الرسمية، عدد 63، الصادرة بتاريخ 26 غشت 1998، والمعدل بالمرسوم التنفيذي رقم (2000-307) والمؤرخ في 14 أكتوبر 2000 والذي يضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، الجريدة الرسمية العدد (60) والصادرة بتاريخ 15 أكتوبر 2000. **الملحق رقم (08)**

[3]- أنظر في ذلك: **الملحق رقم (06)**.

[4]- حيث جاء نص المادة (14) كما يلي: "يلتزم مقدم خدمات "الإنترنت" خلال ممارسة نشاطاته بما يأتي:

- تسهيل النّفاذ إلى خدمات الإنترنت، حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك بإستعمال أنجع الوسائل التقنية.
- المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون.
- إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات "الإنترنت" وصيغة مساعدتهم كلما طلبوا ذلك.
- عرض أي مشروع خاص بإستعمال منظومات الترميز على اللجنة.
- إحترام قواعد حسن السيرة بالإمتناع خاصة من إستعمال أية طريقة غير مشروعة سواء تجاه المستعملين أو تجاه مقدمي خدمات "الإنترنت" الآخرين.
- تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها، طبقاً للأحكام التشريعية المعمول بها.
- إعلام مشتركيه بالمسؤولية المترتبة عليهم فيما يتعلق بمحتوى الصفحات التي يستخرجونها، وفقاً للأحكام التشريعية المعمول بها.
- إتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق". **الملحق رقم (07)**

وبعدها صدر القانون رقم (04-15) المعدل والمتمم لقانون العقوبات، والمتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات عام 2004، والذي جاء بالمواد من (394 مكرر) إلى (394 مكرر 7)، ومع ذلك لم يقرر حينها المشرع مسؤولية مقدم الخدمة، وبقي ذلك الوضع على حاله إلى غاية صدور القانون رقم (16-02) المعدل والمتمم لقانون العقوبات، حيث أنَّ هذا القانون أضاف المادة (394 مكرر 8) والتي نصت على أنه: "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات الإنترنت بمفهوم المادة (02) من القانون رقم 09-04 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:

- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الإطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونًا.
- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن.[1]

وبهذا النص الأخير إستطاع المشرع الجزائري تقرير المسؤولية الجنائية لمقدمي خدمات الإنترنت بشرط إذا لم يحترم مقدم الخدمة الأمر أو الحكم الصادر عن السلطات القضائية، أو الإعذار الموجه إليه من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والقاضي بإتخاذ الإجراءات اللازمة لسحب أو منع الوصول إلى المعلومات غير المشروعة والمتنازع فيها، وفي حالة عدم إحترام مقدم خدمات الإنترنت لهذا الإعذار أو الحكم أو الأمر تترتب مسؤوليته.

وهو إتجاه حسن من المشرع الجزائري نحو إقصاء الإلتزام العام بمراقبة كل المعلومات الواردة أو التي يتم إيوائها من طرف هؤلاء الوسطاء، ما عدا المراقبة المفروضة عليهم في الحالات السابقة، وهو حل تشريعي له ما يبرره في الواقع، إذ أنه من غير الممكن على مقدم الخدمة

[1]- أنظر في ذلك: **الملحق رقم (06)**.

مهما كانت إمكانياته مراقبة جميع المعلومات الواردة على شبكة الإنترنت والتي تقدر بمئات الملايين.[1]

والملاحظ هنا أيضًا أنّ المشرع الجزائري على غرار المشرع الفرنسي يعتبر أنَّ مضمون ومحتوى المعلومات يجب أن يكون غير شرعي، وهذا بصفة موضوعية، كصدور حكم قضائي يقضي بعدم شرعية بعض المعلومات الموجودة على الشبكة أو التي تم نشرها على الموقع الإلكتروني، ومما سبق يتضح إذن أنّ هناك ميل نحو إقرار مسؤولية مقدم الخدمة إلاَّ إذا كانت المعلومة المتنازع فيها غير شرعية بصورة قانونية واضحة.

كما فرض القانون رقم (09-04) وفي إطار مساعدة السلطات المكلفة بالتحريات القضائية على مقدمي خدمات الإنترنت حفظ المعطيات المتعلقة بحركة السير وهذا لمدة سنة واحدة إبتداءًا من تاريخ التسجيل، وهي المعطيات التي حددتها المادة (11) منه، كتلك التي تسمح بالتعرف على مستعملي الخدمة أو المرسل إليهم الإتصال، وأنه وفي حالة إخلال مقدم الخدمة بهذا الإلتزام بما يؤدي إلى عرقلة حسن سير التحريات والتحقيقات القضائية، يعاقب الشخص الطبيعي من ستة (6) أشهر إلى خمس (5) سنوات، وبغرامة من 50.000 دج إلى 500.000 دج، أما الشخص المعنوي فيعاقب وفق القواعد المقررة في قانون العقوبات.

ب- بالنسبة لعلة التجريم: تتجسد علة التجريم هنا في أنَّ المتهم "مقدم الخدمة" يستخدم وظيفته أو المهمة الموكلة إليه كمقدم خدمة الإنترنت في عدم تنفيذ إلتزاماته المنصوص عليها، والمتمثلة عمومًا في حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، وعدم توفيره لمستخدمي خدماته أو لأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة.

وكذا عدم توفير المساعدة الفنية التي يحتكم إليها والتي تتيح لجهات الأمن أو القضاء ممارسة إختصاصاتها وفقًا للقانون، في الحصول على البيانات والمعلومات الخاصة بالمستخدمين للشبكة، والتي يحظر على غيرهم القيام بها[2]، وذلك مع مراعاة حرمة الحياة الخاصة التي يكفلها كل من الدستور والقانون.

---

[1]- **رشيدة بوكر:** المرجع السابق، ص159.

[2]- **محمد علي سويلم:** المرجع السابق، ص473.

كما تتمثل علة التجريم هنا من أنَّ مقدم الخدمة وبحكم موقعه ووظيفته يمتنع في تنفيذ القرارات والأوامر الصادرة من الجهات المختصة بسحب أو حجب أحد المواقع أو الروابط أو المحتوى الإلكتروني أو بمنع الدخول إليها.

وفضلاً عن ذلك كله فإنَّ المشرع الجنائي يستهدف إلزامية إحترام القرارات والأحكام القضائية ويمنع عرقلتها تحقيقًا للصالح العام، وهذا بإعتبار جهاز القضاء الحارس الطبيعي والحامي الحقيقي للحقوق الأساسية والحريات العامة.

ثانيا: الركن المادي للجريمة

يمثل الركن المادي إحدى الدعائم التي ترتكز عليها جرائم الإيواء المعلوماتي، ومن ثم المسؤولية الجنائية الناشئة عنها، ويعد تخلفه مانعًا لقيام هذه الجريمة ونفيًا للمساءلة فيها، فالركن المادي هو بمثابة الصورة المادية التي تظهر بها واقعة الإيواء المعلوماتي المُجرَّمة عبر شبكة الإنترنت والمجسدة في عدم المشروعية الفعلية لهذا النشاط.[1]

ويقوم الركن المادي في هذه الجريمة على الشرط المفترض، وكذا النشاط الإجرامي، وأيضًا محل هذا النشاط، وأخيرًا النتيجة الإجرامية المترتبة على هذا النشاط.

أ- الشرط المفترض: وهو في الحقيقة عبارة عن عنصر قانوني يستقل ويتميز عن أركان الجريمة، ويسمى بالشرط المفترض لقيام الجريمة أي أنه مفترض وجوده كمركز قانوني تحميه القاعدة الجنائية من أي إنتهاك لهذا الشرط أو عدواناً عليه.[2]

ويتمثل الشرط المفترض في هذه الجريمة بصفة الجاني أو المتهم، وهو أن يكون "مقدم خدمات الإنترنت" على النحو المارُّ بنا بيانه وتفصيله، أي أنه من أهم خصائص هذه الجريمة أنها تندرج ضمن طائفة "جرائم الفاعل الخاص" إذ يشترط توافر صفة معينة في الفاعل بأن يكون من مقدمي خدمات تقنية المعلومات ومن في حكمهم.

ب- النشاط الإجرامي: يتخذ النشاط الإجرامي أو السلوك المجرم في هذه الجريمة صورتين إثنتين، الأولى هي "صورة السلوك الإيجابي" والثانية هي "صورة السلوك السلبي".

---

[1]- **عادل بوزيدة:** المرجع السابق، ص136.

[2]- **عبد العظيم مرسي وزير:** شرح قانون العقوبات، القسم العام، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، مصر، 2006، ص202.

فالسلوك الإيجابي يتحقق بفعل بث المحتوى المعلوماتي غير المشروع وجعله متاحًا عبر الشبكة والمواقع الإلكترونية[1]، وتوفير الإمكانيات الفنية والتقنية لتسهيل ذلك البث.

أما السلوك السلبي يتحقق بفعل الإمتناع عن إتيان الواجبات القانونية المفروضة عليهم تجاه الأنشطة المعلوماتية محل الإيواء، والمتمثلة أساسًا في عدم إلتزام مقدمي خدمات الأإنترنت عن تنفيذ الإلتزامات المنصوص عليها، وهذا النشاط عبارة عن سلوك سلبي وهو القعود عن إتيان سلوك معين كان يتطلبه المشرع في واقعة الحال، وذلك سواءً بإتخاذ سلوك مغاير له أم بوقوف كلي عن إتيان السلوك[2]، وبالأحرى هو إمتناع وإحجام مقدم الخدمة عن القيام بواجب معين يلزمه به القانون، والمتمثل أساسًا في عدم تنفيذه للقرارات والأوامر الصادرة من الجهات المختصة بسحب أو حجب أحد المواقع أو الروابط أو المحتوى والمشار إليه في نص المادة (394 مكرر 8) من (ق ع ج)، لأنَّ مصدر هذا الالتزام هو نص القانون، لأنّ الركن المادي لهذه الجريمة ليس هو تخلف سلوك معين من جانب مقدم الخدمة، وإنما هو تخلف حدث معين يأمر القانون بتحقيقه.[3]

وكل من الصورتين الإيجابية والسلبية في هذه الجريمة تدخل ضمن طائفة الصور التبادلية، أي الجرائم ذات السلوك التبادلي، التي يكفي لقيام الركن المادي لها بإرتكاب أحد الأفعال أو الصور التجريمية، كما تقع الجريمة بإرتكاب أحد الأفعال دون أن يعد ذلك تعددًا ماديًا للجرائم[4]، كما أنَّ هذا النوع من الجرائم يضم أفعال تندرج ضمن طائفة الجرائم الوقتية، مما يترتب عليه مسألة تحديد بدء حساب مدة تقادم الدعوى الجنائية من اليوم التالي لإرتكاب الفعل المجرم.[5]

ج- محل النشاط الإجرامي: يتمثل محل النشاط الإجرامي في سجل النظام المعلوماتي المتوفر عبر الشبكة، وهو عبارة عن مجموعة برامج تم إدارتها ومعالجة بياناتها ومعلوماتها بأي وسيلة لتقنية المعلومات وكافة الإمكانيات الإلكترونية والفنية التي من شأنها تقديم خدمة معلوماتية، بمعنى أن محل النشاط الإجرامي في هذه الجريمة يشمل أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين وإسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات والبيانات،

---

[1]- **عادل بوزيدة:** المرجع السابق، ص136.

[2]- **رمسيس بهنام:** النظرية العامة للقانون الجنائي، منشأة المعارف، الإسكندرية، مصر، 1997، ص324.

[3]- **محمد علي سويلم:** المرجع السابق، ص448.

[4]- **رمسيس بهنام:** النظرية العامة للقانون الجنائي، المرجع السابق، ص374.

[5]- **حسني الجندي:** المرجع السابق، ص190.

ويشمل ذلك كل ما له علاقة بالمضمون أو المحتوى المعلوماتي الذي تم وضعه على الشبكة أو الموقع بالوسائل المستخدمة سلكيًا أو لاسلكيًا.

د- النتيجة الإجرامية: يكفي لتحقق النتيجة الإجرامية في هذا النوع من الجرائم، عدم إمتثال أو عدم تنفيذ مقدم الخدمة لإلتزاماته المشار إليها سلفًا، ولا يشترط أن تقع نتيجة محددة أو معينة لهذا السلوك، أو أن يتحقق ضرر معين.[1]

إذ يكفي إمتناع مقدم الخدمة عن تنفيذ القرار الصادر عن الجهات المختصة بسحب أو حجب المواقع أو الروابط أو المحتويات الإلكترونية المشار إليها في القانون، ولا يشترط أن تقع جريمة معينة نتيجة لهذا السلوك السلبي أو أن تتحقق نتيجة أخرى، وأساس ذلك أن هذه الجريمة تعد من جرائم "الحدث المتخلف"، فإذا تحققت نتيجة أخرى غير متوقعة كنا بصدد جريمة "الحدث المحظور"[2] كظرف مشدد لها والذي لا يعلق القانون وجود الجريمة عليه، ولا يكون هناك محلاً لإستمرار الإلتزام بالعمل على منع الحدث[3].

حيث ينصرف معنى النتيجة الجرمية إلى ذلك الأثر الذي يحدثه تخزين المحتوى عبر الشبكة والمواقع الإلكترونية كأثر قانوني للسلوك الإجرامي وفق ما يعتد به المشرع في نصوص التجريم[4].

أما رابطة السببية هنا فتكمن في تلك الصلة الجامعة بين الفعل المعلوماتي المجرم وبين النتيجة الجرمية المحققة عبرها[5]، على الرغم من صعوبة تحديد هذه الرابطة السببية في جرائم الإيواء المعلوماتي، ذلك أنَّ عملية إيواء المحتويات المجرمة عبر الشبكة والمواقع الإلكترونية تمر بمراحل تقنية عديدة وعبر أجهزة وأنظمة شديدة التعقيد، الأمر الذي يحول بالضرورة دون سهولة تحديد رابطة السببية بين سلوك الإيواء المعلوماتي المجرم وبين النتيجة المحققة عبر مواقع الإنترنت.[6]

---

[1]- **محمد علي سويلم:** المرجع السابق، ص476.

[2]- **رمسيس بهنام:** نظرية التجريم في القانون الجنائي، منشأة المعارف، الإسكندرية، مصر، 1996، ص58.

[3]- **محمد علي سويلم:** المرجع نفسه، ص454.

[4]- **عادل بوزيدة:** المرجع السابق، ص137

[5]- **رؤوف عبيد:** السببية في القانون الجنائي، مطبعة نهضة مصر، ط2، القاهرة، مصر، 1966، ص8 وما بعدها.

[6]- **ممدوح عبد الحميد عبد المطلب:** جرائم إستخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، ط1، الشارقة، الإمارات العربية المتحدة، 2000، ص56.

ثالثًا: الركن المعنوي للجريمة

للركن المعنوي أهمية بالغة في تجريم الأنشطة المعلوماتية عبر شبكة الإنترنت والمواقع الإلكترونية، فلا جريمة بغير ركن معنوي، فهو حتمية لازمة لبحث المسؤولية الجنائية لهذا النوع من الجرائم في إكتمال بنيانها القانوني إبتداءً، والذي ذهب إلى القول بأن الركن المعنوي للجريمة هو نفسه ركن المسؤولية فيها.[1]

بحيث تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي، والذي يتألف بدوره من عنصرين هما "العلم والإرادة"، فالعلم يقتضي إدراك مقدم الخدمة لحقيقة النشاط الإجرامي الصادر عنه، وهو عدم تنفيذه لإلتزاماته القانونية والمنصوص عنها، والمتمثلة أساسًا في جملة الإلتزامات التي تم شرحها سلفًا.

كما ينبغي أن تتجه إرادة الجاني إلى ذلك النشاط المُجرَّم، فإذا إنتفت هذه الإرادة إنتفى معها القصد الجنائي، ولا أهمية للبواعث على السلوك الإجرامي، إذ لا يعتد القانون بأي منها،[2] والإرادة بهذا المعنى يجب أن تصدر عن فاعل يسأل عنها ويتحمل تبعات الجزاء المقرر لها، بنية وإرادة إرتكاب جريمة الإيواء المعلوماتي، فهي وإن كانت تتكون من العناصر العقلية والنفسية فإنه من مقتضيات العدالة أن لا توقع العقوبة إلاَّ على شخص له عليها سيطرة ممتدة إلى كل أجزائها، وأنه متى أنزلت العقوبة على شخص ليس له السيطرة الكاملة على إرادته ذات الأصول النفسية فلا قيام للمسؤولية الجنائية أصلاً.

ومعنى ذلك أنه بقدر سيطرة نفسية الجاني على المادة المعلوماتية محل النشاط الإجرامي والمتمثل في نشاط الإيواء عبر الشبكة تتحدد صورة الركن المعنوي والقصد الجنائي في الجرائم المرتكبة عبرها، فإن إتجهت نفسيته إلى إقتراف خطأ بمعناه العام، فإنَّ هذا الخطأ هو العنصر الجوهري الذي تقوم عليه مسؤوليته الجنائية، بحيث لا يمكن تحميل الشخص نتائج الفعل المنسوب إليه، إلاَّ إذا ثبت أنه كان مقترفًا ذلك الفعل بخطأ صادر عن إرادته الحرة والواعية.[3]

---

[1]– **عبد الله أوهايبية:** شرح قانون العقوبات، المرجع السابق، ص77. – **سليمان عبد المنعم:** النظرية العامة لقانون العقوبات، المرجع السابق، ص511.

[2]– **حسني الجندي:** التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، المرجع السابق، ص214.

[3]– **علي أحمد راشد:** المبادئ العامة في القانون الجنائي، دار النهضة العربية، القاهرة، مصر، 1974، ص353.

الفرع الثاني: العقوبات المقررة لجريمة الإيواء المعلوماتي

بالنسبة للعقوبات المقررة لهذه الجريمة لابد علينا هنا أيضًا أن نذكر كل من العقوبات الأصلية والعقوبات التكميلية تباعًا ثم بعد ذلك عقوبة الشروع في الجريمة وعقوبة الإشتراك والمساهمة الجنائية.

أولاً: العقوبات الأصلية لجريمة الإيواء المعلوماتي

وهنا نميز بين العقوبات الأصلية المقررة للشخص الطبيعي والعقوبات الأصلية المقررة للشخص المعنوي.

أ- بالنسبة للشخص الطبيعي: ونذكر هنا كل من التشريع الفرنسي وكذا التشريع المصري بإعتبارهما موضوع الدراسة المقارنة، ثم بعد ذلك التشريع الجزائري فيما ذكروه جميعًا من عقوبات مقررة على الشخص الطبيعي المدان بهذه الجريمة.

1. في التشريع الفرنسي: لقد عاقب المشرع الفرنسي مقدم خدمات الإنترنت، كونه شخص طبيعي بعقوبة الحبس خمس (5) سنوات وغرامة مالية قدرها 300 ألف يورو وذلك:

- إذا لم يخطر عن إختراق للبيانات الشخصية إلى اللجنة الوطنية للمعلوماتية والحريات أو صاحب الشأن[1].

- إذا قام بإجراء معالجة إلكترونية دون مراعاة الإحتياطات اللازمة والمنصوص عليها في المادة (34) من القانون رقم (78-17)[2].

---

[1]- ***Article 226-17-1: Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13***

« Le fait pour un fournisseur de services de communications électroniques ou pour un responsable de traitement de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des articles 33 et 34 du règlement (UE) 2016/679 du 27 avril 2016 précité ou des dispositions du II de l'article 83 et de l'article 102 de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Est puni des mêmes peines le fait pour un sous-traitant de ne pas notifier cette violation au responsable de traitement en méconnaissance de l'article 33 du règlement (UE) 2016/679 du 27 avril 2016 précité ou de l'article 102 de la loi n° 78-17 du 6 janvier 1978 précité».

[2]- ***Article 226-17 : Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13***

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende».

– إذا قام بإهمال عند تنفيذ معالجة إلكترونية للبيانات الشخصية دون مراعاة الإجراءات اللازمة التي يجب إتباعها[1].

2. في التشريع المصري: عاقب المشرع المصري على هذه الجريمة بعقوبات سالبة للحرية وبغرامات مالية تتفاوت حسب نوع الجريمة المدان بها مقدم الخدمة ومنها:

– عقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة إمتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط المحتوى المشار إليه...[2].

– عقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة...[3].

– عقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة إمتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها...[4].

– عقوبة الغرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه، كل مقدم خدمة أخل بأي من إلتزاماته المنصوص عليها... وتضاعف عقوبة الغرامة في حالة العود...[5].

– يعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، كل مقدم خدمة خالف أحكام...[6].

– يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام...[7].

---

[1]– ***Article 226-16: Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13***

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés».

[2]– المادة (30) من القانون المصري رقم (175 لسنة 2018).

[3]– المادة (31) من القانون المصري رقم (175 لسنة 2018).

[4]– المادة (32) من القانون المصري رقم (175 لسنة 2018).

[5]– المادة (1/33) من القانون المصري رقم (175 لسنة 2018).

[6]– المادة (2/33) من القانون المصري رقم (175 لسنة 2018).

[7]– المادة (3/33) من القانون المصري رقم (175 لسنة 2018).

كما نص المشرع المصري على العقوبات المشددة لهذه الجريمة في حالة وجود الظروف المشددة في الجريمة، وذلك بموجب نص المادة (34) من نفس القانون بقولها: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الإقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الإجتماعي، تكون العقوبة السجن المشدد"[1].

3. في التشريع الجزائري: عاقب المشرع الجزائري بدوره على هذه الجريمة بموجب نص المادة (394 مكرر 8) من (ق ع ج) بقولها: "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج أو بإحدى هاتين العقوبتين فقط، مقدم خدمات الإنترنت..."[2].

كما ذكرت المادة (11) من القانون رقم (09-04) السالف الذكر، عقوبة مقدم الخدمة بقولها: "دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، ويعاقب الشخص المعنوي بالغرامة وفقًا للقواعد المقررة في قانون العقوبات"[3].

كما نصَّت أيضًا المادة (2/10) من القانون رقم (09-04) بقولها: "... ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق"[4].

ب- بالنسبة للشخص المعنوي: إذا كان مقدم خدمات الإنترنت شخص معنوي، وتم إدانته بهذه الجريمة، فإنه تسري عليه أحكام المادة (394 مكرر 4) من (ق ع ج) والتي جاء فيها: "يعاقب

---

[1]- أنظر في ذلك: **الملحق رقم (04).**

[2]- أنظر في ذلك: **الملحق رقم (05).**

[3]- أنظر في ذلك: **الملحق رقم (06).**

[4]- وهذا ما نصت عليه المادة (11) من قانون الإجراءات الجزائية بقولها: " تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون الإضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه ..."، الأمر رقم (15-02) المؤرخ في 2015/07/23 المعدل والمتمم لقانون الإجراءات الجزائية رقم (66-155).

الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

كما يمكن أن تقضي المحكمة فضلاً عن عقوبة الغرامة بعقوبة "حل الشخص المعنوي"، ويعتبر الحل من العقوبات الماسة بوجود الشخص المعنوي وما يتبعه من إجراءات متعلقة بتصفيته وإنهائه من الحياة السياسية أو الإقتصادية أو الإجتماعية، بحيث أن عقوبة الحل تماثل عقوبة الإعدام بالنسبة للشخص الطبيعي[1]، إذ هي من العقوبات الأصلية التي تتمثل في حل الشخص المعنوي[2].

ونظرًا لخطورة هذه العقوبة فقد أحاطتها القوانين المعمول بها بعدد من الضوابط والضمانات التي تضيق من نطاقها، وتثير عقوبة الحل صعوبات خاصة من الناحية العملية تتمثل أساسًا في أن هذه العقوبة لا تسمح بأي حال من الأحوال بمنح فرصة لرد الإعتبار، وهي على عكس عقوبة الإلغاء من مزاولة نشاط معين، أو سحب ترخيص بمزاولة نشاط معين مؤقتًا أو نهائيًا[3].

كما لا يمكن تطبيق عقوبة الحل على الأشخاص الإعتبارية الأجنبية، إلا إذا وجد مبدأ المعاملة بالمثل في قانون دولة الشخص الإعتباري الأجنبي، كما تثير هذه المسألة أيضًا العديد من الصعوبات خلال فترة التصفية حول القانون الواجب التطبيق، والشخص الذي يعينه القضاء مصفيًا وغيرها من الصعوبات.

ج- تشديد العقوبة: وهو ما ذكرته أيضًا المادة (394 مكرر 3) من (ق ع ج) بقولها: "تضاعف العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

ثانيًا: العقوبات التكميلية لجريمة الإيواء المعلوماتي

وهو ما نصت عليه المادة (394 مكرر 6) من (ق ع ج) بقولها: "مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقًا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أُرتكبت بعلم مالكها".

---

[1]- **محمد علي سويلم:** المرجع السابق، ص456.

[2]- أنظر في ذلك نص المادة (18 مكرر) من (ق ع ج) تحت عنوان "العقوبات المطبقة على الأشخاص المعنوية"، لا سيما العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح.

[3]- وهذا ما ذكرته نص المادة (9) من (ق ع ج) في فقرتها السادسة بقولها: "المنع المؤقت من ممارسة مهنة أو نشاط".

ثالثًا: عقوبة الشروع والإشتراك في جريمة الإيواء المعلوماتي

سبق القول أن جريمة الإيواء المعلوماتي تأخذ صورتها المعتادة متى توافرت جميع أركانها، وتحققت جُلُّ عناصرها القانونية، وذلك بفعل شخص واحد، غير أنه يمكن أن تقوم هذه الجريمة بفعل أكثر من شخص، فتأخذ وصف جريمة مساهمة جنائية بالإشتراك فيها، كما قد يعاقب عليها القانون متى توافرت بعض عناصر الركن المادي، وتخلف بعضها الآخر لأسباب خارجة عن إرادة الجاني، وهو ما يصطلح عليه بالشروع في الجريمة[1].

أ- الشروع في جريمة الإيواء المعلوماتي: نصت المادة (394 مكرر 7) من (ق ع ج) بقولها: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

ويُعبِّر العقاب على الشروع في مثل هذه الجرائم على إهتمام المشرع بالآثار القانونية المترتبة عن مخالفة القواعد الجزائية التي تعنى بحماية بعض المصالح وصيانتها من كل عدوان[2]، بحيث يمثل الشروع في جريمة الإيواء المعلوماتي عبر الشبكة إحدى الصور أو الأشكال الخاصة التي يتخذها السلوك المجرم لمقدمي خدمات الإنترنت، ومثالها أن يستغل هؤلاء الوسطاء خطورة نشاط معلوماتي أو مضمون أو محتوى معلوماتي، ثم عزمهم على القيام بنشاط مجرم بغية تحقيق نتيجة إجرامية، بشرط توافر القصد الجرمي لدى مقدم الخدمة، إذ يتميز هذا البدء والعزم بكونه ذا طبيعة عمدية مبني على قصد محدد[3] لإرتباطه المباشر بالنتائج التي أراد الجاني تحقيقها بإتيانه وقائع الإيواء المعلوماتي الغير مشروع، ليترتب عن هذا إستبعاد فكرة الشروع من جرائم الإيواء غير العمدية، لأنه لا يتصور وجود شروع في جرائم الخطأ المرتبطة بخدمة إيواء المواقع الإلكترونية عبر شبكة الإنترنت حتى وإن تحققت النتيجة الضارة لسبب خارج عن إرادة الفاعل[4].

ب- الإشتراك في جريمة الإيواء المعلوماتي: لقد نصت المادة (394 مكرر 5) من (ق ع ج) بقولها: "كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

---

[1]- **عادل بوزيدة:** المرجع السابق، ص139.

[2]- ***VITALIS Andre :*** *Informatique et liberté, Ed, Economica, Paris, France, 1981, P145.*

[3]- **عبد الله أوهايبية:** شرح قانون العقوبات، المرجع السابق، ص142.

[4]- **عادل بوزيدة:** المرجع السابق، ص140.

ومفاد ذلك أنَّ الأصل في جرائم الإيواء المعلوماتي كغيرها من الجرائم ترتكب من فاعل أو شخص واحد، والإستثناء في ذلك أن تقع هذه الجرائم من طرف العديد من الجناة أحياناً، وفي أحيان أخرى يكون هذا التعدد لازمًا وحتميًا لإكتمال البنيان القانوني للسلوك المجرم وفق ما يحدده نص التجريم، بحيث يأخذ مقدم خدمات الإنترنت وصف المساهم الأصلي في جريمة الإيواء المعلوماتي، متى ساهم مساهمة مباشرة في إرتكابه لهذه الجريمة، أو أنه حرض الغير على إتيانها، بأن يدفعه إلى إرتكاب السلوك غير المشروع عبر الشبكة أو المواقع الإلكترونية، وهذا من خلال خلق الفكرة الجرمية لديهم أو تشجيعهم عليها، وذلك بإحدى وسائل التحريض المقررة قانوناً[1].

ومن هنا يراد بالمساهمة الجنائية في إطار خدمات الإيواء المعلوماتي، هو تعاون أكثر من شخص في إرتكاب واقعة الإيواء المعلوماتي عبر مواقع وصفحات الإنترنت، وهي تمثل الصورة الخاصة التي تتخذها هذه الجريمة، بحيث تقوم على وحدة الجريمة من جهة وتعدد الجناة من جهة أخرى، ويتجه رأي في الفقه الجنائي إلى إعتبار المسؤول عن إستغلال الموقع الإلكتروني – متعهد الإيواء – فاعلاً أصليًا في الجريمة لأنه يحقق العلانية، أما مستخدم الموقع أو المستأجر له فإنه شريك في الجريمة[2].

وهذا ما قضت به محكمة النقض الفرنسية في حكم شهير لها، بأن جريمة متعهدي الإيواء المعلوماتي يلزم لتوافرها وجود ركن العلانية – كجريمة التحريض على الفسق والفجور – وأن الفاعل الأصلي في هذه الجريمة هو متعهد الإيواء أو المستغل *L'exploitant*، وأن المستأجر للموقع الإلكتروني أو مصمم الصفحة *Le Créateur* يعتبر شريكًا في الجريمة فقط، وبناءً عليه قضت المحكمة أنه لما كان الفاعل في هذه الجريمة وفقًا للقواعد العامة في قانون العقوبات هو من يقوم بعمل من الأعمال المكونة لها، ولما كانت العلانية ركناً في الجريمة، فإن المستغل – متعهد الإيواء – يعد فاعلاً في الجريمة، أما المطلع أو المتصفح الذي يتدخل للإطلاع على هذه المواقع، فهو لا يقوم بأي دور في تكوين الجريمة[3].

---

[1]– عادل بوزيدة: المرجع نفسه، ص142.

[2]– ***MASCALA Corinne :*** *Droit pénal de l'informatique et droit des personnes. (Ed dalloz), Paris, France, 2004, P202.*

[3]– *Crim, 8 Déc 1998, Bull crim, N°=335, P607.*

خَـــاتِـــمَة

خاتمة:

لعلنا بذلك نكون قد وصلنا إلى خاتمة هذه الدراسة وبيَّنا أهم معالم وأحكام المسؤولية الجنائية للمجرم المعلوماتي، وبيَّنا معها كيف تحول المجتمع الإنساني في الوقت الحاضر إلى الإعتماد كليًا على المعلوماتية بشكل أشبه بالثورة التي لا تقل في الأهمية عن الثورة الصناعية، والتي أثرت في الفكر الإنساني بواسطة دخول الحاسب الآلي إلى كل بيت وكل نشاط أو خدمة تمارسها وتقدمها أي من المؤسسات أو الإدارات أو الشركات وأيًّا كانت طبيعتها.

وحتى لا نقع في تكرار ما تم تناوله بالشرح في هذه الدراسة، سوف نعمد مباشرة من خلال هذه الخاتمة إلى ذكر أهم النتائج والتوصيات والمقترحات التي توصل إليها الباحث من حياكة ونسيج لغوي وقانوني في إخراج أطروحة هذه الدكتوراه.

أولاً: بالنسبة للنتائج

بعد البحث في ثنايا هذا الموضوع توصلنا إلى جملة من النتائج أهمها:

✓ كشفت هذه الدراسة على أن عالم الجريمة في إتساع مستمر ومقلق، حيث أصبح يتقدم بتقدم وتطور التكنولوجيا والوسائل الإلكترونية المتطورة بإستمرار لا نظير له، وأصبحت الجريمة أكثر قوة بفضل التقنية الحديثة.

✓ أكدت هذه الدراسة على أن الإنترنت والحاسوب صيحة العصر الحالي ولغة العالم الإنساني الجديد فهي لسان التخاطب بكل لغات ولهجات العالم، وهذا كنتيجة منطقية للتطورات التكنولوجية الحاصلة ومظهر من مظاهر مجتمع جديد يفرض نفسه علينا شئنا أم أبينا.

✓ كشفت هذه الدراسة على أن الناس اليوم أصبحوا تقريباً لا يستطيعون العيش بدون جهاز حاسوب أو شبكة الإنترنت ولا حتى الإستغناء عن ذلك الهاتف النقال، حتى أصبحت بمثابة وسائل ضرورية لا مجال للإبتعاد عنها، ورغم أن هذه التكنولوجيات الحديثة قدمت الكثير من الخدمات التي تهدف إلى تسهيل حياة الأفراد وتعاملاتهم اليومية، إلا أنها أصبحت منبعًا لإزدياد معدل الجريمة وعنصرًا فعالاً في تنفيذها، فهذه التطورات التكنولوجية في الحقيقة من أهم مسببات تزايد عدد الجرائم وتنوعها بشكل واسع وملفت للنظر.

✓ أثبتت هذه الدراسة إلى أن التعامل مع شبكة الإنترنت في الأمور اليومية لحياة الإنسان ترتب عليها ظهور جرائم مستحدثة لها طابع ومظهر مستنكر نتج عن إستخدام هذه الشبكة بشكل سيء من قبل بعض الأفراد الذين يتمتعون بالخبرة الفنية والمعرفة التقنية للحواسيب.

✓ كما كشفت هذه الدراسة أن القانون الجنائي لا يتطور دائمًا بنفس الوتيرة والسرعة التي تتطور بها الحياة التكنولوجية ومهارة الذهن البشري والإجتماعي، والذي سخر نظم المعلوماتية المستحدثة للإستخدامات السيئة، حيث وجدت العديد من الثغرات القانونية التي أُعتبرت بمثابة قصور تشريعي في مواجهة الإجرام المعلوماتي الحديث، وبالتالي عدم إمكانية إحتضان القانون الجنائي لهذه الطائفة من الجرائم بشكل كافي.

✓ كما كشفت هذه الدراسة أنه نظرًا للطبيعة الخاصة للجريمة المعلوماتية لا يوجد إتفاق على وضع تعريف موحد لها، أو إستعمال مصطلح معين للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة التقنية والرقمنة وكل ما له علاقة بتكنولوجيا الإعلام والإتصال، فهي جريمة تتم في فضاء إفتراضي يتسم بالتطور والتغيير والإنتشار العالمي العابر للحدود الوطنية.

✓ كما بينت هذه الدراسة أيضًا أن الجريمة المعلوماتية ليست صنفًا واحدًا، بل هي متعددة التصنيفات سواء ما تعلق منها بمعطيات الحاسوب كمحل للجريمة أو دور الحاسوب كوسيلة في إرتكابها، أو بإستخدام شبكة الإنترنت لتسهيل إرتكاب عديد أنواع هذه الجرائم المتعلقة بالحواسيب والإنترنت.

✓ إتضح لنا من هذه الدراسة أن النصوص العقابية التقليدية سواءً الموجودة في قانون العقوبات أو القوانين المكملة له لا تكفي فعليًا لمواجهة هذه الجرائم المستحدثة وهذا بسبب الطبيعة الخاصة لهذه الجرائم، على الرغم من تدارك المشرع الجزائري لهذه المسألة بإستحداث نصوص قانونية سواء بالقانون رقم (04-15) أو القانون رقم (09-04) واللذان تم الإشارة إليهما سلفًا، ومع ذلك لا تزال السياسة التشريعية الجنائية في الجزائر في هذا الجانب تشهد تراجعًا بعض الشيء، وهذا مقارنة مع الكثير من الدول، ومع ذلك كان المشرع الجزائري سباق إلى وضع القواعد الأساسية لهذه الجريمة بدءًا من سنة 2004، وهذه الخطوة كانت الأساس في مكافحة الجرائم المعلوماتية.

✓ كما أكدت هذه الدراسة أن الجريمة المعلوماتية تميزت بخصائص متفردة عن باقي الجرائم التقليدية الأخرى، سواء ما تعلق بالجريمة المعلوماتية ذاتها أو ما تعلق بالمجرم المعلوماتي من حيث الذكاء والإحترافية، فهي جرائم يغلب عليها الطابع الفني والتقني في إتيانها.

✓ وكشفت هذه الدراسة أيضًا عن مدى خطورة الإجرام الإلكتروني والمعلوماتي، وذلك بسبب السرعة على التنفيذ والقدرة على التنكر والتخفي ومحو كل آثار الجريمة في ثواني، وما يترتب عن

ذلك من أضرار جسيمة سواء النفسية أو الإجتماعية أو الإقتصادية، والتي يصعب أحياناً جبر الضرر الناجم عنها.

✓ وأثبتت الدراسة أيضًا أن هذه الجرائم ترتكب ضد البيانات والمعلومات والتطبيقات التي تحتويها النظم المعلوماتية، وأن المصلحة محل الحماية في الجريمة المعلوماتية هي حماية الحق في المعلومات ككيان معنوي ذو قيمة شخصية وإقتصادية في آن واحد، فمحل الحماية هنا هو دائمًا المعطيات إما بذاتها أو بما تمثله بدلالتها، سواء كانت هذه المعطيات مخزنة داخل النظام أو موجودة على أحد وسائط التخزين أو تكون في طور النقل أو التبادل ضمن وسائل الإتصال المدمجة مع نظام الحوسبة، كالمعلومات المعالجة والمخزنة أو البرامج بأنواعها أو البيانات المستخرجة والمتبادلة بين مختلف النظم.

✓ وأوضحت هذه الدراسة أيضًا أن الإعتداء على الكيانات المادية للحاسوب وما في حكمه يخرج عن نطاق الجريمة المعلوماتية، لأن هذه الكيانات المادية تعتبر محل ملائم لتطبيق نصوص التجريم التقليدية الناظمة للجرائم الواقعة على الأموال.

✓ كما بينت هذه الدراسة أن الشخص الذي يقوم بإرتكاب الجريمة المعلوماتية وهو "المجرم المعلوماتي" كثيرًا ما يكون شخص ذو خبرة وتخصص في مجال الحاسبات الآلية وله معرفة بالنظم المعلوماتية، مما يتيح له الدخول إلى هذه النظم والمواقع أو الصفحات والقيام بأفعال قد تضر فعلاً بالآخرين، وهم ضحايا الإجرام المعلوماتي.

✓ كما أكدت هذه الدراسة إلى أن مبدأ الشرعية الجنائية وهو من أهم المبادئ الدستورية التي تقوم عليها نظريات التجريم والعقاب، أنه يعتبر مصدر الصفة غير المشروعة للفعل وفق نص قانوني تجريمي واضح، بالإضافة إلى أن إعمال هذا المبدأ يترتب عليه أهم نتيجة وهي عدم جواز التوسع في تفسير النصوص التجريمية وعدم جواز القياس عليها في إطار قانون العقوبات والقوانين المكملة له.

✓ كشفت هذه الدراسة أن هناك بعض الجرائم المعلوماتية والمرتبكة عبر شبكة الإنترنت قد يكون الجاني في دولة والمجني عليه في دولة أخرى، ففي مجتمع الإنترنت تذوب كل الحدود الجغرافية بين الدول وهذا لإرتباط العالم بشبكة إتصالات واحدة مما يسهل إرتكاب هذا النوع من الجرائم من خلال مسافات جد بعيدة قد تصل إلى دول وحتى قارات.

✓ أثبتت الدراسة أن العديد من نصوص قانون العقوبات الجزائري والمنظمة لبعض الجرائم المعلوماتية بوجه عام، أنها أصبحت فعلاً غير قابلة للإنطباق على ما يشهده العالم اليوم من جرائم تقنية المعلومات بدلالتها الواسعة، مما يستدعي معه تدخلاً تشريعيًا واضحًا لمواجهة الأنشطة الجرمية المستحدثة.

✓ كشفت الدراسة أن المشرع الجزائري يعتبر من بين المشرعين الأوائل الذين تفطنوا إلى خطورة الإجرام الإلكتروني وما كان يوجد من فراغ تشريعي في مواجهته، حيث سارع بدوره إلى تعديل قانون العقوبات عام 2004، ثم عام 2006 وبعدها تعديل 2016، وأدرج قِسمًا خاصًا جديدًا وهو "القسم السابع مكرر" تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات *Les atteintes au système de traitement de donnés*" فتناول فيه أبرز وأخطر الجرائم المعلوماتية التي يمكن أن يرتكبها المجرم المعلوماتي على المنظومة المعلوماتية، وذلك بالمواد من (394 مكرر) إلى (394 مكرر 8) من (ق ع ج).

✓ كما أثبتت هذه الدراسة أن المشرع الجزائري إستعمل مصطلح "منظومة معلوماتية" بدلاً من مصطلح "نظام معلوماتي" وحسن فعل في ذلك، وهذا لترك الباب مفتوحًا في حالة ظهور منظومات معلوماتية جديدة مع تعدد إستعمالها، مع إشتراطه عدم خضوع هذه المنظومة للحماية الفنية، حيث يهدف المشرع من وراء ذلك إلى إضفاء الحماية الجنائية على كافة المنظومات المعلوماتية المتعددة والمختلفة بغض النظر عن تمتعها بنظام الحماية الفنية أم لا.

✓ كما أثبتت هذه الدراسة أن المشرع الجزائري إنتهج نفس مسلك التشريعات الجنائية الحديثة، وذلك عندما حمى المعلومات المبرمجة داخل النظام المعلوماتي ضد كل أفعال الحصول عليها بطريقة غير مشروعة، وهذا من خلال النص على جريمة الدخول غير المشروع، لكن – كما رأينا – أن هذا الأسلوب في التجريم لحماية النظم المعلوماتية هو في الحقيقة أسلوب غير مباشر، وغير كافي للإحاطة بحالات الإعتداء.

✓ كشفت الدراسة أن المشرع توسع في مفهوم جريمة الدخول أو البقاء غير المشروع داخل النظام، ليشمل كل أفعال العبث والتلاعب في المعطيات المخزنة داخل النظام سواء بالإدخال أو بالإزالة أو بالتعديل وهذا بقصد ضمان سريتها وسلامتها.

✓ أثبتت الدراسة أن المشرع الجزائري وسَّع أيضًا من حماية المعطيات والمعلومات المعالجة آليًّا وعدم المساس بسلامتها حتى وهي موجودة خارج النظام المعلوماتي سواءً عن طريق الحيازة أو الإفشاء أو النشر أو الإستعمال وغيرها.

✓ كشفت الدراسة أن المشرع وضع عقوبات مختلفة سواءً بالنسبة للحالة البسيطة للجريمة المعلوماتية أو بالنسبة للحالة المشددة لها، وذلك بمضاعفة عقوبة الحبس والغرامة معًا، وهذا تبعًا لنوع كل جريمة، وكذا تبعًا لصفة المجني عليه فيها، خاصة إذا ما مسَّت الجريمة المعلوماتية مؤسسات الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

✓ كما كشفت الدراسة أن المشرع تبنى مبدأ مسؤولية الشخص المعنوي الذي قد يرتكب إحدى الجرائم المعلوماتية المنصوص عليها قانونًا.

✓ كما قررت هذه الدراسة توسيع نطاق تطبيق العقوبة ليشمل كل من حالة الشروع في إرتكاب الجريمة وكذا حالة الإشتراك والإتفاق الجنائي.

✓ أكدت هذه الدراسة أيضًا على تقرير عقوبات تكميلية إلى جانب العقوبات الأصلية كالمصادرة والغلق والتي تتماشى مع هذا النوع من الإجرام.

✓ وكشفت هذه الدراسة أن كثرة النصوص القانونية المتناثرة بين هذا القانون وذاك، جعلت من الجرائم المعلوماتية خالية من الغطاء التشريعي الموحد الذي لابد أن يحتويها وأساليبها وصورها ووضع كل جريمة مع العقوبة التي تناسبها.

✓ أثبتت الدراسة أن الوصف الجنحي لكل الجرائم المعلوماتية تقريبًا، جعلها جرائم تتشابه من حيث تكييفها والجهات القضائية الناظرة فيها وحتى من حيث العقوبات المقررة لها، وهذا ما ينعكس بدوره على السياسة العقابية الردعية ومدى نجاعتها في تحقيق فكرة الردع بنوعيه العام والخاص.

ثانيًا: التوصيات

من جملة التوصيات التي يمكن للباحث أن يذكرها في هذه الدراسة، نجد ما يلي:

- ✓ على المشرع الجزائري التدخل السريع في وضع تشريع جديد لمواجهة القصور الموجود في التشريعات والقوانين الحالية، أو إستحداث قانون جديد يتعلق بجرائم تقنية المعلومات وتجريم إستخدام التقنيات العلمية الحديثة، وكذا السعي إلى وضع قانون جديد خاص بالإنترنت بإعتبارها أوسع إنتشارًا من وسائل النشر أو العلانية الأخرى.
- ✓ نشر الوعي بأهمية الإستغلال والإستخدام العقلاني للبرامج المعلوماتية وإيجاد حلول وقائية فعالة لحمايتها من كل أشكال التصميم والإصطناع والتقليد والتزوير المعلوماتي.
- ✓ نوصي بالتوعية الإعلامية المستمرة للمخاطر الناتجة عن سوء إستخدام شبكة الإنترنت وما قد تلحقه من أضرار مادية ومعنوية جسيمة على الأمن القومي والإقتصادي وأمن المجتمعات والأفراد.
- ✓ الزيادة في تطوير القدرات التقنية والفنية على شبكة الإنترنت، وإنشاء رقابة فعلية للتحري المباشر على مرتكبي الجرائم المعلوماتية حال دخولهم على الشبكة والمواقع الإلكترونية من خلال التتبع الفني للجهاز أو الخط الذي أُرتكبت منه الجريمة.
- ✓ على المشرع الجزئري بضرورة تفعيل دور المجتمع المدني وخاصة الجمعيات للقيام بدورها بما يلزم لوقاية الشباب والأطفال القصر من الوقوع في الممارسات الخاطئة والإستخدامات السيئة للوسائل الإلكترونية وما ينجم عنها من سلوكيات ضارة ماديًا ومعنويًا وأخلاقيًا عبر شبكة الإنترنت.
- ✓ ضرورة توعية الفرد والمجتمع بالآثار السلبية والخطيرة للإستخدام غير العقلاني للوسائل التكنولوجية الحديثة، لأن الجانب الردعي لا يكفي لوحده لمجابهة الجريمة الإلكترونية بمختلف أنواعها.
- ✓ على المشرع الجنائي في كافة الدول العربية على إبرام إتفاقيات تعاون فيما بين البرلمانات العربية وهذا على غرار البرلمان الأوروبي بغية تعزيز التعاون التشريعي والقضائي والشرطوي بجميع هيئاته لمواجهة هذه التحديات الناجمة عن الجرائم المعلوماتية.
- ✓ ضرورة التوجه نحو زيادة التعاون الدولي والإقليمي لمواجهة الجرائم المستحدثة في البيئة المعلوماتية، وذلك من خلال الدخول في إتفاقيات ومعاهدات دولية وإقليمية تسعى إلى تبادل الخبرات والمعلومات في المسائل المتعلقة بهذا النوع من الإجرام لاسيما تسليم المجرمين في المجال المعلوماتي.

ثالثًا: الإقتراحات

رغم الجهود التي بذلتها الجزائر ولا زالت تبذل، فإن هذه التحديات تبقى عصية على الحل في كثير من الأحيان، وذلك في ظل غياب إستراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها لا سيما في الوقت الراهن والذي لم يبادر بعد المشرع الجنائي في الجزائر إلى خلق تشريع عقابي شامل وأوسع يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تناسب هذا العصر الرقمي.

ومن هذه الدراسة التي قمنا بها، توصلنا إلى جملة من الإقتراحات نذكرها تباعًا، ونهيب بالمشرع الجزائري أن يأخذ بها:

- ✓ كما أننا لاحظنا من خلال هذه الدراسة عدم نص المشرع الجزائري على بعض الجرائم المستحدثة رغم خطورتها على الفرد والمجتمع، ومن قبيل ذلك مثلاً جريمة الترويج والإتجار بالمخدرات الرقمية، جريمة التزوير المعلوماتي وإستعمال المزور الرقمي، جريمة سرقة المال المعلوماتي وإخفاء المسروقات الرقمية، جريمة الإتلاف المعلوماتي وإفساد النظام المعلوماتي ... وغيرها كثير، وعليه يجب على المشرع تدارك هذا الفراغ التجريمي لهذه الأفعال المستنكرة بشدة داخل المجتمع، وهذا من خلال تعديل النصوص التجريمية التقليدية أو إستحداث نصوص أخرى جديدة تتلاءم وطبيعة هذه الجرائم.
- ✓ يستوجب على المشرع إخضاع الجرائم المعلوماتية بنصوص خاصة صريحة ومباشرة، للعقاب على الأفعال التي تتم من خلال التقنية الرقمية، وذلك خشية من إفلات المجرم المعلوماتي من المساءلة الجنائية عن أفعال خطرة يترتب عليها المساس الصارخ بالحياة الخاصة والأسرار الهامة، أو الإعتداء على الذمة المالية للغير، وغيرها من الصور الإجرامية الخطيرة، لذلك وجب على المشرع أن يبادر إلى تنظيم كل ما هو موضوعي وواقعي بما يحقق نوع من التوازن بين نشأة الحق وطريقة الوصول إليه وحمايته.
- ✓ ضرورة الإسراع في سن تشريع جديد بشأن قانون مكافحة الجرائم المعلوماتية، وأن ينسجم هذا التشريع مع أحكام الدستور في عدم المساس بالحقوق الأساسية والحريات العامة المادية منها والمعنوية، لذا فكلنا أمل أن يتدخل المشرع الجنائي الجزائري لوضع إطار قانوني جديد صيانة لأسس ومبادئ النظام المعلوماتي من جهة، وكذا كفالة الحقوق والمصالح والمراكز القانونية التي

يهددها الإجرام المعلوماتي، وهذا إما بإستحداث نصوص قانونية خاصة بجرائم تقنية المعلومات أو بتعديل دقيق في نصوص قانون العقوبات.

✓ تشديد العقوبات المتعلقة بالقرصنة والإختراق المعلوماتي لما يمثله من خطر داهم على سلامة وأمن الوطن والمواطن، وبخاصة المستتر خلف وسطاء مقدمي خدمات الإنترنت، وإعتبارها بمثابة جريمة مشددة وبخاصة إذا كان الهدف منها إخفاء مرتكب هذه الجرائم.

✓ ونرى مما سبق دراسته بالمقارنة مع بعض القوانين أن بعض التشريعات العربية قد أصابت حين أفردت تشريعًا خاصًا تواجه به الجرائم المعلوماتية، وهذا ما نفضله وندعو به المشرع الجزائري للعمل به، لأن جرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات لم تكن شاملة لجميع الجرائم المعلوماتية.

وأخيرا وليس بالأخير... أرجوا من الله سبحانه وتعالى أن أكون قد وفقت في هذه الدراسة وإبرازها في هذا المدى من الأطروحة، فإن كان ذلك ... فمن الله وحده وله الشكر والحمد والفضل والمنة ... وإن لم أوفق فمن نفسي والشيطان ... ولكن عذري في ذلك يعلمه الله أنني قد إجتهدت ولكل مجتهد نصيب.

وآخر دعوانا أن الحمد لله رب العالمين ...

المَلاَحِقِ

الملحق رقم (01)

مجلس أوروبا
مجموعة المعاهدات
الأوروبية - رقم ١٨٥

الاتفاقية المتعلقة بالجريمة الإلكترونية

{بودابست}

٢٠٠١/١١/٢٣

1

الديباجة

إن الدول الأعضاء في مجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية؛

إذ تأخذ في الاعتبار أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛

واعترافاً منها بقيمة تعزيز التعاون مع الدول الأخرى الأطراف في هذه الاتفاقية؛

واقتناعاً منها بالحاجة إلى إتباع سياسة جنائية مشتركة، كمسألة ذات أولوية، بهدف حماية المجتمع من الجريمة الإلكترونية، من خلال تبني تشريع ملائم ودعم التعاون الدولي، من بين أمور أخرى؛

وإدراكاً منها بعمق التغييرات التي أحدثتها الرقمنة والالتقائية والعولمة المتواصلة لشبكات الكومبيوتر؛

وإذ يساورها القلق بشأن مخاطر إمكانية استخدام شبكات الكومبيوتر والمعلومات الإلكترونية أيضا لارتكاب جرائم جنائية، وأن الأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات؛

واعترافاً منها بالحاجة إلى التعاون بين الدول والقطاع الخاص في مجال مكافحة الجريمة الإلكترونية، والحاجة إلى حماية المصالح المشروعة عند استخدام وتطوير تكنولوجيا المعلومات؛

وإيماناً منها بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم تعزيز التعاون الدولي في المسائل الجنائية وتسريع وتيرته وتوظيفه بشكل جيد؛

واقتناعاً منها بأن هذه الاتفاقية ضرورية لردع الأعمال الموجهة ضد سرية وسلامة وتوافر نظم الكومبيوتر، والشبكات والبيانات بالإضافة إلى إساءة استخدام هذه النظم والشبكات والبيانات، وذلك بالتنصيص على تجريم سلوكيات من هذا القبيل، كما هو مبين في هذه الاتفاقية واعتماد الصلاحيات الكافية من أجل مكافحة فعالة لمثل هذه الجرائم الجنائية من خلال تيسير كشفها، والتحقيق بشأنها، ومقاضاتها على المستويين الوطني والدولي على حد سواء، وكذلك عن طريق توفير ترتيبات من أجل تحقيق تعاون دولي سريع وموثوق؛

وحرصاً منها على ضرورة تأمين التوازن الملائم بين المصالح المتصلة بإنفاذ القانون من جهة واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام ١٩٥٠ بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام ١٩٦٦ المتعلق بالحقوق المدنية والسياسية، وغيرها من المعاهدات الدولية بشأن حقوق الإنسان السارية والتي تؤكد حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير، بما في ذلك حرية البحث عن مختلف أنواع المعلومات والأفكار وتلقيها ونقلها بغض النظر عن الحدود، علاوة على الحقوق المتعلقة باحترام الخصوصية؛

وحرصاً منها كذلك على الحق في حماية البيانات الشخصية، الذي تخوله على سبيل المثال اتفاقية مجلس أوروبا لعام ١٩٨١ بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛

وإذ تأخذ في الاعتبار اتفاقية الأمم المتحدة لعام ١٩٨٩ بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام ١٩٩٩ بشأن أسوأ صور عمل الأطفال؛

وإذ تأخذ بعين الاعتبار اتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي، وكذلك المعاهدات المماثلة القائمة بين الدول الأعضاء في مجلس أوروبا وغيرها من الدول، وتؤكد على أن الاتفاقية الحالية ترمي إلى استكمال تلك الاتفاقيات بغية تعزيز فعالية التحقيقات والإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بنظم وبيانات الكومبيوتر، والتمكين من جمع الأدلة في الجرائم الجنائية ذات الطابع الإلكتروني؛

وإذ ترحب بالتطورات الأخيرة التي تعزز التفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية، بما في ذلك الإجراء الذي اتخذته منظمة الأمم المتحدة، ومنظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي ومجموعة الثمانية؛

وإذ تذكر بتوصيات لجنة الوزراء رقم ١٠/٨٥ بشأن التطبيق العملي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية، والتوصية رقم ٢/٨٨ بشأن القرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة، والتوصية رقم ١٥/٨٧ التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم ٤/٩٥ بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات مع إشارة خاصة إلى الخدمات الهاتفية، بالإضافة إلى التوصية رقم ٩/٨٩ بشأن الجرائم ذات الصلة بالكمبيوتر التي توفر مبادئ توجيهية للهيئات التشريعية الوطنية بشأن تعريف بعض جرائم الكومبيوتر، والتوصية رقم ١٣/٩٥ بشأن المشاكل التي يطرحها قانون الإجراءات الجنائية علاقة بتكنولوجيا المعلومات؛

ومراعاة للقرار رقم ١ الذي تبناه وزراء العدل الأوروبيون في مؤتمرهم الواحد والعشرين (براغ، في ١٠ و١١ يونيو/حزيران ١٩٩٧) والذي أوصى لجنة الوزراء بدعم الجهود التي تبذلها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) في مجال الجريمة الإلكترونية بغية تقريب أحكام القوانين الجنائية الوطنية من بعضها البعض، وتمكين استخدام الوسائل الفعالة لإجراء التحقيقات في مثل هذه الجرائم، بالإضافة إلى القرار رقم ٣ المعتمد خلال المؤتمر الثاني لوزراء العدل الأوروبيين (لندن، ٨ و٩ يونيو/حزيران ٢٠٠٠) والذي شجع الأطراف المتفاوضة على مواصلة جهودهم بغرض إيجاد حلول ملائمة لتمكين أكبر عدد ممكن من الدول أن تصبح أطرافاً في الاتفاقية، وأقر بالحاجة إلى نظام سريع وفعال للتعاون الدولي يأخذ بعين الاعتبار وكما يجب الشروط الخاصة بمكافحة الجريمة الإلكترونية؛

وبالنظر لخطة العمل التي اعتمدها رؤساء الدول والحكومات الأعضاء في مجلس أوروبا بمناسبة انعقاد القمة الثانية (ستراسبورغ، ١٠ و١١ أكتوبر/تشرين الأول ١٩٩٧) بغية إيجاد ردود مشتركة لتطور تكنولوجيات المعلومات الحديثة وفقاً لمعايير وقيم مجلس أوروبا؛

اتفقت على ما يلي:

الباب الأول- استخدام المصطلحات

المادة ١- التعريفات

لأغراض هذه الاتفاقية:

أ. يُقصد بـ " منظومة الكومبيوتر " أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات؛

ب. يُقصد بـ " بيانات الكومبيوتر " أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة؛

ج. يُقصد بـ " مُقدم الخدمة "

١) أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و

٢) أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

د. يُقصد بـ" بيانات حركة الاتصالات" أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءاً في سلسلة الاتصالات، توضح المنشأ، والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية.

الباب الثاني: التدابير الواجب اتخاذها على الصعيد الوطني

القسم الأول: القانون الجنائي الموضوعي

الفصل الأول: الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكومبيوتر

المادة ٢ – النفاذ غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة ٣ – الاعتراض غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية غير صادقة أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة ٤ – التدخل في البيانات

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.

٢. يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة ١ في ضرر جسيم.

المادة ٥ – التدخل في النظام

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها.

المادة ٦ – إساءة استخدام الأجهزة

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق:

أ. عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى:

١. جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛

٢. كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥؛ و

ب. حيازة إحدى المواد المشار إليها في الفقرة أ (١) أو (٢) أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥. ويجوز للدولة الطرف أن تشترط بموجب القانون أن تكون حيازة عدد من هذه المواد سابقة لإلحاق المسؤولية الجنائية.

٢. لا يجوز تُفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع ، الشراء بغرض الاستخدام، الاستيراد، التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها بالفقرة ١ من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من ٢ إلى ٥ من هذه الاتفاقية، بل بالأحرى للاستخدام المرخص لغرض اختبار أو حماية نظام الكمبيوتر.

٣. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة ١ من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع، توزيع أو إتاحة هذه المواد المشار إليها في الفقرة ١- أ (٢) من هذه المادة.

الفصل الثاني: الجرائم ذات الصلة بالكومبيوتر.

المادة ٧ – التزوير المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: إدخال، تغيير، حذف أو إتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

المادة ٨ – الاحتيال المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ. أي إدخال، تغيير، حذف أو إتلاف لبيانات الكومبيوتر؛

ب. أي تدخل في وظيفة نظام الكومبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق، على منفعة اقتصادية ذاتية أو لفائدة شخص آخر.

الفصل الثالث: الجرائم ذات الصلة بالمحتوى

المادة ٩ – الجرائم ذات الصلة بمواد إباحية عن الأطفال

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق:

أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكومبيوتر؛
ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكومبيوتر؛
ج. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكومبيوتر؛
د. الحصول على مواد إباحية عن الأطفال عبر نظام الكومبيوتر لصالح الشخص ذاته أو لفائدة الغير؛
هـ. حيازة مواد إباحية عن الأطفال داخل نظام الكومبيوتر أو على دعامة لتخزين بيانات الكومبيوتر.

٢. لغرض الفقرة ١ أعلاه، تشمل عبارة " مواد إباحية عن الأطفال " المواد الإباحية التي تعرض بشكل مرئي:
أ. قاصر وهو يمارس سلوكا جنسيا واضحا؛
ب. شخص يبدو قاصرا وهو يمارس سلوكا جنسيا واضحا؛
ج. صور واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا واضحا.

٣. لغرض الفقرة ٢ أعلاه ، يشمل مصطلح " قاصر " كافة الأشخاص دون سن الثامنة عشر. ويجوز لأي دولة طرف أن تشترط حداً عمرياً أدنى لا يقل عن سن السادسة عشر.

٤. يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين "د" و "ه" من الفقرة ١ والبندين "ب" ، "ج" من الفقرة ٢.

الفصل الرابع: الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

المادة ١٠ – الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في ٢٤ يوليو/تموز ١٩٧١ والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكومبيوتر.

٢. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق ذات الصلة، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة الويبو بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكومبيوتر.

٣. يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين ١ و٢ من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين ١ و٢ من هذه المادة.

الفصل الخامس: المسؤولية الإضافية والعقوبات

المادة ١١ – المحاولة، والمساعدة والتحريض

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ١٠ من هذه الاتفاقية، وذلك بنية ارتكاب جريمة من هذا القبيل.

٢. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: محاولة ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من ٣ إلى ٥، ٧، ٨ و٩. ١ (أ) و(ج) من هذه الاتفاقية.

٣. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة ٢ من هذه المادة كلياً أو جزئياً.

المادة ١٢ – مسؤولية الشركات

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن الجرائم المنصوص عليها في هذه الاتفاقية التي تُرتكب لمصلحتها من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضوا في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قيادياً داخلها، وذلك بناء على:

أ. سلطة تمثيل الشخص الاعتباري؛

ب. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

ج. سلطة ممارسة الرقابة لدى الشخص الاعتباري.

٢. بالإضافة إلى الحالات المنصوص عليها مسبقا في الفقرة ١ من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان مساءلة الشخص الاعتباري في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة ١ في ارتكاب جريمة منصوص عليها وفقا لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

٣. رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية، مدنية أو إدارية.

٤. لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

المادة ١٣ – العقوبات والتدابير

١. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من ٢ إلى ١١ مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية.

٢. تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقا للمادة ١٢ وإخضاعهم لعقوبات أو تدابير فعالة، متناسبة ورادعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

القسم الثاني: القانون الإجرائي

الفصل الأول: أحكام مشتركة

الملحق رقم (02)

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجـة :

إن الدول العربية الموقعة،

رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

وإلتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

فقد اتفقت على ما يلي:

الفصل الأول
أحكام عامة

المادة الأولى: الهدف من الاتفاقية:

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادة الثانية: المصطلحات:

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1- **تقنية المعلومات:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة.

2- **مزود الخدمـة:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3- **البيانـات :** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها...

الأمانة العامة لجامعة الدول العربية – إدارة الشؤون القانونية – الشبكة القانونية العربية www.arablegalnet.org

4- **البرنامج المعلوماتي:** مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.
5- **النظام المعلوماتي:** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.
6- **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.
7- **الموقـــع :** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
8- **الالتقـــاط :** مشاهدة البيانات أو المعلومات أو الحصول عليها.
9- **معلومات المشترك:** أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:
أ - نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
ب- هويـــة المشـــترك وعنوانـــه البريـــدي أو الجغرافـــي أو هاتفـــه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.
ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادة الثالثة: مجالات تطبيق الاتفاقية:

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

1 – ارتكبت في أكثر من دولة.
2- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.
3- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.
4- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

المادة الرابعة: صون السيادة:

1- تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.
2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الثاني

التجريم

المادة الخامسة: التجريم:

تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية.

المادة السادسة: جريمة الدخول غير المشروع:

1- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:
أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
ب- الحصول على معلومات حكومية سرية.

المادة السابعة: جريمة الاعتراض غير المشروع:

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادة الثامنة: الاعتداء على سلامة البيانات:

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.
2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم.

المادة التاسعة: جريمة إساءة استخدام وسائل تقنية المعلومات:

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب- كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

المادة العاشرة: جريمة التزوير:

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادة الحادية عشرة: جريمة الاحتيال:

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:
1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3- تعطيل الأجهزة والبرامج والمواقع الالكترونية.

المادة الثانية عشرة: جريمة الإباحية:

1- انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.
3- يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

المادة الثالثة عشرة: الجرائم الأخرى المرتبطة بالإباحية:

المقامرة والاستغلال الجنسي.

المادة الرابعة عشرة: جريمة الاعتداء على حرمة الحياة الخاصة:

الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات .

المادة الخامسة عشرة: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المادة السادسة عشرة: الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:

1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.
2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.
3- الاتجار بالأشخاص.
4- الاتجار بالأعضاء البشرية.
5- الاتجار غير المشروع بالأسلحة.

المادة السابعة عشرة: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة:

انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

المادة الثامنة عشرة: الاستخدام غير المشروع لأدوات الدفع الالكترونية:

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.
3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة التاسعة عشرة: الشروع والاشتراك في ارتكاب الجرائم:

1- الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.
2- الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.
3- يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً.

المادة العشرون: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية:

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً.

المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

الفصل الثالث

الأحكام الإجرائية

المادة الثانية والعشرون: نطاق تطبيق الأحكام الإجرائية:

1- تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والاجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.
2- مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على:
   أ- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية.
   ب- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات.
   ج- جمع الأدلة عن الجرائم بشكل إلكتروني.
3- أ- يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا

الملحق رقم (03)

Code pénal

- *Partie législative (Articles 111-1 à 727-3)*
    - *Livre III : Des crimes et délits contre les biens (Articles 311-1 à 324-9)*
        - *Titre II : Des autres atteintes aux biens (Articles 321-1 à 324-9)*
            - *Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8)*

Article 323-1

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

Article 323-2

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

Article 323-3

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

Article 323-3-1

Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25

« Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

Article 323-4

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 () JORF 22 juin 2004

« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».

Article 323-4-1

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

« Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende ».

Article 323-5

« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 ».

Article 323-6

Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

« Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ».

Article 323-7

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 () JORF 22 juin 2004

« La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines ».

Article 323-8

Création LOI n°2015-912 du 24 juillet 2015 - art. 18

« Le présent chapitre n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'Etat désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code ».

الملحق رقم (04)

الجريدة الرسمية - العدد ٣٢ مكرر (ج) فى ١٤ أغسطس سنة ٢٠١٨ ٣

قانون رقم ١٧٥ لسنة ٢٠١٨
فى شأن مكافحة جرائم تقنية المعلومات

باسم الشعب

رئيس الجمهورية

قرر مجلس النواب القانون الآتى نصه ، وقد أصدرناه :

الباب الأول

الأحكام العامة

تعريفات

مادة (١)

فى تطبيق أحكام هذا القانون ، يُقصد بالكلمات والعبارات التالية المعنى المبين قرين كل منهما :

الجهاز : الجهاز القومى لتنظيم الاتصالات .

الوزير المختص : الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات .

البيانات والمعلومات الإلكترونية : كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه ، بواسطة تقنية المعلومات ، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات ، وما فى حكمها .

بيانات شخصية : أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده ، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى .

بيانات حكومية : بيانات متعلقة بالدولة أو إحدى سلطاتها ، أو أجهزتها أو وحداتها ، أو الهيئات العامة ، أو الهيئات المستقلة أو الأجهزة الرقابية ، أو غيرها من الأشخاص الاعتبارية العامة وما فى حكمها ، والمتاحة على الشبكة المعلوماتية أو على أى نظام معلوماتى أو على حاسب أو ما فى حكمها .

المعالجة الإلكترونية : أى عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية ، وذلك باستخدام أى وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى .

تقنية المعلومات : أى وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات ، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا .

مقدم الخدمة : أى شخص طبيعى أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات ، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه فى أى من تلك الخدمات أو تقنية المعلومات .

المستخدم : كل شخص طبيعى أو اعتبارى ، يستعمل خدمات تقنية المعلومات ، أو يستفيد منها بأى صورة كانت .

البرنامج المعلوماتى : مجموعة الأوامر والتعليمات المعبر عنها بأى لغة أو رمز أو إشارة والتى تتخذ أى شكل من الأشكال ، ويمكن استخدامها بطريق مباشر أو غير مباشر فى حاسب آلى لأداء وظيفة أو تحقيق نتيجة ، سواء كانت هذه الأوامر والتعليمات فى شكلها الأصلى أو فى أى شكل آخر تظهر فيه من خلال حاسب آلى ، أو نظام معلوماتى .

النظام المعلوماتى : مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات ، أو تقديم خدمة معلوماتية .

شبكة معلوماتية : مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معًا ، ويمكنها تبادل المعلومات والاتصالات فيما بينها ، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية ، والتطبيقات المستخدمة عليها .

الموقع : مجال أو مكان افتراضى له عنوان محدد على شبكة معلوماتية ، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة .

مدير الموقع : كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية ، بما فى ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه .

الحساب الخاص : مجموعة من المعلومات الخاصة بشخص طبيعى أو اعتبارى ، تخول له دون غيره الحق فى الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتى .

البريد الإلكترونى : وسيلة لتبادل رسائل إلكترونية على عنوان محدد ، بين أكثر من شخص طبيعى أو اعتبارى ، عبر شبكة معلوماتية ، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلى وما فى حكمها .

الاعتراض : مشاهدة البيانات أو المعلومات أو الحصول عليها ، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه ، وذلك لأسباب غير مشروعة ودون وجه حق .

الاختراق : الدخول غير المرخص به أو المخالف لأحكام الترخيص ، أو الدخول بأى طريقة غير مشروعة إلى نظام معلوماتى أو حاسب آلى أو شبكة معلوماتية وما فى حكمها .

المحتوى : أى بيانات تؤدى بذاتها أو مجتمعة مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو إشارة إلى بيانات أخرى .

الدليل الرقمى : أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها ، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة .

الخبرة : كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل فى مجالات تقنية المعلومات .

حركة الاتصال (بيانات المرور) : بيانات ينتجها نظام معلوماتى تبين مصدر الاتصال وجهته والوجهة المرسل منها والمرسل إليها والطريق الذى سلكه وساعته وتاريخه وحجمه ومدته ونوع الخدمة .

الحاسب : كل جهاز أو معدة تقنية تكون قادرة على التخزين وأداء عمليات منطقية أو حسابية ، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات .

دعامة إلكترونية : أى وسيط مادى لحفظ وتداول البيانات والمعلومات الإلكترونية ، ومنها الأقراص المدمجة والأقراص الضوئية والذاكرة الإلكترونية وما فى حكمها .

الأمن القومى : كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدة وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطنى ومجلس الأمن القومى ، ووزارة الدفاع والإنتاج الحربى، ووزارة الداخلية ، والمخابرات العامة ، وهيئة الرقابة الإدارية ، والأجهزة التابعة لتلك الجهات .

جهات الأمن القومى : رئاسة الجمهورية ، ووزارة الدفاع ، ووزارة الداخلية ، والمخابرات العامة ، وهيئة الرقابة الإدارية .

التزامات وواجبات مقدم الخدمة

مادة (٢)

أولاً - مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣ ، يلتزم مقدمو الخدمة بما يأتى :

١ - حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات ، لمدة مائة وثمانين يومًا متصلة . وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتى :

(أ) البيانات التى تمكن من التعرف على مستخدم الخدمة .

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة .

(جـ) البيانات المتعلقة بحركة الاتصال .

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال .

(هـ) أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز .

٢ - المحافظة على سرية البيانات التى تم حفظها وتخزينها ، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة ، ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته ، أو أى بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون ، أو الأشخاص والجهات التى يتواصلون معها .

٣ - تأمين البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها أو تلفها .

ثانيا - مع عدم الإخلال بأحكام قانون حماية المستهلك ، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة ، بالشكل والطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة ، البيانات والمعلومات الآتية :

١ - اسم مقدم الخدمة وعنوانه .

٢ - معلومات الاتصال المتعلقة بمقدم الخدمة ، بما فى ذلك عنوان الاتصال الإلكترونى .

٣ - بيانات الترخيص لتحديد هوية مقدم الخدمة ، وتحديد الجهة المختصة التى يخضع لإشرافها .

٤ - أى معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة ، ويصدر بتحديدها قرار من الوزير المختص .

ثالثا : مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور ، يلتزم مقدمو الخدمة والتابعون لهم ، أن يوفروا حال طلب جهات الأمن القومى ووفقًا لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقًا للقانون .

رابعا : يلتزم مقدمو خدمات تقنية المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين ، ويُحظر على غيرهم القيام بذلك .

نطاق تطبيق القانون من حيث المكان

مادة (٣)

مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات ، تسرى أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها فى هذا القانون ، متى كان الفعل معاقبًا عليه فى الدولة التى وقع فيها تحت أى وصف قانونى ، وذلك فى أى من الأحوال الآتية :

١ - إذا ارتُكبت الجريمة على متن أى وسيلة من وسائل النقل الجوى أو البرى أو المائى ، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها .

٢ - إذا كان المجنى عليهم أو أحدهم مصريًا .

٣ - إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها فى جمهورية مصر العربية .

٤ - إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة ، تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية .

٥ - إذا كان من شأن الجريمة إلحاق ضرر بأى من مواطنى جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأى من مصالحها ، فى الداخل أو الخارج .

٦ - إذا وُجد مرتكب الجريمة فى جمهورية مصر العربية ، بعد ارتكابها ولم يتم تسليمه .

التعاون الدولى فى مجال مكافحة جرائم تقنية المعلومات

مادة (٤)

تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها ، أو تطبيقًا لمبدأ المعاملة بالمثل ، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنية المعلومات ، والمساعدة على التحقيق فيها ، وتتبع مرتكبيها .

على أن يكون المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة فى هذا الشأن .

الباب الثانى
الأحكام والقواعد الإجرائية
مأمورو الضبط القضائى

مادة (٥)

يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومى بالنسبة إلى الجرائم التى تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم .

الأوامر القضائية المؤقتة

مادة (٦)

لجهة التحقيق المختصة ، بحسب الأحوال ، أن تصدر أمراً مسببًا لمأمورى الضبط القضائى المختصين ، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمرة واحدة ، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون ، بواحد أو أكثر مما يأتى :

١ - ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه . ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر ، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ .

٢ - البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط .

٣ - أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه ، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو النظام التقنى .

وفى كل الأحوال ، يجب أن يكون أمر جهة التحقيق المختصة مسببًا .

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة ، فى المواعيد ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية .

الإجراءات والقرارات الصادرة فى شأن طلبات حجب المواقع

مـادة (٧)

لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يُبث من داخل الدولة أو خارجها ، بوضع أى عبارات أو أرقـام أو صـور أو أفلام أو أى مواد دعـائية أو ما فى حكمها ، بما يُعد جريمة من الجرائم المنصوص عليها فى هذا القانون ، ويشكل تهديداً للأمن القومى أو يعرِّض أمن البلاد أو اقتصادها القومى للخطر ، أن تأمر بحجب الموقع أو المواقع محل البث ، كلما أمكن تحقيق ذلك فنيًا .

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة ، منعقدة فى غرفة المشورة خلال أربع وعشرين ساعة مشفوعًا بمذكرة برأيها. وتُصدر المحكمة قرارها فى الأمر مسببًا إما بالقبول أو بالرفض ، فى مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها .

ويجـوز فى حالة الاستعجال لوجود خطر حالٍّ ، أو ضرر وشيك الوقوع ، أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز ، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة فى الفقرة الأولى من هذه المادة وفقًا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه .

وعلى جهة التحرى والضبط التى قامت بالإبلاغ أن تحرر محضراً تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يُعرض على جهات التحقيق خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذى وجهته للجهاز ، وتتبع فى شأن هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة . وتصدر المحكمة المختصة قرارها فى هذه الحالة إما بتأييد ما تم من إجراءات حجب ، أو بوقفها .

فإذا لم يُعرَض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد ، يعد الحجب الذى تم كأن لم يكن .

ولمحكمة الموضوع أثناء نظر الدعـوى ، أو بناءً على طلب جهة التحقيـق أو الجهاز أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب ، أو تعديل نطاقه .

وفى جميع الأحوال ، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية ، أو بصدور حكم نهائى فيها بالبراءة .

التظلم من القرارات الصادرة فى شأن طلبات حجب المواقع

مـادة (٨)

لكل من صدر ضده قرار قضائى من المنصوص عليها فى المادة (٧) من هذا القانون، وللنيابة العامة ولجهة التحقيق المختصة ولكل ذى شأن ، أن يتظلم منه أو من إجراءات تنفيذه أمام محكمة الجنايات المختصة بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال. فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم .

وفى جميع الأحوال، يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة ، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز وكل ذى شأن ، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به .

المنع من السفر

مـادة (٩)

يجوز للنائب العام أو من يفوضه من المحامين العموم الأوّل بنيابات الاستئناف ، ولجهات التحقيق المختصة ، عند الضرورة أو عند وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون أو الشروع فى ارتكابها ، أن يأمر بمنع المتهم من السفر خارج البلاد ، أو بوضع اسمه على قوائم ترقب الوصول ، بأمر مسبب لمدة محددة .

ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة ، خلال خمسة عشر يومًا من تاريخ علمه به . فإذا رفُض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم .

ويكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة ، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تُعلَن بها النيابة العامة والمتظلم ، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز خمسة عشر يومًا من تاريخ التقرير به ، بحكم مسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق المختصة حسب الأحوال ، ولها فى سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها فى هذا الشأن .

ويجوز للنيابة العامة وجهات التحقيق المختصة فى كل وقت العدول عن الأمر الصادر منها ، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة ، إذا دعت الضرورة لذلك .

وفى جميع الأحوال ، ينتهى المنع من السفر بمرور سنة من تاريخ صدور الأمر ، أو بصدور قرار بألا وجه لإقامة الدعوى الجنائية ، أو بصدور حكم نهائى فيها بالبراءة ، أيهما أقرب .

الخبراء

مادة (١٠)

يُنشأ بالجهاز سجلان لقيد الخبراء، يُقيَّد بأولهما الفنيون والتقنيون العاملون بالجهاز ، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به .

وتُطبَّق على الخبراء فى ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء .

واستثناء من تلك القواعد ، تسرى على الخبراء المقيدين بالسجل الثانى القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وُجد .

وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد فى كل من السجلين .

فى الأدلة الرقمية

مـادة (١١)

يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتى أو من برامج الحاسب ، أو من أى وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون .

البـاب الثـالث

الجرائم والعقوبات

مـادة (١٢)

مع عدم الإخلال بأى عقوبة أشد منصوص عليها فى قانون العقوبات أو أى قانون آخر ، ومع مراعاة أحكام قانون الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦ ، يعاقب على الجرائم التالية بالعقوبات المبينة قرين كل جريمة .

(الفصل الأول)

الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها

مـادة (١٣)

يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئى .

جريمة الدخول غير المشروع

مـادة (١٤)

يُعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه .

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى ، تكون العقوبة الحبس مدة لا تقل عن سنتين ، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين .

جريمة تجاوز حدود الحق فى الدخول

مـادة (١٥)

يُعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له ، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول .

جريمة الاعتراض غير المشروع

مـادة (١٦)

يُعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من اعترض بدون وجه حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلى وما فى حكمها .

جريمة الاعتداء على سلامة البيانات
والمعلومات والنظم المعلوماتية

مادة (١٧)

يعاقب بالحبس مدة لا تقل عن سنتين ، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أى نظام معلوماتى وما فى حكمه ، أيًا كانت الوسيلة التى استخدمت فى الجريمة .

جريمة الاعتداء على البريد الإلكترونى
أو المواقع أو الحسابات الخاصة

مادة (١٨)

يعاقب بالحبس مدة لا تقل عن شهر ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس .

فإذا وقعت الجريمة على بريد إلكترونى أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة ، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين .

جريمة الاعتداء على تصميم موقع

مادة (١٩)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف أو عطل أو أبطأ أو شوَّه أو أخفى أو غيَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعى بغير وجه حق .

جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

مـادة (٢٠)

يعاقب بالحبس مدة لا تقل عن سنتين ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، أو تجاوز حدود الحق المخـول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريداً إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة ، أو مملوكًا لها ، أو يخصها .

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكوميـة ، تكون العقوبة السجن ، والغـرامة التى لا تقل عن مـائة ألف جنيـه ولا تجاوز خمسمائة ألف جنيه .

وفى جميع الأحوال ، إذا ترتب على أى من الأفعـال السابقة إتلاف تلك البيـانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى ، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها ، أو إلغاؤها كليًا أو جزئيًا ، بأى وسيلة كانت ، تكون العقوبة السجن ، والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه .

جريمة الاعتداء على سلامة الشبكة المعلوماتية

مـادة (٢١)

يعـاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من تسبب متعمداً فى إيقاف شبكة معلوماتيـة عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها .

ويعاقب كل من تسبب بخطئه فى ذلك بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين .

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامـة أو تمتلكها أو تدار بمعـرفتهـا تكون العقوبة السـجن المشـدد ، وبغرامـة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه .

البرامج والأجهزة والمعدات المستخدمة
فى ارتكاب جرائم تقنية المعلومات
مـادة (٢٢)

يعاقب بالحبس مدة لا تقل عن سنتين ، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدَّر أو تداول بأى صورة من صور التداول ، أى أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أى بيانات مماثلة ، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون ، وثبت أن ذلك السلوك كان بغرض استخدام أى منها فى ارتكاب أو تسهيل ارتكاب أى جريمة من الجرائم المنصوص عليها فى هذا القانون ، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء .

(الفصل الثانى)
الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات
جرائم الاحتيال والاعتداء على بطاقات البنوك
والخدمات وأدوات الدفع الإلكترونى
مـادة (٢٣)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن ثلاثين ألف جنيه ، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين ، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات فى الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية .

فإن قصد من ذلك استخدامها فى الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين .

وتكون العقوبة الحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو إحدى هاتين العقوبتين ،إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير .

الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكترونى

مادة (٢٤)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين ، كل من اصطنع بريداً إلكترونيًا أو موقعًا أوحسابًا خاصًا ونسبه زوراً إلى شخص طبيعى أو اعتبارى .

فإذا استخدم الجانى البريد أو الموقع أو الحساب الخاص المصطنع فى أمر يسئ إلى ما نُسب إليه ، تكون العقوبة الحبس الذى لا تقل مدته عن سنة ، والغرامة التى لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين .

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة ، تكون العقوبة السجن ، والغرامة التى لا تقل عن مائة ألف جنيه ، ولا تزيد على ثلاثمائة ألف جنيه .

(الفصل الثالث)

الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع

مادة (٢٥)

يعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى أو انتهك حرمة الحياة الخاصة ، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته ، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته ، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما فى حكمها ، تنتهك خصوصية أى شخص دون رضاه ، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة .

مـادة (٢٦)

يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات ، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من تعمد استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة ، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه .

(الفصل الرابع)

الجرائم المرتكبة من مدير الموقع

مـادة (٢٧)

فى غير الأحوال المنصوص عليها فى هذا القانون ، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه ، ولا تزيد على ثلاثمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا .

مـادة (٢٨)

يعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها فى هذا القانون والتى وقعت على موقع أو حساب أو بريد إلكترونى بقصد إعاقة عمل الجهات الرسمية المختصة .

مـادة (٢٩)

يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أوالنظام المعلوماتى عَرَّض أيًا منها لإحدى الجرائم المنصوص عليها فى هذا القانون .

ويعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى تسبب بإهماله فى تَعرّض أى منها لإحدى الجرائم المنصوص عليها فى هذا القانون ،وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة فى اللائحة التنفيذية لهذا القانون .

(الفصل الخامس)

المسئولية الجنائية لمقدمى الخدمة

مادة (٣٠)

يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه ، أو بإحدى هاتين العقوبتين ، كل مُقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المشار إليه فى الفقرة الأولى من المادة (٧) من هذا القانون . فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة ، وفاة شخص أو أكثر ، أو الإضرر بالأمن القومى ، تكون العقوبة السجن المشدد ، والغرامة التى لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط .

مادة (٣١)

يعاقب بالحبس مدة لا تقل سنة ، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل مقدم خدمة خالف الأحكام الواردة بالبند (٢) من الفقرة أولاً من المادة (٢) من هذا القانون ، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمى الخدمة .

مادة (٣٢)

يعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه ، أوبإحدى هاتين العقوبتين ، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها فى المادة (٦) من هذا القانون .

مـادة (٣٣)

يعاقب بغرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه ، كل مقدم خدمة أخل بأى من التزاماته المنصوص عليها فى البند (١) من الفقرة (أولاً) من المادة (٢) من هذا القانون . وتضاعف عقوبة الغرامة فى حالة العود ، وللمحكمة أن تقضى بإلغاء الترخيص .

ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولاتجاوز مائتى ألف جنيه ، كل مقدم خدمة خالف أحكام الفقرة (ثانيًا) و(رابعًا) من المادة (٢) من هذا القانون .

ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبالغرامة التى لا تقل عن مائتى ألف جنيه ولا تجاوز مليون جنيه ، كل مقدم خدمة خالف أحكام الفقرة (ثالثًا) من المادة (٢) من هذا القانون .

(الفصل السادس)

الظروف المشددة فى الجريمة

مـادة (٣٤)

إذا وقعت أى جريمة من الجرائم المنصوص عليها فى هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومى للبلاد أو بمركزها الاقتصادى أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعى ، تكون العقوبة السجن المشدد .

(الفصل السابع)

المسئولية الجنائية للشخص الاعتبارى

مـادة (٣٥)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تزيد على مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل مسئول عن الإدارة الفعلية لأى شخص اعتبارى إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى المخصص للكيان الذى يديره لأى جريمة من الجرائم المنصوص عليها فى هذا القانون ولم يبلغ بذلك الجهات الرسمية المختصة وقت علمه بالجريمة .

مـادة (٣٦)

فى الأحوال التى ترتكب فيها أى من الجرائم المنصوص عليها فى هذا القانون باسم ولحساب الشخص الاعتبارى ، يعـاقب المسئول عن الإدارة الفعليـة إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقًا لمصلحة له أولغيره بذات عقوبة الفاعل الأصلى .

وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبارى للنشاط مدة لا تزيد على سنة ، ولها فى حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتبارى بحسب الأحوال ، ويتم نشر الحكم فى جريدتين يوميتين واسعتى الانتشار على نفقة الشخص الاعتبارى .

مـادة (٣٧)

فى تطبيق أحكام هذا القانون ، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التى تقوم بها الجريمة .

(الفصل الثامن)

العقوبات التبعية

مـادة (٣٨)

مع عدم الإخلال بحقوق الغير حسن النية ، على المحكمة فى حالة الحكم بالإدانة فى أى جريمة من الجرائم المنصوص عليها فى هذا القانون أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونًا ، أو غيرها مما يكون قد استخدم فى ارتكاب الجريمة ، أو سهل أو ساهم فى ارتكابها .

وفى الحالات التى يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية ، وكان الشخص الاعتبارى المُدان بأى جريمة منصوص عليها فى هذا القانون لم يحصل على الترخيص فيحكم فضلاً عن العقوبات المقررة بالغلق .

مـادة (٣٩)

للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين ، لارتكابه جريمة من الجرائم المنصوص عليهـا فى هذا القانون ، أثنـاء وبسـبب تـأديته لوظيفتـه ، أن تقضى بعزله من وظيفته مؤقتًا ، إلا فى الحالات المشار إليها فى المادة (٣٤) من هذا القانون فيكون العزل وجوبيًا .

(الفصل التاسع)

الشروع والإعفاء من العقوبة

مـادة (٤٠)

يعاقب كل من شرع فى ارتكاب الجنح المنصوص عليها فى هذا القانون بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة .

مـادة (٤١)

يعفى من العقوبات المقررة للجرائم المنصوص عليها فى هـذا القـانون كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء فى تنفيذ الجريمة وقبل كشفها .

ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف فى التحقيق فيها إذا مكن الجانى أو الشريك ، فى أثناء التحقيق ، السلطات المختصة من القبض على مرتكبى الجريمة الآخرين ، أو على ضبط الأموال موضوع الجريمة ، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها ، أو على القبض على مرتكبى جريمة أخرى مماثلة لها فى النوع والخطورة .

ولا يخل حكم هذه المادة ، بوجوب القضاء برد المال المتحصل من الجرائم المنصوص عليها فى هذا القانون .

الصلح والتصالح

مادة (٤٢)

يجوز للمتهم فى أى حالة كانت عليها الدعوى الجنائية ، وقبل صيرورة الحكم باتًا ، إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام ، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك فى الجنح المنصوص عليها فى المواد (١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون .

ولا يُنتج إقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون .

كما لا يُقبل التصالح إلا من خلال الجهاز فى الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون .

ولا يسقط حق المتهم فى التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثى الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر ، وذلك قبل صدور حكم نهائى فى الموضوع .

وفى جميع الأحوال يجب على المتهم الذى يرغب فى التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغاً يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة . ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة ، بحسب الأحوال .

ويترتب على الصلح انقضاء الدعوى الجنائية ، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية .

الباب الرابع

أحكام انتقالية وختامية

مادة (٤٣)

يلتزم مقدمو الخدمة والمخاطبون ، بأحكام هذا القانون والتزاماته باتخاذ الإجراءات اللازمة لتقنين أوضاعهم خلال سنة من تاريخ العمل بأحكامه .

مادة (٤٤)

يُصدر رئيس مجلس الوزراء اللائحة التنفيذية لهذا القانون خلال ثلاثة أشهر من تاريخ العمل به .

مادة (٤٥)

يُنشر هذا القانون فى الجريدة الرسمية ، ويُعمل به من اليوم التالى لتاريخ نشره .

يُبصم هذا القانون بخاتم الدولة ، ويُنفذ كقانون من قوانينها .

صدر برئاسة الجمهورية فى ٣ ذى الحجة سنة ١٤٣٩هـ

(الموافق ١٤ أغسطس سنة ٢٠١٨م) .

عبد الفتاح السيسى

الملحق رقم (05)

القسم السابع مكرر من قانون العقوبات الجزائري:

تحت عنوان: (المساس بأنظمة المعالجة الآلية للمعطيات) الصادر بالقانون رقم (قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004). المعدل والمتمم لقانون العقوبات والصادر بالأمر رقم 66-156.

المادة 394 مكرر: (القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006)

يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

- تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

- وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50000 دج إلى 300000 دج.

المادة 394 مكرر 1: (القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006)

يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500000 دج إلى 4000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

المادة 394 مكرر 2: (القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006)

يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1000000 دج إلى 10000000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

المادة 394 مكرر 3: (القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004)

تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.

المادة 394 مكرر 4: (القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004)

يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

المادة 394 مكرر 5: (القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004)

كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم النصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

المادة 394 مكرر 6: (القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004)

مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

المادة 394 مكرر 7: (القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004)

يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

المادة 394 مكرر 8: (قانون رقم 16-02 مؤرخ في 19 يونيو سنة 2016)

دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث (3) سنوات وبغرامة من 2000000 دج إلى 10000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الإنترنت" بمفهوم المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:

- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو لجعل الدخول إليها غير ممكن.

الملحق رقم (06)

25 شعبان عام 1430 هـ
16 غشت سنة 2009 م

الجريدة الرّسميّة للجمهوريّة الجزائريّة / العدد 47

5

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة
الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع
التزامات مقدمي الخدمات
مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

الملحق رقم (07)

مراسيم تنظيميّة

مرسوم تنفيذيّ رقم 98 - 257 مؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998، يضبط شروط وكيفيّات إقامة خدمات " أنترنات " واستغلالها.

إنّ رئيس الحكومة،

- بناء على تقرير وزير البريد والمواصلات،

– وبناء على الدّستور، لا سيّما المادّتان 85 – 4 و 125 (الفقرة 2) منه،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمّن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمّن القانون المدنيّ، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 59 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمّن القانون التّجاري، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 89 المؤرّخ في 27 ذي الحجّة عام 1395 الموافق 30 ديسمبر سنة 1975 والمتضمّن قانون البريد والمواصلات، المعدّل والمتمّم،

– وبمقتضى القانون رقم 90 – 07 المؤرّخ في 8 رمضان عام 1410 الموافق 3 أبريل سنة 1990 والمتعلّق بالإعلام، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 90 – 22 المؤرّخ في 27 محرّم عام 1411 الموافق 18 غشت سنة 1990 والمتعلّق بالسّجلّ التّجاريّ، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 95 – 06 المؤرّخ في 23 شعبان عام 1415 الموافق 25 يناير سنة 1995 والمتعلّق بالمنافسة ،

– وبمقتضى الأمر رقم 97 – 10 المؤرّخ في 27 شوّال عام 1417 الموافق 6 مارس سنة 1997 والمتعلّق بحقوق المؤلّف والحقوق المجاورة،

– وبمقتضى المرسوم رقم 83 – 71 المؤرّخ في 23 ربيع الأوّل عام 1403 الموافق 8 يناير سنة 1983 الّذي يحدّد صلاحيّات وزير البريد والمواصلات،

– وبمقتضى المرسوم الرّئاسيّ رقم 97 – 230 المؤرّخ في 19 صفر عام 1418 الموافق 24 يونيو سنة 1997 والمتضمّن تعيين رئيس الحكومة،

– وبمقتضى المرسوم الرّئاسيّ رقم 97 – 231 المؤرّخ في 20 صفر عام 1418 الموافق 25 يونيو سنة 1997 والمتضمّن تعيين أعضاء الحكومة،

– وبمقتضى المرسوم التّنفيذيّ رقم 97 – 40 المؤرّخ في 9 رمضان عام 1417 الموافق 18 يناير سنة 1997 والمتعلّق بمعايير تحديد النّشاطات والمهن المقنّنة الخاضعة للقيد في السّجلّ التّجاريّ وتأطيرها،

يرسم ما يأتي :

المادّة الأولى : يضبط هذا المرسوم شروط وكيفيات إقامة خدمات " أنترنات " واستغلالها.

المادّة 2 : تعرّف خدمات " أنترنات " كما يأتي :

– خدمة " و ا ب " الواسعة النّطاق (World Wide Web (W. W. W. WEB :

خدمة تفاعلية للا طّلاع أو احتواء صفحات متعدّدة الوسائط " MULTIMEDIA " (نصوص، رسوم بيانيّة، صوت أو صورة) موصولة بينها عن طريق صلات تسمّى نصوص متعدّدة " Hy pertexte ".

– البريد الإلكتروني E. MAIL :

خدمة تبادل رسائل إلكترونية بين المستعملين.

– تلنات " TELNET " :

خدمة النفاذ إلى حواسب متباعدة بصيغة المحاكاة الطرفية.

– بروتوكول نقل الملفّات (FTP) " FILE TRANSFER PROTOCOL " :

خدمة تعبئة الملفات عن بعد بصيغة نقطة إلى نقطة.

– منبر التّحاور " NEWSGROUPS " :

خدمة تسمح بتبادل المعلومات بين مجموعة من المستعملين ذوي اهتمام مشترك حول موضوع معيّن.

المادّة 3 : تقدّم خدمات " أنترنات " من موقع يتوفّر على وسائل للإعلام الآليّ والاتّصالات.

ويقصد بالموقع أيّ مكان يحتوي موزّعا أو عدّة موزّعات للمعطيات الضّروريّة لتقديم خدمات "أنترنات ".

المادّة 4 : لا يرخص بإقامة خدمات " أنترنات " واستغلالها لأغراض تجارية ضمن الشّروط المحدّدة أدناه، إلاّ للأشخاص المعنويّين الخاضعين للقانون الجزائريّ، المدعوين أدناه " مقدّمو الخدمات " وبرأسمال يملكه فقط أشخاص معنويّون خاضعون للقانون العامّ و / أو أشخاص طبيعيّون من جنسيّة جزائريّة.

المادّة 5 : يرسل إلى الوزير المكلّف بالاتّصالات طلب التّرخيص بإقامة خدمات " أنترنات " واستغلالها، بالنّسبة لكلّ موقع يحدّد مسبّقا.

يجب أن يرفق الطّلب بملفّ يتكوّن من الوثائق الآتية :

- طلب يحرّر على نموذج تعدّه لجنة خدمات "أنترنات " المنصوص عليها في المادّة 15 أدناه،

- نسخة من القانون الأساسيّ الّذي يخوّل الشّخص المعنويّ تقديم هذه الخدمات،

- نسخة من النّشرة الرّسميّة الخاصّة بالإعلانات القانونية والمتضمّنة تسجيل الشّخص المعنويّ،

- إثبات تسديد تكاليف دراسة الملّف المحدّد مبلغها بموجب قرار مشترك بين الوزيرين المكلّفين بالماليّة والاتّصالات،

- عرض مفصّل عن الخدمات الّتي يقترح الطّالب تقديمها وكذلك شروط وكيفيّات النّفاذ إلى هذه الخدمات،

- دراسة تقنيّة حول الشّبكة المقترحة وحول التّجهيزات والبرامج المعلوماتيّة التّابعة لها، مع تحديد هيكلتها و كذلك صيغ الوصل بالشّبكة العموميّة للاتّصالات،

- التزام من المصالح المختصّة في الوزارة المكلّفة بالاتّصالات ، يثبت إمكانيّة إقامة الوصلة المخصّصة ، الضّروريّة لنقل خدمات "أنترنات".

يخضع الأشخاص المعنويّون الرّاغبون في استغلال خدمات "أنترنات " لاحتياجاتهم الخاصّة ، انطلاقا من موقع موصول مباشرة بالخارج، لنفس هذه الشّروط ، باستثناء الشّروط المتعلّقة بقانونهم الأساسيّ الّذي يخوّلهم تقديم هذه الخدمات.

يجب إيداع ملفّ طلب التّرخيص لدى المصالح المختصّة في الوزارة المكلّفة بالاتّصالات مقابل وصل استلام.

المادّة 6 : يأمر الوزير المكلّف بالاتّصالات المصالح المؤهّلة بإجراء تحقيق تأهيليّ فور استلام طلب التّرخيص بالاستغلال.

وبعد انتهاء التّحقيق يعرض الملفّ المرفق بالطّلب على اللّجنة المنصوص عليها في المادّة 15 أدناه.

المادّة 7 : يسلّم الوزير المكلّف بالاتّصالات رخصة الاستغلال بناء على موافقة اللّجنة المذكورة.

المادّة 8 : تسلّم رخصة الاستغلال لمدّة غير محدّدة ولايمكن التّنازل عنها.

المادّة 9 : يجب على الوزير المكلّف بالاتّصالات أن يبرّر قرارات رفض الرّخصة وأن يبلّغها للطّالب.

المادّة 10 : في حالة رفض الرّخصة ، يمكن الطّالب تقديم طعن مكتوب إلى الوزير المكلّف بالاتّصالات قصد :

- تقديم عناصر معلومات أو إثباتات جديدة لدعم طلبه،

- الحصول على دراسة تكميليّة،

غير أن طلب الطّعن يجب أن يصل إلى الوزير المكلّف بالاتّصالات في أجل ثلاثة (3) أشهر، ابتداء من تاريخ تبليغ رفض الرّخصة.

المادّة 11 : على الطّالب القيام بتركيب التّجهيزات والبرامج المعلوماتيّة الضّروريّة لإقامة الخدمات واستغلالها، في أجل أقصاه سنة، ابتداء من تاريخ تبليغ الرّخصة.

المادّة 12 : يجب أن تبلّغ إلى الوزير المكلّف بالاتّصالات في أجل شهرين (2) كلّ التّعديلات الطّارئة على القانون الأساسيّ الخاصّ بمقدّم خدمات "أنترنات".

المادّة 13 : يمكن أن يتمّ سحب الرّخصة مؤقّتا أو نهائيّا في الحالات الآتية :

– حلّ الشّخص المعنويّ أو إفلاسه أو تصفيته قضائيا،

– الإخلال بأحكام هذا المرسوم،

– عندما يخلّ الشّخص المؤهّل لتمثيل مقدّم خدمات " أنترنات" ، بالتّشريع والتّنظيم المعمول بهما وبأعراف المهنة إخلالا خطيرا.

المادّة 14 : يلتزم مقدّم خدمات "أنترنات " خلال ممارسة نشاطاته بما يأتي :

– تسهيل النّفاذ إلى خدمات أنترنات ، حسب الإمكانيات المتوفّرة إلى كلّ الرّاغبين في ذلك باستعمال أنجع الوسائل التّقنيّة،

– المحافظة على سرّيّة كلّ المعلومات المتعلّقة بحياة مشتركيه الخاصّة وعدم الإدلاء بها إلاّ في الحالات المنصوص عليها في القانون،

– إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النّفاذ إلى خدمات " أنترنات" وصيغة مساعدتهم كلّما طلبوا ذلك،

– عرض أيّ مشروع خاصّ باستعمال منظومات التّرميز على اللّجنة،

– احترام قواعد حسن السّيرة بالامتناع خاصّة عن استعمال أيّة طريقة غير مشروعة سواء تجاه المستعملين أو تجاه مقدّمي خدمات "أنترنات" الآخرين،

– تحمّل مسؤوليّة محتوى الصّفحات وموزّعات المعطيات الّتي يستخرجها ويأويها، طبقا للأحكام التّشريعيّة المعمول بها،

– إعلام مشتركيه بالمسؤوليّة المترتّبة عليهم فيما يتعلّق بمحتوى الصّفحات الّتي يستخرجونها ، وفقا للأحكام التّشريعيّة المعمول بها،

– اتّخاذ كلّ الإجراءات اللاّزمة لتأمين حراسة دائمة لمضمون الموزّعات المفتوحة لمشتركيه، قصد منع النّفاذ إلى الموزّعات الّتي تحتوي معلومات تتعارض مع النّظام العامّ أو الأخلاق.

المادّة 15 : تشكّل لجنة تتولّى ما يأتي :

– دراسة طلبات التّرخيص باستغلال خدمات "أنترنات " والبتّ فيها،

– تقديم توصيات في مجالات تطوير خدمات " أنترنات " وترقيتها وتأمينها،

– إنشاء لجان خاصّة ضمنها ، حسب الحاجة،

– البتّ في كلّ المسائل المعروضة عليها والمتعلّقة بمجال نشاطها.

تعدّ اللّجنة نظامها الدّاخليّ وتصادق عليه.

المادّة 16 : تتشكّل اللّجنة من الأعضاء الآتي ذكرهم :

– ممثّل الوزير المكلّف بالاتّصالات ، رئيسا،

– ممثّل وزير الدّفاع الوطنيّ،

– ممثّل وزير الشّؤون الخارجيّة،

– ممثّل الوزير المكلّف بالماليّة،

– ممثّل الوزير المكلّف بالدّاخليّة،

– ممثّل الوزير المكلّف بالاتّصال والثّقافة،

– ممثّل الوزير المكلّف بالتّعليم العالي والبحث العلميّ،

– ممثّل الوزير المكلّف بالتّجارة،

– مدير موادّ المواصلات السّلكيّة واللاّسلكيّة ومصالحها في الوزارة المكلّفة بالاتّصالات.

يمكن اللّجنة إشراك كلّ شخص قادر على المساهمة في مداولاتها.

تتولّى مصالح الوزارة المكلّفة بالاتّصالات أمانة اللّجنة.

المادّة 17 : يكون الوزير المكلّف بالاتّصالات مؤهّلا لإجراء كلّ المراقبات حول احترام شروط استعمال الرّخصة ، بالاتّصال مع المصالح والهيئات المختصّة.

المادّة 18 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998.

أحمد أويحيى

الملحق رقم (08)

17 رجب عام 1421 هـ
15 أكتوبر سنة 2000 م
الجريدة الرّسميّة للجمهوريّة الجزائريّة / العدد 60
15

مرسوم تنفيذيّ رقم 2000 - 307 مؤرّخ في 16 رجب عام 1421 الموافق 14 أكتوبر سنة 2000، يعدّل المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 الّذي يضبط شروط وكيفيّات إقامة خدمات "أنترنات" واستغلالها.

إنّ رئيس الحكومة،

- بناء على تقرير وزير البريد والمواصلات،

- وبناء على الدّستور، لاسيّما المادّتان 85 - 4 و125 (الفقرة 2) منه،

- وبمقتضى المرسوم الرّئاسيّ رقم 2000 - 256 المؤرّخ في 26 جمادى الأولى عام 1421 الموافق 26 غشت سنة 2000 والمتضمّن تعيين رئيس الحكومة،

- وبمقتضى المرسوم الرّئاسيّ رقم 2000 - 257 المؤرّخ في 26 جمادى الأولى عام 1421 الموافق 26 غشت سنة 2000 والمتضمّن تعيين أعضاء الحكومة،

- وبمقتضى المرسوم التّنفيذي رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 الّذي يضبط شروط وكيفيّات إقامة خدمات "أنترنات" واستغلالها،

يرسم ما يأتي :

المادّة الأولى : يعدّل هذا المرسوم أحكام المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998والمذكور أعلاه.

المادّة 2 : تعدّل أحكام المادّة 2 من المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 والمذكور أعلاه، كما يأتي :

"*المادّة 2* : تحدّد خدمات "أنترنات" بقرار من الوزير المكلّف بالمواصلات السّلكيّة واللاسلكيّة".

المادّة 3 : تعدّل أحكام المادّة 4 من المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 والمذكور أعلاه، كما يأتي :

"*المادّة 4* : لا يرخّص بإقامة خدمات "أنترنات" واستغلالها لأغراض تجارية ضمن الشروط المحدّدة أدناه، إلا للأشخاص المعنويين الخاضعين للقانون الجزائري الّذين يدعون أدناه "مقدّمي خدمات أنترنات".

لا يخضع لأحكام هذا المرسوم عرض الخدمات من نوع "أنترنات" في الموقع للمرتفقين الزوّار أو المشتركين عبر المحطّات الطرفية الموصولة بمقدّم خدمات "أنترنات".

غير أنّ استغلال الخدمات المنصوص عليها في الفقرة السّابقة يخضع لتصريح مسبق يحرّر في نموذج استمارة تقدّمها مصالح الوزارة المكلّفة بالمواصلات السّلكيّة واللاّسلكية. ويسجّل هذا التّصريح لدى هذه المصالح مقابل إشعار بالاستلام".

المادّة 4 : تعدّل أحكام المطة الأولى من المادّة 5 من المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 والمذكور أعلاه، كما يأتي :

"*المادّة 5* : .....

- طلب يحرّر على نموذج نمطي.

(الباقي بدون تغيير)".

المادّة 5 : يعوّض لفظ "رخصة" المستعمل في صلب المرسوم التّنفيذيّ رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998والمذكور أعلاه بلفظ "ترخيص".

المادّة 6 : تعدّل أحكام المادّة 16 من المرسوم التّنفيذي رقم 98 - 257 المؤرّخ في 3 جمادى الأولى عام 1419 الموافق 25 غشت سنة 1998 والمذكور أعلاه، كما يأتي :

"*المادّة 16* : تتشكل اللّجنة من الأعضاء الآتي ذكرهم :

- ممثّل الوزير المكلّف بالمواصلات السلكية واللاسلكية، رئيسا،

- ممثّل وزير الدّفاع الوطني،

- ممثّل وزير الداخلية.

يمكن اللّجنة أن تستعين بأي شخص من شأنه أن يساهم في مداولاتها.

تتولّى مصالح الوزارة المكلّفة بالمواصلات السلكية واللاسلكية أمانة اللّجنة".

المادّة 7 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 16 رجب عام 1421 الموافق 14 أكتوبر سنة 2000.

علي بن فليس

الملحق رقم (09)

قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 46 و136 و137-2 و138 و140 و144 منه،

– وبمقتضى العهد الدولي المتعلق بالحقوق المدنية والسياسية الموافق عليه من طرف الجمعية العامة للأمم المتحدة يوم 16 ديسمبر سنة 1966 والذي انضمّت إليه الجزائر بموجب المرسوم الرئاسي رقم 89-67 المؤرخ في 11 شوال عام 1409 الموافق 16 مايو سنة 1989،

– وبمقتضى القانون العضوي رقم 98-01 المؤرخ في 4 صفر عام 1419 الموافق 30 مايو سنة 1998 والمتعلق باختصاصات مجلس الدولة وتنظيمه وعمله، المعدل والمتمم،

– وبمقتضى القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 والمتعلق بالإعلام،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم،

– وبمقتضى الأمر رقم 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون التجاري، المعدل والمتمم،

– وبمقتضى القانون رقم 84-17 المؤرخ في 8 شوال عام 1404 الموافق 7 يوليو سنة 1984 والمتعلق بقوانين المالية، المعدل والمتمم،

– وبمقتضى القانون رقم 85-05 المؤرخ في 26 جمادى الأولى عام 1405 الموافق 16 فبراير سنة 1985 والمتعلق بحماية الصحة وترقيتها، المعدل والمتمم،

– وبمقتضى الأمر رقم 95-24 المؤرخ في 30 ربيع الثاني عام 1416 الموافق 25 سبتمبر سنة 1995 والمتعلق بحماية الأملاك العمومية وأمن الأشخاص فيها،

– وبمقتضى القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 15-03 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 والمتعلق بعصرنة العدالة،

– وبمقتضى القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الباب الأول
أحكام عامة

المادّة الأولى : يهدف هذا القانون إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المادّة 2 : يجب أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألاّ تمس بحقوق الأشخاص وشرفهم وسمعتهم.

المادّة 3 : لأغراض هذا القانون، يقصد بما يأتي :

"**المعطيات ذات الطابع الشخصي**" : كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية،

"**الشخص المعني**" : كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة،

"**معالجة المعطيات ذات الطابع الشخصي**" المشار إليها أدناه "معالجة" : كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف،

"**موافقة الشخص المعني**" : كل تعبير عن الإرادة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية.

"**المعالجة الآلية**" : العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها،

"**معطيات حساسة**" : معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية،

"**مضمون غير شرعي**" : كل مضمون مخالف للقوانين السارية لاسيما مضمون ذو طابع تخريبي أو من شأنه المساس بالنظام العام والمضمون ذو الطابع الإباحي أو المنافي للآداب العامة،

"**معطيات جينية**" : كل معطيات متعلقة بالصفات الوراثية لشخص أو عدة أشخاص ذوي قرابة،

"**معطيات في مجال الصحة**" : كل معلومة تتعلق بالحالة البدنية و/أو العقلية للشخص المعني، بما في ذلك معطياته الجينية،

"**ملف**" : كل مجموعة معطيات مهيكلة ومجمعة يمكن الولوج إليها وفق معايير محددة،

"**الاتصال الإلكتروني**" : كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية،

"**المسؤول عن المعالجة**" : شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها،

"**معالج من الباطن**" : كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة،

"**الغير**" : كل شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان آخر غير الشخص المعني والمسؤول عن المعالجة والمعالج من الباطن والأشخاص المؤهلون لمعالجة المعطيات الخاضعون للسلطة المباشرة للمسؤول عن المعالجة أو المعالج من الباطن،

"**المرسل إليه**" : الشخص الطبيعي أو المعنوي أو السلطة العمومية أو المصلحة أو أي كيان آخر يتلقى معطيات ذات طابع شخصي،

"**تنازل أو إيصال**" : كل كشف أو إعلام بمعطيات لشخص غير الشخص المعني،

"**الربط البيني للمعطيات**" : أي شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة

لغاية محددة مع معطيات أخرى يمسكها مسؤول أو مسؤولون آخرون عن المعالجة أو يمسكها نفس المسؤول لنفس الغرض أو لأغراض أخرى.

"**السلطة الوطنية**" : السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي المنصوص عليها في هذا القانون.

"**مقدم الخدمات**" :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو للمستعملين،

"**الاستكشاف المباشر**" : إرسال أي رسالة، مهما كانت دعامتها وطبيعتها، موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمات.

"**غلق المعطيات**" : جعل الدخول إليها غير ممكن.

المادّة 4 : يطبق هذا القانون على المعالجة الآلية الكلية أو الجزئية للمعطيات ذات الطابع الشخصي وكذا على المعالجة غير الآلية للمعطيات ذات الطابع الشخصي الواردة أو التي يمكن ورودها في ملفات يدوية.

ويطبق هذا القانون على معالجة المعطيات ذات الطابع الشخصي التي تقوم بها الهيئات العمومية أو الخواص :

1 – عندما تتم من طرف شخص طبيعي أو معنوي يكون المسؤول عنها مقيما على التراب الوطني أو فوق تراب دولة لها تشريع معادل للتشريع الوطني في مجال المعالجة الآلية للمعطيات ذات الطابع الشخصي.

يعتبر مقيما بالجزائر، المسؤول عن المعالجة الذي يمارس نشاطا بالتراب الجزائري في إطار منشأة أيّا كان شكلها القانوني،

2 – عندما يكون المسؤول عنها غير مقيم على التراب الوطني ويلجأ بغرض معالجة معطيات ذات طابع شخصي إلى وسائل آلية أو غير آلية توجد فوق التراب الوطني، باستثناء المعالجات التي تستعمل لأغراض العبور فوق التراب الوطني.

في هذه الحالة، يجب على المسؤول عن المعالجة، دون الإخلال بمسؤوليته الشخصية، أن يبلّغ السلطة الوطنية بهوية ممثله المقيم بالجزائر الذي يحلّ محلّه في جميع حقوقه والتزاماته الناتجة عن أحكام هذا القانون ونصوصه التطبيقية.

المادّة 5 : تخضع لأحكام هذا القانون المعالجات الآلية للمعطيات ذات الطابع الشخصي المتعلقة بالصحة، التي يكون الغرض منها بحث ودراسة وتقييم وتحليل المعطيات المرتبطة بنشاطات العلاج أو الوقاية، باستثناء :

– معالجة المعطيات ذات الطابع الشخصي التي يكون الغرض منها المتابعة العلاجية أو الطبية الفردية للمرضى،

– المعالجة التي تسمح بإجراء دراسات انطلاقا من المعطيات التي تم جمعها طبقا لما هو وارد في البند السابق، عندما تتم من قبل القائمين بهذه المتابعة لاستعمالهم الحصري،

– المعالجات التي يكون الغرض منها التعويض أو الرقابة من قبل الهيئات المكلفة بالتأمين على المرض،

– المعالجات التي تتم داخل مؤسسات الصحة من قبل الأطباء المسؤولين عن المعلومة الطبية.

المادّة 6 : تستثنى من مجال تطبيق هذا القانون المعطيات ذات الطابع الشخصي :

1 – المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، شرط عدم إحالتها للغير أو نشرها،

2 – المحصل عليها والمعالجة لمصلحة الدفاع والأمن الوطنيين،

3 – المحصل عليها والمعالجة لأغراض الوقاية من الجرائم ومتابعة مرتكبيها وقمعها وتلك المحتواة في قواعد البيانات القضائية التي تخضع إلى النص الذي أحدثت بموجبه ولأحكام المادة 10 من هذا القانون.

الباب الثاني

المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي

الفصل الأول

الموافقة المسبقة ونوعية المعطيات

المادّة 7 : لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلاّ بالموافقة الصريحة للشخص المعني.

إذا كان الشخص المعني عديم أو ناقص الأهلية، تخضع الموافقة للقواعد المنصوص عليها في القانون العام.

يمكن الشخص المعني أن يتراجع عن موافقته في أي وقت.

لا يمكن إطلاع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة إلاّ من أجل إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليه وبعد الموافقة المسبقة للشخص المعني.

غير أنّ موافقة الشخص المعني لا تكون واجبة، إذا كانت المعالجة ضرورية :

– لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة،

– لحماية حياة الشخص المعني،

– لتنفيذ عقد يكون الشخص المعني طرفا فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه،

– للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه،

– لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعه على المعطيات،

– لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/أو حقوقه وحرياته الأساسية.

المادّة 8 : لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بطفل إلا بعد الحصول على موافقة ممثله الشرعي أو، عند الاقتضاء، بترخيص من القاضي المختص.

يمكن القاضي الأمر بالمعالجة حتى دون موافقة ممثله الشرعي، إذا استدعت المصلحة الفضلى للطفل ذلك.

يمكن القاضي العدول في أي وقت عن ترخيصه.

المادّة 9 : يجب أن تكون المعطيات الشخصية :

أ – معالجة بطريقة مشروعة ونزيهة،

ب – مجمعة لغايات محددة، وواضحة ومشروعة وألاّ تعالج لاحقا بطريقة تتنافى مع هذه الغايات،

ج – ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها أو معالجتها،

د – صحيحة وكاملة ومحيّنة إذا اقتضى الأمر،

هـ – محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها.

يمكن السلطة الوطنية، في حالة وجود مصلحة مشروعة بناء على طلب من المسؤول عن المعالجة، أن تأذن بحفظ المعطيات ذات الطابع الشخصي لغايات تاريخية أو إحصائية أو علمية بعد المدة المشار إليها في الفقرة (هـ) من هذه المادة.

يكلف المسؤول عن المعالجة، تحت مراقبة السلطة الوطنية، بضمان احترام أحكام هذه المادة.

المادّة 10 : لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن إلاّ من قبل السلطة القضائية والسلطات العمومية والأشخاص المعنويين الذين يسيّرون مصلحة عمومية، ومساعدي العدالة في إطار اختصاصاتهم القانونية.

يجب أن تحدد المعالجة المنصوص عليها في هذه المادة المسؤول عن المعالجة والغاية منها والأشخاص المعنيين بها والغير الذي يحق له الاطلاع على هذه المعلومات ومصدرها والإجراءات الواجب اتخاذها لضمان سلامة المعالجة.

المادّة 11 : لا يمكن أن تؤسس الأحكام القضائية التي تقتضي تقييما لسلوك شخص، على المعالجة الآلية للمعطيات ذات الطابع الشخصي المتضمنة تقييم بعض جوانب شخصيته.

لا يمكن كذلك، لأي قرار آخر ينشئ آثارا قانونية تجاه شخص، أن يتخذ فقط بناء على المعالجة الآلية للمعطيات يكون الغرض منها تحديد صفات الشخص المعني أو تقييم بعض جوانب شخصيته.

لا تعتبر متخذة بناء على معالجة آلية فقط، القرارات التي تتم في إطار إبرام عقد أو تنفيذه والتي يكون الشخص المعني قد أتيحت له فيها إمكانية تقديم ملاحظاته وكذا القرارات التي تستجيب لطلبات الشخص المعني.

الفصل الثاني
الإجراءات المسبقة عن المعالجة

المادّة 12 : ما لم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها طبقا للأحكام المنصوص عليها في هذا القانون.

القسم الأول

التصريح

المادّة 13 : يودع التصريح المسبق الذي يتضمن الالتزام بإجراء المعالجة وفقا لأحكام هذا القانون، لدى السلطة الوطنية ويمكن تقديمه بالطريق الإلكتروني.

يسلم وصل الإيداع أو يرسل بالطريق الإلكتروني، فورا أو في أجل أقصاه 48 ساعة.

يمكن أن تكون المعالجات التابعة لنفس المسؤول عن المعالجة والتي تتم لنفس الغرض أو لأغراض مرتبطة محل تصريح واحد.

يمكن المسؤول عن المعالجة، تحت مسؤوليته، أن يباشر في عملية المعالجة بمجرد استلامه الوصل المنصوص عليه في هذه المادة.

المادّة 14 : يجب أن يتضمن التصريح ما يأتي :

1 – اسم وعنوان المسؤول عن المعالجة وعند الاقتضاء اسم وعنوان ممثله،

2 – طبيعة المعالجة وخصائصها والغرض أو الأغراض المقصودة منها،

3– وصف فئة أو فئات الأشخاص المعنيين والمعطيات أو فئات المعطيات ذات الطابع الشخصي المتعلقة بهم،

4 – المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات،

5– طبيعة المعطيات المعتزم إرسالها إلى دول أجنبية،

6 – مدة حفظ المعطيات،

7– المصلحة التي يمكن الشخص المعني عند الاقتضاء، أن يمارس لديها الحقوق المخولة له بمقتضى أحكام هذا القانون وكذا الإجراءات المتخذة لتسهيل ممارسة هذه الحقوق،

8 – وصف عام يمكّن من تقييم أولي لمدى ملاءمة التدابير المتخذة من أجل ضمان سرّية وأمن المعالجة،

9 – الربط البيني أو جميع أشكال التقريب الأخرى بين المعطيات، وكذا التنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال، سواء مجانا أو بمقابل.

يجب إخطار السلطة الوطنية فورا بأي تغيير للمعلومات المذكورة أعلاه، أو بأي حذف يطال المعالجة.

في حالة التنازل عن ملف معطيات، يلزم المتنازل له بإتمام إجراءات التصريح المنصوص عليها في هذا القانون.

المادّة 15 : تحدد السلطة الوطنية قائمة بأصناف معالجات المعطيات ذات الطابع الشخصي التي ليس من شأنها الإضرار بحقوق وحريات الأشخاص المعنيين وحياتهم الخاصة والتي تكون محل تصريح مبسط يجب أن يشار فيه إلى العناصر المذكورة في البنود 1 و2 و3 و4 و5 و6 من المادة 14 أعلاه.

تحدد السلطة الوطنية قائمة المعالجات غير الآلية للمعطيات ذات الطابع الشخصي التي يمكن أن تكون موضوع التصريح المبسط المنصوص عليه في هذه المادة.

المادّة 16 : لا تطبق إلزامية التصريح على المعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطلع عليه الجمهور أو كل شخص يثبت أن له مصلحة مشروعة في ذلك.

غير أنه في هذه الحالات، يجب تعيين مسؤول عن معالجة المعطيات يكشف عن هويته للعموم وتبلّغ إلى السلطة الوطنية، ويكون مسؤولا عن تطبيق الأحكام المتعلقة بحقوق الأشخاص المعنيين المنصوص عليها في هذا القانون.

يجب على المسؤول عن المعالجة المعفى من التصريح، أن يوصل إلى كل شخص قدم طلبا بذلك المعلومات المتعلقة بالغاية من المعالجة وهوية المسؤول عنها وعنوانه والمعطيات المعالجة والمرسل إليهم .

القسم الثاني

الترخيص

المادّة 17 : تقرر السلطة الوطنية إخضاع المعالجة المعنية لنظام الترخيص المسبق عندما يتبيّن لها، عند دراسة التصريح المقدم لها، أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

يجب أن يكون قرار السلطة الوطنية مسببا وأن يبلّغ إلى المسؤول عن المعالجة في أجل العشرة (10) أيام التي تلي تاريخ إيداع التصريح.

المادّة 18 : تمنع معالجة المعطيات الحساسة.

غير أنه يمكن الترخيص بمعالجة المعطيات الحساسة لأسباب تتعلق بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بناء على الموافقة الصريحة

للشخص المعني، وفي حالة وجود نص قانوني يقضي بذلك أو بترخيص من السلطة الوطنية.

يمنح الترخيص بمعالجة المعطيات الحساسة أيضا، في الحالات الآتية :

أ) إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر وفي حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بموافقته،

ب) تنفيذ المعالجة، بناء على موافقة الشخص المعني، من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي، في إطار نشاطاتها الشرعية، شرط أن تخص المعالجة فقط أعضاء هذه المنظمة أو الأشخاص الذين تربطهم بها اتصالات منتظمة تتعلق بغايتها وألاّ ترسل المعطيات إلى الغير دون موافقة الأشخاص المعنيين.

ج) إذا كانت المعالجة تخص معطيات صرح بها الشخص المعني علنا عندما يمكن استنتاج موافقته على معالجة المعطيات من تصريحاته.

د) أنّ المعالجة ضرورية للاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء وأن تكون قد تمت حصريا لهذه الغاية.

هـ) معالجة المعطيات الجينية، باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي، والقيام بتشخيصات طبية وفحوصات أو علاجات.

وفي كل الأحوال، تبقى التدابير المنصوص عليها في هذا القانون لحماية هذه المعطيات، مضمونة.

المادّة 19 : يتم الربط البيني لملفات تابعة لشخص أو عدة أشخاص معنويين يسيّرون مرفقا عموميا لأغراض مختلفة مرتبطة بالمنفعة العامة، بموجب ترخيص من السلطة الوطنية.

يخضع الربط البيني للملفات التابعة للأشخاص الطبيعية التي يتم لأغراض مختلفة، إلى ترخيص من السلطة الوطنية.

يجب أن يسمح الربط البيني للملفات ببلوغ أهداف مشروعة وشرعية بالنسبة للمسؤولين عن المعالجة ولا يمكن أن يتضمن أي تمييز أو تقليص من الحقوق والحريات والضمانات الممنوحة للأشخاص المعنية.

تحدد كيفيات تطبيق هذه المادة، عند الاقتضاء، عن طريق التنظيم.

المادّة 20 : يجب أن يتضمن طلب الترخيص المعلومات المذكورة في المادة 14 من هذا القانون.

تتخذ السلطة الوطنية قرارها في أجل شهرين (2) من تاريخ إخطارها، ويمكن تمديد هذا الأجل لنفس المدة بقرار مسبب لرئيسها.

يعتبر عدم رد السلطة الوطنية في الأجل المذكور في هذه المادة، رفضا للطلب.

المادّة 21 : ترخص السلطة الوطنية بمعالجة المعطيات ذات الطابع الشخصي التي تهدف إلى تحقيق مصلحة عامة للبحث أو الدراسة أو التقييم في مجال الصحة، في إطار احترام المبادئ المنصوص عليها في هذا القانون، وبالنظر إلى المصلحة العامة التي يهدف إلى تحقيقها البحث أو الدراسة أو التقييم.

يمكن السلطة الوطنية، إذا كانت المعالجة لها نفس الأغراض وتتعلق بمعطيات مماثلة وبنفس فئات المرسل إليهم، تسليم ترخيص واحد لنفس الطالب.

الباب الثالث

السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

المادّة 22 : تنشأ، لدى رئيس الجمهورية، سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي، يشار إليها أدناه "السلطة الوطنية" يحدد مقرها بالجزائر العاصمة.

تتمتع السلطة الوطنية، بالشخصية المعنوية والاستقلال المالي والإداري.

تقيد ميزانية السلطة الوطنية في ميزانية الدولة وتخضع للمراقبة المالية طبقا للتشريع المعمول به.

تعدّ السلطة الوطنية نظامها الداخلي الذي يحدد، لا سيما كيفيات تنظيمها وسيرها، وتصادق عليه.

المادّة 23 : تتشكل السلطة الوطنية من :

– ثلاث (3) شخصيات، من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية،

– ثلاثة (3) قضاة، يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة،

– عضو عن كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية،

– ممثل (1) عن المجلس الوطني لحقوق الإنسان،

– ممثل (1) عن وزير الدفاع الوطني،

– ممثل (1) عن وزير الشؤون الخارجية،

– ممثل (1) عن الوزير المكلف بالداخلية،

– ممثل (1) عن وزير العدل، حافظ الأختام،

– ممثل (1) عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة،

– ممثل (1) عن الوزير المكلف بالصحة،

– ممثل (1) عن وزير العمل والتشغيل والضمان الاجتماعي.

يتم اختيار أعضاء السلطة الوطنية، حسب اختصاصهم القانوني و/أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي.

يمكن السلطة الوطنية أن تستعين بأي شخص مؤهل، من شأنه مساعدتها في أشغالها.

يعين رئيس وأعضاء السلطة الوطنية، بموجب مرسوم رئاسي، لعهدة مدتها خمس (5) سنوات، قابلة للتجديد.

المادّة 24 : يؤدي أعضاء السلطة الوطنية، قبل التنصيب في وظائفهم، اليمين أمام مجلس قضاء الجزائر، في الصيغة الآتية :

"أقسم بالله العظيم أن أؤدي مهمتي كعضو في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بكل استقلالية وحياد وشرف ونزاهة، وأن أحافظ على سرّية المداولات".

المادّة 25 : تكلف السلطة الوطنية بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة.

وتتمثل مهامها، في هذا الصدد، لاسيما في :

1 – منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي،

2 – إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم،

3 – تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة،

4 – تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها،

5 – الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون،

6 – الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة،

7 – الأمر بإغلاق معطيات أو سحبها أو إتلافها،

8 – تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي،

9 – نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون،

10 – تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل،

11 – إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون،

12 – وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي،

13 – وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

في إطار ممارسة مهامها، تعلم السلطة الوطنية النائب العام المختص فورا، في حالة معاينة وقائع تحتمل الوصف الجزائي.

تعدّ السلطة الوطنية تقريرا سنويا حول نشاطها ترفعه إلى رئيس الجمهورية.

المادّة 26 : يجب على رئيس وأعضاء السلطة الوطنية المحافظة على الطابع السرّي للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد انتهاء مهامهم، ما لم يوجد نص قانوني يقضي بخلاف ذلك.

لا يجوز لرئيس السلطة الوطنية وأعضائها أن يمتلكوا، بصفة مباشرة أو غير مباشرة، مصالح في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي.

يستفيد رئيس وأعضاء السلطة الوطنية من حماية الدولة ضد التهديدات أو الإهانات أو الاعتداءات، من أي طبيعة كانت، التي قد يتعرضون لها بسبب أو خلال تأديتهم مهامهم أو بمناسبتها.

يحدد النظام التعويضي لأعضاء السلطة الوطنية وشروط وكيفيات منحه، عن طريق التنظيم.

المادّة 27 : تزود السلطة الوطنية بأمانة تنفيذية، يسيّرها أمين تنفيذي ويساعده في مهامه مستخدمون.

يؤدي الأمين التنفيذي ومستخدمو الأمانة التنفيذية، أمام مجلس قضاء الجزائر، اليمين في الصيغة الآتية :

" أقسم بالله العظيم أن أؤدي وظائفي بكل نزاهة، وأن أحافظ على سرّية المعلومات التي أطّلع عليها ".

يلزم الأمين التنفيذي ومستخدمو الأمانة التنفيذية بالحفاظ على سرّية المعلومات التي يطّلعون عليها أثناء أو بمناسبة ممارسة مهامهم.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 28 : ينشأ سجل وطني لحماية المعطيات ذات الطابع الشخصي، يمسك من طرف السلطة الوطنية، وتقيد فيه :

– الملفات التي تكون السلطات العمومية مسؤولة عن معالجتها،

– الملفات التي يكون الخواص مسؤولين عن معالجتها،

– مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية،

– التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلّمها،

– المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في هذا القانون.

تعفى من التقييد في السجل الوطني الملفات التي يكون الغرض الوحيد من معالجتها مسك سجل موجه بموجب مقتضيات تشريعية أو تنظيمية، لإطلاع العموم غير أنّه تدرج بالسجل الوطني المذكور، وجوبا، هوية الشخص المسؤول عن المعالجة حتى يتمكن الأشخاص المعنيون من ممارسة الحقوق المنصوص عليها في هذا القانون.

تحدد شروط وكيفيات مسك السجل الوطني عن طريق التنظيم.

المادّة 29 : يمكن أن تحدد السلطة الوطنية بموجب أنظمة، الشروط والضمانات المرتبطة بحقوق الشخص المعني في المجالات المتعلقة بحرية التعبير والصحة والشغل والبحث التاريخي والإحصائي والعلمي والمراقبة عن بعد واستعمال تكنولوجيات الإعلام والاتصال، بالتنسيق مع القطاعات المعنية.

المادّة 30 : يمكن السلطة الوطنية أن تقرر تأمين الإرسال، لا سيما عن طريق تشفيره، في حالة ما إذا كان سير المعطيات ذات الطابع الشخصي في الشبكة، ويمكن أن يحتوي على مخاطر على حقوق الأشخاص المعنيين وحرياتهم والضمانات الممنوحة لهم.

المادّة 31 : يحدد القانون الأساسي لمستخدمي السلطة الوطنية بنص خاص.

الباب الرابع
حقوق الشخص المعني

الفصل الأول
الحق في الإعلام

المادّة 32 : ما لم يكن على علم مسبق بها، يجب على المسؤول عن المعالجة أو من يمثله إعلام مسبقا وبصفة صريحة ودون لبس، كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي، بالعناصر الآتية :

– هوية المسؤول عن المعالجة وعند الاقتضاء، هوية ممثله،

– أغراض المعالجة،

– كل معلومة إضافية مفيدة، لاسيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

إذا لم يتم جمع المعطيات ذات الطابع الشخصي لدى الشخص المعني، يجب على المسؤول عن المعالجة أو من يمثله، قبل تسجيل المعطيات أو إرسالها للغير، أن يزوده بالمعلومات المشار إليها أعلاه، ما لم يكن قد علم بها مسبقا.

في حالة جمع المعلومات في شبكات مفتوحة، يجب إعلام الشخص المعني، ما لم يكن على علم مسبق، بأنّ المعطيات ذات الطابع الشخصي المتعلقة به يمكن أن تتداول في الشبكات دون ضمانات السلامة وأنها قد تتعرض للقراءة والاستعمال غير المرخص من طرف الغير.

المادّة 33 : لا تطبق إلزامية الإعلام المنصوص عليها في المادة 32 من هذا القانون :

أ – إذا تعذر إعلام الشخص المعني، ولاسيما في حالة معالجة المعطيات ذات الطابع الشخصي لأغراض إحصائية أو تاريخية أو علمية، يلزم المسؤول عن المعالجة في هذه الحالة بإشعار السلطة الوطنية باستحالة إعلام الشخص المعني وتقديم لها سبب الاستحالة،

ب – إذا تمت المعالجة تطبيقا لنص قانوني،

ج – إذا تمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية.

الفصل الثاني

الحق في الولوج

المادّة 34 : يحق للشخص المعني أن يحصل من المسؤول عن المعالجة، على :

– التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، وأغراض المعالجة وفئات المعطيات التي تنصبّ عليها والمرسل إليهم،

– إفادته، وفق شكل مفهوم، بالمعطيات الخاصة به التي تخضع للمعالجة وكذا بكل معلومة متاحة حول مصدر المعطيات.

يحق للمسؤول عن المعالجة أن يطلب من السلطة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة، ويمكنه الاعتراض على الطلبات التعسفية، لاسيما من حيث عددها وطابعها المتكرر، ويقع على عاتقه إثبات الطابع التعسفي لهذا الطلب.

الفصل الثالث

الحق في التصحيح

المادّة 35 : يحق للشخص المعني أن يحصل مجانا، من المسؤول عن المعالجة على :

أ – تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة لهذا القانون بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات على الخصوص، أو لكون معالجتها ممنوعة قانونا. ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة مجانا، لفائدة الطالب في أجل عشرة (10) أيام من إخطاره.

في حالة الرفض أو عدم الرد على الطلب خلال الأجل المذكور أعلاه، يحق للشخص المعني إيداع طلب التصحيح لدى السلطة الوطنية، التي تكلف أحد أعضائها للقيام بكل التحقيقات الضرورية والعمل على إجراء التصحيحات اللازمة في أقرب الآجال، وإخبار الشخص المعني بمآل طلبه.

ب – تبليغ الغير الذي أوصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي، يتم تطبيقا للنقطة (أ) أعلاه، ما لم يكن ذلك مستحيلا.

يمكن استعمال الحق المنصوص عليه في هذه المادة من قبل ورثة الشخص المعني.

الفصل الرابع

الحق في الاعتراض

المادّة 36 : يحق للشخص المعني أن يعترض، لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي.

وله الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية، ولاسيما التجارية منها، من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة.

لا تطبق أحكام الفقرة الأولى من هذه المادة إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا كان تطبيق هذه الأحكام قد استبعد بموجب إجراء صريح في المحرر الذي يرخص بالمعالجة.

الفصل الخامس

منع الاستكشاف المباشر

المادّة 37 : يمنع الاستكشاف المباشر، بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، باستعمال بيانات شخص طبيعي، في أي شكل من الأشكال، لم يعبر عن موافقته المسبقة على ذلك.

غير أنه يرخص بالاستكشاف المباشر عن طريق البريد الإلكتروني، إذا ما طلبت البيانات مباشرة من المرسل إليه، وفقا لأحكام هذا القانون، بمناسبة بيع أو تقديم خدمات، إذا كان الاستكشاف المباشر يخص منتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي أو

المعنوي، وتبيّن للمرسل إليه، بشكل صريح لا يشوبه لبس إمكانية الاعتراض دون مصاريف، باستثناء التكلفة المرتبطة بإرسال الرفض، على استعمال بياناته وقت جمع هذه الأخيرة وكلما وجّه إليه بريد إلكتروني لأجل الاستكشاف.

وفي جميع الحالات، يمنع إرسال رسائل بواسطة آليات الاتصال الهاتفي وجهاز الاستنساخ البعدي والبريد الإلكتروني لأجل الاستكشاف المباشر دون الإشارة إلى بيانات صحيحة لتمكين المرسل إليه من إرسال طلب توقيف هذه الإيصالات دون مصاريف غير تلك المرتبطة بإرسالها.

كما يمنع إخفاء هوية الشخص الذي أوصلت لفائدته الرسائل وكذا ذكر موضوع لا صلة له بالخدمات المقترحة.

الباب الخامس

التزامات المسؤول عن المعالجة

الفصل الأول

سرّية وسلامة المعالجة

المادّة 38 : يجب على المسؤول عن المعالجة وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، خصوصا عندما تستوجب المعالجة إرسال معطيات عبر شبكة معيّنة وكذا حمايتها من أي شكل من أشكال المعالجة غير المشروعة.

ويجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها.

المادّة 39 : عندما تجرى المعالجة لحساب المسؤول عن المعالجة، يجب على هذا الأخير، اختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها.

تنظم عملية المعالجة من الباطن بموجب عقد أو سند قانوني يربط المعالج من الباطن بالمسؤول عن المعالجة، وينص خصوصا على ألاّ يتصرف المعالج من الباطن إلاّ بناء على تعليمات من المسؤول عن المعالجة وعلى تقيده بالالتزامات المنصوص عليها في المادة 38، أعلاه.

تقيد عناصر العقد أو السند القانوني المتعلق بحماية المعطيات وكذا المتطلبات المتعلقة بالتدابير المنصوص عليها في الفقرة الأولى من المادة 38 أعلاه، كتابة أو في شكل آخر معادل، وذلك لأغراض حفظ الأدلة.

المادّة 40 : يلزم المسؤول عن المعالجة والأشخاص الذين أطلّعوا، أثناء ممارسة مهامهم على معطيات ذات طابع شخصي، بالسر المهني، حتى بعد انتهاء مهامهم، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول.

المادّة 41 : لا يجوز لأي شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن الذي يلج إلى معطيات ذات طابع شخصي، أن يعالج هذه المعطيات دون تعليمات المسؤول عن المعالجة، باستثناء حالة تنفيذ التزام قانوني.

الفصل الثاني

معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين

المادّة 42 : ما عدا في حالة موافقتهم الصريحة، يجب الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها من قبل مؤدي خدمات التصديق الإلكتروني لأغراض تسليم وحفظ الشهادات المرتبطة بالتوقيع الإلكتروني، من الأشخاص المعنيين بها مباشرة، ولا يجوز معالجتها لأغراض غير تلك التي جمعت من أجلها.

الفصل الثالث

معالجة المعطيات ذات الطابع الشخصي في مجال الاتصالات الإلكترونية

المادّة 43 : إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فورا السلطة الوطنية والشخص المعني، إذا أدى ذلك إلى المساس بحياته الخاصة، ما لم تقرر السلطة الوطنية أنّ الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من قبل مقدم الخدمات.

يجب على كل مقدم خدمات أن يمسك جردا محيّنا حول الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي والإجراءات التي اتخذها بشأنها.

الفصل الرابع

نقل المعطيات نحو دولة أجنبية

المادّة 44 : لا يجوز لمسؤول عن معالجة نقل المعطيات ذات طابع شخصي إلى دولة أجنبية إلاّ بترخيص للسلطة الوطنية وفقا لأحكام هذا القانون، وإذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها.

تقدّر السلطة الوطنية المستوى الكافي من الحماية الذي تضمنه دولة معنيّة، لاسيما وفقا للمقتضيات القانونية المعمول بها في هذه الدولة ولإجراءات الأمن المطبقة فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة.

وفي جميع الأحوال، يمنع إرسال وتحويل معطيات ذات الطابع الشخصي إلى دولة أجنبية عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة.

المادّة 45 : استثناء على أحكام المادة 44 من هذا القانون، يمكن المسؤول عن المعالجة نقل معطيات ذات طابع شخصي نحو دولة لا تتوفر فيها الشروط التي تنص عليها المادة المذكورة، في الحالات الآتية :

1 – الموافقة الصريحة للشخص المعني،

2 – إذا كان النقل ضروريا :

أ – للمحافظة على حياة هذا الشخص،

ب – للمحافظة على المصلحة العامة،

ج – احتراما لالتزامات تسمح بضمان إثبات أو ممارسة حق أو الدفاع عنه أمام القضاء،

د – تنفيذا لعقد بين المسؤول عن المعالجة والشخص المعني أو تنفيذا لإجراءات سابقة للعقد والمتخذة بناء على طلب هذا الأخير،

هـ – لإبرام أو تنفيذ عقد مبرم أو سيبرم بين المسؤول عن المعالجة والغير، لمصلحة الشخص المعني،

و – تنفيذا لإجراء يتعلق بتعاون قضائي دولي،

ز – للوقاية من إصابات مرضية أو تشخيصها أو معالجتها.

3 – إذا تم النقل تطبيقا لاتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه،

4 – بناء على ترخيص السلطة الوطنية، إذا كانت المعالجة تتطابق مع أحكام المادة 2 من هذا القانون.

الباب السادس

أحكام إدارية وجزائية

الفصل الأول

الإجراءات الإدارية

المادّة 46 : تتخذ السلطة الوطنية في حق المسؤول عن المعالجة في حال خرقه لأحكام هذا القانون، الإجراءات الإدارية الآتية :

– الإنذار،

– الإعذار،

– السحب المؤقت لمدة لا تتجاوز سنة، أو السحب النهائي لوصل التصريح أو للترخيص،

– الغرامة.

تكون قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة وفقا للتشريع الساري المفعول.

المادّة 47 : تصدر السلطة الوطنية غرامة قدرها 500.000 دج ضد كل مسؤول عن المعالجة :

– يرفض، دون سبب شرعي، حقوق الإعلام والولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32 و34 و35 و36 من هذا القانون،

– لا يقوم بالتبليغ المنصوص عليه في المواد 4 و14 و16 من هذا القانون.

في حالة العود، تطبق العقوبات المنصوص عليها في المادة 64 من هذا القانون.

المادّة 48 : دون الإخلال بالعقوبات الجزائية المنصوص عليها في هذا القانون، يمكن السلطة الوطنية، حسب الحالة ودون أجل، سحب وصل التصريح أو الترخيص إذا تبيّن بعد إجراء المعالجة موضوع التصريح أو الترخيص، أنها تمس بالأمن الوطني أو أنها منافية للأخلاق أو الآداب العامة.

الفصل الثاني

القواعد الإجرائية

المادّة 49 : يمكن السلطة الوطنية القيام بالتحريات المطلوبة ومعاينة المحلات والأماكن التي تتم فيها المعالجة، باستثناء محلات السكن، ويمكنها للقيام بمهامها الولوج إلى المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها.

لا يعتدّ أمام السلطة الوطنية بالسرّ المهني.

المادة 50 : إضافة إلى ضباط وأعوان الشرطة القضائية، يؤهل أعوان الرقابة الآخرون الذين تلجأ إليهم السلطة الوطنية، للقيام ببحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون، تحت إشراف وكيل الجمهورية.

المادة 51 : تعاين الجرائم المنصوص عليها في هذا القانون بواسطة محاضر، يجب أن توجه فورا إلى وكيل الجمهورية المختص إقليميا.

المادة 52 : يمكن لكل شخص يدّعي أنه تم المساس بحق من حقوقه المنصوص عليها في هذا القانون، أن يطلب من الجهة القضائية المختصة اتخاذ أي إجراءات تحفظية لوضع حد لهذا التعدي أو للحصول على تعويض.

المادة 53 : تختص الجهات القضائية الجزائرية بمتابعة الجرائم المنصوص عليها في هذا القانون، التي ترتكب خارج إقليم الجمهورية، من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري.

كما تختص الجهات القضائية الجزائرية بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية.

الفصل الثالث

الأحكام الجزائية

المادة 54 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب على خرق أحكام المادة 2 من هذا القانون، بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج.

المادة 55 : يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة، لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية.

المادة 56 : يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون.

ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له.

المادة 57 : يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، كل من قام، دون الموافقة الصريحة للشخص المعني وفي غير الحالات المنصوص عليها في هذا القانون، بمعالجة المعطيات الحساسة.

المادة 58 : يعاقب بالحبس من ستة (6) أشهر إلى سنة (1) وبغرامة من 60.000 دج إلى 100.000 دج، أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو باستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها.

المادة 59 : يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج، كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة.

المادة 60 : يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي.

المادة 61 : يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل من عرقل عمل السلطة الوطنية :

1 – بالاعتراض على إجراء عملية التحقق في عين المكان،

2 – عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة،

3 – عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح.

المادة 62 : دون الإخلال بالأحكام الجزائية التي يستدعي تطبيقها طبيعة المعلومات المعنية، يعاقب الشخص المشار إليه في المادتين 23 و27 من هذا القانون، لإفشائه معلومات محمية بموجب هذا القانون، بالعقوبات المنصوص عليها في المادة 301 من قانون العقوبات.

المادّة 63 : يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين فقط، كل من يلج، دون أن يكون مؤهلا لذلك إلى السجل الوطني المنصوص عليه في المادة 28 من هذا القانون.

المادّة 64 : يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل مسؤول عن المعالجة يرفض دون سبب مشروع، حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32 و34 و35 و36 من هذا القانون.

المادّة 65 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بغرامة من 200.000 دج إلى 500.000 دج المسؤول عن المعالجة الذي يخرق الالتزامات المنصوص عليها في المادتين 38 و39 من هذا القانون.

يعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص.

المادّة 66 : يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين فقط، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية، خلافا لأحكام المادة 43 من هذا القانون.

المادّة 67 : يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من هذا القانون.

المادّة 68 : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج، كل من قام، في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية، المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن.

المادّة 69 : يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف، بالنظر إلى مهامه، بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل، ولو عن إهمال، الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك.

المادّة 70 : يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون، وفقا للقواعد المنصوص عليها في قانون العقوبات.

المادّة 71 : يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب الجريمة.

يؤهل أعضاء ومستخدمو السلطة الوطنية لمعاينة مسح هذه المعطيات.

المادّة 72 : يصادر محل الجريمة بغرض إعادة تخصيصه أو تدميره في إطار احترام التشريع الساري المفعول.

يتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير.

المادّة 73 : يعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون، بنفس العقوبات المقررة للجريمة التامة.

المادّة 74 : في حالة العود، تضاعف العقوبات المنصوص عليها في هذا الفصل.

الباب السابع

أحكام انتقالية ونهائية

المادّة 75 : تحت طائلة العقوبات المنصوص عليها في المادة 56 من هذا القانون، يجب على الأشخاص الذين يمارسون نشاط معالجة المعطيات ذات الطابع الشخصي عند تاريخ صدور هذا القانون، الامتثال لأحكامه في أجل أقصاه سنة (1) من تاريخ تنصيب السلطة الوطنية.

المادة 76 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرر بالجزائر في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018.

عبد العزيز بوتفليقة

الملحق رقم (10)

★

قرار المجلس الدستوري رقم 24/ ق.م د /21 مؤرخ في 26 شوال عام 1442 الموافق 7 يونيو سنة 2021، يتعلق بمراقبة دستورية الأمر المتعلق بحماية المعلومات والوثائق الإدارية.

إن المجلس الدستوري،

بناء على إخطار رئيس الجمهورية المجلس الدستوري، بالرسالة المؤرخة في 2 يونيو سنة 2021، والمسجلة بالأمانة العامة للمجلس الدستوري بتاريخ 2 يونيو سنة 2021 تحت رقم 65، قصد مراقبة دستورية الأمر المتعلق بحماية المعلومات والوثائق الإدارية،

– وبناء على الدستور لاسيما المواد 139 و142 و197 (الفقرة الأولى) 198 و224 منه،

– وبمقتضى النظام المؤرخ في 7 رمضان عام 1440 الموافق 12 مايو سنة 2019 المحدد لقواعد عمل المجلس الدستوري، المعدل والمتمم،

– وبعد الاستماع إلى العضو المقرر،

في الشكل :

– اعتبارا لشغور المجلس الشعبي الوطني الذي تم حله في أول مارس 2021، بموجب المرسوم الرئاسي رقم 21-77 المؤرخ في 9 رجب عام 1442 الموافق 21 فبراير سنة 2021،

– واعتبارا أن الأمر موضوع الإخطار تم عرضه على مجلس الوزراء في جلسته المنعقدة بتاريخ 30 مايو سنة 2021، بعد أخذ رأي مجلس الدولة،

– واعتبارا أن الأمر، موضوع الإخطار، جاء وفقا للمادتين 139 و142 من الدستور،

– واعتبارا أن إخطار رئيس الجمهورية المجلس الدستوري لمراقبة دستورية الأمر المتعلق بحماية المعلومات والوثائق الإدارية، جاء وفقا لأحكام المادة 142 (الفقرة 2) من الدستور،

في الموضوع :

– فيما يخص تأشيرات الأمر موضوع الإخطار :

– فيما يخص عدم الإستناد إلى المادة 34 من الدستور ضمن تأشيرات الأمر موضوع الإخطار :

– اعتبارا أن المادة 34 من الدستور مفادها أنه لا يمكن تقييد الحقوق والحريات والضمانات إلا بموجب قانون، ولأسباب مرتبطة بحفظ النظام العام والأمن، وحماية الثوابت الوطنية وكذا تلك الضرورية لحماية حقوق وحريات أخرى يكرّسها الدستور،

– واعتبارا أن الأمر المتعلق بحماية المعلومات والوثائق الإدارية يجرم العديد من الأفعال ويعاقب عليها بعقوبات جزائية الأمر الذي قد يقيّد من ممارسة بعض الحقوق والحريات المكفولة دستوريا مما يلزم المشرّع مراعاة احترام أحكام المادة 34 من الدستور، ومن ثم فإن هذه المادة تُعدّ سندا دستوريا أساسيا للأمر موضوع الإخطار،

– واعتبارا بالنتيجة، فإن عدم الاستناد إلى المادة 34 من الدستور ضمن تأشيرات الامر موضوع الإخطار، يعد سهوا يتعيّن تداركه،

– فيما يخص عدم الاستناد إلى المادة 47 من الدستور ضمن تأشيرات الأمر موضوع الإخطار :

– اعتبارا أن المادة 47 من الدستور في فقرتيها 2 و3، تنص على أنه لكل شخص الحق في سرّية مراسلاته واتصالاته الخاصة في أي شكل كانت، وأن حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي،

– واعتبارا أن الأمر موضوع الإخطار، يضع قواعد لحماية المعلومات والوثائق الإدارية سواء كانت شخصية أو عمومية تملكها السلطات العمومية، ومن ثم فإن المادة 47 من الدستور تعد سندا دستوريا للأمر موضوع الإخطار،

– واعتبارا بالنتيجة، فإن عدم الاستناد إلى المادة 47 من الدستور ضمن تأشيرات الأمر، موضوع الإخطار، يعد سهوا يتعيّن تداركه،

– فيما يخص عدم الإستناد إلى الأمر رقم 75–58 المتضمن القانون المدني، المعدل والمتمم، ضمن تأشيرات الأمر موضوع الإخطار :

– اعتبارا أن الفصل الرابع من الأمر موضوع الإخطار الذي جاء تحت عنوان المسؤولية المدنية والتأديبية، يستند في تأسيسه للمسؤولية المدنية والتأديبية عما يصيب السلطات العمومية من ضرر نتيجة نشر وثيقة مصنّفة أو إفشاء معلومات تخصها، وما ترتبه من حق في التعويض نتيجة ذلك، إلى قواعد القانون المدني، مما يجعل من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم، سندا للأمر موضوع الإخطار،

– واعتبارا بالنتيجة، فإن عدم الاستناد إلى الأمر رقم 75-58 المتضمن القانون المدني، المعدل والمتمم، ضمن تأشيرات الامر، موضوع الإخطار، يعد سهوا يتعيّن تداركه،

– فيما يخص عدم الاستناد إلى القانون رقم 18-07 ضمن تأشيرات الأمر موضوع الإخطار :

– اعتبارا أن القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، يهدف إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها، ومن ثمة فهو يُعدّ سندا أساسيًا للأمر موضوع الإخطار،

– واعتبارا بالنتيجة، فإن عدم الاستناد إلى القانون رقم 18-07، ضمن تأشيرات الأمر، موضوع الإخطار، يعد سهوا يتعيّن تداركه.

لهذه الأسباب

يقرّر ما يأتي :

في الشكل :

أولا : أن إجراءات الإعداد والمصادقة على الأمر المتعلق بحماية المعلومات والوثائق الإدارية، جاءت تطبيقا للمادة 142 من الدستور، فهي دستورية.

ثانيا : أن إخطار رئيس الجمهورية المجلس الدستوري بخصوص مراقبة دستورية الأمر المتعلق بحماية المعلومات والوثائق الإدارية، تم تطبيقا لأحكام المادة 142 (الفقرة 2) والمادة 224 من الدستور، فهو دستوري.

في الموضوع :

أولاً : فيما يخص تأشيرات الأمر موضوع الإخطار:

– تضاف الإشارة إلى المادتين 34 و47 من الدستور ضمن تأشيرات الأمر موضوع الإخطار.

– إدراج الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم، ضمن تأشيرات الأمر موضوع الإخطار.

– إدراج القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ضمن تأشيرات الأمر موضوع الإخطار.

ثانيًا : تعد أحكام الأمر المتعلق بحماية المعلومات والوثائق الإدارية، دستورية.

ثالثًا : يبلّغ هذا القرار إلى رئيس الجمهورية.

رابعًا : ينشر هذا القرار في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

بهذا تداول المجلس الدستوري في جلساته المنعقدة بتاريخ 24 و25 و26 شوال عام 1442 الموافق 5 و6 و7 يونيو سنة 2021.

رئيس المجلس الدستوري

كمال فنيش

محمد حبشي، نائبا للرئيس،

سليمة مسراتي، عضوة،

شادية رحاب، عضوة،

إبراهيم بوتخيل، عضوا،

محمد رضا أوسهلة، عضوا،

عبد النور قراوي، عضوا،

خديجة عباد، عضوة،

سماعيل بليط، عضوا،

الهاشمي براهمي، عضوا،

أمحمد عدة جلول، عضوا،

عمر بوراوي، عضوا.

أمر رقم 21-09 مؤرّخ في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021، يتعلق بحماية المعلومات والوثائق الإدارية.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 34 و47 و54 و55 و139 و141 (الفقرة 2) و142 و198 و224 منه،

– وبمقتضى القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 والمتعلق بالإعلام،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم،

– وبمقتضى القانون رقم 88-09 المؤرخ في 7 جمادى الثانية عام 1408 الموافق 26 يناير سنة 1988 والمتعلق بالأرشيف الوطني،

– وبمقتضى القانون رقم 90-11 المؤرخ في 26 رمضان عام 1410 الموافق 21 أبريل سنة 1990 والمتعلق بعلاقات العمل، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-03 المؤرّخ في 19 جمادى الثانية عام 1427 الموافق 15 يوليو سنة 2006 والمتضمن القانون الأساسي العام للوظيفة العمومية،

– وبمقتضى القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

– بعد رأي مجلس الدولة،

– وبعد الاستماع إلى مجلس الوزراء،

– وبعد الأخذ بقرار المجلس الدستوري،

يصدر الأمر الآتي نصه :

الفصل الأول
أحكام عامة

المادّة الأولى : يهدف هذا الأمر إلى حماية المعلومات والوثائق الإدارية للسلطات العمومية.

المادّة 2 : تخضع لأحكام هذا الأمر المعلومات والوثائق المصنفة المتعلقة بالدولة ومؤسساتها و هيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية وكل مؤسسة تملك الدولة كل أو بعض رأسمالها وكل مؤسسة تقدم خدمة عمومية والتي تدعى في النص "السلطات المعنية".

المادّة 3 : يقصد، في مفهوم هذا الأمر، بما يأتي :

1- الموظف العمومي :

- كل شخص يشغل منصبا تشريعيا أو تنفيذيا أو إداريا أو قضائيا أو في أحد المجالس الشعبية المحلية المنتخبة، سواء أكان معيّنا أو منتخبا، دائما أو مؤقتا، مدفوع الأجر أو غير مدفوع الأجر، بصرف النظر عن رتبته أو أقدميته،

- كل شخص آخر يتولى، ولو مؤقتا، وظيفة أو وكالة بأجر أو بدون أجر، ويساهم بهذه الصفة في خدمة هيئة عمومية أو مؤسسة عمومية أو أي مؤسسة أخرى تملك الدولة كل أو بعض رأسمالها، أو أي مؤسسة أخرى تقدم خدمة عمومية،

- كل شخص آخر معرّف بأنه موظف عمومي أو من في حكمه طبقا للتشريع والتنظيم المعمول بهما.

2- الوثيقة : المراسلات والمحررات والمستندات التي أنشأتها أو حصلت عليها أي من السلطات المعنية أثناء ممارسة نشاطها.

3- الوثائق المصنفة : أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها.

4- المعلومات : أي حدث أو خبر مهما كان مصدره، وثيقة أو صورة أو شريط صوتي أو مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية، يؤدي الكشف عنها إلى المساس بالسلطات المعنية.

المادّة 4 : تعد الوثائق المنصوص عليها في هذا الأمر ملكية عمومية، وهي غير قابلة للتصرف فيها أو لاكتسابها بأي طريقة كانت.

المادّة 5 : لا تمس الأحكام الواردة في هذا الأمر بحق المواطن في الوصول إلى المعلومة.

الفصل الثاني
قواعد حماية المعلومات والوثائق المصنفة

المادّة 6 : تصنف الوثائق، حسب درجة حساسيتها، إلى الأصناف الآتية :

- **"سرّي جدا"**، ويتضمن الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي،

- **"سرّي"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة،

- **"واجب الكتمان"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية،

- **"توزيع محدود"**، ويتضمن الوثائق التي يؤدي إفشاؤها إلى المساس بمصالح الدولة و لا يجوز الاطلاع عليها إلاّ من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهمة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 7 : تلزم السلطات المعنية بتأمين وثائقها ومعلوماتها وحمايتها، وتتخذ التدابير اللازمة لتصنيفها وتنظيم تداولها وحفظها وفقا للأحكام المنصوص عليها في التشريع والتنظيم المعمول بهما، ولا سيما ما يتعلق منها بالأرشيف الوطني.

يجب أن يخضع موظفو السلطات المعنية إلى تكوين خاص في استعمال المعلومات والوثائق المصنفة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 8 : لا يمكن أن تكون مراسلات السلطات المعنية مع وإلى الغير، محل نشر أو تداول أو توزيع إلاّ بموافقتها، ما لم ينص القانون على خلاف ذلك.

المادّة 9 : يجب على السلطات المعنية، في حال تسريب معلومات أو وثائق مصنفة، إخطار الجهات المختصة فورا قصد فتح تحقيق.

المادّة 10 : يحظر على أيّ كان نشر أو إفشاء محاضر وأوراق التحريات والتحقيق القضائي أو تمكين من لا صفة له من حيازتها، مع مراعاة الاستثناءات المنصوص عليها في قانون الإجراءات الجزائية.

المادّة 11 : يمنع على أيّ كان اطلع، بحكم عمله أو مسؤوليته، على وثيقة مصنفة أو حصل عليها بأي صورة كانت، أخذ نسخ أو صور منها أو نشر محتواها كله أو بعضه، أو إعلام الغير بوجودها، إلاّ بموافقة السلطة المعنية.

المادّة 12 : يجب على كل شخص يحوز وثيقة مصنفة دون أن يكون مؤهلا لذلك، تسليمها إلى السلطات المعنية ويمنع عليه إفشاء مضمونها، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 13 : يجب على السلطات المعنية، في إطار محاربة المعلومات الكاذبة والمحرّفة، تفعيل الاتصال المؤسساتي والإعلام الفوري للرأي العام.

الفصل الثالث

التزامات الموظف العمومي

المادّة 14 : يلتزم الموظف العمومي، تحت طائلة العقوبات المنصوص عليها في هذا الأمر، بالسرّ المهني وعدم إفشاء محتوى أي وثيقة أو أي معلومة اطلع عليها أثناء أو بمناسبة ممارسة مهامه، ما لم ينص القانون على خلاف ذلك.

ويبقى هذا المنع ساريا لمدة عشر (10) سنوات من توقف أو انتهاء العلاقة المهنية للموظف العمومي بالاستقالة أو التسريح أو العزل أو الإحالة على التقاعد أو لأي سبب آخر، مع مراعاة أحكام المادة 50 من هذا الأمر.

المادّة 15 : يمنع على الموظف العمومي إخراج الوثائق المصنفة أو نسخ منها أو صور عنها من مكان العمل، أو طبعها أو نسخها خارج المؤسسات الرسمية، ما لم تقتض ضرورة المصلحة أو طبيعة العمل ذلك.

المادّة 16 : يمنع الموظف العمومي من الإدلاء لوسائل الإعلام أو في وسائل التواصل الاجتماعي بأي معلومة أو تعليق أو تصريح أو مداخلة حول المعلومات و/أو الوثائق التي اطلع عليها، بحكم مهامه، أو حول مسائل ما زالت قيد الدراسة لدى الجهة التي يعمل فيها، ما لم يكن مرخصا له بذلك.

الفصل الرابع

المسؤولية المدنية والتأديبية

المادّة 17 : يجوز للسلطات المعنية طلب تعويض عما أصابها من ضرر نتيجة نشر وثيقة مصنفة أو إفشاء معلومات تخصها، طبقا للقواعد المنصوص عليها في التشريع المعمول به، دون الإخلال بالمتابعات الجزائية المحتملة.

المادّة 18 : يمكن الجهة القضائية المختصة، بناء على طلب إحدى السلطات المعنية، أن توقف، تحت طائلة غرامة تهديدية يومية، نشر أي وثيقة مصنفة.

المادّة 19 : بغضّ النظر عن الأحكام المخالفة المنصوص عليها في التشريع الساري المفعول، يتعرض الموظف العمومي الذي يفشي عمدا وثائق مصنفة إلى التسريح من العمل.

المادّة 20 : يتعرض الموظف العمومي الذي يتسبب، بإهماله، في إفشاء وثائق مصنفة أو يقوم بإخراجها أو بإخراج نسخ منها أو صور عنها خارج مكان العمل أو يقوم بطبعها خارج المصلحة في غير الحالات التي تقتضيها المصلحة، إلى المساءلة التأديبية طبقا للتشريع الساري المفعول.

الفصل الخامس

قواعد إجرائية

المادّة 21 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا الأمر التي ترتكب خارج التراب الوطني إضرارا بالدولة الجزائرية أو بمؤسساتها.

المادّة 22 : في إطار تطبيق أحكام هذا الأمر، يتعيّن على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ووضع تحت تصرفها المعطيات التي يتعيّن عليهم حفظها تطبيقا لأحكام هذا الأمر.

ويتعيّن على مقدمي الخدمات كتمان سرّية العمليات التي ينجزونها وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء سرّ التحقيق.

المادّة 23 : يمكن الجهة القضائية المختصة إصدار أمر إلى مقدمي الخدمات، من أجل :

– التحفظ الفوري على المعطيات المتعلقة بالمحتوى و/أو بحركة السير المرتبطة بالجرائم المنصوص عليها في هذا الأمر، وفقا للكيفيات المحددة في التشريع الساري المفعول،

– التدخل الفوري، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول، لسحب أو تخزين المحتويات التي يتيحون الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تشكل جريمة من الجرائم المنصوص عليها في هذا الأمر، أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين هذه المحتويات أو لجعل الدخول إليها غير ممكن.

المادّة 24 : يجوز للجهة القضائية المختصة، بمناسبة التحقيق في إحدى الجرائم المنصوص عليها في هذا الأمر، أن تأمر أي شخص بتسليمها أي معلومات أو معطيات تكون مخزنة بواسطة استعمال وسائل تكنولوجيات الإعلام والاتصال، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 25 : يمكن لضابط الشرطة القضائية المختص أن يضع، عبر الشبكات الإلكترونية، آليات تقنية للتبليغ عن الجرائم المنصوص عليها في هذا الأمر، ويعلم بذلك فورا وكيل الجمهورية، المختص الذي يأمر بالاستمرار في العملية أو بإيقافها.

المادّة 26 : تباشر النيابة العامة تحريك الدعوى العمومية تلقائيا في الجرائم المنصوص عليها في هذا الأمر.

المادّة 27 : يمكن اللجوء إلى أساليب التحري الخاصة المنصوص عليها في التشريع الساري المفعول، من أجل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا الأمر.

الفصل السادس

الأحكام الجزائية

المادّة 28 : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين، الموظف العمومي الذي ينشر أو يفشي أو يطلع الغير أو يسمح له بأخذ صور من المعلومات أو الوثائق المصنفة "توزيع محدود".

وتكون العقوبة بالحبس من سنة (1) إلى خمس(5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج إذا أدى ذلك إلى المساس بالاعتبار الواجب للسلطات المعنية.

المادّة 29 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، الموظف العمومي الذي يفشي أو ينشر معلومة أو وثيقة مصنفة " واجب الكتمان" إلى علم الجمهور أو إلى علم شخص لا صفة له في الاطلاع عليها أو يسمح له بأخذ صور منها أو يترك الغير يقوم بذلك.

وتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 500.000 دج إلى 1.000.000 دج، إذا كانت الوثائق مصنفة "سرّي جدا" أو "سرّي ".

المادّة 30 : تكون العقوبة الحبس من ثلاثة (3) أشهر إلى سنة (1) والغرامة من 30.000 دج إلى 100.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 28 أعلاه، نتيجة عدم مراعاة الموظف العمومي الأحكام التشريعية و/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 29 أعلاه، نتيجة عدم مراعاة الموظف العمومي للأحكام التشريعية و/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

المادّة 31 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج كل شخص مؤتمن بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليه وأفشاها في غير الحالات التي يوجب أو يرخص القانون بالتبليغ عنها.

المادّة 32 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من ينشر محاضر و/ أو أوراق التحريات والتحقيق القضائي أو يفشي محتواها أو يمكّن من لا صفة له من حيازتها.

المادّة 33 : يعاقب بالحبس من خمس (5) سنوات إلى خمس عشرة (15) سنة وبغرامة من 500.000 دج إلى 1.500.000 دج، كل من أطلع الغير بمقابل، أيّا كانت طبيعته، على معلومة أو وثيقة مصنفة أو يسّر لغيره ذلك.

المادّة 34 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سبع (7) سنوات إلى خمس عشرة (15) سنة وبغرامة من 700.000 دج إلى 1.500.000 دج، كل من يقوم بالأفعال المذكورة في المادّة 33 أعلاه، تنفيذا لخطة مدبرة داخل الوطن أو خارجه.

المادّة 35 : يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين، كل من يحوز وثيقة مصنفة، دون أن يكون مؤهلا لذلك، ولم يقم بتسليمها إلى السلطات المعنية.

وتطبق العقوبات المنصوص عليها في المادتين 28 و29 من هذا الأمر، حسب الحالة، إذا قام بإفشاء مضمونها.

المادّة 36 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يرتكب من غير الفاعلين أو الشركاء، الأفعال الآتية :

1 – إخفاء الوثيقة المصنفة أو الأشياء أو الأدوات التي استعملت أو كانت ستستعمل في ارتكاب الجرائم المنصوص عليها في هذا الأمر والأشياء أو المواد أو الأموال المتحصلة منها مع علمه بذلك.

2 – إتلاف أو اختلاس أو إخفاء أو تزييف عمدا وثيقة عمومية أو خاصة من شأنها تسهيل البحث عن الجرائم المنصوص عليها في هذا الأمر ومعاقبة مرتكبيها.

المادّة 37 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل من يدخل دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو

أي وسيلة أخرى من وسائل تكنولوجيات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير وجه حق على معلومات أو وثائق مصنفة.

وتضاعف العقوبة في حال نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة.

المادّة 38 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها كليا أو جزئيا.

ويعاقب بنفس العقوبة كل من ينشر المعلومات والوثائق المصنفة أو محتواها كليا أو جزئيا على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام.

المادّة 39 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من عشر (10) سنوات إلى خمس عشرة (15) سنة وبغرامة من 1.000.000 دج إلى 1.500.000 دج، كل من يقوم عمدا بنشر أو بث، عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، معلومة أو وثيقة مصنفة، بغرض المساس بالنظام العام والسكينة العمومية.

المادّة 40 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من يمتنع عن تقديم الوثائق المنصوص عليها في المادة 24 من هذا الأمر.

المادّة 41 : يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 30.000 دج إلى 100.000 دج، أو بإحدى هاتين العقوبتين، كل من يقوم بنشر أو تداول أو توزيع المراسلات الإدارية التي لا تندرج ضمن الوثائق المصنفة الصادرة من أو إلى السلطات المعنية دون موافقتها أو في غير الحالات التي يسمح فيها القانون بذلك.

وتكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج في حالة العود.

المادّة 42 : يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا الأمر، بالعقوبات المنصوص عليها في قانون العقوبات.

المادّة 43 : كل من أنشأ أو شارك في جمعية أو اتفاق تشكل أو تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، يعاقب بالعقوبات المقررة للجريمة التامة، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل.

المادّة 44 : دون المساس بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، وكذا الأموال المتحصلة منها، وإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

المادّة 45 : يمكن الجهة القضائية المختصة الحكم على مرتكبي الجرائم المنصوص عليها في هذا الأمر، بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكنها الحكم على الموظف العمومي بالمنع من ممارسة وظيفة عليا نهائيا أو لمدة لا تقل عن خمس (5) سنوات ولا تزيد عن عشر (10) سنوات.

المادّة 46 : يعاقب بالعقوبات المقررة للفاعل، كل من يحرّض بأي وسيلة كانت، على ارتكاب الجرائم المنصوص عليها في هذا الأمر.

المادّة 47 : يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا الأمر، بالعقوبات المقررة للجريمة التامة.

المادّة 48 : مع مراعاة أحكام المادة 41 من هذا الأمر، تضاعف العقوبات المنصوص عليها في هذا الأمر في حالة العود.

الفصل السابع

أحكام ختامية

المادّة 49 : تطبق على إفشاء سرّ الدفاع الوطني وإفشاء السرّ الطبي العقوبات المنصوص عليها في قانون العقوبات.

المادّة 50 : تبقى المعلومات والوثائق المصنفة خاضعة لأحكام هذا الأمر إلى حين رفع السرّية عنها من قبل السلطات العمومية.

المادّة 51 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021.

عبد المجيد تبون

الملحق رقم (11)

أمر رقم 21-09 مؤرّخ في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021، يتعلق بحماية المعلومات والوثائق الإدارية.

إنّ رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 34 و47 و 54 و55 و139 و141 (الفقرة 2) و142 و198 و224 منه،

– وبمقتضى القانون العضوي رقم 12-05 المؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 والمتعلق بالإعلام،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدل والمتمم،

– وبمقتضى القانون رقم 88-09 المؤرخ في 7 جمادى الثانية عام 1408 الموافق 26 يناير سنة 1988 والمتعلق بالأرشيف الوطني،

– وبمقتضى القانون رقم 90-11 المؤرخ في 26 رمضان عام 1410 الموافق 21 أبريل سنة 1990 والمتعلق بعلاقات العمل، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-03 المؤرّخ في 19 جمادى الثانية عام 1427 الموافق 15 يوليو سنة 2006 والمتضمن القانون الأساسي العام للوظيفة العمومية،

– وبمقتضى القانون رقم 08-09 المؤرخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،

– بعد رأي مجلس الدولة،

– وبعد الاستماع إلى مجلس الوزراء،

– وبعد الأخذ بقرار المجلس الدستوري،

يصدر الأمر الآتي نصه :

الفصل الأول
أحكام عامة

المادّة الأولى : يهدف هذا الأمر إلى حماية المعلومات والوثائق الإدارية للسلطات العمومية.

المادّة 2 : تخضع لأحكام هذا الأمر المعلومات والوثائق المصنفة المتعلقة بالدولة ومؤسساتها وهيئاتها التشريعية والقضائية والتنفيذية والإدارات العمومية والجماعات المحلية وكل مؤسسة تملك الدولة كل أو بعض رأسمالها وكل مؤسسة تقدم خدمة عمومية والتي تدعى في النص "السلطات المعنية".

المادّة 3 : يقصد، في مفهوم هذا الأمر، بما يأتي :

1- الموظف العمومي :

- كل شخص يشغل منصبا تشريعيا أو تنفيذيا أو إداريا أو قضائيا أو في أحد المجالس الشعبية المحلية المنتخبة، سواء أكان معيّنا أو منتخبا، دائما أو مؤقتا، مدفوع الأجر أو غير مدفوع الأجر، بصرف النظر عن رتبته أو أقدميته،

- كل شخص آخر يتولى، ولو مؤقتا، وظيفة أو وكالة بأجر أو بدون أجر، ويساهم بهذه الصفة في خدمة هيئة عمومية أو مؤسسة عمومية أو أي مؤسسة أخرى تملك الدولة كل أو بعض رأسمالها، أو أي مؤسسة أخرى تقدم خدمة عمومية،

- كل شخص آخر معرّف بأنه موظف عمومي أو من في حكمه طبقا للتشريع والتنظيم المعمول بهما،

2- الوثيقة : المراسلات والمحررات والمستندات التي أنشأتها أو حصلت عليها أي من السلطات المعنية أثناء ممارسة نشاطها،

3- الوثائق المصنفة : أي مكتوب ورقي أو إلكتروني أو رسم أو مخطط أو خريطة أو صورة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو إلكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها،

4- المعلومات : أي حدث أو خبر مهما كان مصدره، وثيقة أو صورة أو شريط صوتي أو مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية، يؤدي الكشف عنها إلى المساس بالسلطات المعنية.

المادّة 4 : تعد الوثائق المنصوص عليها في هذا الأمر ملكية عمومية، وهي غير قابلة للتصرف فيها أو لاكتسابها بأي طريقة كانت.

المادّة 5 : لا تمس الأحكام الواردة في هذا الأمر بحق المواطن في الوصول إلى المعلومة.

الفصل الثاني
قواعد حماية المعلومات والوثائق المصنفة

المادّة 6 : تصنف الوثائق، حسب درجة حساسيتها، إلى الأصناف الآتية :

- **"سرّي جدا"**، ويتضمن الوثائق التي يلحق إفشاؤها خطرا بالأمن الوطني الداخلي والخارجي،

- **"سرّي"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا خطيرا بمصالح الدولة،

- **"واجب الكتمان"**، ويتضمن الوثائق التي يلحق إفشاؤها ضررا أكيدا بمصالح الحكومة أو الوزارات أو الإدارات أو إحدى الهيئات العمومية،

- **"توزيع محدود"**، ويتضمن الوثائق التي يؤدي إفشاؤها إلى المساس بمصالح الدولة ولا يجوز الاطلاع عليها إلاّ من قبل الأشخاص المؤهلين بحكم الوظيفة أو المهمة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 7 : تلزم السلطات المعنية بتأمين وثائقها ومعلوماتها وحمايتها، وتتخذ التدابير اللازمة لتصنيفها وتنظيم تداولها وحفظها وفقا للأحكام المنصوص عليها في التشريع والتنظيم المعمول بهما، ولا سيما ما يتعلق منها بالأرشيف الوطني.

يجب أن يخضع موظفو السلطات المعنية إلى تكوين خاص في استعمال المعلومات والوثائق المصنفة.

تحدد شروط وكيفيات تطبيق هذه المادة عن طريق التنظيم.

المادّة 8 : لا يمكن أن تكون مراسلات السلطات المعنية مع وإلى الغير، محل نشر أو تداول أو توزيع إلاّ بموافقتها، ما لم ينص القانون على خلاف ذلك.

المادّة 9 : يجب على السلطات المعنية، في حال تسريب معلومات أو وثائق مصنفة، إخطار الجهات المختصة فورا قصد فتح تحقيق.

المادّة 10 : يحظر على أيّ كان نشر أو إفشاء محاضر وأوراق التحريات والتحقيق القضائي أو تمكين من لا صفة له من حيازتها، مع مراعاة الاستثناءات المنصوص عليها في قانون الإجراءات الجزائية.

المادّة 11 : يمنع على أيّ كان اطلع، بحكم عمله أو مسؤوليته، على وثيقة مصنفة أو حصل عليها بأي صورة كانت، أخذ نسخ أو صور منها أو نشر محتواها كله أو بعضه، أو إعلام الغير بوجودها، إلاّ بموافقة السلطة المعنية.

المادّة 12 : يجب على كل شخص يحوز وثيقة مصنفة دون أن يكون مؤهلا لذلك، تسليمها إلى السلطات المعنية ويمنع عليه إفشاء مضمونها، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 13 : يجب على السلطات المعنية، في إطار محاربة المعلومات الكاذبة والمحرّفة، تفعيل الاتصال المؤسساتي والإعلام الفوري للرأي العام.

الفصل الثالث

التزامات الموظف العمومي

المادّة 14 : يلزم الموظف العمومي، تحت طائلة العقوبات المنصوص عليها في هذا الأمر، بالسرّ المهني وعدم إفشاء محتوى أي وثيقة أو أي معلومة اطلع عليها أثناء أو بمناسبة ممارسة مهامه، ما لم ينص القانون على خلاف ذلك.

ويبقى هذا المنع ساريا لمدة عشر (10) سنوات من توقف أو انتهاء العلاقة المهنية للموظف العمومي بالاستقالة أو التسريح أو العزل أو الإحالة على التقاعد أو لأي سبب أخر، مع مراعاة أحكام المادة 50 من هذا الأمر.

المادّة 15 : يمنع على الموظف العمومي إخراج الوثائق المصنفة أو نسخ منها أو صور عنها من مكان العمل، أو طبعها أو نسخها خارج المؤسسات الرسمية، ما لم تقتض ضرورة المصلحة أو طبيعة العمل ذلك.

المادّة 16 : يمنع الموظف العمومي من الإدلاء لوسائل الإعلام أو في وسائل التواصل الاجتماعي بأي معلومة أو تعليق أو تصريح أو مداخلة حول المعلومات و/أو الوثائق التي اطلع عليها، بحكم مهامه، أو حول مسائل ما زالت قيد الدراسة لدى الجهة التي يعمل فيها، ما لم يكن مرخصا له بذلك.

الفصل الرابع

المسؤولية المدنية والتأديبية

المادّة 17 : يجوز للسلطات المعنية طلب تعويض عما أصابها من ضرر نتيجة نشر وثيقة مصنفة أو إفشاء معلومات تخصها، طبقا للقواعد المنصوص عليها في التشريع المعمول به، دون الإخلال بالمتابعات الجزائية المحتملة.

المادّة 18 : يمكن الجهة القضائية المختصة، بناء على طلب إحدى السلطات المعنية، أن توقف، تحت طائلة غرامة تهديدية يومية، نشر أي وثيقة مصنفة.

المادّة 19 : بغضّ النظر عن الأحكام المخالفة المنصوص عليها في التشريع الساري المفعول، يتعرض الموظف العمومي الذي يفشي عمدا وثائق مصنفة إلى التسريح من العمل.

المادّة 20 : يتعرض الموظف العمومي الذي يتسبب، بإهماله، في إفشاء وثائق مصنفة أو يقوم بإخراجها أو بإخراج نسخ منها أو صور عنها خارج مكان العمل أو يقوم بطبعها خارج المصلحة في غير الحالات التي تقتضيها المصلحة، إلى المساءلة التأديبية طبقا للتشريع الساري المفعول.

الفصل الخامس

قواعد إجرائية

المادّة 21 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا الأمر التي ترتكب خارج التراب الوطني إضرارا بالدولة الجزائرية أو بمؤسساتها.

المادّة 22 : في إطار تطبيق أحكام هذا الأمر، يتعيّن على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ووضع تحت تصرفها المعطيات التي يتعيّن عليهم حفظها تطبيقا لأحكام هذا الأمر.

ويتعيّن على مقدمي الخدمات كتمان سرّية العمليات التي ينجزونها وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء سرّ التحقيق.

المادّة 23 : يمكن الجهة القضائية المختصة إصدار أمر إلى مقدمي الخدمات، من أجل :

– التحفظ الفوري على المعطيات المتعلقة بالمحتوى و/أو بحركة السير المرتبطة بالجرائم المنصوص عليها في هذا الأمر، وفقا للكيفيات المحددة في التشريع الساري المفعول،

– التدخل الفوري، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول، لسحب أو تخزين المحتويات التي يتيحون الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تشكل جريمة من الجرائم المنصوص عليها في هذا الأمر، أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين هذه المحتويات أو لجعل الدخول إليها غير ممكن.

المادّة 24 : يجوز للجهة القضائية المختصة، بمناسبة التحقيق في إحدى الجرائم المنصوص عليها في هذا الأمر، أن تأمر أي شخص بتسليمها أي معلومات أو معطيات تكون مخزنة بواسطة استعمال وسائل تكنولوجيات الإعلام والاتصال، تحت طائلة العقوبات المنصوص عليها في هذا الأمر.

المادّة 25 : يمكن لضابط الشرطة القضائية المختص أن يضع، عبر الشبكات الإلكترونية، آليات تقنية للتبليغ عن الجرائم المنصوص عليها في هذا الأمر، ويعلم بذلك فورا وكيل الجمهورية، المختص الذي يأمر بالاستمرار في العملية أو بإيقافها.

المادّة 26 : تباشر النيابة العامة تحريك الدعوى العمومية تلقائيا في الجرائم المنصوص عليها في هذا الأمر.

المادّة 27 : يمكن اللجوء إلى أساليب التحري الخاصة المنصوص عليها في التشريع الساري المفعول، من أجل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا الأمر.

الفصل السادس

الأحكام الجزائية

المادّة 28 : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين، الموظف العمومي الذي ينشر أو يفشي أو يطلع الغير أو يسمح له بأخذ صور من المعلومات أو الوثائق المصنفة "توزيع محدود".

وتكون العقوبة بالحبس من سنة (1) إلى خمس(5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج إذا أدى ذلك إلى المساس بالاعتبار الواجب للسلطات المعنية.

المادّة 29 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج، الموظف العمومي الذي يفشي أو ينشر معلومة أو وثيقة مصنفة " واجب الكتمان" إلى علم الجمهور أو إلى علم شخص لا صفة له في الاطلاع عليها أو يسمح له بأخذ صور منها أو يترك الغير يقوم بذلك.

وتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 500.000 دج إلى 1.000.000 دج، إذا كانت الوثائق مصنفة "سرّي جدا" أو "سرّي ".

المادّة 30 : تكون العقوبة الحبس من ثلاثة (3) أشهر إلى سنة (1) والغرامة من 30.000 دج إلى 100.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 28 أعلاه، نتيجة عدم مراعاة الموظف العمومي الأحكام التشريعية و/ أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج أو إحدى هاتين العقوبتين، إذا ارتكبت الجريمة المنصوص عليها في المادة 29 أعلاه، نتيجة عدم مراعاة الموظف العمومي للأحكام التشريعية و/أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظائفه.

المادّة 31 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج كل شخص مؤتمن بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلي بها إليه وأفشاها في غير الحالات التي يوجب أو يرخص القانون بالتبليغ عنها.

المادّة 32 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من ينشر محاضر و/ أو أوراق التحريات والتحقيق القضائي أو يفشي محتواها أو يمكّن من لا صفة له من حيازتها.

المادّة 33 : يعاقب بالحبس من خمس (5) سنوات إلى خمس عشرة (15) سنة وبغرامة من 500.000 دج إلى 1.500.000 دج، كل من أطلع الغير بمقابل، أيّا كانت طبيعته، على معلومة أو وثيقة مصنفة أو يسّر لغيره ذلك.

المادّة 34 : دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول، يعاقب بالحبس من سبع (7) سنوات إلى خمس عشرة (15) سنة وبغرامة من 700.000 دج إلى 1.500.000 دج، كل من يقوم بالأفعال المذكورة في المادّة 33 أعلاه، تنفيذا لخطة مدبرة داخل الوطن أو خارجه.

المادّة 35 : يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو باحدى هاتين العقوبتين، كل من يحوز وثيقة مصنفة، دون أن يكون مؤهلا لذلك، ولم يقم بتسليمها إلى السلطات المعنية.

وتطبق العقوبات المنصوص عليها في المادتين 28 و29 من هذا الأمر، حسب الحالة، إذا قام بإفشاء مضمونها.

المادّة 36 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يرتكب من غير الفاعلين أو الشركاء، الأفعال الآتية :

1 – إخفاء الوثيقة المصنفة أو الأشياء أو الأدوات التي استعملت أو كانت ستستعمل في ارتكاب الجرائم المنصوص عليها في هذا الأمر والأشياء أو المواد أو الأموال المتحصلة منها مع علمه بذلك.

2 – إتلاف أو اختلاس أو إخفاء أو تزييف عمدا وثيقة عمومية أو خاصة من شأنها تسهيل البحث عن الجرائم المنصوص عليها في هذا الأمر ومعاقبة مرتكبيها.

المادّة 37 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل من يدخل دون ترخيص إلى منظومة معلوماتية أو موقع إلكتروني أو شبكة إلكترونية أو

أي وسيلة أخرى من وسائل تكنولوجيات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير وجه حق على معلومات أو وثائق مصنفة.

وتضاعف العقوبة في حال نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة.

المادّة 38 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها كليا أو جزئيا.

ويعاقب بنفس العقوبة كل من ينشر المعلومات والوثائق المصنفة أو محتواها كليا أو جزئيا على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام.

المادّة 39 : دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من عشر (10) سنوات إلى خمس عشرة (15) سنة وبغرامة من 1.000.000 دج إلى 1.500.000 دج، كل من يقوم عمدا بنشر أو بث، عن طريق الاتصالات الإلكترونية أو منظومة معلوماتية، معلومة أو وثيقة مصنفة، بغرض المساس بالنظام العام والسكينة العمومية.

المادّة 40 : يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج، كل من يمتنع عن تقديم الوثائق المنصوص عليها في المادة 24 من هذا الأمر.

المادّة 41 : يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 30.000 دج إلى 100.000 دج، أو بإحدى هاتين العقوبتين، كل من يقوم بنشر أو تداول أو توزيع المراسلات الإدارية التي لا تندرج ضمن الوثائق المصنفة الصادرة من أو إلى السلطات المعنية دون موافقتها أو في غير الحالات التي يسمح فيها القانون بذلك.

وتكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 60.000 دج إلى 200.000 دج في حالة العود.

المادّة 42 : يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا الأمر، بالعقوبات المنصوص عليها في قانون العقوبات.

المادّة 43 : كل من أنشأ أو شارك في جمعية أو اتفاق تشكل أو تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، يعاقب بالعقوبات المقررة للجريمة التامة، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل.

المادّة 44 : دون المساس بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في هذا الأمر، وكذا الأموال المتحصلة منها، وإغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

المادّة 45 : يمكن الجهة القضائية المختصة الحكم على مرتكبي الجرائم المنصوص عليها في هذا الأمر، بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات.

كما يمكنها الحكم على الموظف العمومي بالمنع من ممارسة وظيفة عليا نهائيا أو لمدة لا تقل عن خمس (5) سنوات ولا تزيد عن عشر (10) سنوات.

المادّة 46 : يعاقب بالعقوبات المقررة للفاعل، كل من يحرّض بأي وسيلة كانت، على ارتكاب الجرائم المنصوص عليها في هذا الأمر.

المادّة 47 : يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا الأمر، بالعقوبات المقررة للجريمة التامة.

المادّة 48 : مع مراعاة أحكام المادة 41 من هذا الأمر، تضاعف العقوبات المنصوص عليها في هذا الأمر في حالة العود.

الفصل السابع

أحكام ختامية

المادّة 49 : تطبق على إفشاء سرّ الدفاع الوطني وإفشاء السرّ الطبي العقوبات المنصوص عليها في قانون العقوبات.

المادّة 50 : تبقى المعلومات والوثائق المصنفة خاضعة لأحكام هذا الأمر إلى حين رفع السرّية عنها من قبل السلطات العمومية.

المادّة 51 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 27 شوّال عام 1442 الموافق 8 يونيو سنة 2021.

عبد المجيد تبون

قَـــائمَة
المَصَادِر وَالمَرَاجِع

قائمةالمصادر والمراجع

أولاً: قائمة المصادر

أ- القرآن الكريم.

1- سورة النمل: الآية (19).

2- سورة الرحمن: الآية (33).

3- سورة البقرة: الآية (143).

ب- المعاجم والموسوعات:

4- **معجم:** القانون الصادر عن مجمع اللغة العربية، الهيئة العامة لشؤون المطابع الأميرية، القاهرة، مصر، 1999.

5- **معجم:** مصطلحات الحاسب، مطبعة الخوارزمي، القاهرة، مصر، د.ت.ن. تأليف – علي يوسف علي.

6- **موسوعة:** الحاسب والمعلومات، الدار المنهجية للنشر والتوزيع، عمان، الأردن، 2016، تأليف – جبريل بن حسن العريشي وحميدة بنت عبيد الصبحي.

7- **موسوعة:** القاموس الموسوعي في المعلومات والإتصالات والمعلوماتية القانونية، ط1، مكتبة صادر، بيروت، لبنان، 2004، تأليف – عبد الحسن الحسيني.

8- **موسوعة:** القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت، منشورات اتحاد المصارف العربية، ج1، ط1، القاهرة، مصر، 2002، تأليف – يونس عرب.

9- **موسوعة:** الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، ط3، مطابع المكتب المصري الحديث، القاهرة، مصر، 1991، تأليف – علاء الدين فهمي وآخرون.

10- **موسوعة:** الموسوعة الشاملة لمصطلحات الحاسوب الإلكتروني، مطابع المكتب المصري الحديث للنشر والتوزيع، القاهرة، مصر، 1991، تأليف – محمد فهمي طلبة.

11- **موسوعة:** جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الاسكندرية، مصر، 2007، تأليف – محمد عبد الله أبو بكر.

12- **موسوعة:** مصطلحات الكمبيوتر والإنترنت، د.د.ت، القاهرة، مصر، د.ت.ن، تأليف – عبد الفتاح مراد.

ثانيًا: قائمة المراجع

أ- الكتب والمؤلفات القانونية (باللغة العربية):

I) الكتب العامة:

13- **أحسن بوسقيعة:** الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، ط 14، ج1، 2012.

14- **أحمد فتحي سرور:** الشرعية الدستورية وحقوق الانسان في الاجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، 1955.

15- **أحمد فتحي سرور:** القانون الجنائي الدستوري، دار الشروق، القاهرة، مصر، 2002.

16- **أحمد فتحي سرور:** الوسيط في قانون العقوبات، القسم الخاص، ط4، دار النهضة العربية، القاهرة، مصر، 1991.

17- **أمين مصطفى محمد السيد:** شرح قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011.

18- **باسم شهاب:** مبادئ القسم العام لقانون العقوبات وفقًا لأحدث التعديلات بالقانون رقم 23 لسنة 2006، دار المطبوعات الجامعية، وهران، الجزائر، 2007.

19- **جباري عبد المجيد:** دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، 2012.

20- **جلال ثروت:** النظرية العامة لقانون العقوبات، مؤسسة الثقافة الجامعية، الإسكندرية، مصر، د.ت.ن.

21- **حسن المرصفاوي:** قواعد المسؤولية الجنائية في التشريعات العربية، معهد البحوث والدراسات العربية، القاهرة، مصر، 1972.

22- **حسني الجندي:** الوجيز في شرح قانون العقوبات، القسم العام، ط 1، دار النهضة العربية، القاهرة، مصر، 2007.

23- **رمسيس بهنام:** النظرية العامة للقانون الجنائي، منشأة المعارف، الإسكندرية، مصر، 1997.

24- **رمسيس بهنام:** شرح قانون العقوبات العام، منشأة المعارف، الإسكندرية، مصر، 1971.

25- **رمسيس بهنام:** نظرية التجريم في القانون الجنائي، منشأة المعارف، الإسكندرية، مصر، 1996.

26- **رؤوف عبيد:** السببية في القانون الجنائي، مطبعة نهضة مصر، ط2، القاهرة، مصر، 1966.

27- **سعد ماهر حمزة:** علم الإقتصاد، دار المعارف، الإسكندرية، مصر، 1967.

28- **سليمان عبد المنعم:** النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، مصر، 2014.

29- **سميحة القليوبي:** الملكية الصناعية وفقا لأحكام القانون المصري لحماية الملكية الفكرية رقم (82 لسنة 2002)، دار النهضة العربية، القاهرة، مصر، 2009.

30- **صالح نبيه صالح:** النظرية العامة للقصد الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

31- **عبد العظيم مرسي وزير:** شرح قانون العقوبات، القسم العام، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، مصر، 2006.

32- **عبد الله سليمان:** شرح قانون العقوبات، القسم العام، دار الهدى، عين مليلة، الجزائر، د.ت.ن.

33- **عبد الواحد العلمي:** المبادئ العامة للقانون الجنائي المغربي، مطبعة النجاح الجديدة، المغرب، 1998.

34- **عز الدين طعباش:** شرح القسم الخاص من قانون العقوبات الجزائري، الجرائم الواقعة ضد الأشخاص والاموال، دار بلقيس، الدار البيضاء، الجزائر، د.ت.ن.

35- **علي أحمد راشد:** المبادئ العامة في القانون الجنائي، دار النهضة العربية، القاهرة، مصر، 1974.

36- **عمر سالم:** شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، مصر، 2010.

37- **عوض محمد عوض:** قانون العقوبات، القسم العام، منشأة المعارف، الاسكندرية، مصر، 2000.

38- **فتوح عبد الله الشاذلي:** شرح قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، مصر، 2001.

39- **فرج القصير:** شرح القانون الجنائي العام، مركز النشر الجامعي، تونس، 2006.

40- **فوزية عبد الستار:** شرح قانون مكافحة المخدرات، دار النهضة العربية، القاهرة، مصر، 1990.

41- **لحسن بن شيخ:** مبادئ القانون الجزائي العام، دار هومة، الجزائر، 2005.

42- **مأمون محمد سلامة:** قانون العقوبات، القسم العام، دار الفكر العربي، القاهرة، مصر، د.ت.ن.

43- **محمد شلال حبيب:** أصول علم الإجرام، العاتك لصناعة الكتاب، توزيع المكتبة القانونية، بغداد، العراق، 2007.

44- **محمود نجيب حسني:** النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، مصر، ط2، 1971.

45- **محمود نجيب حسني:** شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1986.

46- **محمود نجيب حسني:** شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، مصر، 1992.

47- **محمود نجيب حسني:** شرح قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 1988.

48- **نبيل صقر:** الوسيط في شرح جرائم الأموال، دار الهدى، عين مليلة، الجزائر، 2012.

II) الكتب الخاصة:

49- **أحمد خليفة الملط:** الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ط2، 2006.

50- **أحمد عبد الله المراغي:** الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2017.

51- **أحمد عبد الله هلالي:** الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2003.

52- **أحمد عبد الله هلالي:** الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2006.

53- **إدريس النوازلي:** جريمة النصب المعلوماتي، قانوناً وواقعًا وقضاءًا، دار الأفاق المغربية للنشر والتوزيع، مراكش، المغرب، 2015.

54- **أسامة أحمد المناعسة، جلال محمد الزغبي:** جرائم تقنية المعلومات الإلكترونية، ط2، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2014.

55- **أسامة المناعسة:** جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، عمان، الأردن، 2001.

56- **أشرف جابر السيد:** مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، دراسة خاصة لمسؤولية متعهدي الإيواء، دار النهضة العربية، القاهرة، مصر، 2010.

57- **أمال قارة:** الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط2، 2007.

58- **إمام حسنين عطا الله:** جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر والتوزيع، الرياض، السعودية، 2017.

59- **أمير فرج يوسف:** الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008.

60- **أمين طعباش:** الحماية الجنائية للمعاملات الإلكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2015.

61- **إنتصار نوري الغريب:** أمن الكمبيوتر والقانون، دار الراتب الجامعية، بيروت، لبنان، 1996.

62- **أودين سلوم الحايك:** مسؤولية مزودي خدمات الإنترنت التقنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2009.

63- **أيمن عبد الله فكري:** جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

64- **بلال أمين زين الدين:** جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، مصر، 2008.

65- **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، ط1، دار النهضة العربية، القاهرة، مصر، 2001.

66- **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي والأحكام الموضوعية للجرائم المتعلقة بالإنترنت، ط2، دار النهضة العربية، القاهرة، مصر، 2002.

67- **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، ط1، دار النهضة العربية، القاهرة، مصر، 1992.

68- **جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، ط2، دار النهضة العربية، القاهرة، مصر، 2012.

69- **جميل عبد الباقي الصغير:** الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، مصر، 2002.

70- **جميل عبد الباقي الصغير:** القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن إستخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، مصر، 1992.

71- **حسام شوقي:** حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية، القاهرة، مصر، 2003.

72- **حسن طاهر داوود:** جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، السعودية، 2000.

73- **حسني الجندي:** التشريعات الجنائية الخاص في دولة الإمارات العربية المتحدة، قانون مكافحة جرائم تقنية المعلومات، ط1، دار النهضة العربية، القاهرة، مصر، 2006.

74- **حسني الجندي:** التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث، شرح قانون مكافحة جرائم تقنية المعلومات، ط2، دار النهضة العربية، القاهرة، مصر، 2009.

75- **حسني الجندي:** قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، الكتاب الثالث، دار النهضة العربية، القاهرة، مصر، 2009.

76- **خالد حسن أحمد لطفي:** جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الإبتزاز الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2019.

77- **خالد عياد الحلبي:** إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، عمان، الأردن، 2011، ص33.

78- **خالد ممدوح إبراهيم:** الإدارة الإلكترونية، الدار الجامعية، القاهرة، مصر، 2010.

79- **خالد ممدوح إبراهيم:** الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2009.

80- **خالد ممدوح إبراهيم:** أمن الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2008.

81- **خالد ممدوح ابراهيم:** حوكمة الإنترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2011.

82- **خيرت علي محرز:** التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، الإسكندرية، مصر، 2012.

83- **دينا عبد العزيز فهمي:** الحماية الجنائية من إساءة إستخدام مواقع التواصل الإجتماعي، دار النهضة العربية، القاهرة، مصر، 2018.

84- **ذياب البداينة:** الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، عمان، الأردن، 2002.

85- **رامي متولي القاضي:** مكافحة الجرائم المعلوماتية في التشريعات المقارنة، دار النهضة العربية، القاهرة، مصر، 2011.

86- **رشاد خالد عمر:** المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الاسكندرية، مصر، 2013.

87- **رشيدة بوكر:** الحماية الجزائية للتعاملات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2019.

88- **رضا متولي وهدان:** الخطأ المفترض في المسؤولية عن أضرار الحاسبات الآلية، الأساس والضوابط، دار الفكر والقانون، الإسكندرية، مصر، 2009، ص25.

89- **زيدان زيبحة:** الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.

90- **سامي علي حامد عياد:** الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007.

91- **سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، مصر، 2013.

92- **سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية "الإنترنت"، دار النهضة العربية، القاهرة، مصر، 2007.

93- **سليمة سعيدي، بلال حجاز:** جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، مصر، 2017.

94- **سهيل محمد الغرام:** الوجيز في جرائم الإنترنت، مكتبة الجامعة الأردنية، عمان، الأردن، 2009.

95- **سيد أحمد محمود:** دور الحاسب، الكمبيوتر، أمام القضاء المصري والكويتي نحو إلكترونية القضاء، دار النهضة العربية، القاهرة، مصر، 2009.

96- **شرين دبابنة:** جرائم الإنترنت في المجتمع من منظور إجتماعي، دار الحامد للنشر والتوزيع، عمان، الأردن، 2015.

97- **شيماء عبد الغني محمد عطاء الله:** الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، مصر، 2007.

98- **صليحة علي صداقة:** الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2017.

99- **طارق إبراهيم الدسوقي عطية:** الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.

100- **طارق عبد الله الشدى:** آلية البناء الأمني لنظام المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، السعودية، 2000.

101- **طه السيد أحمد الرشيدي:** مدى المواجهة التشريعية لجرائم المعلومات، دار الكتب والدراسات العربية، الاسكندرية، مصر، 2016.

102- **طوني ميشال عيسى:** التنظيم القانوني لشبكة الإنترنت، دار صادر للمنشورات الحقوقية، بيروت، لبنان، 2001.

103- **عادل بوزيدة:** المسؤولية الجزائية لمتعهدي إيواء المواقع الإلكترونية، المركز الأكاديمي للنشر، القاهرة، مصر، 2019.

104- **عادل يحي:** السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2014.

105- **عاطف حليم،** الكمبيوتر: دار الكتب المصرية، القاهرة، مصر، 1987.

106- **عايد رجا الخلايلة:** المسؤولية التقصيرية الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

107- **عبد الرحمن عبد العزيز الشنيعي:** أمن المعلومات وجرائم الحاسب الآلي، (د.د.ن)، 1995.

108- **عبد الرحمن عبد الله السند:** الأحكام الفقهية للتعاملات الإلكترونية، ط3، دار الوراق، الرياض، السعودية، 2006.

109- **عبد الرزاق محمد الدليمي:** الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر والتوزيع، عمان، الأردن، 2011.

110- **عبد الفتاح بيومي حجازي:** الأحداث والانترنت، دار الفكر الجامعي، الاسكندرية، مصر، مصر، 2004.

111- **عبد الفتاح بيومي حجازي:** التجارة الإلكترونية العربية، الكتاب الثاني، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، دار النهضة العربية، القاهرة، مصر، 2003.

112- **عبد الفتاح بيومي حجازي:** الجريمة المعلوماتية في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

113- **عبد الفتاح بيومي حجازي:** الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2002.

114- **عبد الفتاح بيومي حجازي:** النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2002.

115- **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الإجرام والمجرم المعلوماتي، ط1، دار النهضة العربية، القاهرة، مصر، 2009.

116- **عبد الفتاح بيومي حجازي:** نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، مصر، 2008.

117- **عبد القادر القهوجي:** الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية، مصر، 1999.

118- **عبد القادر القهوجي:** الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، لبنان، 1999.

119- **عبد القادر القهوجي:** الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة، الإسكندرية، مصر، 1997.

120- **عبد القادر القهوجي:** الحماية الجنائية لبرنامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.

121- **عبد الله الكرجي، صليحة حاجي:** التعاقد الرقمي ونظم الحماية الإلكترونية، مطبعة الأُمنية، الرباط، المغرب، 2015.

122- **عبد الله سيف الكيتوب:** الأحكام الإجرائية لجريمة الإحتيال المعلوماتي، دار النهضة العربية، القاهرة، مصر، 2013.

123- **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

124- **عبد الهادي بن زيطة:** حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، (د.ت.ن).

125- **عصام عبد الفتاح مطر:** التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الاسكندرية، مصر، 2015.

126- **عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار النهضة العربية، القاهرة، مصر، 2000.

127- **علاء الدين الإبراهيمي:** الجرائم الإلكترونية، الوسائل وطرق الوقاية، مكتبة عنابة للنشر والتوزيع، عنابة، الجزائر، 2016.

128- **علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، الأردن، 2009.

129- **علي عبود جعفر:** جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2013.

130- **علي عدنان الفيل:** المسؤولية الجزائية عن إساءة إستخدام بطاقة الإئتمان الإلكترونية، ط1، المؤسسة الحديثة للكتاب، بيروت، لبنان، 2011.

131- **عماد مجدي عبد الملك:** جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011.

132- **عماد محمد سلامة:** الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل، عمان، الأردن، ط1، 2005.

133- **عمار عباس الحسيني:** جريمة الإتلاف المعلومات، دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت، لبنان، 2019.

134- **عمر الفاروق الحسيني:** المشكلات الهامة في الجرائم المتصلة بالحاسوب وأبعادها الدولية، دار النهضة العربية، القاهرة، مصر، ط2، 1995.

135- **عمرو عيسى الفقي:** الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، مصر، 2006.

136- **غنية باطلي:** الجريمة الإلكترونية، دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016.

137- **فاروق علي الحفناوي:** قانون البرمجيات، ط1، دراسة متعمقة في الأحكام القانونية لبرمجيات الكمبيوتر، دار الكتاب الحديث، القاهرة، مصر، 2003.

138- **فاروق محمد الأباصيري:** عقد الإشتراك في قواعد المعلومات عبر شبكة الإنترنت، دراسة لعقود التجارة الإلكترونية الدولية، دار النهضة العربية، القاهرة، مصر، 2003.

139- **فتحي محمد أبو عزت:** الحماية الجنائية الموضوعية والإجرائية للإعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007.

140- **فتحي محمد عزت:** الحماية الموضوعية والجزائية والحق في الخصوصية للكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، مصر، 2007.

141- **فخري محمود خليل:** جرائم البلطجة الإلكترونية تتحدى التشريعات والقضاء وتدعم المجرم والجريمة المستحدثة، دراسة مقارنة، د.د.ن 2019.

142- **فراس محمد العزة:** مهارات الحاسوب والبرمجيات الجاهزة، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2003.

143- **فريد منعم جبور:** حماية المستهلك عبر الإنترنت ومكافحة الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.

144- **لينا محمد الأسدي:** مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، دار الحامد للنشر والتوزيع، عمان، الأردن، 2015.

145- **ماجد عمارة:** المسؤولية القانونية الناشئة عن إستخدام فيروس الكمبيوتر، دار النهضة العربية، القاهرة، مصر، د.ت.ن.

146- **محمد أحمد فكيرين:** أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، لبنان، 1993.

147- **محمد السعيد رشدي:** الإنترنت والجوانب القانونية لنظم المعلومات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997.

148- **محمد السيد خشبة:** مقدمة في الحاسبات الإلكترونية، د. د. ن، القاهرة، مصر، 1984.

149- **محمد الشناوي:** جرائم النصب المستحدثة، دار الكتب القانونية، القاهرة، مصر، 2008.

150- **محمد أمين الرومي:** جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004.

151- **محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت –الجريمة المعلوماتية–، دار الثقافة للنشر والتوزيع، القاهرة، مصر، 2001.

152- **محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت، دار الثقافة، عمان، الأردن، 2004.

153- **محمد حامد مرهج الهايتي:** جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006.

154- **محمد حامد مرهج الهيتي:** التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

155- **محمد حماد مرهج الهيتي:** الخطأ المفترض في المسؤولية الجنائية، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2005.

156- **محمد حسام محمود لطفي:** الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، القاهرة، مصر، 1987.

157- **محمد حسين علي محمود:** التزوير بإستخدام الوسائل الإلكترونية، دار النهضة العربية، القاهرة، مصر، 2017.

158- **محمد حسين منصور:** المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

159- **محمد خليفة:** الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

160- **محمد سامي الشوا:** ثورة المعلومات وإنعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة، مصر، 2003.

161- **محمد طارق عبد الرؤوف الخن:** جريمة الإحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2011.

162- **محمد عبد الظاهر حسين:** المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، مصر، 2002.

163- **محمد عبد الظاهر حسين:** الإتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2001.

164- **محمد عبد الكريم حسين الداوودي:** المسؤولية الجنائية لمورد خدمة الإنترنت، منشورات الحلبي الحقوقية، ط1، لبنان، 2017.

165- **محمد عبد الله سلامة:** جرائم الكمبيوتر والإنترنت، ط1، منشأة المعارف، الاسكندرية، مصر، 2006.

166- **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2005.

167- **محمد عبيد الكعبي:** الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009.

168- **محمد علي العريان:** الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2011.

169- **محمد علي العريان:** الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2004.

170- **محمد علي سويلم:** شرح قانون جرائم تقنية المعلومات المصري، دار المطبوعات الجامعية، الإسكندرية، مصر، 2019.

171- **محمد علي قطب:** الجرائم المستحدثة وطرق مواجهتها، دار الفجر للنشر والتوزيع، القاهرة، مصر، 2009.

172- **محمد مأمون سليمان:** التحكيم الإلكتروني، دار الجامعة الجديدة، الاسكندرية، مصر، 2011.

173- **محمد محمد شتا:** فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، مصر، 2001.

174- **محمد محمد صالح الألفي:** المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، المكتب المصري الحديث، ط1، الإسكندرية، مصر، 2005.

175- **محمد محمود مكاوي:** الجوانب الأخلاقية والإجتماعية للجرائم المعلوماتية، المكتبة العصرية، المنصورة، مصر، 2010.

176- **محمد نصر محمد:** الوسيط في الجرائم المعلوماتية، ط1، مركز الدراسات العربية للنشر والتوزيع، القاهرة، مصر، 2015.

177- **محمود أمحمد عبابنة:** جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

178- **محمود رجب فتح الله:** الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2019.

179- **محمود عبد الله حسين علي:** سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2002.

180- **محمود كبيش:** الحماية الجنائية لسرية الحاسبات البنكية في القانون المصري، دار النهضة العربية، القاهرة، مصر، 1996.

181- **مدحت عبد الحليم رمضان:** الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2001.

182- **مروان بن مرزوق الروقي:** القصد الجنائي في الجرائم المعلوماتية، مكتبة القانون والإقتصاد، الرياض، السعودية، 2013.

183- **مشتاق طالب وهيب النعيمي:** تزوير المعلومات كأحد صور الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2018.

184- **مصطفى محمد موسى:** أساليب إجرامية بالتقنية الرقمية، ماهيتها ومكافحتها، دراسة مقارنة، دار الكتب القانونية، القاهرة، مصر، 2005.

185- **مصطفى محمد موسى:** دليل التحري عبر شبكة الإنترنت، دار الكتب القومية، القاهرة، مصر، 2010.

186- **مفيد الزيدي:** قضايا العولمة المعلوماتية، دار أسامة للنشر والتوزيع، عمان، الأردن، 2003.

187- **ممدوح عبد الحميد عبد المطلب:** جرائم إستخدام الكمبيوتر وشبكة المعلومات العالمية، دار الفتح للطباعة والنشر، ط1، الشارقة، الإمارات العربية المتحدة، 2000.

188- **منير محمد الجهيني وممدوح محمد الجهيني:** جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2005.

189- **نائلة عادل محمد فريد قور:** جرائم الحاسب الإقتصادية، ط1، دار النهضة العربية، القاهرة، مصر، 2004.

190- **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، ط1، بيروت، لبنان، 2005.

191- **نائلة عادل محمد فريد قورة:** جرائم الحاسب الآلي الإقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

192- **نبيل صقر:** جرائم الكمبيوتر والإنترنت، دار الهدى، عين مليلة، الجزائر، 2012.

193- **نبيل صقر:** جرائم الكمبيوتر والإنترنت، دار الهلال للخدمات العلمية، الجزائر، 2005.

194- **نسيم دردور:** الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2013.

195- **نعيم مغبغب:** حماية برامج الكمبيوتر في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.

196- **نهلا عبد القادر المومني:** الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2008.

197- **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1992.

198- **هشام محمد فريد رستم:** قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، القاهرة، مصر، 1994.

199- **هلال أحمد:** حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 1999.

200- **هلالي عبد الإله أحمد:** الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، 2003.

201- **يزيد بوحليط:** الجرائم الإلكترونية فى القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

202- **يوسف أبو الحجاج:** أشهر جرائم الكمبيوتر والأنترنت، دار الكتاب العربي، القاهرة، مصر، 2010.

203- **يوسف حسن يوسف:** الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2011.

204- **يونس عرب:** دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والأنترنت، ط1، إتحاد المصارف العربية، بيروت، لبنان، 2002.

III) الأعمال الجامعية:

• أطروحات الدكتوراه:

205- **أحمد حسام طه تمام:** الجرائم الناشئة عن إستخدام الحاسب الآلي، دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 2001.

206- **أحمد كيلان عبد الله صكر:** حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي، دكتوراه، كلية الحقوق، جامعة بغداد، العراق، 2007.

207- **تركي بن عبد الرحمن المويشير:** بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2009.

208- **خالد حمدي عبد الرحمن:** الحماية القانونية للكيانات المنطقية، برامج الكمبيوتر، دكتوراه، جامعة عين الشمس، مصر، 1992.

209- **عبد الوهاب ملياني:** أمن المعلومات في بيئة الأعمال الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقياد، تلمسان، الجزائر، 2017.

210- **عزيزة رابحي:** الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018.

211- **عمر محمد أبو بكر بن يونس:** الجرائم الناشئة عن إستخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس القاهرة، مصر، 2004.

212- **عياض راشد عياض المري:** مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود، دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1998.

213- **فايز محمد راجح غلاب:** الجرائم المعلوماتية في القانون الجزائري والقانون اليمني، دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2009.

214- **فيصل بدري:** مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2018.

215- **محمد خليفة:** جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2011.

216- **محمد محمد صالح الألفي:** المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2011. غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2011.

217- **محمود علي أحمد مدني:** دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التي يقوم عليها النظام القانوني المصري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، مصر، 2015.

- **رسائل الماجستير:**

218- **أحمد كيلان عبد الله صكر:** الجرائم الناشئة عن إساءة استخدام الحاسوب، ماجستير، كلية الحقوق، جامعة بغداد، العراق، 2002.

219- **بن عقون حمزة:** السلوك الإجرامي للمجرم المعلوماتي، ماجستير، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2011.

220- **بهاء فهمي الكبيجي:** مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2013.

221- **عبد اللطيف معتوق:** الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري، ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2012.

222- **عبد الله دغش العجمي:** المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الكويت، 2014.

223- **فتيحة رصاع:** الحماية الجنائية للمعلومات على شبكة الإنترنت، ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2012.

224- **مريم مسعود:** مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم (09-04)، ماجيستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2013.

225- **نسيم دردور:** جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2013.

226- **نسيمة درار:** واقع المسؤولية المدنية في المعاملات الإلكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2012.

227- **يوسف خليل يوسف العفيفي:** الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة، رسالة ماجستير، كلية الشريعة والقانون، جامعة غزة، فلسطين، 2013.

- **مذكرات التخرج:**

228- **هيام حاجب:** الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة إجازة مهنة القضاء، المدرسة العليا للقضاء، الجزائر، 2008.

- **المقالات والمجلات:**

229- **إبراهيم بن عوض العتيبي:** إستخدام التقنية في التحقيقات الأمنية، مجلة التقنية والامن، كلية الملك خالد، السعودية، العدد 80، 2005.

230- **أحمد فرج:** النظام القانوني لمقدمي خدمات الإنترنت، مجلة المنارة، المجلد 13، ع 9، 2007.

231- **أحمد قاسم فرح:** النظام القانوني لمقدمي خدمات الإنترنت، دراسة مقارنة، مجلة المنارة، المجلد13، العدد09، 2007.

232- **إسماعيل عبد النبي شاهين:** تأمين المعلومات في الإنترنت بين الشريعة والقانون، مجلة كلية الشريعة والقانون، العدد 19، جامعة طنطا، مصر، 2005.

233- **أكمل يوسف السعيد يوسف:** المسؤولية الجنائية لمقدمي المواد الإباحية للأطفال عبر الإنترنت، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، مصر، 2011.

234- **ألاء يعقوب النعيمي:** الوكيل الإلكتروني، مفهومه وطبيعته القانونية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد السابع، العدد 2، الإمارات العربية المتحدة، 2010.

235- **أيمن عبد الحفيظ:** المخاطر التي تتعرض لها شبكة الإنترنت وسبل حمايتها، مجلة مركز بحوث الشرطة، العدد 20، القاهرة، مصر، 2001.

236- **ثامر علي النويران:** الجرائم الإلكترونية وطرق الحد منها، بحث مشاركة في المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، مجلة كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، السعودية، 2015.

237- **جميل زكريا محمود:** الجريمة المعلوماتية وأساليب التأمين، المؤتمر الدولي لأمن المعلومات الإلكترونية، جامعة عمان، 2005.

238- **حسين بن سعيد الغافري:** بحث مقدم بعنوان "الجوانب القانونية للمعلوماتية بين النظرية والتطبيق" مقدم إلى المؤتمر العلمي الأول، والمنعقد في الفترة الممتدة من 13-2011/03/14، كلية الحقوق، جامعة السلطان قابوس، سلطنة عمان، مجلة الكلية، 2011.

239- **ذياب البداينة:** الجرائم الإلكترونية، المفهوم والأساليب، ورقة علمية مقدمة إلى الملتقى الدولي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، جامعة عمان، الأردن، من (02 إلى 2014/09/04)، مجلة الجامعة لعام 2015.

240- **رامي عمر غريب أبو ركبة:** جرائم المساس بأنظمة الكمبيوتر والإنترنت، مجلة كلية الشريعة والقانون، جامعة الأزهر، القاهرة، مصر، العدد 14 لعام 2012.

241- **زاهر رامي:** إستخدام مواقع التواصل الإجتماعي في العالم العربي، مجلة التربية، العدد 15، جامعة عمان الأهلية، عمان، الأردن، 2003.

242- **زينب أحمد عوين:** عدم كفاية قواعد القانون الجنائي في مكافحة الجريمة المعلوماتية، مقال منشور في مجلة كلية الحقوق، جامعة النهرين، بغداد، العراق، المجلد 13، ع 1، 2011.

243- **سامي الرواشدة وأحمد الهياجنة:** مكافحة الجريمة المعلوماتية بالتجريم والعقاب، مجلة القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد الأولى، العدد الثالث، 2009.

244- **سعاد حميدي:** الجرائم الماسة بالنظم المعلوماتية في التشريع المغربي، مجلة المنارة للدراسات القانونية والإدارية، ع13، المغرب، 2016.

245- **سليمان عبد الحميد عثمان محمد:** مسؤولية مزود الخدمة المعلوماتية في القانون البحريني، بحث مقدم ضمن كتاب "المعاملات الرقمية وقانون الإنترنت"، منشورات المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2006.

246- **سيناء عبد الله محسن:** المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، ورقة عمل مقدمة إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المغرب، من (19 إلى 2007/06/20)، مجلة الندوة.

247- **شرين دبابنة:** الجرائم الإلكترونية والقرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، مج 23، ع01، الأكاديمية العربية للعلوم المالية والمصرفية، القاهرة، مصر، 2015.

248- **عبد الجبار الحنيص:** الإستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي، دراسة مقارنة، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الأول، كلية الحقوق، جامعة دمشق، سوريا، 2011.

249- **عبد الرؤوف اللومي:** المسؤولية التقصيرية على شبكة الإنترنت، المجلة القانونية التونسية، مركز النشر الجامعي، تونس، 2007.

250- **عبد الله اليوسف:** التقنية والجرائم المستحدثة، مؤتمر الظواهر الإجرامية المستحدثة وسبل مواجهتها، تونس، في: (28-1999/6/30) مجلة المؤتمر.

251- **عبد المهدي كاظم ناصر، حسين عبيد شعواط:** عقد الإيواء المعلوماتي، مجلة الكوفة للعلوم القانونية والسياسية، العدد 21، جامعة الكوفة، العراق، 2014.

252- **عطاء الله وارد خليل:** أمن المعلومات في ظل الإنفتاح المعلوماتي، مجلة كلية الحقوق، جامعة بنها، مصر، ع 6، لعام 2011.

253- **عمر السعيد رمضان:** فكرة النتيجة في قانون العقوبات، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، مصر، العدد 31 لسنة 1961.

254- **عمر الشريف:** التنظيم التشريعي لجرائم الاتصالات في مصر، مجلة التشريع، السنة الأولى، العدد الثاني، القاهرة، مصر، 2004.

255- **عمر محمد خير الحاج:** العولمة وآثارها في تطور الجريمة، مجلة الأمن والقانون، كلية شرطة دبي، الإمارات العربية المتحدة، س10، ع1، 2002.

256- **فريحة حسين:** الجرائم الإلكترونية والإنترنت، مجلة المعلوماتية، جامعة الجزائر، ع 36، 2011.

257- **فضيلة عاقلي:** الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مقال منشور بأعمال المؤتمر الدولي الرابع عشر، تحت عنوان "الجرائم الإلكترونية"، طرابلس، لبنان، في الفترة من 24-25 مارس 2017.

258- **فيروز لطرش:** الجريمة الإلكترونية في الجزائر من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، ع1، جامعة زيان عاشور، الجلفة، الجزائر، 2016.

259- **لورنس سعيد الحوامدة:** الجرائم المعلوماتية، أركانها وآلية مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، العدد الثالث، 2016.

260- **محمد الأمين البشري:** التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنت، من (1-2000/5/3)، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ط 03، مج 03- 2004.

261- **محمد مزاولي:** المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة الدراسات والأبحاث القانونية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد01، لعام 2009.

262- **محمد نصر:** المسؤولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت، المجلة الجنائية القومية، مج 59، ع 1، دار المنظومة، عمان، الأردن، 2016.

263- **محمود محمد المرزوقي:** جرائم الحاسب الآلي، مقال منشور في المجلة العربية للفقه والقضاء، الصادرة عن منظمة الدول العربية، القاهرة، مصر، العدد 28، 2003.

264- **مختارية بوزيدي:** ماهية الجريمة الإلكترونية، مجلة أعمال الملتقى الوطني، بعنوان آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، تحت إشراف مركز جيل البحث العلمي، الجزائر العاصمة 29 مارس 2017.

265- **مروة أديب محمد الجوهري:** الحاسوب والإعجاز العددي في القرآن الكريم، مجلة كلية العلوم الإسلامية، جامعة القاهرة، مصر، مج08، عدد15، 2014.

266- **مليكة عطوي:** الجريمة المعلوماتية، مجلة حوليات، جامعة الجزائر1، العدد21 لسنة 2012.

267- **نائل عبد الرحمن صالح:** واقع جرائم الحاسب في التشريع الأردني، القانون والكمبيوتر والإنترنت، مجلة كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الأول، 2004.

268- **هدى حامد قشقوش:** جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة 25 إلى 28 أكتوبر 1993.

269- **هشام عبد السيد الصافي محمد بدر الدين:** الجرائم الالكترونية في مصر ودستورية مبدأ الشرعية الجنائية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، طرابلس، لبنان، العدد 14 لعام 2017.

270- **هشام محمد فريد رستم:** الجرائم المعلوماتية، بحث مقدم إلى المؤتمر العلمي الدولي حول القانون والكمبيوتر والإنترنت، كلية الحقوق، جامعة العين، الإمارات العربية المتحدة، مجلة الكلية لعام 2001.

271- **هشام محمد فريد رستم:** جرائم الفضاء الإفتراضي، مجلة أكاديمية الشرطة، القاهرة، مصر، 2013.

272- **هلالي عبد الله أحمد:** المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء إتفاقية بودابست، مجلة الحقوق، جامعة البحرين، المجلد السادس، العدد13، 2009.

273- **وسيم طعمة:** السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، دمشق، سوريا، المجلد رقم 39، العدد 68، لعام 2017.

IV) القوانين الدولية والوطنية:

- **القوانين الدولية:**

274- الاتفاقية الأوروبية لحقوق الانسان لعام 1950.

275- الإتفاقية الدولية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات لعام 1989.

276- الإتفاقية الدولية حول الإجرام المعلوماتي والمبرمة بمدينة بودابست في دولة المجر، بتاريخ 2001/11/08 تحت إشراف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

277- الإتفاقية الأورو متوسطية والمؤرخة في 22 أفريل2002، والتي كانت تهدف إلى ربط الجهود بين الدول الأوروبية من جهة والدول المطلة على الحوض الأبيض المتوسط من جهة أخرى، وقد صادقت الجزائر على هذه الإتفاقية بتاريخ 25 أكتوبر 2003 والتي دخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم (07-375) المؤرخ في 01 ديسمبـــر 2007، (ج ر المؤرخة في 09 ديسمبر 2007 ع77).

278- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي حررت بمدينة القاهرة في جمهورية مصر العربية بتاريخ 21 ديسمبر 2010، والتي صادقت عليها الجزائر بتاريخ 08 سبتمبر 2014، بموجب المرسوم الرئاسي رقم (14-252)، ج ر رقم (57) المؤرخة في 28 سبتمبر 2014.

279- القانون الفرنسي رقم (719-2000) المؤرخ في 01 أوت 2000 المعدل للقانون رقم (1067-1986) المؤرخ في 30 سبتمبر1986 والمتعلق بحرية الإتصالات.

280- القانون الفرنسي رقم (575-2004) والمتعلق باثقة في الإقتصاد الرقمي والمؤرخ في 21 جوان 2004.

- **القوانين الوطنية:**

❖ **القوانين الجزائرية:**

281- الدستور الجزائري لعام 2020.

282- الأمر رقم (75-47) والمؤرخ في 17 يونيو 1975 والمعدل والمتمم لقانون العقوبات الجزائري.

283- الأمر رقم (03-05) المؤرخ في 19 يوليو 2003، والمتعلق بحقوق المؤلف والحقوق المجاورة، المعـــدل والمتـــمم للأمر رقم (73-14) ج ر العدد 44، المؤرخ في 23 يوليو 2003.

284- الأمر رقم (15-02) المؤرخ في 2015/07/23 المعدل والمتمم لقانون الإجراءات الجزائية رقم (66-155).

285- الأمر رقم (21-09) المؤرخ في 08 يونيو 2021، يتعلق بحماية المعلومات والوثائق الإدارية، ج ر، عدد (45) المؤرخة في 09 يونيو 2021.

286- القانون العضوي رقم (12-05) المؤرخ في 12 يناير 2012 والمتعلق بقانون الإعلام، الجريدة الرسمية، العدد 02 في 15 يناير2012.

287- قانون العقوبات الصادر بالأمر رقم (66-156) والمؤرخ في 08 يونيو 1966، ج ر رقم (49) المؤرخة في 11 يونيو 1966.

288- القانون رقم (11-14) المؤرخ في 02 غشت 2011، المعدل والمتمم لقانون العقوبات الجزائري.

289- القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات الجزائري.

290- القانون رقم (06-23) المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات الجزائري.

291- القانون رقم (16-02) المؤرخ في 19 يونيو 2016، المعدل والمتمم لقانون العقوبات الجزائري.

292- القانون رقم (14-01) والمؤرخ في 4 فبراير 2014، المعدل والمتمم لقانون العقوبات الجزائري.

293- القانون رقم (09-04) والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمؤرخ في 5 أوت 2009، ج ر العدد 47، المؤرخة في 16 أوت 2009، ج ر المؤرخة في 2009/08/16، ع 47.

294- القانــون رقــم (82-04) مؤرخ في 13 فبراير 1982 المعدل والمتمم لقانون العقوبات الجزائري.

295- القانون رقم (07/18) المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018، ج ر عدد 34، المؤرخة في 10 يونيو 2018.

296- القانون المدني الجزائري الصادر بالأمر رقم (75-58) المؤرخ في 26 سبتمبر 1975 المعدل والمتمم بآخر تعديل له بالقانون رقم (07-05) المؤرخ في 13 مايو 2007.

297- القانون رقم (18-07) مؤرخ في 10 يونيو 2018، يتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد (34) المؤرخة في 10 يونيو 2018.

298- المرسوم الرئاسي رقم (89-67) والمؤرخ في 1989/05/16، ج ر، ع20، في 1989/05/17.

299- المرسوم التنفيذي رقم (98-257) مؤرخ في 25 أوت 1998 والمتعلق بضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، ج ر، عدد 63، الصادرة بتاريخ 26 أوت 1998،

300- المرسوم التنفيذي رقم (2000-307) والمؤرخ في 14 أكتوبر 2000 والذي يضبط شروط وكيفيات إقامة خدمات الإنترنت وإستغلالها، ج ر، العدد (60) والصادرة بتاريخ 15 أكتوبر 2000.

301- قرار المجلس الدستوري رقم (24/ق م د/21) المؤرخ في 07 يونيو 2021، يتعلق بمراقبة دستورية الأمر المتعلق بحماية المعلومات والوثائق الإدارية، ج ر، عدد (45) المؤرخة في 09 يونيو 2021.

❖ **القوانين العربية:**

302- القانون السوري رقم (17 لسنة 2012) والمتعلق بمكافحة الجريمة المعلوماتية.

303- القانون القطري رقم (14 لسنة 2014) والمتعلق بمكافحة الجريمة الإلكترونية.

304- القانون الكويتي رقم (63 لسنة 2015) والمتعلق بمكافحة جرائم تقنية المعلومات.

305- القانون المصري رقم (175 لسنة 2014)، المتعلق بمكافحة جرائم تقنية المعلومات.

306- القانون العماني رقم (12 لسنة 2011)، المتعلق بمكافحة جرائم تقنية المعلومات.

307- القانون الإماراتي رقم (5 لسنة 2012)، المتعلق بمكافحة جرائم تقنية المعلومات.

308- القانون المغربي رقم (07 لسنة 2003) المتعلق بالإجرام الإلكتروني.

309- القانون السعودي رقم (17 لسنة 2007) المتعلق بجرائم تقنية المعلومات.

310- القانون السوداني (13 لسنة 2007) المتعلق بالإجرام المعلوماتي.

311- القانون الأردني رقم (27 لسنة 2015) المتعلق بجرائم تقنية المعلومات.

312- قانون البحريني رقم (05 لسنة 2015) المتعلق بالإجرام الإلكتروني والإنترنت.

313- المرسوم التشريعي السوري رقم (17 لسنة 2012) المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

314- قرار وزارة الثقافة المصرية رقم (82 لسنة 1993) في شأن تنفيذ قانون حماية حق المؤلف، والذي عدل القانون رقم (354 لسنة 1954) في المادة الثانية منه، والمنشور بالجريدة الرسمية، العدد 104، المؤرخة في 1993/5/9.

315- قرار وزارة الإتصالات وتكنولوجيا المعلومات المصرية رقم (109 لسنة 2005) في شأن إصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم (15 لسنة 2004) في مادته الأولى، والمنشور بالجريدة الرسمية، العدد 115، والمؤرخة في 2005/5/25.

316- قرار محكمة النقض المصرية، الطعن رقم (17639) جلسة بتاريخ 1998/12/17، عن (مج، ق، ق)، ج6، لسنة 2000.

317- الطعن رقم (21609 س.ق 62) جلسة بتاريخ 10 ديسمبر 1995، مج.أ.ن، س46، ج1.

318- الطعن رقم (2358 س.ق 54) جلسة بتاريخ 24 مايو 1985 مج. أ.ن، س 36، ج1.

319- الطعن رقم (2534 س.ق 59) جلسة بتاريخ 6 فبراير 1990 مج. أ.ن، س 41، ج1.

ب- الكتب والمؤلفات القانونية (باللغة الفرنسية):

I) الكتب والمؤلفات الفرنسية:

317- ***AUVERT Patrick :*** *L'application du droit de la presse au réseau internet , (JCP) N°3, France, 1999.*

318- ***BENSOUSSAN Alain :*** *Internet « aspects juridiques », Ed. Hermes, Paris, France, 1998.*

319- ***BENSOUSSAN Alain :*** *L'informatique et le droit, memento guide, édition (HERMES), Paris, France, Tome I, 1994, P211.*

320- ***BOSSAN Jérôme :*** *Le droit pénal confronté à la diversité des intermédiaires de l'internet (R S C, N°02) ed. Dalloz, Paris, France ,2013.*

321- ***CASILE Jean-François:*** *Le code pénal à l'épreuve de la délinquance informatique, presse universitaires (D'AIX) Marseille, (PUAM), France, 2002.*

322- ***CHAMPY (G) :*** *Fraude informatique, thèse, université Aix- Marseille 3, France, 1990.*

323- ***CHRISTIANE (F-S) :*** *Le droit à l'épreuve, de l'internet, 4eme édition, dalloz, Paris, France, 2006.*

324- ***DEVEZ (J) :*** *Les qualifications pénales appliables aux fraudes informatiques, Acte du 8ème congrés de l'AFDP, grenoble 28-30 Novembre 1985, Ed Economica, Paris, France, 1986.*

325- ***El AZZOUZI Ali:*** *La cybercriminalité au maroc 1ere Ed (Bishoop Solution) casablanca, Maroc, 2010.*

326- ***FOREST (D) et KAUFMAN (G) :*** *Droit de l'informatique, édition gualino extenso, Paris, France, 2010.*

327- ***FRANCILLON (J) :*** *Application à la télématique et à l'internet des régles de responsabilité propres au droit de la presse et de la communication audiovisuelle (R S C N°3) ED. Dalloz, Paris, France, 1999.*

328- ***GARE (Th) et GINESTET (c) :*** *droit pénal et procédure pénal, Imprimé par (I.M.E) paris, France,2012.*

329- ***GARRAUD (R) :*** *Traité théorique et pratique du droit pénal français (sériy2, tome 1) ED. D, Paris,1987.*

330- ***GASSIN (R) :*** *Le droit pénal de l'informatique, les systèmes de traitements automatique des données, commentaire de la loi N° (88-18) du 03/01/1988 relative à la fraud informatique, (J.C.P) Oct 1988.*

331- ***GASSIN (R)****: Fraude informatique, Ed, Dalloz, Paris, France, 1995.*

332- ***GASTON (S), LEVASSEUR (G), BOULOC (B) :*** *Droit pénal général, 16emeédition, dalloz, Paris, France, 1997.*

333- ***GUAY (PJ) :*** *« la relation intelligence crime » le cas de d élinquants esxuels sous juridication fédérale, ph (D) thèse, universit é de montréal, France, 2001.*

334- ***GUILLAUME Champy :*** *La fraude informatique (T 2. Ed. D), Paris, france, 1992.*

335- ***HERBERT (M) :*** *droit de l'informatique et des télécommunication Ed, Litec, Paris, France, 1989.*

336- ***HUET (J), MAISL (H) :*** *droit de l'informatique et des télécommunications, édition, LITEC, Paris, France, 1989.*

337- ***LARGUIER (J), CONTE (Ph) :*** *Droit pénal spécial, 13eme édition, Dalloz, Paris, France, 2005.*

338- ***LARGUIER (J), CONTE (Ph), FOURNIER (S) :*** *Droit Pénal Spécial, 15eme éd, Dalloz, Paris, France, 2013.*

339- ***LINANT (XAV), HOLLANDE (AL) :*** *Pratique du droit de l'informatique, 5eme Ed, Dalloz, Paris, France, 2002.*

340- ***MASCALA Corinne :*** *Droit pénal de l'informatique et droit des personnes. (Ed dalloz), Paris, France, 2004.*

341- ***MICHEL Véron :*** *droit pénal spécial, 6eme édition Armand colin, Paris, France, 1998.*

342- ***NIDAL (Ch) :*** *La criminalité informatique devant la justice pénale, édition juridique sader, Beyrouth, liban, 2004.*

343- ***OLIVIER Cachard :*** *Droit du commerce éléctronique, (R.D.A.I) N°3, Ed, D, Paris, France, 2004.*

344- ***CONTE (Ph), PATRICK Maistre du Chambon :*** *Droit pénal général, 7eme, édition, Armand collin, Paris, France, 2004.*

345- ***QUÉMÉNER (M), CHARPENEL (Y) :*** *Cybercriminalité et droit pénal appliqué, économica, Paris, France, 2010.*

346- ***QUEMENER (M), FERRY (J) :*** *Cybercriminalité défimondial, economica, 2eme édition, Paris, France, 2009.*

347- ***ROBERT (P):*** *le petit Robert, Dictionnaire Alphabetical et la anallogique logos de la langue française, (V 1, Ed. D), Paris, france, 1983.*

348- ***ROSE (Ph) :*** *La criminalité informatique 2ème édition (ED.p.u.f) Paris, France, 1995.*

349- ***SARGOS (P), MASSE (M) :*** *Le droit pénal spécial né de l'informatique, édition cujas, Paris, France, 1980.*

350- ***SEDALLIAN (V) :*** *Droit de l'internet, réglementation, responsabilité, contrats net press, (Ed. D), paris, france 1997.*

351- ***SHERIDAN Mouris :*** *l'ordinateur comme cible de la criminalité, (vol d'ordinateurs et piratage), périodique, problèmes politiques et siciaux, N° 953, éd, les documentations françaises, paris, France, 2008.*

352- ***SIEBER (U) :*** *Les crimes informatiques et d'autres crimes dans le domain de la technologie informatiqe, (R.I.D.P), 1993.*

353- ***TASRPALAS (A) :*** *Le moment et la duree de les infractions pénales, Ed, D, Paris, France, 1996.*

354- ***VALÉRIE Sédallian :*** *Droit de l'internet, réglementation, résponsabilités, contrats, Collection association des utilisateurs d'internet (Ed, Net press), Paris, France, 1997.*

355- ***VERGUTCH (p) :*** *la représsion des délits informatique dans une pérspéctive informtionale, thèse université de Montpellier (I), France, 1996, P169-171.*

356- ***VÉRON Michel:*** *Droit pénal spécial, 6ème édition, Armand colin, paris, France, 1998.*

357- ***VITALIS Andre :*** *Informatique et liberté, Ed, Economica, Paris, France, 1981.*

358- ***VIVANT (M), Autres :*** *l'informatique et le droit pénal (les biens informatiques, objets d'une fraude). Lamy informatique, France 1991.*

II) القوانين الفرنسية:

359- ***JORF :*** *N° 0143 DU 22 juin 2004 (p.11168, texte N° :2, loi N° : 2004- 575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

360- ***Loi :*** *Du 29 juillet 1881 sur la liberté de la presse, modifié par ordonnance du 26 Aôut 1944, modifié par loi N° : (1952-336) du 25Mars1952 (JORF) du 26Mars1952.*

361- ***Loi :*** *N° (1982-652) du 29 Juillet 1982 sur la communication audiovisuelle.*

362- ***Loi :*** *N° (2000-719) du 1 Aôut 2000, modifiant la loi N° (1986-1067) du 30 septembre 1986, relative à la liberté de communication (JORF) N°(177) du 2 Aôut 2000.*

363- ***Loi :*** *N° (2000-719) du 1er Aôut 2000.*

364- ***Loi :*** *N° (2004-575) du 21 juin 2004, pour la confiance dans l'économie numérique.*

365- ***Loi :*** *N° (2004-575) du 21 Juin 2004, pour la confiance dans l'économie numérique. Modifié par loi N°: (2016-444) du 13 Avril 2016.*

366- ***Loi :*** *N° (2004-575) du 21 juin 2004 pour la confiance dans l'économie numérique. Modifié par loi N° (2016-444° du 13 avril 2016, visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées.*

367- ***Loi :*** *N°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004.*

368- ***Loi :*** *N°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004.*

369- ***Loi :*** *N°2013-1168 du 18 décembre 2013 - art. 25*

370- ***Loi :*** *N°2015-912 du 24 juillet 2015.*

371- ***Loi :*** *N° (2016-444) du 13 Avril 2016.*

372- ***Loi :*** *N° (2016-444) du 13 Avril 2016.*

373- ***Conseil Détat :*** *« Internet et les réseaux numériques » étude adoptée par l'assemblée générale du conseil d'état, section du rapport et des études, le 2juillet1998, (la documentation française) Paris, France,1998.*

374- ***Crim*** *: 8 Déc 1999, JCP 2000, P 395. NCP 104-E, éd. D. Paris, France, 2009.*

375- ***Crim*** *: 5 Janv 1994, Gaz-Pal, 1996, Somm, 419- 12 Déc 1996 Bull, Crim N° 465.*

ج- الكتب والمؤلفات القانونية (باللغة الإنجليزية):

376- ***CHUCH Eastton, JEFF Taylor :*** *Computer crime investigation and the law, Boston (U.S.A), 2011.*

377- ***DAVID (Th) :*** *Current trends in computer crime, computer control quarterly, Vol (09 N°(01), Ed, 1991.*

378- ***KENNETH (C) Brancik :*** *Insider computer fraud, new york, U.S.A, 2008, p403.*

379- ***MARTIN Wasik:*** *Crime and the computer, oxford university, 1991.*

380- ***THOMAS (J) SMEDINGHOFF :*** *The legal guide to developing and marketing software, john wille & sons, 1986.*

د- المواقع الإلكترونية:

381- *http://www.statutes.legis.state.tx.us/docs/pe/htm/pe.33.htm*

382- *www.hrdoegypt.org*

383- *www.ic3.gov*

384- *www.neelwalurat.com*

385- *www.arabicacademy.org.eg*

386- *http://www.statutes.legis.state.tx.us/docs/pe/htm/pe.33.htm*

387- *http://www.usdoj.gov/criminal/cybercrime/maxwelleplea.htm*

388- *http: // www.assemblée–nationale.fr*

389- *https://www.mpicc.de/en/home/sieber.html*

390- *https://m.dw.com*

391- *https://ar.m.wikipédia.org*

الـــفَهرَس

العنوان	الصفحة
البَاب التّمهِيدي: ماهية الجريمة المعلوماتية وتحديد طبيعتها القانونية	11
الفَصل الأَوّل: مفهوم الجريمة المعلوماتية والمجرم المعلوماتي	13
المبحث الأول: تعريف الجريمة المعلوماتية وسماتها الخاصة	15
المطلب الأول: تعريف الجريمة المعلوماتية	16
الفرع الأول: التعريف الإصطلاحي للجريمة المعلوماتية	17
أولاً: بالنسبة للتسميات والمصطلحات الشائعة	18
أ- الجريمة المعلوماتية *L'infraction d'informatique*	18
ب- الجريمة الإلكترونية *L'infraction électronique*	19
ج- جرائم الكمبيوتر أو الحاسوب *Crimes computer*	19
د- جرائم الإنترنت *Crimes sur Internet*	21
هـ- جرائم مواقع التواصل الإجتماعي *Crimes sur les réseaux sociaux*	22
و- جرائم تقنية المعلومات *Crimes liés aux technologies de l'information*	23
ثانيًا- بالنسبة للتسميات والمصطلحات غير الشائعة	23
أ-جرائم تكنولوجيات الإعلام والإتصال *Crimes liés aux technologies de l'information et de la communication*	24
ب- جرائم المساس بأنظمة المعالجة الآلية للمعطيات *Des atteintes aux systèmes de traitement automatisé de données*	24

ج- الجريمة السيبرانية *Cyber crime*	25
د- جرائم الوسط الرقمي أو البيئة الرقمية *Environnement numérique*	26
الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية	28
أولاً- التعريف على أساس الوسيلة المستعملة لإرتكاب الجريمة (الإتجاه الفني)	29
ثانيًا- التعريف على أساس معرفة الفاعل بتقنية المعلومات (الإتجاه الشخصي)	32
ثالثًا- التعريف على أساس محل وموضوع الجريمة (الإتجاه الموضوعي)	35
الفرع الثالث: التعريف القانوني للجريمة المعلوماتية	40
أولاً: في القوانين الغربية	40
أ- تعريف القانون الأمريكي	41
ب- تعريف إتفاقية الأمم المتحدة	41
ج- تعريف القانون البلجيكي	41
ثانيًا- في القوانين العربية	41
أ- تعريف جامعة الدول العربية	41
ب- تعريف القانون السوري	42
ج- تعريف القانون السعودي	42
د- تعريف القانون القطري	42
هـ- تعريف القانون الكويتي	42

و- تعريف القانون الجزائري	43
المطلب الثاني: السمات الخاصة بالجريمة المعلوماتية	43
الفرع الأول: خصوصية الجريمة المعلوماتية من حيث مميزاتها	43
أولاً: أنها من الجرائم المنظمة والعابرة للحدود الوطنية	43
ثانيًا: أنها جريمة يصعب إكتشافها وإثباتها بسهولة	46
ثالثًا: أنها جريمة لا يتم الإبلاغ عنها في أغلب الأحيان	48
رابعًا: أنها جريمة قليلة المخاطرة وسهلة التنفيذ	49
خامسًا: أنها جريمة ذات جاذبية ومغرية لمرتكبيها	50
سادسًا: أنها جريمة غير أخلاقية	50
سابعًا: أنها جريمة تقع أثناء المعالجة الآلية للبيانات	51
الفرع الثاني: خصوصية الجرائم المعلوماتية من حيث وسائل إرتكابها وخطورة وقوعها	51
أولاً: من حيث وسائل إرتكابها	51
ثانيًا: من حيث خطورتها والأضرار الناجمة عنها	53
المبحث الثاني: تعريف المجرم المعلوماتي ودوافعه الإجرامية	56
المطلب الأول: تصنيفات المجرم المعلوماتي وأهم صفاته	57
الفرع الأول: تصنيفات المجرم المعلوماتي	57
أولاً: المجرمون الهواة والمبتدؤون	57

أ- طائفة المتحايلون *Fraudeurs _ Pranksters*	58
ب- طائفة الدخلاء أو المتسللون *Malicious Harckers*	59
ج- طائفة القراصنة – الهاكرز *Hackers* -	60
1- أصحاب القبعة البيضاء *White hats*	61
2- أصحاب القبعة الرمادية *Grey hats*	61
3- أصحاب القبعة السوداء *Black hats*	61
ثانيًا: المجرمون المحترفون	61
أ- طائفة أصحاب المشكلات الخاصة *Personal problem solvers*	62
ب- طائفة الكراكرز *Crackers*	63
ج- طائفة المخربون *Vandales*	64
الفرع الثاني: صفات وسمات المجرم المعلوماتي	66
أولاً: المجرم المعلوماتي إنسان إجتماعي بطبعه	67
ثانيًا: المجرم المعلوماتي يتميز بالذكاء والمعرفة والمهارة	68
ثالثًا: المجرم المعلوماتي شخص محترف ومتخصص	70
رابعًا: المجرم المعلوماتي شخص طبيعي	71
خامسًا: المجرم المعلوماتي شخص لا يستعمل العنف	71
سادسًا: المجرم المعلوماتي شخص يعود للإجرام	72

المطلب الثاني: دوافع المجرم المعلوماتي على المستويين الفردي والمجتمعي	73
الفرع الأول: الأسباب والدوافع الفردية (الشخصية)	73
أولاً: البحث عن التعلم والإثارة والمتعة والتحدي	74
ثانيًا: الدافع النفسي والمؤثرات الشخصية	75
ثالثًا: دافع الحقد والإنتقام	76
رابعًا: دافع كسب المال وتحقيق أرباح	78
الفرع الثاني: الأسباب والدوافع المجتمعية (الإجتماعية)	80
أولاً: التحضر والعولمة	80
ثانيًا: الحرمان والفقر والبطالة	81
ثالثًا: ضعف القانون وتطبيقاته في الجريمة المعلوماتية	81
الفَصل الثّانِي: الطبيعة القانونية للجريمة المعلوماتية	83
المبحث الأول: الأركان القانونية العامة للجريمة المعلوماتية	85
المطلب الأول: الركن الشرعي للجريمة المعلوماتية	86
الفرع الأول: مبررات مبدأ الشرعية الجنائية أمام الجرائم المعلوماتية	87
أولاً- تحقيق فكرة العدالة الجنائية	87
ثانيًا- تحقيق فكرة الردع العقابي والمساواة في العقاب	88
ثالثًا- تحقيق فكرة العلم بوجود النص الجنائي	88

رابعًا– تحقيق فكرة الأمن القومي والإقتصادي	90
خامسًا– تحقيق فكرة التوازن بين الواقع والقانون	90
الفرع الثاني: الحماية الجنائية للمال المعلوماتي	91
الفرع الثالث: دستورية الشرعية الجنائية للجريمة المعلوماتية	93
المطلب الثاني: الركن المادي للجريمة المعلوماتية	94
الفرع الأول: السلوك الإجرامي	94
الفرع الثاني: النتيجة الإجرامية	96
الفرع الثالث: العلاقة السببية ما بين السلوك الإجرامي والنتيجة	98
المطلب الثالث: الركن المعنوي للجريمة المعلوماتية	100
المبحث الثاني: أقسام الجريمة المعلوماتية	103
المطلب الأول: جرائم الحاسوب	104
الفرع الأول: مفهوم الحاسب الآلي– الكمبيوتر *Ordinateure-Computer*	104
أولاً– تعريف الحاسب الآلي	104
أ– في الفقه	104
ب– في التشريع	106
ثانيًا– خصائص ووظائف الحاسب الآلي	107
أ– بالنسبة للخصائص	107

ب- بالنسبة للوظائف	108
ثالثًا- مكونات الحاسب الآلي	109
أ- المكونات المادية للحاسوب *Hard Ware*	109
ب- المكونات المعنوية للحاسوب *Soft Ware*	110
الفرع الثاني: التطور التاريخي لجرائم الحاسوب	111
الفرع الثالث: تعريف جرائم الحاسوب وأهم صورها	14
أولاً: تعريف جرائم الحاسوب	14
ثانيًا: صور جرائم الحاسوب	115
المطلب الثاني: جرائم الإنترنت	116
الفرع الأول: تعريف شبكة الإنترنت (الشبكة المعلوماتية)	117
أولاً: في الإصطلاح	117
ثانيًا: في التشريع	119
الفرع الثاني: تاريخ نشأة الإنترنت	121
الفرع الثالث: ماهية جرائم الإنترنت وأهم صورها	124
أولاً: بداية جريمة الإنترنت	124
ثانيًا: تعريف جريمة الإنترنت	125
ثالثًا: صور جرائم الإنترنت	125

البَاب الأَوّل: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي	128
الفصل الأول: الإطار المفاهيمي لجريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي	131
المبحث الأول: مفهوم جريمة الدخول أو البقاء غير المشروع وإبراز أهم خصائصها	133
المطلب الأول: تعريف جريمة الدخول أو البقاء غير المشروع	134
الفرع الأول: التعريف الإصطلاحي للجريمة	134
أولاً: الغش المعلوماتي والتواصل غير المصرح به مع النظام	134
ثانيًا: الإستعمال والإنتفاع المعلوماتي بدون وجه حق	135
أ- موقف الهيئات الدولية:	137
1. موقف المجلس الأوروبي	137
2. موقف منظمة التعاون الإقتصادي والتنمية	137
ب- موقف التشريعات الوطنية	138
1. التشريع الكندي	138
2. التشريع الأسترالي	138
3. التشريع المصري	138
4. التشريع الإماراتي	139
5. موقف المشرع الجزائري	139

ثالثاً: القرصنة المعلوماتية	139
أ- القراصنة الهواة (الهاكرز *Hackers*)	140
ب- القراصنة المحترفون (الكراكز *Crackers*)	141
رابعًا: الإعتراض الإلكتروني والإلتقاط الهوائي	142
أ- القانون الأمريكي	146
ب- القانون البرتغالي	146
ج- القانون السوداني	147
د- القانون العماني	147
هـ- القانون السوري	147
و- القانون الإماراتي	147
ز- القانون الأردني	147
ح- القانون المصري	148
خامسًا: الإختراق *Piratage*	148
أ- إختراق الأجهزة الخادمة	149
ب- التعرض للبيانات أثناء إنتقالها	149
ج- إختراق الأجهزة الشخصية	150
الفرع الثاني: التعريف الفقهي للجريمة	151

الفرع الثالث: التعريف القانوني للجريمة	153
أولاً: في الإتفاقيات الدولية	153
أ- الإتفاقية الأوروبية للإجرام المعلوماتي	154
ب- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات	154
ثانيًا: في القوانين الوطنية	155
أ- القانون الكويتي	155
ب- القانون العماني	155
ج- القانون الإماراتي	155
هـ- القانون الأردني	156
و- القانون المصري	156
ثالثًا: موقف المشرع الجزائري	156
المطلب الثاني: خصائص جريمة الدخول أو البقاء غير المشروع	158
الفرع الأول: من حيث إعتمادها على تقنية المعلومات والوسائل التكنولوجية في إرتكابها	158
الفرع الثاني: من حيث صفة الفاعل في إرتكاب هذه الجريمة	160
الفرع الثالث: من حيث طبيعة السلوك الإجرامي المكوّن للجريمة	160
الفرع الرابع: من حيث علاقة الجريمة بالمعطيات المعالجة داخل النظام	161
الفرع الخامس: من حيث عدم مشروعية الأفعال التي ترتكب بها الجريمة	162

المبحث الثاني: ضرورة وجود نظام المعالجة الآلية للمعطيات في قيام الجريمة	165
المطلب الأول: تعريف نظام المعالجة الآلية للمعطيات	166
الفرع الأول: التعريف الفقهي للنظام المعلوماتي (نظام المعالجة الآلية للمعطيات)	166
أولاً: الإتجاه المقيد في تعريف النظام المعلوماتي	166
ثانيًا: الإتجاه الموسع في تعريف النظام المعلوماتي	167
الفرع الثاني: التعريف القانوني للنظام المعلوماتي (نظام المعالجة الآلية للمعطيات)	170
أولاً: في الإتفاقيات الدولية	170
أ- إتفاقية بودابست	170
ب- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات	172
ثانيًا: في القوانين الوطنية	173
أ- القانون الفرنسي	173
ب- القانون السوري	174
ج- القانون الأردني	175
د- القانون المصري	175
ثالثًا: موقف المشرع الجزائري من تعريف نظام المعالجة الآلية للمعطيات	177
المطلب الثاني: ضرورة خضوع نظام المعالجة الآلية للحماية الأمنية	178
الفرع الأول: أنواع النظم المعلوماتية من حيث توافرها على الحماية الأمنية	179

أولاً: الأنظمة المعلوماتية المنفتحة بدون حماية	179
ثانيًا: الأنظمة المعلوماتية المنغلقة بدون حماية	179
ثالثًا: الأنظمة المعلوماتية المنغلقة والمحمية	179
الفرع الثاني: وسائل الحماية الأمنية في النظم المعلوماتية	179
أولاً: وسائل الأمن المادية	180
ثانيًا: وسائل الأمن غير المادية	180
ثالثًا: الحماية الجنائية للنظم المعلومتية بين التضييق والتوسيع	181
أ- الإتجاه المضيق في الحماية الجنائية للنظم:	182
ب- الإتجاه الموسع في الحماية الجنائية للنظم:	183
رابعًا: موقف المشرع الجزائري من هذه المسألة	185
الفصل الثاني: أركان وعناصر جريمة الدخول أو البقاء غير المشروع والعقوبات المقررة لها	187
المبحث الأول: الأركان والعناصر القانونية لقيام جريمة الدخول أو البقاء غير المشروع	189
المطلب الأول: الركن الشرعي لجريمة الدخول أو البقاء غير المشروع	190
الفرع الأول: نطاق نص التجريم	191
أولاً: في إطار الاتفاقيات الدولية	191
أ- الإتفاقية الأوروبية لمكافحة الإجرام المعلوماتي	191
ب- الإتفاقية العربية لمكافحة الإجرام المعلوماتي	192

ثانيًا: في إطار القوانين الوطنية	192
أ- في القانون السويدي	192
ب- في القانون النرويجي	192
ج- في القانون الفرنسي	192
د- في القانون السوري	193
هـــ- في القانون المصري	193
و- في القانون الجزائري	193
الفرع الثاني: علة نص التجريم	194
المطلب الثاني: الركن المادي لجريمة الدخول أو البقاء غير المشروع	195
الفرع الأول: الصورة البسيطة لجريمة الدخول أو البقاء غير المشروع	196
أولاً: جريمة الدخول غير المشروع	196
أ- تعريف فعل الدخول غير المشروع *Accés illicite*	197
1. التعريف الفقهي لفعل الدخول غير المشروع:	198
2. التعريف القانوني لفعل الدخول غير المشروع:	199
ب- المعايير القانونية الخاصة بفعل الدخول غير المشروع:	200
1. معيار السلوك المجرم لفعل الدخول	201
1.1. الإتجاه الأول	202

2.1. الإتجاه الثاني	203
2. معيار الشروع في جريمة الدخول	207
3. معيار المحل في جريمة الدخول	208
4. معيار النتيجة في جريمة الدخول	211
أ- تعريف فعل البقاء غير المشروع *Présence illégale*	213
ثانيًا: جريمة البقاء غير المشروع	213
1. التعريف الفقهي لفعل البقاء	214
2. التعريف القانوني لفعل البقاء	214
ب- الأحكام القانونية لفعل البقاء غير المشروع	215
1. صور فعل البقاء غير المشروع	215
1.1. البقاء غير المشروع بفعل الدخول المشروع	215
2.1. البقاء غير المشروع بفعل الدخول غير المشروع	217
2. الطبيعة القانونية لفعل البقاء غير المشروع	218
3. درجة الخطورة في جريمة البقاء غير المشروع	221
ثالثًا: موقف المشرع الجزائري من جريمة الدخول أو البقاء غير المشروع	222
الفرع الثاني: الصورة المشددة لجريمة الدخول أو البقاء غير المشروع	225
أولاً: حذف المعطيات *La Suppression des données*	227

أ- الإعاقة أو العرقلة *Entrave*:	228
ثانيًا: تغيير المعطيات *La modification des données*	229
ثالثًا: تخريب نظام إشتغال المنظومة *L'altération du fonctionnement de système*	229
ب-الإخلال أو الإرباك *Perturber*	230
المطلب الثالث: الركن المعنوي لجريمة الدخول أو البقاء غير المشروع	231
الفرع الأول: من حيث الصورة البسيطة للجريمة	231
الفرع الثاني: من حيث الصورة المشددة للجريمة	237
المبحث الثاني: الإجراءات العقابية والردعية المقررة لجريمة الدخول أو البقاء غير المشروع	239
المطلب الأول: العقوبات الأصلية والعقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع	240
الفرع الأول: العقوبات الأصلية لجريمة الدخول أو البقاء غير المشروع	240
أولاً: عقوبة الشخص الطبيعي	240
أ- بالنسبة لعقوبة الصورة البسيطة	240
ب- بالنسبة لعقوبة الصورة المشددة	241
ثانيًا: عقوبة الشخص المعنوي	242
الفرع الثاني: العقوبات التكميلية لجريمة الدخول أو البقاء غير المشروع	245
أولاً: المصادرة *La confiscation*	246

ثانيًا– الغلق *La fermeture*	246
أ– إغلاق المواقع *Les sites*	247
ب– إغلاق المحل أو مكان الإستغلال *Lieux d'exploitation*	247
المطلب الثاني: أحكام عقوبة الإشتراك والشروع في جريمة الدخول أو البقاء غير المشروع	247
الفرع الأول: عقوبة الإشتراك في الجريمة (الإتفاق الجنائي)	250
الفرع الثاني: عقوبة الشروع في الجريمة (المحاولة الجنائية)	254
البَاب الثّانِي: جرائم المساس بالمعطيات المعالجة آليًا والموجودة داخل وخارج النظام المعلوماتي	258
الفصل الأول: جريمة التلاعب بالمعلومات الموجودة داخل النظام المعلوماتي	260
المبحث الأول: مفهوم جريمة التلاعب المعلوماتي	262
المطلب الأول: تعريف جريمة التلاعب المعلوماتي وأهم خصائصها	263
الفرع الأول: التعريف بالجريمة	263
الفرع الثاني: خصائص الجريمة	264
أولاً– أنها من جرائم الدخول المسموح به	264
ثانيًا– أنها من جرائم الوسيلة الحاسوباتية	264
ثالثاً– أنها من جرائم الدخول غير المسوح به	265
رابعًا– أنها من جرائم الإعتداء على المعلومات	265

خامساً- أنها من الجرائم ذات النشاط الإيجابي	265
المطلب الثاني: الطبيعة القانونية لجريمة التلاعب المعلوماتي	266
الفرع الأول: تغيير الحقيقة المعلوماتية بإحدى الطرق المنصوص عليها	266
الفرع الثاني: المعلومات داخل النظام المعلوماتي والجديرة بالحماية الجنائية	267
الفرع الثالث: ضرورة إستحداث نصوص خاصة لحماية المعلومات داخل النظام المعلوماتي	268
المبحث الثاني: أركان جريمة التلاعب المعلوماتي والعقوبات المقررة لها	270
المطلب الأول: أركان جريمة التلاعب المعلوماتي	271
الفرع الأول: الركن الشرعي للجريمة	271
أولاً- بالنسبة لنص التجريم	271
ثانيا- بالنسبة لعلة التجريم	272
الفرع الثاني: الركن المادي للجريمة	272
أولا- السلوك المجرم	273
أ- فعل الإدخال *L'introduction*	273
ب- فعل الإزالة (المحو) *L'éffacement*	276
ج-فعل التعديل *Modification*	279
ثانيًا- النتيجة الإجرامية	281

الفرع الثالث: الركن المعنوي للجريمة	282
المطلب الثاني: العقوبات المقررة لجريمة التلاعب المعلوماتي	284
الفرع الأول: بالنسبة للعقوبات الأصلية	285
الفرع الثاني: بالنسبة للعقوبات التكميلية	286
الفصل الثاني: جريمة الإعتداء على المعطيات الموجودة خارج النظام المعلوماتي	289
المبحث الأول: جريمة التعامل غير المشروع في معطيات النظام المعلوماتي	291
المطلب الأول: أركان جريمة التعامل غير المشروع في معطيات النظام المعلوماتي	292
الفرع الأول: الركن الشرعي للجريمة	292
أولاً- بالنسبة لنص التجريم	292
ثانيًا- بالسنبة لعلة التجريم	294
أ- الناحية الأولى	294
ب- الناحية الثانية	294
الفرع الثاني: الركن المادي للجريمة	295
أولاً: التعامل في معطيات صالحة لإرتكاب جريمة ماسة بنظام المعلومات	295
أ- التصميم *La Comception*	296
1. إصطناع البرامج *Logiciel artificiel*	297
2. تقليد البرامج *Logiciel traditionnel*	298

3. إستنساخ البرامج *Clonage de logiciel*	299
ب- البحث *La Recherche*	301
ج- التجميع *Le Rassemblement*	302
د- التوفير *Metter à disposition*	303
و- الإتجار *La Commercialisation*	304
هـ- النشر *La Diffusion*	305
1. الجلب والإستيراد *Importer*	306
2. البيع *Vendre*	307
3. التداول *Commerce*	308
ثانيًا- التعامل غير المشروع في معطيات متحصلة من الجريمة	308
أ- الحيازة *La possession*	309
ب- الإفشاء *La Révelation*	312
ج- النشر *La Diffusion*	315
د- الإستعمال *Faire un Usage*	316
الفرع الثالث: الركن المعنوي للجريمة	317
المطلب الثاني: العقوبات المقررة لجريمة التعامل غير المشروع في معطيات النظام	319
الفرع الأول: بالنسبة للعقوبات الأصلية	319

أولاً: العقوبات المقررة للشخص الطبيعي	319
أ- العقوبة البسيطة للجريمة	319
ب- العقوبة المشددة للجريمة	320
ثانيا: بالنسبة للعقوبات المقررة للشخص المعنوي	322
ثالثا: بالنسبة لعقوبة الإشتراك في الجريمة والشروع فيها	322
أ- بالنسبة لعقوبة الإشتراك	322
ب- بالنسبة لعقوبة الشروع	322
الفرع الثاني: بالنسبة للعقوبات التكميلية	323
المبحث الثاني: جرائم مقدمي خدمة الإنترنت	325
المطلب الأول: مفهوم مقدمي خدمات الإنترنت	327
الفرع الأول: تعريف مقدمي خدمات الإنترنت	327
أولاً: التعريف الإصطلاحي	328
أ- الوسيط الإلكتروني	328
ب- متعهد الإيواء الإلكتروني	329
ج- مقدمي خدمة الإنترنت	329
ثانيًا: التعريف الفقهي	330
ثالثًا: التعريف القانوني	331

أ- في الإتفاقيات الدولية	331
ب- في القوانين الوطنية	332
الفرع الثاني: طبيعة الوظيفة التقنية لمقدمي الخدمات وإلتزاماتهم القانونية	333
أولاً: طبيعة الوظيفة التقنية لمقدمي الخدمات	333
ثانيًا- الإلتزامات القانونية لمقدمي خدمات الإنترنت	335
أ- أهم الإلتزامات التي جاءت في التشريعات المقارنة	335
ب- إلتزامات مقدمي خدمة الإنترنت في التشريع المصري	337
ج- إلتزامات مقدمي خدمات الإنترنت في التشريع الجزائري	338
المطلب الثاني: أساس المسؤولية الجنائية لمقدمي خدمات الإنترنت	340
الفرع الأول: الإتجاه الأول القائل بعدم مسؤولية المزود أو الوسيط أو الخادم	341
الفرع الثاني: الإتجاه الثاني القائل بتقرير مسؤولية المزود أو الوسيط أو الخادم	342
أولاً: مساءلة مقدمي الخدمة طبقًا لأحكام المسؤولية المفترضة	342
ثانيًا: مساءلة مقدم الخدمة طبقاً للأحكام العامة للمسؤولية الجنائية	344
الفرع الثالث: موقف المشرع الجزائري من هذه المسالة	346
المطلب الثالث: تقرير المسؤولية الجنائية لمقدمي خدمات الإنترنت	348
الفرع الأول: أركان جريمة الإيواء المعلوماتي	348
أولاً: الركن الشرعي لجريمة الإيواء المعلوماتي	348

أ- بالنسبة لنص التجريم	348
1. في التشريع الفرنسي	348
2. في التشريع المصري	350
3. في التشريع الجزائري	351
ب- بالنسبة لعلة التجريم	353
ثانيا: الركن المادي للجريمة	354
أ- الشرط المفترض	354
ب- النشاط الإجرامي	354
ج- محل النشاط الإجرام	355
د- النتيجة الإجرامية:	356
ثالثًا: الركن المعنوي للجريمة	357
الفرع الثاني: العقوبات المقررة لجريمة الإيواء المعلوماتي	358
أولاً: العقوبات الأصلية لجريمة الإيواء المعلوماتي	358
أ- بالنسبة للشخص الطبيعي	358
1. في التشريع الفرنسي	358
2. في التشريع المصري	359
3. في التشريع الجزائري	360

ب- بالنسبة للشخص المعنوي	360
ج- تشديد العقوبة	361
ثانيًا: العقوبات التكميلية لجريمة الإيواء المعلوماتي	361
ثالثًا: عقوبة الشروع والإشتراك في جريمة الإيواء المعلوماتي	362
أ- الشروع في جريمة الإيواء المعلوماتي	362
ب- الإشتراك في جريمة الإيواء المعلوماتي	362
خـــــاتمـــة: (النتائج، التوصيات، الإقتراحات)	364
الملاحـــــق	373
قائمة المصادر والمراجع	450
الفهـــــرس	483

ملخص :

لقد أحدثت ثورة المعلومات الإلكترونية والتكنولوجية تغييرا جذريا في المفاهيم العامة للنظرية العامة للجريمة عموما، حيث أصبح من الضروري إعادة النظر في تلك المفاهيم والأحكام التقليدية التي كان ينظر من خلالها إلى الجريمة والمسؤولية الجنائية للمجرم، وهذا لاسيما مع ظهور نوع جديد من الإجرام يطلق عليه اليوم بالجريمة المعلوماتية، لذلك فإن هذه الدراسة تتجه إلى تحديد الإطار الموضوعي الذي يواجه به المشرع الجنائي الجزائري الجريمة المعلوماتية ومرتكبيها، وهذا إلى جانب كل من التشريع الفرنسي وكذا نظيره التشريع المصري.

الكلمات المفتاحية: الجريمة المعلوماتية – جرائم تقنية المعلومات – جرائم الإنترنت – جرائم الحواسيب – المجرم المعلوماتي.

Résumé :

La révolution de l'information électronique et technologique a radicalement changé les concepts généraux de la théorie générale du crime en général, car il est devenu nécessaire de reconsidérer ces concepts et décisions traditionnels à travers lesquels le crime et la responsabilité pénale du criminel ont été envisagés, en particulier avec l'émergence. D'un nouveau type de crime appelé aujourd'hui l'informatique criminelle, cette étude tend donc à définir le cadre objectif dans lequel le législateur pénal algérien affronte la criminalité informationnelle et ses auteurs, en plus de la législation française et de son homologue égyptien.

Mots clés: *Criminalité informatique − Criminalité informatique − Cybercriminalité − Criminalité informatique −Le criminel de l'information.*

Abstruct :

The electronic and technological information revolution has radically changed the general concepts of the general theory of crime in general, as it has become necessary to reconsider those traditional concepts and rulings through which crime and the criminal responsibility of the criminal were viewed, especially with the emergence of a new type of crime called today crime Informatics, therefore, this study tends to define the objective framework in which the Algerian criminal legislator confronts information crime and its perpetrators, in addition to both the French legislation and its Egyptian counterpart.

Key Words: *Information crime − It crime − Internet crime − Computer crime − The information criminal.*