وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم: القانون العام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

آليات مكافحة الجريمة الإلكترونية على المستويين الدولي و الوطني

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق.

التخصص: قانون جنائي وعلوم جنائية

من إعداد الطالب(ة):

بقدار شيماء

تحت إشراف الأستاذ(ة):

أ / آيت بن أعمر غنية

أعضاء لجنة المناقشة

الأستاذة:	مرابط حبيبة	رئيسا
الأستاذة:	آيت بن أعمر غنية	مشرفا مقررا
الأستاذة:	علاق نوال	مناقشا

السنة الجامعية: 2023/2022

نوقشت يوم : 2023/06/15

كلمة شكر

بداية الشكر لله عز وجل الذي وفقنا لإتمام هذا العمل المتواضع
كما أشكر الأستاذة المؤطرة " آيت بن أعمر غنية " والتي ساعدني كثيرا في إعداد مذكرتي ، جعلها الله في ميزان حسناته يوم لا ظل إلا ظله.
كما أتقدم بالشكر الجزيل إلى أعضاء لجنة المناقشة الذين تشرفت بقبولهم مناقشة هذه المذكرة.
والشكر موصول لجميع أساتذة كلية الحقوق والعلوم السياسية عبد الحميد بن باديس جامعة مستغانم من درسني ومن لم يدرسني
وختاما أشكر كل من ساهم معي وساعدني في إنجاز هذا العمل من بعيد أوقريب ولو بالكلمة الطيبة والدعم المعنوي

إهداء

أهدي ثمرة جهدي وتعبي إلى :

الوالدين الكريمين أطال الله في عمرهما

الأخوة والأخوات أدامهم الله نعمة لا تزول

زملاء درب الدراسة أنار الله لهم الطريق

إلى كل طالب علم

قائمة المختصرات

قائمة المختصرات

ق.إ.ج: قانون الإجراءات الجزائية

ق.ع: قانون العقوبات

ق.م: قانون المدني

ج.ر: الجريدة الرسمية

ص: صفحة

ص ص: صفحة من إلى

مقدمة

مقدمة

نتيجة للتطور التكنولوجي في مجال المعلوماتية، نشـأت انماط مسـتحدثة من الجرائم التي تسـمى بالجريمة الإلكترونية أو الرقمية، مما نتج عنها الإهتمام الدولي والوطني من خلال خلق و إستحداث آليات قانونية وتكاثف الجهود لمواجهتتها.

لقد برز الإهتمام الدولي و الوطني بالجريمة الإلكترونية من خلال تفعيل آليات للحد منها تمثلت في إتفاقيات أبرزها ما خرجت به الأمم المتحدة من توصـيات و كذا المجلس الأروبي من خلال اتفاقية بودابسـت 2001 لمكافحة الجريمة المعلوماتية و القانون العربي النموذجي الإسترشادي بخصوص مكافحة الجرائم الإلكترونية الذي أصدرته الجامعة العربية.

كما أن المشرع الجزائري من نصوصه القانونية لمواجهة الجريمة الإلكترونية تماشيا مع تطور هذه الجرائم في المجتمع.

ومن هنا تبرز أهمية دراسـة هذا الموضـوع من الناحيتين العلمية والعملية معا حيث يمكن إجمال هذه الأهمية من الناحية العلمية في إنتشـار جريمة الإلكترونية كنوع مسـتحدث من الجرائم لابد من التطرق إليه، أما من الناحية العملية فيمكن القول أن إنتشـار هذه الجرائم في مختلف المجتمعات عامة والمجتمع الجزائري بصـفة خاصـة أصـبح يهدد الأمن الإلكتروني.

بالنسبة لحدود هذه الدراسة فقد رأينا تحديدها زمنيا بشكل أساسي في إطار القوانين بدءا من المؤتمر الدولي الأول لحقوق الإنسـان الخاص بأثر التقدم التكنولوجي على حقوق الإنسـان مؤتمر طهران (1968)اتفاقية طهران و اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية إلى غاية التشـريع الوطني الجزائري، حيث قامت الجزائر بتعديل قانون العقوبات بموجب القـانون رقم 04-15 المؤرخ في 10 نوفمبر2004، والـذي أدخـل عليـه تعـديـل في 20ديسـمبر2006، والذي يتضـمن قانون العقوبات الجزائري القسـم السـابع 394 إلى 394

مكرر 6، و التي تناولت تحت عنوان المســـاس بأنظمة المعالجة الآلية للمعطيات ضـــمن المواد من 394 إلى 394 مكرر 6،

كما يتحدد مكان دراستنا في بعض التشريعات الدولية و الوطنية منها السعودية ومصر والجزائر وكذا الغربية منها التشريع الفرنسي ، بالإضافة إلى التشريع الأمريكي، ذلك في بعض جوانب هذه الدراســة ، دون إهمال موقف الجامعة العربية و مجلس الأروبي ، وهذا راجع لأهمية هذا الموضـوع على المسـتوى الدولي ، مع الإشـارة أن نطاق الدراسـة ينحصـر أكثر في إطار آليات مكافحة الجريمة الإلكترونية في التشريع الدولي والوطني.

وما دفعنا إلى إختيار هذا الموضــوع أســباب متعددة منها الذاتية والموضــوعية، أما عن الأسباب الذاتية تكمن في الرغبة الشخصية لمعالجة هذا الموضوع وميولنا لمعرفة الأسباب والدوافع التي أدت إلى إتســاع دائرة هذه الجرائم على المســتوى الدولي و الوطني، وكذلك محاولة إثراء المكتبة القانونية بمثل هذه المواضيع.

أما عن الأسباب الموضـوعية فإن الإنتشـار الرهيب لمثل هذه الجرائم يؤدي إلى ضـرورة معرفة الأســباب ومحاولة تدارك النصــوص القانونية التي تعاقب على ارتكابها لتكون رادعا قويا يحول بين الأشــخاص وتلك الأفعال، كما أنه من بين الأســباب الموضــوعية الأخرى إحجام غالبية الطلبة عن تناول مثل هذه المواضـيع ونقص الدراسـات في مجالها مع أنها من تعتبر من القضايا التي تهدد استقرار على مستويين الدولي و الوطني.

ولبلوغ أهداف الدراســة والإجابة على التســاؤلات إعتمدت على دراســات أنجزت من قبل متمثلة في كتب قانونية متخصــصــة وعلى مقدمتها كتاب عبد العال الدريبي، محمد صــادق اســماعيل المتخصــص في الجرائم الإلكترونية إضــافة لمجموعة من الكتب و البحوث القانونية تطرقت لموضوع الجريمة الإلكترونية بشكل عام، أو في شكل نقاط.

خلال إعداد هذه الدراسـة واجهتنا صـعوبات، كان من أبرزها قلة المراجع في كلية الحقوق لجامعة مستغانم في موضوع دراستنا خاصة الجزائرية منها.

وعليه من خلال ما تقدم ارتأينا طرح الإشكالية التالية:

ما مدى تكاثف التعاون الدولي و الوطني في مواجهة الجريمة الإلكترونية؟

وللإجابة على هذا الإشكال فقد اعتمدنا على المنهج الوصفي لوصف الجريمة الإلكترونية على سبيل المثال، والمفاهيم المتعلقة بالموضوع وإعطائها الدلالات العلمية ومن ثم الوصول إلى تفسيرات منطقية متعلقة بموضوع الدراسة، كما اعتمدنا على المنهج التحليلي في تحليل بعض النصوص القانونية وإسقاطها على موضوع البحث.

الحديث عن آليات مكافحة الجريمة الإلكترونية على مستويين الدولي و الوطني يستوجب تحديد مفهومها وهذا من خلال التطرق إلى تعريفها وتحديد أركانها ، وضرورة تبيين الأحكام والجزاءات المقررة لها.

لمعالجة كل هذه النقاط ارتأينا تقسيم خطة بحثنا إلى فصلين، تطرقنا في الفصل الأول إلى ماهية الجريمة الإلكترونية من خلال المبحثين، المبحث الأول تناولنا فيه مفهوم الجريمة الإلكترونية ، أما المبحث الثاني خصائص و أنواع الجريمة الإلكترونية.

وتطرقنا في الفصل الثاني إلى آليات مكافحة الجريمة الإلكترونية من خلال مبحثين أيضا، المبحث الأول المواجهة الدولية و الوطنية للجريمة الإلكترونية ، والمبحث الثاني القواعد الإجرائية للتحقيق في الجريمة الإلكترونية .

الفصل الأول

ماهية الجريمة الإلكترونية

الفصل الأول: ماهية الجريمة الإلكترونية

لقد أفرزت ثورة الإتصـالات والمعلومات وسـائل جديدة للبشـرية تجعل الحياة أفضـل من ذي قبل؛ غير أنها فتحت الباب على مصـراعيه لظهور صـور من السـلوك المتنحرف اجتماعيا التي لم يكن من الممكن وقوعها في الماضي.

فمن جهة أولى أتاحت نظم الكمبيوتر (الحاسـوب) ظهور صـور جديدة من الجرائم لم تكن موجودة في الماضـي؛ وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات؛ ومن جهة ثانية أتاحت هذه النظم الفرصـة لارتكاب الجرائم التقليدية بطرق غير تقليدية ؛ كما هو الشـأن بالنسـبة لجرائم الغش وإتلاف وإفسـاد المعلومات المخزنة في قواعد المعلومات[1]، ومن ثم ينقسـم هذا الفصـل إلى مبحثين، تناول المبحث الأول مفهوم الجريمة الإلكترونية، وإختص المبحث الثاني بالحديث عن خصائص الجريمة الإلكترونية وطبيعتها.

[1]–عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة، ط 01، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص39.

المبحث الأول: مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية لها مسميات كثيرة، فهى جريمة الكومبيوتر والإنترنت والبعض الآخر يطلق عليها الجريمة المعلوماتية، وهي جريمة إساءة إستخدام تقنية المعلومات، وهناك من يطلق عليها – الجرائم المستحدثة – .

– والذى يتصدى لتعريف هذه الجريمة ، قد يتناول تعريفها من زاوية فنية أو زاوية قانونية والقائلون بالتعريف الفني يميلون إلى القول بأن الجريمة المعلوماتية هي (نشاط إجرامى تستخدم فيه تقنية الحاسب الآلى بطريقة مباشرة أوغير مباشرة كوسيلة أوهدف لتنفيذ الفعل الإجرامي المقصود).

– ويرى هذا الجانب الفقهى أن تعريف جرائم الحاسب الآلى من الناحية القانونية[1]، ولدراسة هذه الجريمة يتطلب تعريف الجريمة الإلكترونية(المطلب الأول)، وبيان أطراف ودوافع لارتكاب الجريمة الإلكترونية(المطلب الثاني).

المطلب الأول: تعريف الجريمة الإلكترونية

من خلال هذا المطلب سوف نعرج بتعريف الجريمة الإلكترونية من خلال الفرع الأول ثم أركانها الفرع الثاني.

الفرع الأول: تعريف الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية "بإساءة استخدام الكمبيوتر، ثم احتيال الكمبيوتر"، "فالجريمة المعلوماتية"، بعدها "جرائم الكمبيوتر"، و"الجريمة المرتبطة

[1]–عبد الفتاح البيومي حجازي، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي، د،ط، دار الكتب القانونية، مصر، 2007، ص20.

بالكمبيوتر"، ثم "جرائم التقنية العالية"، إلى "جرائم الهاكرز"، "فجرائم الانترنت"، وأخيرا "السيبر كرايم.

وقد حاولت العديد من الأعمال الأكاديمية تعريف" الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية، مهتمة بتعريف دقيق للمصطلح، فمن أصل حوالي 200 مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، استخدم أقل من خمسة في المائة كلمة "الجرائم الإلكترونية" في العنوان أوفي السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو مصطلح "جرائم الكمبيوتر"، و"الإتصالات الإلكترونية"، و "تكنولوجيا المعلومات"، أو"الجريمة ذات التقنية العالية، وفي الممارسة العملية فإن العديد من هذه المفردات من التشريعات التي تم إنشاؤها للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية، مثل الدخول غير المصرح به لنظام الكمبيوتر، أوالتدخل في نظام الكمبيوتر أوالبيانات، حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "الجريمة الإلكترونية" في عنوان فعل أوقانون مثل: " قانون الجرائم الإلكترونية .

وتعرف الجريمة بأنها: "الارتكاب المتعمد لفعل ضار من الناحية الإجتماعية أوفعل خطير محظور يعاقب عليه القانون، وتمثل الجرائم الإلكترونية مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أوأجهزة إلكترونية أوشبكة الانترنت أوتبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أوالتحقيق فيها ومقاضاة فاعليها، يقول الدكتور محمد صالح العادلي": "الجريمة الإلكترونية هي الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، أوهي المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات".

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: "الجريمة التي : تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا"، وقد اتجه جانب كبير من الفقهاء إلى

اعتماد التعريف الذي تبنته منظمة التعاون الاقتصـــادي والتنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983[1] من أنها: "كل ســـلوك غير مشـــروع، أوغير أخلاقي، أوغير مصـــرح به، يتعلق بالمعالجة الآلية للبيانات أونقلها"، وهو تعريف تبنى أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أونقلها .

ويمكن تعريف الجريمة الإلكترونية بأنها كل أشـكال السـلوك غير المشـروع، والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالانترنت، والتي تمس به أوبمحتوياته أوبالعمليات التي تتم بواسطته، بغرض إلحاق الضـرر بالضـحية أوالكسـب المادي أوغير ذلك من الأغراض، من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها[2].

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال إستخدام الأجهزة الإلكترونية ينتج منها حصـول المجرم على فوائد مادية أومعنوية مع تحميل الضـحية خسـارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصـنة من أجل السـرقة أوإتلاف المعلومات الموجودة في الأجهزة، ومن تم ابتزاز الأشخاص بإستخدام تلك المعلومات.

فقد انقســم أنصــار تعريف الجريمة من الجانب التقني والفني فالبعض اســتند إلى موضــوع الجريمة والبعض الأخر إلى وسيلة الجريمة.

– أهم التعريفات التي استندت على موضوع الجريمة

ويذهب أصـــحاب هذا الإتجاه الفقهي إلى التركيز على الجانب الموضـــوعي في تعريف الجريمة الإلكترونية بإعتبار أن هذه الجريمة ليسـت الجريمة التي يسـتخدم الحاسـب الألي كأداة في إرتكابها حسب بل تقع على الحاسب الألي أوفي داخل نظامه.

فعرفت الجريمة الإلكترونية من قبل أنصــار هذا الإتجاه بأنها (نشــاط غير مشــروع لنســخ أوتغيير أوحذف أوالوصــول الى المعلومات المخزونة داخل الحاســب أوالتي تحول عن طريقه)

[1]-ياسمينة بونعارة، الجريمة الإلكترونية، مجلة المعيار، العدد39، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، 2015، ص276.

[2]– المرجع نفسه، ص 278.

وعرفت كذلك بأنها غش معلوماتي ينصـــرف إلى كل ســـلوك غير مشـــروع يتعلق بالمعلومات المعالجة ونقلها.

– أهم التعريفات التي استندت على وسيلة الجريمة:

– إن أنصـــــار هذا الإتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق بإســـــتخدام الكمبيوتر كوسيلة لإرتكاب الجريمة، وبالتالي تعرف على أنها «فعل إجرامي يستخدم الكمبيوتر في إرتكابه كأداة رئيســـية كما تعرف بأنها كل أشـــكال الســـلوك غير المشـــروع الذي يرتكب باســـتخدام الحاســـوب»، وكذلك تعرف بـأنها «الجريمـة التي تلعب فيها البيانـات الكمبيوتريـة والبرامج المعلوماتية دورا رئيســـا» وإنها كل فعل أوإمتناع من شـــأنه الإعتداء على الأمواج المادية أوالمعنوية يكون ناتجا بطريقة مباشـرة أوغير مباشـرة عن تدخل التقنية المعلوماتية»، يعتبر هذا التعريف الأخير الرأي الراجح لتبنيه من قبل العديد من الباحثين والدارسين نظرا لشمولية بحيث يعبر عن الطابع التقني أوالمميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها : الجريمة التي تلعب فيها البيانات الحاســـوبية والبرامج المعلوماتية دورا رئيســـيا ، وقد اتجه جانب كبير من الفقهاء إلى إعتماد التعريف الذي تبنته منظمة التعاون الاقتصـادي والتنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983 من أنها كل سلوك غير مشروع، أوغير أخلاقي، أوغير مصرح به يتعلق بالمعالجة الآلية للبيانات أونقلها»، وهو تعريف تبنى أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الألية للبيانات أونقلها، كما يعرفها خبراء منظمة التعاون الاقتصـــادي والتنمية OECD بأنها « كل ســـلوك غير مشـــروع أوغير أخلاقي أوغير مصرح به يتعلق بالمعالجة الألية للبيانات أونقلها « ويعرفها الفقيه الفرنسي Vivant بأنها مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب .

وقد جاء في توصـيات مؤتمر الأمم المتحدة العاشـر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا ســنة 2000 تعريف الجريمة الإلكترونية بأنها أية جريمة يمكن إرتكابها بواســطة نظام

حاسوبي أوشبكة حاسوبية، أوداخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية. جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية.

أما التعريف الدولي للجريمة الإلكترونية فهو يعتمد في الغالب على الغرض من إستخدام المصطلح: فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر وأنظمة تمثل جوهر الجريمة الإلكترونية كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أومالية أوضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر[1].

-أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة بتكنولوجيات الإعلام والإتصال فإنه يعرفها بأنها: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أويسهل إرتكابها عن طريق منظومة معلوماتية أونظام للإتصالات الإلكترونية». وهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أووسيلة أودعامة لجرائم تقليدية، ولولا هذه النظم المعلوماتية وشبكات الإتصالات ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم.

على خلاف المشرع الفرنسي الذي لم يعطي تعريفا للجريمة الإلكترونية، فإن المشرع الجزائري قد إصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب المادة الثانية من القانون 09-04 على أنها «جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أوأية جريمة ترتكب أويسهل إرتكابها عن طريق منظومة معلوماتية أونظام للاتصالات الإلكترونية.

[1]-بوضياف اسمهان، الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، مسيلة، الجزائر، 2018، ص ص 351،352.

ويلاحظ على هذا التعريف ما يلي:

أولا: أن المشـــرع الجزائري قد إعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكترونية، وثانيها معيار موضوع الجريمة المســـاس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أوالركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانيا: كما حدد المشـــرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أويســـهل إرتكابها عليه، وهذا ما يوســـع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري[1].

الفرع الثاني: أركان الجريمة الإلكترونية

لابد لقيام الجريمة الإلكترونية من أركان واجب توافرها وهذا ما ســـوف نتناوله من خلال الاتي ذكره:

البند الأول: الركن القانوني للجريمة الإلكترونية

تستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بهذا الخصوص، فقد بذلت هيئة الأمم المتحدة بالإضـــافة إلى المجلس الأوروبي جهودا مضـــنية لاقناع الدول بضـرورة وضـع التشـريعات الملائمة لمواجهة جرائم المعلوماتية وتعزيز التعاون الدولي في هذا المجال ذلك التوصـــية رقم (89) المتعلقة بالجرائم المرتبطة بالحاســـب الآلي التي أصـــدرها المجلس وكمثال على الأوروبي والإتفاقية التي تخص الإجرام المعلوماتي أوالسيبيري الموقعة في نوفمبر سنة 2001 ببودابست و دخلت حيز التنفيذ في جويلية سنة 2004 ، وصادقت عليها بعض أعضـــاء المجلس الأوروبي بالإضـــافة إلى كندا و اليابان والولايات المتحدة الأمريكية وجنوب إفريقيا حيث جعل منها وثيقة دولية ملزمة بالنسبة للدول الاطراف فيها.

[1]– بوضياف اسمهان، المرجع السابق، ص353.

وتواجه المشـــرع عند تنظيمه لمجال الحماية الجنائية من مخاطر جرائم المعلوماتية جملة من العراقيل تتمثل أولاها في مدى إمكانية ملاءمة النصـــوص التقليدية مع هذا الطابع المســـتجد من الجرائم حيث أن الاخلال بمبدا الشـرعية والوقوع في التفاسـير الموسـعة يخل بمبادئ القانون الجنائي ، وقد ظهرت إختلافات في تقدير المشـــرعين بين من يرى ضـــرورة وضـــع نصـــوص جديدة خاصـــة بجرائم المعلوماتية أوتكييف النصـــوص القديمة مع هذه الجرائم ، ومن يرى أن النصـــوص التقليدية تفي بالغرض ولا حاجة لتضـــييع الوقت بالتشريع لجرائم عادية ترتكب بوسائل تقنية متطورة.

فبينما يرى البعض أن إدراج النصـوص المجرمة للأفعال التي تقع بواسـطة جهاز الحاسـب الآلي أو الأنترنت أو تقع اعتداءا عليهما ضـــمن النصـــوص القديمة يخل بالبنيان القانوني للجريمة من حيث أن المشـرع يتطلب في الجرائم التقليدية سـلوكا محددا يتحقق به الركن المادي للجريمة ، فضـــلا عن الطابع المادي للنتيجة الإجرامية مما لا يتوافق وطبيعة المحل غير الملموس في الجرائم المعلومـاتيـة ، في حين أن البعض الآخر يـذهـب إلى إعتبـار أن الجرائم المعلوماتية والمرتبطة بالتكنولوجيات الحديثة ما هي إلا جرائم عادية استعمل فيها الحاسب الآلي كوسـيلة لإرتكاب الجريمة، وأن المطلوب من المشـرع هو العقاب عليها بواسـطة النصـوص التقليدية .

ولأن مراحل إرتكاب هذه الجرائم تتســـم بتعقيدها فالمطلوب من المشـــرع إلمـاما كبيرا بالمصـطلحات التقنية ومعرفة دقيقة للأفعال التي من شـأنها أن تشـكل جريمة معلوماتية ، حتى لا يتم المساس بحرية تلقي و تبادل المعارف و الحفاظ على الحق في إحترام الحياة الخاصة[1].

جرم المشرع الجزائري بعد صدور القانون 04/15 المعدل والمتمم للأمر 66/156 المتضمن قانون العقوبات (القانون 04/15) ، 2015 بعض الإعتداءات التي يكون محلها نظام المعالجة

[1]– معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشـــريع الجزائري و التشـــريع المقارن، مذكرة لنيل شـــهادة ماجســـتير في العلوم القانونية، تخصـــص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم الســـياســـية، باتنة، 2011،2012، ص25.

الآلية للمعطيات[1] ، وما يســـمى بالمال المعلوماتي وكل هذه الجرائم وإن اختلفت في أركانها وعقوبتها إلا أن ما يجمعها هو أنها تحقق حماية جنائية لنظم المعالجة الآلية للمعطيات ويعرف نظام المعالجة الآلية للمعطيات بأنه كل مركب يتكون من وحدة أومجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرنامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتائج معينة وهي معالجة المعطيات وعليه يكون هذا المركب خاضع للحماية التقنية وذلك ضمن أحكام القسم السابع مكرر منه (المواد من 394 مكرر إلى 394 مكرر 8 الأمر 66/156 المتضمن قانون العقوبات المعدل والمتمم[2]).

[1]–تنص المادة رقم 02 من قانون رقم 09 – 04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإسلام والاتصال ومكافحتها:

يقصد في مفهوم هذا القانون بما يأتي :

1 – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أويسهل ارتكابها عن طريق منظومة معلوماتية أونظام للاتصالات الإلكترونية

ب – منظومة معلوماتية : أي نظام منفصل أومجموعة من الأنظمة المتصلة ببعضها البعض أوالمرتبطة، يقوم واحد منها أوأكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

ج– معطيات معلوماتية: أي عملية عرض للوقائع أوالمعلومات أوالمفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

د – مقدمي الخدمات :

1 – أي كيان عام أوخاص يقدم المستعملي خدماته. القدرة على الاتصال بواسطة منظومة معلوماتية و/أونظام للاتصالات.

2 –و أي كيان آخر يقوم بمعالجة أوتخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أوالمستعمليها.

هـ – المعطيات المتعلقة بحركة السيرة 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 الإتصالات الإلكترونية : أي تراسل أوإرسال أواستقبال علامات أوإشارات أوكتابات أو صور أو أصوات أومعلومات مختلفة بواسطة أي وسيلة إلكترونية.

[2]–جعود سعاد،الحماية الجزائية لتكنولوجيات الإعلام و الإتصال في التشريع الجزائري–دراسة مقارنة،مجلة الرسالة للدراسات والبحوث الإنسانية، العدد04،جامعة العربي التبسي، الجزائري،2022، ص219.

البند الثاني: الركن المادي للجريمة الإلكترونية

يكون للركن المادي للجريمة الإلكترونية صـــورتين، الأولى متمثلة في الإعتداء على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الإعتداء الأول وهو الدخول والبقاء غير المشروع في نظام المعالجة الآلية وتنطوي تحت هذا النوع أفعال ؛ فعل الدخول والبقاء و عرقلة أوالتعطيل ، أما النوع الثاني متمثل في الإعتداء العمدي على نظام المعالجة الآلية للمعطيات، وتندرج تحته أفعال فعل الإدخال والمحو و التعديل والصـــورة الثانية متمثلة في الإعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي[1].

ولتكون الجريمة لا بد من ارتكاب فعل مادي محسوس أوامتناع عن إتيان عمل إذ لا بد لهذه النية يعاقب عليه القانون، فالجريمة ليســـت مجرد وجود نية جرمية أن تجد في كيان مادي محسوس، هذا السلوك المادي المحسوس الذي ينص عليه قانون هو ما يعرف بالركن المادي للجريمة، والذي يشكل شرطا أساسيا للبدء في عملية البحث عن توافر الجريمة من عدمه.

إن ضرورة أن يكون هناك تجسيد خارجي لما يدور في الأذهان من رغبات وأفكار جرمية له ما يبرره من جهة صعوبة الغور في أعماق النفس البشرية لإثبات حالة نسية مجردة، ومن جهة أخرى فإن مجرد الرغبات والنوايا الدفينة التي لا تحمل اعتداء ولا تنتج ضـــررا للغير لا مبرر لبحثها وترتيب العقاب عليها، ولتمام الركن المادي لا بد من توافر عناصر ثلاثة وهي:

-سلوك جرمي(أولا).

-نتيجة جرمية(ثانيا).

- علاقة سببية بينهما(ثالثا).

[1]-إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصـدي للجريمة الإلكترونية، مجلة الآفاق للبحوث و الدراسـات، العدد04، المركز الجامعي إليزي، الجزائر،2019،ص189.

أولا: السلوك الجرمي للجريمة الإلكترونية

ذكرنا أن نقطة البدء في البحث عن الجريمة ومعاقبة فاعليها تكون بإظهار النوايا والرغبات إلى حيز الواقع المادي المحسوس بإتيان الفاعل سلوكاً يشكل خرقاً الأمر المشرع بصورة سلبية أوإيجابية.

هذا السلوك الجرمي لا يوجد في الواقع العملي بصورة واحدة، بل يتدافع بعدة علاج لكل منها ما يميزه، فقد يوجد السلوك الجرمي بفعل إيجابي كإطلاق النار فى أحد الأشخاص وقتله، أوسرقة بيت، إذ يفترض في هذه الصورة الإيجابية تحريك الجاني لعضو من أعضائه بشكل إرادي بغية إحداث نتيجة معينة في الواقع، سواء أكانت هذه الحركة على شكل حركة واحدة كالقتل بطعنة سكين واحدة مثلا أوقد يكون السلوك الجرمي الإيجابي مجموعة من الحركات كطعن المجني عليه عدة طعنات متتالية.

أما عن مصدر هذا السلوك الإيجابي يستوي آن يصدر عن أي من أعضاء كاليد أوالقدم في القتل واللسان في جرائم العام والقدح، سواء أكان الفعل من العضو البشري مباشرة، أوباستخدام أداة يتوصل بها الجانب لتحقيق فعله كاستخدام سكين أومسدس لإتمام القتل.

وكما أن الركن المادي يقع بفعل إيجابي، يمكن أن يقع بفعل سلبي يأخذ وصف الإمتناع عن إتيان أمر يوجبه المشرع، كامتناع الأم عن إرضاع وليدها بحيث يؤدي ذلك إلى وفاته، على أن المعول عليه هنا لظهور حالة الإجرام أن يكون الامتناع عن أمر وجوبي يكلف به الشخص، فإن لم يكن من إلزام على الشخص فلا يوصف امتناعه بالجريمة، كامتناع شخص عادي عن القيام بعملية إنقاذ غريق حتى ولو كان يعرف السباحة، إذا لا تتوافر في الحالة الأخير جريمة تستوجب الملاحقة القانونية السلوك الجرمي قد يأتي بصورة بسيطة، وقد يتضمن عملية معقدة

تحتوي سلسلة سلوكيات لازمة كالاحتيال، إذ لا بد في جرائم الاحتيال من الكذب ثم تدعيم هذا الكذب بمظاهر خارجية[1].

وكما يوجد السلوك الجرمي بصفة وقتية محددة من حيث الزمان، فقد يوجد بصورة مستمرة تتمثل بقابلية السلوك الجرمي والنتيجة للإستمرار في الزمن كحمل سلاح ناري بدون ترخيص وحجز حرية إنسان بدون وجه حق، وهذا المفهوم يختلف عن الجريمة الثابتة والتي يكون فيها السلوك الجرمي واحدا ثابتا، في حين الاستمرارية تكون للنتيجة، ومثالها في التقنية الحديثة برامج الحاسب الآلي الموجه لإتلاف البيانات وهذا الإتلاف ما يعرف باسم (الفيروسات) (Viruses) والتي تمتلك القدرة على التكاثر والانتشار بعد إطلاقها للمرة الأولى.

لتنوع صور السلوك الجرمي في الواقع أهمية كبيرة تظهر من خلال تحديد الاختصاص القضائي والقانوني واجب التطبيق وبدء سريان مدة التقادم وغيرها مما لا يسمح المجال هنا يبحثها، وفي الجريمة المستحدثة لا يخفى الانقلاب الكبير في محتوى ومضمون وطبيعة الفاعل

هذا السلوك الجرمي الذي تطور بتطور وسائل متاحة جديدة وجدت بين يدي وهي ذات علاقة بتقنية الحاسب الآلي، وتفاعلية مع تقنية نظم المعلومات بشكل عام بما في ذلك شبكات الاتصال المعلوماتي.

هذا السلوك الذي طورته أيضاً عقلية الفاعل الذكية التي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيداً، أوجدت بلا شك مصاعب جمة إما على مستوى تحديد ماهية السلوك الجرمي وعناصره وأركانه ، أومن حيث متابعة هذا السلوك وتحقيقه وجمع أدلة إثباته أومن حيث نسبة هذا السلوك إلى فاعل معين وهي أمور أظهرت إلى حيز الواقع نمطا مستحدثا من الإجرام أدى إلى انقلاب في النظرية العامة للجريمة من خلال المحاور التالية:

[1]-جلال محمد الزغبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الإلكترونية–دراسة مقارنة، ط01، دار الثقافة للنشر والتوزيع، 2010،ص49.

-طبيعة السلوك والنتيجة والعلاقة بينهما زمانياً ومكانياً.

-نسبة السلوك إلى الفاعل والمساهمين

-عجز النصوص التقليدية عن استيعاب القوالب الجرمية المستحدثة[1].

ثانيا: النتيجة الجرمية للجريمة الإلكترونية

تطرح مسألة النتيجة الإجرامية في جرائم المعلوماتية مشاكل عدة ، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية ، فلو قام احد المجرمين في أمريكا باختراق جهاز حاسب آلي رئيسي وهو ما يعرف باسم " الخادم Server " في احد البنوك في فرنسا ، وهذا الجهاز الخادم موجود في الصين فمعرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا ما يثير أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن[2].

ثالثا: العلاقة السببية للجريمة الإلكترونية

حتى يتم الركن المادي بعناصره كافة لا بد أن تكون هناك علاقة سببية السلوك الجرمي الذي أتاه الجاني والنتيجة الحاصلة، بحيث يمكن القول أن هذه النتيجة من ذلك السلوك، فإذا انتفت العلاقة السببية فلا مجال لمساءلة الفاعل.

إثبات العلاقة السببية يختلف بحسب وجود فعل أوسلوك جرمي واحد أوعدة سلوكيات جرمية متعاصرة أومتعاقبة، إذ في الحالة الأولى هل يكون الأمر سهلا في إثبات تحقيق النتيجة بفعل سلوك الجاني أم لا؟ ولكن الإشكالية في رأينا تثار عندما توجد عدة أفعال ونتيجة واحدة.

[1]- جلال محمد الزغبي، أسامة أحمد مناعسة، المرجع السابق، ص ص49،50

[2]-معتوق عبد اللطيف، المرجع السابق، ص24.

للإجابة على تلك الإشكالية أتى الفقه الجزائي بنظريتين:

أ : نظرية تعادل الأسباب

تعمل هذه النظرية على أساس أن كافة الأفعال المتعاقبة مرتبطة بعلاقة سببية مع النتيجة، وبالتالي يسأل جميع من أتى تلك الأفعال الجرمية، مثال ذلك، شخص ضرب آخر ضربة غير قاتلة على رأسه، ونقل إلى المستشفى وتعرضت سيارة الإسعاف الحادث يموت على أثره المصاب، فهل يسأل في هذه الحالة من ضرب ومن تسبب فيالحادث عن جريمة قتل.

ولأن انتقادات كثيرة وجهت لهذه النظرية، خصوصاً عدم العدالة، قيل بنظرية الأسباب المتفاوتة.

ب: نظرية الأسباب المتفاوتة

تعطي هذه النظرية لكل سبب قوة سببية مع النتيجة الجرمية التي حدثت ثم تختار أقوى العلاقات ومن ذلك:

-نظرية السبب الأخير تعتبر هذه النظرية أن العلاقة السببية تثبت بين النتيجة والسبب الأخير وهو في المثال السابق حادث التصادم، لكن في هذا توسيع لدائرة الإفلات من العقاب وغياب القاعدة العدالة.

– نظرية السبب الأقوى توازن هذه النظرية بين جميع الأسباب والأفعال التي عاصرت وقوع النتيجة، ثم ترجح السبب الذي ترى أنه الأقوى لإحداث النتيجة. نظرية السبب المتحرك في هذه النظرية السبب المتحرك هو المسؤول عن إحداث الجريمة، وبالتالي تقوم معه العلاقة السببية، وذلك مع التمييز بين السبب المتحرك والسبب الساكن، مثال ذلك: شخص يصاب فيتوفى مع العلم أنه مريض بالقلب، هنا الإصابة التي تعرض لها هي السبب المتحرك، ومرض القلب هو السبب الساكن، ولكن في هذا تجاهل للسبب الساكن الذي قد يكون عاملا أساسيا في إحداث النتيجة. نظرية السبب الكافي وفق هذه النظرية تقوم العلاقة السببية بين النتيجة والفعل أوالسلوك الجرمي الكافي وفق المجرى العادي للأمور لتحقيق النتيجة فمثلا إذا ضرب شخص ضربة

خفيفة لا تؤدي إلى وفاته وتوفي، فهل يمكن إقامة علاقة سببية بين هذا الفعل وتحقق الوفاة بحادث تعرضت له سيارة الإسعاف أثناء نقل المصاب إلى المستشفى، بينما تقوم العلاقة السببية بين النتيجة وهي الوفاة والسلوك إن كان بحد ذاته كافياً لوقوع النتيجة كضرب المجني عليه على رأسه ضربة قاتلة[1].

البند الثالث: الركن المعنوي للجريمة الإلكترونية

ويتخذ صورة القصد الجنائي وهو مستفاد من طبيعة الأفعال التي تقوم بها الجريمة ويقوم القصد الجنائي هنا على عنصرين هما العلم والإرادة.

فالعلم يعني علم الجاني بالصفة الاسمية أوالشخصية للبيانات وأن يعلم أن من طبيعة الحاسوب الالكتروني إجراء المعالجة الإلكترونية لهذه البيانات دون ترخيص من اللجنة المختصة بذلك اما الارادة فهي أن تتجه ارادة الجاني إلى اجراء المعالجة الإلكترونية لهذه البيانات باية صورة كانت أي بالمخالفة لاتخاذ الاجراءات الأولية لاجراء المعالجة الإلكترونية للبيانات، أي أن القصد المتطلب لقيام هذه الجريمة هو القصد العام ولا عبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعله، فسواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للاساءة إلى سمعته الشخص أولمجرد الفضول وحب الإستطلاع، وهذا تطبيق لمبدأ عام هو ما نصت عليه المادة (38) قانون العقوبات العراقي "لا يعتد بالباعث على ارتكاب الجريمة مالم ينص القانون على خلاف ذلك[2]".

المطلب الثاني: أطراف ودوافع إرتكاب الجريمة الإلكترونية

سنتطرق من خلال هذا المطلب إلى أطراف الجريمة الإلكترونية (الفرع الأول)، و دوافع إرتكاب الجريمة الإلكترونية (الفرع الثاني).

---

[1]– جلال محمد الزغبي، أسامة أحمد مناعسة، المرجع السابق، ص ص54،55.

[2]–محمد علي سالم،حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، العدد14،كلية القانون، جامعة بابل،العراق 2007، ص97.

الفرع الأول: أطراف الجريمة الإلكترونية

إن الجرائم المعلوماتية كغيرها من الجرائم تحتاج إلى طرفين الفاعل في الجرائم التقنية ومجني عليه وهذا ما سوف نتناوله بدراسة من خلال الآتي:

البند الأول: الفاعل في الجريمة الإلكترونية

في الجريمة الإلكترونية لانكون بصدد مجرم عادي بل أمام مجرم ذي مهارات تقنية وذي علم بالتكنيك المستخدم في نظام الحاسبات الآلية، فشخصية المجرم المعلوماتي سواء أكان طبيعيا أو معنويا وآلية إرتكاب الجريمة، تجعل منه شخصا يتسم بسمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي، ولعل أهم مايتميز به الشـــخص المذكور أنه يتوافر لديه خبره بالمسائل المعلوماتية ومعرفة كافية بآلية عمل الحاسب الآلي وتشغيله باعتبار أن الإجرام المعلوماتي ينشـــأ من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية أوالبيانات بيد أنه ذلك لا يعني إمكانية تصـــور العنف الموجه ضـــد النظام المعلوماتي فقد يكون محل الجريمة إتلاف الحاسب الالي ذاته أووحدة المعالجة المركزي أي أن ما يمكن الإعتداء عليه قد يكون بهيكلية الحاســـبات لا بمعلوماتها المتنقلة، عبر شـــبكة المعلومات.

ولا يمكن لأي عقوبة أن تحقق هدفها ســـواء في مجال الردع العام أو الردع الخاص مالم نضع في الإعتبار شخصية المجرم حتى يمكن إعادة تاهيله إجتماعيا لكي يندمج بالمجتمع مرة أخرى ليغدو مواطن صـــالحا على إعتبار أن إصـــلاح المجرم هو نقطة الإرتكاز للنظام العقابي الحديث، فالإجرام الإلكتروني يعد إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف على الرغم من تصور الإجرام العنيف الموجه ضد النظام المعلوماتي الذي يتجسد كما بينا بإتلاف الحاسب الالي.

والإجرام الإلكتروني بوصـــفه ظاهرة اجتماعية قد أســـفر عن عوامل مســـتحدثة في أذهان مرتكبيه، إذ يلجا العديد من مرتكبي هذه الجرائم إلى إرتكابها بدافع اللهو أولمجرد إظهار تفوقهم على الآلة أوعلى البرامج المخصصـة لأمن النظم المعلوماتية، دون الحصـول على منفعة مالية بل الإكتفاء بالتفاخر بانفسهم، وأن يظهروا لضحاياهم ضعف أنظمتهم مما يبدوا إنعدام أي خطر اجتماعي للإجرام المعلوماتي وليس الســـبب في ذلك عدم وجود نوايا آثمة ولكن للســـلوك غير الواعي الذي يمكن أن يتسبب في أضرار جسيمة حتى وإن لم يكشف عن أي إعتداء للمجتمع .

وعليه فإن مرتكبي الجرائم الإلكترونية ليســـوا على درجة من الخطورة أوالكفاءة وعلى هذا الأساس يمكن تصنيفهم حسب إمكانياتهم ومقاصدهم من إرتكاب الجريمة إلى صنفين:

الأول: مجرمين مسـتخدمين وهم من تتوافر لديهم خبرة لاباس بها في مجال عمل الحاسـب الآلي ومكوناته ووظائفه الأســـاســـية ومعرفة بعض البرامج التي يجري العمل بها كالبرامج المحاسـبية ولما كان هؤلاء يمارسـون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسـة هواية اللهو وهم لايدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي إلى أفعالهم غير المشروعة بالنسبة إلى نشاط معين.

لذا فإن هذه الفئة من المجرمين تعد أقل خطورة مقارنة بغيرها، ولكن مع ملاحظة ازدياد أعداد المستخدمة لتكنولوجيا (الأنترنيت) وما سيتبعه بلا شك من إزدياد نسبة الجرائم في هذا المجال[1].

فليس من المستبعد احتمال انزلاق هذه الفئة من مجرد هواة صغار للأفعال غير المشروعة إلى محترفين للإجرام وخصوصا إذا ماتم احتضانهم من قبل منظمات إجرامية لتحقيق أغراض خطرة تؤثر بصورة أوبأخرى على معطيات التطور العلمي.

الثاني: مجرمين مبرمجين نظرا إلى المســتوى المهاري الذي يتمتع به المجرمون من دخول و إقتحام للأنظمة الحاســـوبية بكل ســـهولة و اقتدار رغم احتياطات الأمن المتعددة ورغم قلة

[1]–محمد علي سالم، حسون عبيد هجيج ، المرجع السابق، ص89.

العناصـر الخبيرة على إكتشـافها مما تبدو معه خطورة هذه الفئة من المجرمين واضـحة بصـورة كبيرة، إذ غالبا ماتكون جرائم التحويل والنسخ والإضافة للمعلومات على البرامج وتفسير محتواها من هذه الفئة ضـخمة علاوة على أن باسـتطاعة هذه الفئة اسـتخدام الإمكانيات والأسـاليب المعلوماتية ليس في إرتكاب الجريمة فقط بل حتى في التهرب من محاولة كشف أمرهم أوبالعمل على إعاقة ملاحقتهم من خلال تضييع الأدلة الموجودة المؤدية إلى إدانتهم .

من هذا يتضـح أن مرتكب الفعل الجرمي المعلوماتي، قد يكون فاعلا اصـليا أوشـريكا في إرتكابه للجريمة في صـفة الفاعل الأصـلي في الجريمة المعلوماتية غالبا ما تكون من أحد العاملين أوالمستخدمين في منشأة تدار بالنظام المعلوماتي بصرف النظر عن المستفيد من وراء إرتكاب مثل هذه الأفعال، ولما كان هذا النوع من الاجرام يسـتلزم الدقة والتنفيذ للعمليات غير المشـروعة فإنه يسـتلزم كذلك مشـاركة أومسـاعدة اشـخاص آخرين سـواء أكانوا فنيين أم مجرد وسـطاء وقد يكون هذا الإشـتراك سـلبيا يتمثل بالإمتناع ، وفي الغالب الأعم يتمثل بالمسـاعدة الفنية والمادية وخصـوصـا عندما تسـتلزم آليات الابتكار لمخادعة الحاسـب الآلي، الاسـتعانة بمجموعة من الوسطاء أوالـشركاء والمؤتمنين على أسرار أسطوانات الحاسبات الآلية إذ يؤدي هؤلاء الدور الرئيسي في نجاح العملية غير المشروعة أوالمستهدفة[1].

Donn-parker مختص في تحليل الجريمة المعلوماتية بمعهد (Stannifère) للبحوث حدد 7 أصناف للمجرم المعلوماتي:

1- الهواة.

2 المهووسـون وهم الذين يرتكبون الجريمة باسـتخدام العنف الذي من الصـعب تصـوره في المجال، فالحالة الكلاسـيكية الوحيدة هي التي تتعلق بالمبرمج المجنون الذي يهدف إلى تحطيم كل المعلوماتي الأنظمة.

[1]- محمد علي سالم، حسون عبيد هجيج ، المرجع السابق، ص89.

3- الجريمة المنظمة : فجهاز الحاسوب أصبح وسيلة بارونات الجريمة، وعصابات المافيا في تنفيذ الجرائم، فأكبر العائلات الشـــهيرة بتهريب الكوكايين في كولومبيا "جيلبرتو رودريقيز" يمتلك قاعدة تكنولوجية خاصة بحجم وقوة شبكة الاستخبارات السوفياتية .

-4- الحكومات الأجنبية : حيث تستعمل أنظمة الحاسوب للجوسسة.

5- النخبة.

6- المتطرفون الذين يســـتخدمون الشـــبكات المعلوماتية لخدمة و نشـــر أفكارهم الدينية أوالسياسية أوالاقتصادية، نجد هذه الدوافع في مجموعات شهيرة كالألوية الحمراء في إيطاليا.

7-مخربي الأنظمة المعلوماتية وهي طريقتهم في إرضاء رغباتهم[1].

البند الثاني : المجني عليه في الجرائم التقنية.

فكما يمكن أن يرتكب جرائم المعلوماتية شـــخص طبيعي أومعنوي فإن المجني عليه في تلك الجرائم قد يكون كذلك أيضـــا مع أنه الغالبية العظمى من هذه الجرائم تقع على شـــخص معنوي يتمثل بمؤسـسـات وقطاعات مالية وشـركات ضـخمة ، إلا أن المعلومات المجردة تعد في الوقت الحاضـر من أهم المصـالح المسـتهدفة بعد الأموال وخصـوصـا إذا كانت هذه المعلومات ذات أهمية بـالغـة وكـان هدف المجرم المعلومـاتي هو الحصـــول على مقـابـل وعوض عن طريق المقايضـــة غير المشـــروعة لهذه المعلومات أوبيعها لغير أصـــحابها الشـــرعيين وســـواء أكانت المعلومات مخزنة بذاكرة ةالحاســوب أم مدخلة في بنوك المعلومات إذ يتم تشـــويشـــها وإظهارها على غير حقيقتها ويدخل في هذا النوع من ما يتعلق بأسرار الدولة والمشاريع الصناعية .

ففي هذا النوع من الجرائم يكون دور المجني عليه ضـــئيلا وســـلبيا إلى حد كبير إذ يفضـــل الكثير من المجني عليهم الإبقاء على ما لحقهم من إعتداء ســـرا أي يميلون إلى التكتم عما لحقهم من أضـــرار ناتجة عن الجريمة المعلوماتية ولعل مرد ذلك يكمن برغبتهم في الحفاظ على

[1]- أمال قارة، الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي و علوم جنائية، كلية الحقوق والعلوم السياسية، الجزائر، 2005ص27.

مركزهم الإجتماعي أوســـمعتهم التجارية حماية لمركزهم المالي وثقة العملاء بهم، لذا لايرغبون بالكشـف عن الإختلافات الحاصـلة على أجهزتهم الحاسـوبية حتى لا ينظر إلى تدابير الحماية لديهم على أنها ضعيفة غير فعالة فتسبب ضعف الثقة بالمؤسسة ومن ثم عزوف العملاء عنها.

فضـــلا عن عجز المجني عليهم في الإثبات المادي للجريمة وخشـــيتهم إحتمالية المســـاءلة القانونية في الوقت الذي يقع عليهم واجب الإشـــراف على المعلومات المســـتهدفة وإمتلاكهم السلطة اللازمة لإمكان التقدير ووضع الاجراءات الضرورية في حالة حدوث أضرار ناشئة من إفشاء معلومات على قدر من الحساسية والخطورة[1].

الفرع الثاني: دوافع ارتكاب الجريمة الإلكترونية

تسبق الحاجات عادة الدوافع، فالحاجة تنشأ مـــن الشعور بالنقص، أو الحرمان من شيء ما لدى الفرد، مما يؤدي إلى التأثير في القوى الداخلية لديه (الدوافع)، بغرض إشباع هذه الحاجات التي يحقق تواجدها حالة من الرضـــا النفســـي، وتتنوع دوافع الإقدام على الجريمة الإلكترونية باختلاف منفذيها، وتبعا لطبيعة ودرجة خبرته في مجال المعلوماتية، ويمكن تصـــنيف هذه الدوافع إلى صنفين دوافع شخصية ودوافع خارجية.

البند الأول:الدوافع الشخصية

ويمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى دوافع مادية وأخرى ذهنية.

أولا: الدوافع المادية

تحقيق الربح وكســـب المال يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفســه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويســعى إلى الإحتراف حتى يحقق أعلى المكاسـب وبأقل جهد دون أن يترك أثرا وراءه، ولقد أشـارت في هذا الإطار مجلة (Sécurité informatique) وهي مجلة متخصـصــة في الأمن المعلوماتي أن

[1]-محمد علي سالم، حسون عبيد هجيج ، المرجع السابق، ص89.

43 % من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال و 23% من أجل سرقة معلومات و 19% أفعال إتلاف و 15%الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية، فالرغبة في الثراء والربح المادي عادة ما تواجهها صعوبات بالغة لتحقيقها بالطرق القانونية والمقبولة اجتماعيا، لذا يلجأ بعض الأفراد إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر، وسهولة التنفيذ ووفرة المردود وقلة الخطورة، إضافة إلى إمكانية محو الدليل، وتوفر الوسائل التقنية التي تعرقل الوصول إليه مع ضمان التستر وعدم التشهير[1].

تعتبر غاية تحقيق الربح المادي من الدوافع الرئيسية لدى مجرمي المعلوماتية، فأمر إكتشاف ثغرة في النظام المعلوماتي هو السبيل المباشر لغرض تحقيق منفعة مالية(كتحويل الأموال) وبصفة غير مباشرة (التجسس الصناعي أو التجاري)، فحسب رأي كل من الأستاذين" Lamer et Rose، لامر و روز" فإن المجرم للمعلوماتي وانطلاقا من حافز تحقيق الربح المادي فهو يطبق نظرية إقتصادية، فهو يبحث عن أكبر قدر ممكن من الأرباح مقابل أقل قدر ممكن من الخسائر، أما حسب رأي الأستاذ Martin ،مارتن فإن غاية تحقيق الربح المادي من الجرائم المعلوماتية دافع له وجهان الأول يتمثل في الأرباح التي يحققها الجاني كتحويل الأموال إلى حسابه من حساب الغير، والثاني هو الفائدة التي يجنبها من خسائر غيره، كخسارة منافسه لزبائنه بسبب فقدانه لمعطياتهم الإلكترونية.

وقد يتحقق غرض الربح المادي ولكن بأسلوب التهديد والإبتزاز فحسب تقرير السيد " ميكو هيبومان – Mikko Hypomen" مدير مركز البحوث لدى شركة (F.SECURE) فإن بعض المجرمين المعلوماتين يعمدون إلى إرسال رسائل إلكترونية لضحاياهم مسبقا، يخبرونهم فيها بأمر إكتشاف ثغرات أمنية على أنظمتهم المعلوماتية وبأنهم سيقومون بمحو بياناتهم وتدميرها كليا في حال عدم تحويل أموال إلى حساباتهم، وهو ما حدث بالفعل لشركة (Google) في شهر ماي 2004 أين قام ميشال برادلي Michel Bradly، بإرسال تهديدات لهذه الشركة بضرورة دفعها لمبلغ 100.000 دولار وإلا فإنه سيقوم بنشر فيروس وبرنامج غامض من شأنه أن

[1]–ياسمينة بونعارة، المرجع السابق، ص286.

يتسبب لها في تعطيل نظامها المعلوماتي الخاص بتحصيل عائدات الإشهار من الصفحات المدعمة من قبلها، وقد ألقى عليه القبض في ولاية كاليفورنيا الأمريكية بتاريخ 17 ماي 2004.[1]

ثانيا: الدوافع الذهنية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح ، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد وغالباً ما يجدون الوسيلة إلى تحطيمها بل والتفوق عليها.

ويتزايد شيوع هذا الدافع لدي فئات صغار السن من مرتكبي جرائم الكمبيوتر الذين يمضون وقتاً طويلاً أما حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أوالمبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أوبالنقص داخل المنشأة التي يعمل بها.

وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيه أمام العامة[2].

---

[1]–ربيعي حسين،المجرم المعلوماتي–شخصيته وأنواعه، مجلة العلوم الإنسانية، العدد40، جامعة محمد خيضر بسكرة، 2015، ص ص293،292.

[2]–عبد العال الدريبي، محمد صادق اسماعيل، الجرائم الإلكترونية –دراسة قانونية قضائية مقارنة، ط01، المركز القومي للإصدارات القانونية، 2012، ص ص53،52.

البند الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن أبراز أهم هذه الدوافع فيما يلي:

أولا: دافع الإنتقام

يعد هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أوالشركة التي يعمل بها وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية، ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية أوالطرد من الوظيفة، فيتولد لدى المجرم المعلوماتي الرغبة في الإنتقام من رب العمل، ومثال ذلك فقد دفع الإنتقام بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله 06 أشهر وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

ثانيا: دافع التعاون والتواطؤ

هذا النوع كثير التكرار في الجرائم الإلكترونية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أوخارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.

وإذا كانت هذه أبرز الدوافع لارتكاب أنشطة الإعتداء على نظم المعالجة الآلية، ومع ذلك ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة إلى تدميرها أوعلى الأقل حيازتها للقيام بعملية الإبتزاز والحصول على الأموال، لذلك فإن الدوافع في ارتكاب جرائم الإلكترونية قد لا يتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة بل كثيرا

ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أوأكثر من جهة بحيث يسعى كل منهم لتحقيق مآربه الخاصة[1].

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية

إن الأســـلوب أوالطريقة التي يتم من خلالها ارتكاب الجريمة الإلكترونية يختلف عن مجرى الجرائم التقليدية كالقتل مثلا، فإنها قد تميزت بوجود خصـــائص تمتاز بها عن باقي الجرائم[2]، وتنوعت بأسلوبها وطريقتها وهذا ما سوف نوضحه من خلال الآتي:

المطلب الأول: خصائص الجريمة الإلكترونية وطبيعتها

تتميز الجريمة الإلكترونية بخصـــائص كثيرة أهمها أنها جريمة مســـتحدثة ومختلفة من حيث محلها ومخاطرها، ووســـائل إرتكابها، والمشـــكلات الناتجة عنها، فهي تتميز بطبيعة خاصـــة، وتتمتع بعدة خصائص وتختلف من حيث طبيعتها تميزها عن الجريمة التقليدية أهمها:

الفرع الأول: خصائص الجريمة الإلكترونية

سنتناول من خلال هذا الفرع مجموعة من خصائص الجريمة الإلكترونية وهي:

البند الأول:الجريمة الإلكترونية جريمة عابرة للحدود

تمتاز الجريمة الإلكترونية أنها جريمة عابرة للحدود، فليس لها حدود فهي متمردة على عنصـــر والنطاق الجغرافي، حيث تدخل في طائفة الجرائم غير الوطنية، ويرجع ذلك إلى البيئة الإلكترونية التي تقع فيها تلك الجرائم والتي تقوم على الربط الإلكتروني بين الحواســيب، ســواء داخل الدولة الواحدة أوبين عدة دول بواسطة شبكات إلكترونية مثل الانترنات والتي صممت في الأصل لتسهيل عملية نقل المعلومات والإتصالات فأصبحت تستخدم كوسيلة لارتكاب الجرائم، فقد ترتكب جريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية وتتحقق نتيجتها الإجرامية

---

[1]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق ، باتنة،2013،2012.ص 62.

[2]–لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية–دراسة مقارنة، ط،01 دار الحامد للنشر و التوزيع، عمان، 2015، ص24.

في دولة أخرى من العالم مرورا بمزود خدمة أوقنوات اتصـــال في إقليم دولة ثالثة، ويترتب على البعد الوطني للجريمة الإلكترونية عدة إشـــكاليات مشـــابهة لتلك المرتبطة بالجرائم ذات الطابع عبر الوطنية أهمها، إصدار إجراءات التحقيق وضبط المتهمين وملاحقتهم بمبدأ السيادة الوطنية للدولة وخاصـــة في الجرائم التي تتطلب إتخاذ إجراء من إجراءات التحقيق في إقليم دولة أجنبية، وكذلك إشكالية الاختصـاص القضـائي وإشـكالية تحديد القانون واجب التطبق، كما أنه من جهة أخرى تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتا وليس بالقصير في حالات المساعدة القانونية أوالقضـائية بين الدول، والتي تتعارض مع طبيعة الجرائم الإلكترونية التي تتطلب سرعة في التحقيقات .

حيث أن جزءا كبيرا من الأدلة في الجرائم الإلكترونية كما سبق الإشـارة غير ملموس ويزول بسرعة، وهو ما يتطلب أن تكون إجراءات التحقيق وجمع الأدلة بصورة سريعة وآنية.

البند الثاني:الجريمة الإلكترونية جريمة صعبة الإثبات

أهم الخصـائص المميزة لهذه الجرائم أنها صـعبة الإثبات والاكتشـاف مقارنة بالجرائم التقليدية، حيث يصفها البعض بأنها إجرام خفي يأتي الجاني جريمته في الخفاء، وبالتالي يصعب ضبطه، وإنما جريمة معقدة يتســم مرتكبها بالذكاء والاحتراف، لذا فالجريمة تكون أكثر تعقيدا الأمر الذي قد يصعب معرفة أو إكتشاف مرتكبها وهذا بسبب مجموعة من العناصر أهمها:

أولا: إن جزءا كبيرا من الأدلة غير ملموس ويزول بسرعة، ويرجع ذلك إلى أن أنواع العناوين الإلكترونية والبيانات تخزن في ذاكرة النظام الحاسوبي لمدة قصيرة ولا تخزن بشكل دائم.

ثانيا: أنه إذا تم العثور على تلك الأدلة فإنه من الســهولة إتلافها من قبل الجناة، فضــلا عن أن غياب الإعتراف القانوني بطبيعة تلك الأدلة يعد من أهم عوائق الإثبات.

ثالثا: لجوء مرتكبي الجرائم الإلكترونية إلى اسـتخدام وسـائل وأسـاليب متجددة تتميز بالطابع التقني والفني المعقد، والتي يصـعب على أفراد الأجهزة الأمنية التعامل معها مثل جرائم الاعتداء بواســـطة مجموعة حواســـيب يزرع فيها برنامج يخضـــع لتحكم خارجي، ويطلق عليها جرائم

الاعتداء بواسطة شبكة البوت نت، حيث يمكن لأحد القراصنة التحكم في مجموعة من الحواسيب المخترقة الموجودة على إحدى شبكات البوت نت قد تصل إلى ألاف أوملايين الأجهزة.

رابعا : صعوبة الوصول للدليل بفحص كميات هائلة من المعلومات.

خامسا: إحجام المجني عليه في بعض الحالات عن الإبلاغ عن وقوع تلك الجرائم خشية من زعزعة ثقة عملائهم (مثل الجرائم التي تستهدف البنوك أوالشركات)، إذ قد تكون الخسائر الكاملة أكبر من الخسائر الناجمة عن الهجوم الإلكتروني الذي تعرض له.

سادسا: التحديات والصعوبات القانونية التي تعرقل عملية متابعة الجناة التي تنجم عن مشاكل الحدود الأولويات القضائية وذلك نظرا لكون الجرائم المعلوماتية من طائفة الجرائم عابرة الحدود الوطنية[1].

البند الثالث: الجريمة الإلكترونية جريمة سهلة الإرتكاب

لا تتطلب جرائم المعلومات عنفا لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة مماسة العنف والايذاء، كما هو الحال في جريمة القتل أوالاختطاف أوفي صورة الخلع والكسر وغير ذلك.

وعلى هذا الأساس تتميز جرائم المعلومات بأنها من الجرائم الهادئة، أوالناعمة، حيث لا تحتاج الى العنف، وكل ما تحتاج إليه هو عامل الخبرة، والذكاء، والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في ارتكاب الأفعال غير المشروعة، فهي من الجرائم النظيفة التي تستخدم الأرقام والبيانات وليس لها أثر خارجي مادي[2].

[1]– بن مالك اسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها،مجلة البيان للدراسات القانونية والسياسية، العدد 04، كلية الحقوق والعلوم السياسية، برج بوعريريج، الجزائر، 2019،ص114.

[2]– يعيش تمام شوقي،الجريمة المعلوماتية–دراسة تأصيلية،ط01، مطبعة الرمال ، الجزائر، 2019،ص30.

البند الرابع: الجريمة الإلكترونية جريمة مغرية للمجرمين

إذا كانت بعض الجرائم التقليدية تحتاج من مرتكبها إلى قوة عضـــلية لتنفيذها فان جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضـــلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والجاني في ســـبيل تنفيذها لا يحتاج من الوقت إلا ثوان أودقائق معدودات، ولا يحتاج من القوة العضـــلية غير تحريك الأنامل من علي وســـائل الإدخال وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته قد لا ترى بالعين.

ونعومة هذه الجريمة وما تدره من أرباح ومن إشـباع للفضـول عند البعض جعلها من الجرائم المغرية والجذابة للمجرمين[1].

الفرع الثاني: طبيعة الجريمة الإلكترونية

تختلف طبيعة جرائم التقنية وتتنوع بحسب طبيعة السلوك الجرمي ولذا فإن جرائم الحاسب الآلي جرائم أموال، وأيضـــاً هي جرائم أشـــخاص جرائم أمن دولة وجرائم مخلة بالثقة العامة والآداب العامة[2]، وهذا ما سنشير إليه من خلال الآتي:

البند الأول: جرائم التقنية جرائم أموال.

البند الثاني: جرائم التقنية جرائم أشخاص.

البند الثالث: جرائم التقنية جرائم أمن دولة وجرائم مخلة بالثقة العامة والآداب العامة.

البند الرابع: جرائم التقنية جرائم اقتصادية.

البند الأول: جرائم التقنية جرائم أموال

إن الجرائم الإلكترونية وفقاً للمفهوم الذي بيناه آنفاً، تظهر بصورتين:

الأولى: جرائم واقعة باستخدام الحاسب الآلي، ومنها استخدام الحاسب الآلي لتزييف العملة، أو

[1]– محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، العدد 01، مجلة الدراسات و الأبحاث،جامعة زيان عاشور، الجلفة، 2009 ص375.

[2]–جلال محمد الزغبي، أسامة أحمد المناعسة، المرجع السابق، ص84.

التزوير في محررات رسمية، أوالاختلاس ، أو إستخدام الحاسب الآلي لأغراض الدخول غير المشروع للبيانات والمعلومات المخزنة على حاسب آلي آخر، وذلك عبر شبكات الاتصال الدولية، أوبصورة مباشرة بغية الحصول على منافع نقدية أوغيرها، أوأخذ المعلومات والبيانات.

الثانية: جرائم واقعة على الحاسب الآلي بمشتملاته المتعلقة بالجانب المادي، أوبالجانب المعنوي كجرائم تعديل أوتحوير أوتقليد برامج الحاسب الآلي، وجرائم تدمير المعلومات والبيانات الخاصة بالحاسب الآلي نفسه، بالإضافة إلى الجرائم التقليدية العادية التي تطال الجانب المادي للحاسب الآلي كالسرقة والإتلاف.

وفي كلتا الحالتين يمكن أن توصف الجرائم الإلكترونية بأنها جرائم أموال، إذ موضوعها دائماً هو المال، هذا مع التسليم بأن الجانب المعنوي للحاسب الآلي وما يشتمل عليه المال بالمعنى الفني والقانوني.

ولعل ما يدعم وجهة النظر هذه من أن الجرائم الإلكترونية هي جرائم أموال هو ضخامة السلوكيات غير المشروعة والناتجة عن استخدام الحاسب الآلي لتحقيق مكاسب مالية سواء تم ذلك بالغش أوالاحتيال أو أعمال التخريب والهدم أوالمضاربات غير المشروعة، وكلها جرائم تقع على الأموال من منظور قانون العقوبات.

وفي هذه الحالة من الممكن أن تكون الكثير من جرائم الأموال التقليدية جرائم أموال الكترونية أيضاً، فقد تكون الجريمة الإلكترونية جريمة سرقة، وقد تكون جريمة احتيال، وقد تكون أيضا جريمة إساءة ائتمان (خيانة الأمانة)، وقد تكون جريمة إتلاف لمال الغير.

البند الثاني: جرائم التقنية جرائم أشخاص

من الممكن وقوع جرائم أشخاص من خلال النظام الإلكتروني، ولكن هذا الشكل لا يجد الكثير من التطبيقات العملية على أرض الواقع، إذ ينحصر أثرها في مجموعة ضيقة من جرائم الأشخاص وذلك في جرائم الذم والقدح، والتحقير، وجريمة إفشاء الأسرار سواء التجارية

أوالشـــخصـــية، وكذلك جرائم التهديد والتحريض وجرائم الاعتداء على الحياة الخاصـــة عبر الإنترنت[1].

البند الثالث: جرائم التقنية جرائم أمن دولة وجرائم مخلة بالثقة العامة والآداب العامة.

الجرائم الواقعة على أمن الدولة من أهم الجرائم الإلكترونية التي تهدد أمن الدول ومجتمعاتها ما يلي:

أولا:الجماعات الإرهابية اســـتغلت الكثير من الجماعات المتطرفة الطبيعة الاتصـــالية للانترنيت من أجل بث معتقداتها وأفكارها ، بل تعداه الأمر إلى ممارســـات تهدد أمن الدولة المعتدى عليها.

ثانيا: الجريمة المنظمة: إستغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الإتصـــال والانترنيت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.

ثالثا: الجرائم الماسة بالأمن الفكري: يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الأنترنيت، حيث تعطي الأنترنيت فرصـا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

رابعا: جريمة التجسس الإلكتروني : سهلت شبكة الأنترنيت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجســـس على الأشـــخاص أو الدول أوالمنظمات أو الهيئات أوالمؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري والتجسس السياسي، والتجسس الاقتصادي[2].

---

[1]– عبد الله دغش العجمي،المشكلات العلمية والقانونية للجرائم الإلكترونية–دراسة مقارنة، رسالة مقدمة للحصول على شهادة ماجستير، تخصص قانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص ص 18،16.

[2]– أحمد بن خليفة، حفوظة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصدي لها، مجلة الإمتياز لبحوث الإقتصاد والإدارة،العدد03، جامعة الأغواط، الجزائر،2017، ص158.

لكن ليست كافة جرائم التقنية جرائم أمن دولة، إذ قد يمثل بعضها جرائم ماسة بالثقة العامة، أوالآداب والأخلاق العامة.

فقد سهل الحاسب الآلي وسائل وطرق إرتكاب جرائم ترتكب بطرق تقليدية كجرائم تقليد الأختام والطوابع، وتزوير الأوراق البنكية والمسكوكات، بالإضافة إلى إستخدام طرق جديدة للتزوير الجنائي وانتحال الشخصية، ذلك كله اعتمادا أن المشرع لم يأبه في كثير من الأحيان بوسيلة ارتكاب الجريمة لتحققها، لذا أمكن تصور قيام جرائم نشر صور إباحية، أو اقتنائها بقصد توزيعها مع دخول الحاسب الآلي، وانتشرت أكثر مع ظهور الإنترنت.

الفرع الرابع: جرائم التقنية جرائم اقتصادية

لما كان المشرع الجزائي لا يأبه بالوسيلة التي ترتكب بها الجريمة غالباً، فإن الجرائم التقليدية المعروفة لم تتغير من حيث الأركان في زمن الحاسب الآلى، إلا أن ظهور هذه التكنولوجيا ساهم في إيجاد طرق جديدة لاقتراف تلك الجرائم.

يختلف الفقه حول مفهومين للجريمة الاقتصادية، الاتجاه الأول يضيق من مفهوم الجريمة الاقتصادية ليقصرها فقط على السلوكيات المخالفة للقواعد التي تحكم الأسعار، في حين يأخذ اتجاه آخر بمفهوم واسع للجريمة الاقتصادية بحيث تشمل كافة النصوص الجزائية التي وضعت لحماية مصلحة الدولة في الأمور الاقتصادية ومصالح الأفراد الناتجة عن العلاقات الاقتصادية التي تربطهم مع بعضهم البعض على أن الاتجاه الغالب هو تبني المفهوم الواسع للجريمة الاقتصادية فقهاً وقانونا، إذ جاء بتعريف الفقه : "الجرائم الاقتصادية هي الجرائم التي تتضمنها نصوص تجرم أفعالا تنتهك حماية النشاط الاقتصادي و بغض النظر عما إذا كانت الأحكام الجزائية قد وردت في قانون مستقل واحد نطلق عليه قانون العقوبات الاقتصادي، أووردت ضمن عدد من النصوص المتفرقة المنظمة لأنشطة اقتصادية[1].

[1]–جلال محمد الزغبي، أسامة أحمد المناعسة، المرجع السابق، ص88.

المطلب الثاني: أنواع الجرائم الإلكترونية

قد ترتكب الجريمة الإلكترونية بإستعمال النظام المعلوماتي(الفرع الأول)، وقد ترتكب ضد النظام المعلوماتي(الفرع الثاني)، وهذا ما سوف نوضحه من خلال الآتي ذكره.

الفرع الأول: الجريمة الإلكترونية باستخدام النظام المعلوماتي

يشتمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية و مضاعفا لجسامتها.

ويهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة ، إذ تهدف هذه الجرائم الاعتداء على أموال الغير، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أونظمه كوسيلة لتنفيذ الجريمة ، ومنه لا يكون النظام المعلوماتي هو محل الحماية الجنائية. تتعدد صور الجرائم المعلوماتية المرتكبة بإستخدام النظام المعلوماتي بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها ، نتعرض لهذه الأفكار بشكل من التفصيل من خلال البنود البنود الموالية كالآتي:

البند الأول: الجرائم المعلوماتية الواقعة على الأشخاص الطبيعية

تقع هذه الجرائم على الأشخاص وتنقسم بدورها إلى طائفتين بحسب نوع الحقوق المعتدى عليها ودور النظام المعلوماتي في اقترافها.

تتمثل الطائفة الأولى في الجرائم الواقعة على حقوق الملكية الفكرية والأدبية، وأما الطائفة الثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة نتناولها فيما يأتي:

أولا : طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية ، ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج

نظام معلوماتي آخر ، أوحالة تخزين، و إســـتخدام هذه المعلومات أو التفريط فيها دون إذن صـــاحبها، ذلك أن اســتخدام معلومة معينة دون إذن صـــاحبها يتضـــمن إعتداء على حق من الحقوق المعنوية، إضـــافة إلى كونه إعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضـــمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع .

و قد نص المشـــرع الجزائري على حقوق الملكية الفكرية وبراءات الاختراع من خلال عدة نصوص قانونية نذكر من بينها:

المادة: 38 من الدســتور الجزائري التي تنص على أن "حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن.

-حقوق المؤلف يحميها القانون

لا يجوز حجز أي مطبوع أوتســـجيل أوأية وســـيلة أخرى من وســـائل التبليغ والإعلام إلا بمقتضى أمر قضائي".

الأمر 03/05 المؤرخ في 2003.07.19 المتعلق بحقوق المؤلف و الحقوق المحــاورة، والأمر 03/07 المؤرخ في 2003.07.19 المتعلق ببراءات الإختراع .

ثانيا : طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة

لقد كفلت الجزائر حماية الحياة الخاصــة للمواطنين بموجب المادة 39 من الدســتور الجزائري والتي تنص على أنه "لا يجوز انتهاك حرمة حياة المواطن الخاصـــة، وحرمة شـــرفه، ويحميهما القانون، سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة[1]".

ولاشـــك أن الحاســـبات الآلية بما لها قدرة فائقة على تخزين أكبر كم ممكن من المعلومات، أصبحت مخزنا لأهم المعلومات و أكثرها حساسية المتعلقة بالأفراد.

[1]-سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، تلمسان،2010 ،2011، ص34،35.

ولأهمية المعلومات التي تحتويها أنظمة الحسابات الآلية أصبح لهذه الحسابات دورا هاما في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة.

وعليه يمكن أن يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أوعلى الحريات العامة للفرد، كأن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أوإذنه ، أوأن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص بإختراق معلومات تتمثل في أسرار مكتوبة و سير ذاتية و مذكرات حياة شخصية لشخص آخر.

البند الثاني: الجرائم المعلوماتية الواقعة على أسرار الدولة

إن التطرق لمسألة تحديد نوع هذه الجرائم، والتي تكون الجريمة الإلكترونية وسيلة أساسية في ارتكابها، أمر في غاية الصعوبة بالنظر إلى معيار الخطورة ومدى تهديدها للمصالح العامة للأفراد، غير أن أغلب التشريعات قد وضعت ترسانة قانونية عقابية في مواجهة كل ما من شأنه المساس بأمن وسلامة مواطنيها و مؤسساتها الحيوية، و قبل التطرق إلى ذلك يمكن الإشارة إلى مفهوم الجرائم المعلوماتية الماسة بالنظام العام من خلال ما أوردته المادة 15 و 16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بشأن نوع هذه الجرائم و حصرتها فيما يلي:

أولا: نشر أفكار و مبادئ الجماعات الإرهابية و الدعوة لها.

ثانيا: تمويل العمليات الإرهابية و التدريب عليها و تسهيل الإتصالات بين المنظمات الإرهابية.

ثالثا: نشر طرق صناعة المتفجرات .

رابعا: نشر النعرات و الفتن و الإعتداء على الأديان و المعتقدات.

خامسا: القيام بعمليات غسل الأموال أو نشر طرق غسل الأموال[1].

[1]-ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية باتنة، 2016،2015،ص91.

سادسا: الترويج للمخدرات و المؤثرات العقلية.

سابعا: الاتجار بالأشخاص و الاتجار بالأعضاء البشرية.

أما على مستوى التشريع الوطني و بالرغم من كون الجزائر من أول الدول التي أمضت على مضمون هذه الاتفاقية بتاريخ 21 ديسمبر 2010 إلا أنها لم تبذل المجهود الكافي لأجل تجريم هذه السلوكات في قانون العقوبات، ولا زلنا نعتمد على النصوص التقليدية في شاكلة نصوص المواد من 65 إلى 96 من قانون العقوبات المتعلقة بتجريم الأفعال الموصوفة بأنها جرائم تعدي على الدفاع الوطني و الاقتصاد الوطني، وجرائم التآمر ضد الدولة إضافة إلى الجرائم الإرهابية ... وغيرها من النشـــاطات الإجرامية، ولكن دون تحديد مظهرها الإلكتروني، ويبقى الجهد التشـــريعي البارز في هذا المجال هو ما تضـــمنته المادة394 مكرر3 ق 04-05 من قانون العقوبات الجزائري، التي تنص على مضـــاعفة عقوبة مرتكب الجرائم المعلوماتية المنصـــوص عليها في هذا القســـم إذا ما إســـتهدفت الأنظمة المعلوماتية الخاصـــة بهيئات الدفاع الوطني والهيئات والمؤسسات الخاضعة للنظام العام، وهو ما يعني وحسب رأينا إستثناء تطبيق نص المادة 96 من نفس القانون، وحصـــر نطاق التجريم فيما تنص عليه المواد 394 مكرر إلى 394 مكرر2 من نفس القانون، بالرغم من إمكانية تطبيق عقوبات أشد، كل ذلك يشكل تعارضا بين النصوص وغموضا في تطبيقها، و هو ما يستوجب علينا توجيه عناية المشرع الجزائري إلى ضـــرورة الإقتداء بالتوجيهات التي تقترحها الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لوضع نصوص خاصة تسد هذا الفراغ التشريعي[1].

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

إضـــافة إلى الجرائم المعلوماتية التي تقع باســـتخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية يتمثل في الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف إما المكونات المادية للنظام المعلوماتي

[1]-ربيعي حسين، المرجع السابق، ص91.

أوالمكونات المنطقية أوالمعلومات المدرجة بالنظام المعلوماتـــي[1]، و هذا ما سنتطرق له بشيء من التفصيل من خلال الآتي:

البند الأول: جريمة الإعتداء على مكونات المادية لنظام المعلوماتي

يقصـد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملحقة به والتي تسـتخدم في تشـغيله كالأسـطوانات والشـرائط و الكابلات...إلخ، ونتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية وتقليدية ، كأن تكون محلا للسرقة أوخيانة الأمانة أو الإتلاف العمدي كإحراقها، أوضـرب الآلات بشـيء ثقيل أوحاد، أوالعبث بمفاتيح التشـغيل أوخربشـة الشريط و إفساد أسطوانات التشغيل مغناطيسي أوبتعريضـها إلى أي مجال مغناطيس متلف، ويترتب على هذا الإتلاف خسائر كبيرة.

ومن أمثلة ذلك ما حدث في فرنسـا حيث أدى إتلاف معدات مؤسـسـة كبيرة متخصـصـة في بيع الأنظمة و توثيق المعلومات الحســابية إلى خســائر مالية معتبرة قدرت ب 5 ملايين فرنك فرنسي.

ويرى البعض من الفقهاء أنه يندرج ضــمن هذه الطائفة من الجرائم المعلوماتية ســرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى اسـتخدامه في أعمال خاصــة بهم، وعليه تكون واقعة السـرقة منصـبة على وقت الجهاز الذي يمكن تقويمه ماليا و ليس على الأشـياء المادية بمعنى الكلمة، وتجدر الإشـارة أن خطورة واقعة السـرقة لا تكمن في الشـيء المسـروق لضـآلة قيمته، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

البند الثاني: جرائم الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي

تســـتلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة ، وقد تقع هذه الجرائم إما على البرامج التطبيقية وإما على برامج التشغيل[2].

---

[1]–سوير سفيان، المرجع السابق، ص39.

[2]- المرجع نفسه، ص40.

لقد وضحت المذكرة التفسيرية لاتفاقية بودابست لسنة 2001 بأنها، "تخريب نظم الحاسوب بهدف الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الإتصالات إعتداءا على حسن تشغيل نظام الحاسوب، وهذه الإعاقة تكون ناجمة عن إدخال أونقل أومحو أوإتلاف أوطمس أوالإضرار بالبيانات المعلوماتية[1].

ولقد أورد المشرع الجزائري تعريفا لهذا النوع من الجرائم وذلك وقف ما نص عليه في المادة 394 مكرر قانون عقوبات جزائري بالقول : " يعاقب بالحبس من 06 من ستة أشهر إلى ثلاثة سنوات 03 وبغرامة من 50.000إلى 200.000دج كل من أدخل بطريق الغش معطيات في نظام أو أزال أوعدل بطريق الغش المعطيات التي تضمنها" ، وهو التعريف الوارد في نص المادة 323 –2 و3 من قانون العقوبات الفرنسي التي نصت على عقاب كل شخص يتسبب في إعاقة أومنع السير العادي لنظم المعالجة الآلية للمعلومات بعقوبة مقدارها الحبس لمدة 05 سنوات بغرامة مقدارها 150.000أورو ذلك من خلال الإضافة أوالحذف وما يمكن استخلاصه من التعريفين السابقين أن طبيعة هذه الجرائم ترتكز على أسلوبين أساسيين هما: إعاقة سير النظم المعلوماتية و المساس بسلامة المعلومات.

أولا : إعاقة السير العادي للنظم المعلوماتية

أولا نشير إلى أن المشرع لم يتعرض في نص 394 مكرر 01 قانون عقوبات جزائري، إلى مفهوم إعاقة السير العادي للنظم المعلوماتية ، وهو السلوك الإجرامي الذي أولته اتفاقية بودابست أهمية بالغة وقد تجلى ذلك في نص القانون الفرنسي، يقصد بإعاقة سير عمل النظام المعلوماتي،" ذلك الفعل الذي يسبب تباطؤ في عمل النظام أوارتباكا، مما يؤدي إلى تغير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت ."

ويتحقق الركن المادي لهذا النوع من الجريمة من خلال وقوع إعتداء على نظام معلوماتي يسبب إرتباكا في عمله قد يكون دائما في حال استعمال الفيروسات، أو مؤقتا يهدف إلى شل أو

[1]- ربيعي حسين، المرجع السابق، ص58.

تعطيل النظام كما هو الحال في حالة إســـتعمال القنابل المنطقية، أومن خلال إغراق الخادم بالرسائل الإلكترونية لأجل الحد من قدرته على التعامل مع المعلومة .

و على كل حال فإنه يجب أن تكون الإعاقة دون وجه حق ، وبالتالي فإن أولئك الذين تكون لهم الحق في إطار ممارسة أنشطة تصميم الشبكات أوتشغيلها وصيانتها واختبارها، لا تعتبر أنشطتهم غير شرعية إذا ما تسبب في إعاقة النظام[1].

ثانيا :المساس بسلامة المعلومات

إن المســـاس بســـلامة المعلومات des intégrité'l a Atteintes donnés كســـلوك مجرم محصور في فعل الإدخال، التعديل، الحذف للمعطيات المعلوماتية المخزنة في ذاكرة الحاسوب، أوعلى الشبكة هو ما أتفقت عليه أغلب التشريعات كما جاء في نص المادة 394 مكرر 01 ق 04-05 قانون عقوبات جزائري، المادة 323-3 قانون عقوبات فرنســـي، المادة 05 من نظام مكافحة الجريمة المعلوماتية السعودي، ويقوم الفعل المادي لهذه الجريمة من خلال:

أ-حذف أي محو البيانات كليا وتدميرها إلكترونيا، كمحو الذاكرة الرئيســـية للحاســـوب، أواستعمال برمجيات خفية تعمل على محو محتوى الحاسوب أوالشبكة .

ب-تعديل البرامج والمعطيات المعلوماتية من خلال:

1- التلاعب بالبرامج أي بالنظام المعلوماتي بشكل يؤدي إلى إخفاء البيانات كليا أوجزئيا.

2- اختلاس البرامج ويكون عن طريق نسخها عن طريق أسلوب التجسس.

3- تغيير نظم عمل البرامج أي بتزويدها بتعليمات إضـــافية تتيح الوصـــول إلى جميع المعطيات التي يتضمنها الحاسوب.

ج-إدخال برامج جديدة : أي إصـــطناع برنامج كامل أوناقص في الناحية الفنية يخصـــص لارتكاب فعل الغش المعلوماتي[2].

---

[1]- ربيعي حسين، المرجع السابق، ص59.

[2]- المرجع نفسه، ص60.

البند الثالث: الأفعال الإجرامية الأخرى

وجدت هذه الجرائم مجالا تعريفيا في نصوص القانون، فقد عرفها المشرع الجزائري من خلال نص المادة 394مكرر 02.ق 04 .05 قانون عقوبات جزائري بالقول : "يعاقب بالحبس من شـهرين (02)إلى ثلاث (03) سـنوات و بغرامة من 1.000.000 دج إلى 5.000.000دج كل من يقوم عمدا أوعن طريق الغش بما يأتي :

–تصميم أو بحث أوتجميع أو توفير أونشر أوالاتجار في معطيات مخزنة أومعالجة أومرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصـوص عليها في هذا القسـم ." ولعل أن مفهومها يتضح بشكل أفضل وفق نص المادة 09 من الإتفاقية العربية لمكافحة جرائم التقنية الحديثة بوصفها لجرائم إساءة استخدام وسائل تقنية المعلومات على أنها : إنتاج أو بيع أو شراء أو توزيع أو توفير أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المواد من 06 إلى 08 من نص الإتفاقية.

– كلمة سـر أو شـفرة دخول أو معلومات مشـابهة يتم بواسـطتها دخول نظام معلومات ما بقصد إستخدامها لأي من الجرائم المبينة في المواد من 06 إلى 08 من نص الإتفاقية.

– حيازة أي أدوات أو برامج مذكورة في الفقرة أعلاه، بقصـد إسـتخدامها لغايات إرتكاب أي من الجرائم المذكورة في المواد من 06 إلى 08 من نص الاتفاقية.

–و قد تعرضـت اتفاقية بودابسـت قبل ذلك (2001) إلى تجريم هذا النوع من السـلوكات بإعتماد نفس الصـياغة و ذلك وفق ما جاء في نص مادتها السـادسـة (06) ، و ما يمكن ملاحظته أن أغلب النصوص التشريعية قد نصت على تجريم أفعال إساءة إستخدام الحاسوب بالرغم من أنه سـلوك لا يترتب عنه أي ضـرر يمس بأمن وسـلامة النظم المعلوماتية، بإعتباره سلوك خارجي يتم بعيدا عنها، غير أنه ومن جهة أخرى يتيح الاستفادة من الوسائل المادية أو البرمجيات لإرتكاب الجرائم المعلوماتية السالفة الذكر[1].

[1]–ربيعي حسين، المرجع السابق، ص66.

الفصل الثاني

آليات مكافحة الجريمة الإلكترونية

الفصل الثاني: آليات مكافحة الجريمة الإلكترونية

لقد أدت التغيرات التي أحدثها التحول إلى الرقمية وربط شبكات الكمبيوتر ببعضها و إستمرار عولمتها، وكذا التطور الكبير والمتســـارع لدور الكمبيوتر وتزايد الوعي لدى الشـــعوب لأهمية المعلومة بإعتبارها مصــدرا للقوة و الثروة، ومما يدعم هاته الفكرة هو تعميم إســتخدام الكمبيوتر والإنترنت على ســكان الكرة الأرضــية، وانشــغالا بمخاطر إحتمال إســتخدام الحاســوب وشــبكة المعلومات في إرتكاب الجرائم الجنائية، وهي جرائم حديثة، تقف حاجزا أمام تطور المجتمع على كامل الأصـــعدة، الأمر الذي أدى إلى تحرك العديد من المنظمات الدولية والإقليمية لإبرام اتفاقيات في خطوة تهدف إلى مكافحة الجريمة المعلوماتية[1]، وهذا ما ســـنحاول معالجته من خلال هذا الفصـــل حيث ســـنتطرق إلى المواجهة الدولية والوطنية للجريمة(المبحث الأول)، والقواعد الإجرائية للتحقيق في الجريمة الإلكترونية(المبحث الثاني).

[1]-فاروق خلف،الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد02،كلية الحقوق جامعة حمة لخضر، الوادي، الجزائر، 2015، ص 08.

المبحث الأول: المواجهة الدولية و الوطنية للجريمة الإلكترونية

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة، لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة، وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم. كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة.

وهذا ما سوف نحاول معالجته من خلال التطرق إلى مواجهة الجريمة الإلكترونية على المستوى الدولي(المطلب الأول)، و مواجهة الجريمة الإلكترونية على المستوى الوطني(المطلب الثاني).

المطلب الأول: مواجهة الجريمة الإلكترونية على المستوى الدولي

إن تسارع نسق التقدم التكنولوجي وظهور الفضاء الإلكتروني، قد أحدث ثورة الكترونية تشمل جميع المجالات وأضحى من الصعوبة الإستغناء عن هذه الخدمات اللامتناهية، ولكن هاته التقنيات المستحدثة كانت في نفس الوقت محلا وفرصة يستغلها البعض لممارسة أنشطة غير مشروعة، ولما كانت هذه الثورة الإلكترونية لا تخضع لأي حدود ولا تعترف بسيادة الدول أصبح من العسير إخضاعها لنظام قانوني تتكفل دولة ما وبمفردها بالتصدي لهذه الجرائم غير التقليدية، مما يستوجب تطوير البنية التشريعية الدولية ، وفي نفس الوقت إستحداث مسارات للتعاون الدولي مماثلة لإيقاع التطور المتنامي الذي تشهده هذه الجرائم سواء بترقية الآليات التقليدية أوإنشاء آليات جديدة من اجل التصدي لهاته الجرائم ومكافحتها[1].

[1]– قزران مصطفى، زرقين عبد القادر،الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن، العدد 02،جامعة خميس مليانة، الجزائر،2022، ص1225.

وهذا ما سوف نعالجة من خلال الفرع التالية:

الفرع الأول: دور الأمم المتحدة في مواجهة الجريمة الإلكترونية

توجت منظمة الأمم المتحدة، جهودها في ميدان حماية الحياة الخاصـــة في مواجهة التقدم التقني وحماية الأفراد وحرياتهم من خطر التعدي عليها، وذلك في المؤتمر الدولي الأول لحقوق الإنســـان الخاص بأثر التقدم التكنولوجي على حقوق الإنســـان مؤتمر طهران (1968) والتي تبنت الجمعية العامة للأمم المتحدة توصياته والتي أبرز ما جاء فيها، أن الحاسبات الإلكترونية تمثل أكبر تهديد للحياة الخاصـــة والحرية الشـــخصـــية، إذ أنها تعد من أدوات المراقبة وأجهزة التطفل الحديثة وخاصـة إذا تم تخزين البيانات الشـخصـية على الحاسـب الآلي وتحليلها، مما يكشف عن أنماط التعامل والعلاقات[1].

تبذل الأمم المتحدة جهودا لا يســـتهان بها في مجال محاولة التصـــدي للجرائم المعلوماتية وتؤكد على وجوب تعزيز العمل المشـــترك بين أعضـــاء المنظمة من أجل التعاون للحد من انتشـارها وتعاظم آثارها، وقد حظيت الجرائم المعلوماتية بإهتمام مؤتمرات الأمم المتحدة، وأبرزها ما جاء في هذا المجال مايلي:

عقد منظمة الأمم المتحدة المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أفريل 2015 بدولة قطر، وكان الموضـــوع الرئيســـي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوســـع للتصـــدي للتحديات الإجتماعية والإقتصـــادية وتعزيز ســـيادة القانون على الصـــعيدين الوطني والدولي، ومشـــاركة الجمهور" وقررت الجمعية العامة قرارها (67/184) النظر في ما يلي: إنشـــاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجرائم المعلوماتية.

عقد منظمة الأمم المتحدة المؤتمر الثاني عشر من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان "اســـتراتيجيات شـــاملة لتحديات عالمية نظم منع الجريمة والعدالة الجنائية وتطورها في

[1]–محمد أمين شوابكة، جرائم الحاسوب والأنترنت –الجريمة المعلوماتية، ط01، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص73.

عالم متغير، وتضـــمن جدول أعمال المؤتمر ثمانية بنود: من بينها جرائم الإنترنت، حيث دعت لجنـة منع الجريمـة والعدالـة الجنـائيـة إلى عقد اجتمـاع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها.

البند الأول: قرارات وتوصيات الجمعية العامة للأمم المتحدة :

أولا: القرار (45/121) العام 1990، وكذلك نشـــر دليل منع الجرائم المتصـــلة بأجهزة الكمبيوتر ومكافحتها في العام 1994[1].

ثـانيـا:القرار رقم (55/63) المؤرخ في 04/12/2000، والقرار رقم (56/121) المؤرخ في 19/12/2001 بشـــأن «مكافحة اســـتخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات»، يدعو هذا القرار الدول الأعضـاء، عقد وضـع التشـريعات الوطنية لمكافحة إســـاءة اســـتعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

ثـالثـا: القرار رقم (57/239) في 31/01/2003 والقرار رقم (58/199) المؤرخ في 30/01/2004 بشـأن إنشـاء ثقافة عالمية للأمن السـيبراني ودعوة الدول الأعضـاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

رابعـا: قرار لجنـة مكـافحـة المخـدرات (48/5) حول تعزيز التعـاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات".

خامســا: التوصـيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB)، التي نشــرت العام 2005 توصــيات للحد من انتشــار المبيعات غير المشــرعة من المواد الخاضعة للرقابة ولاسيما المستحضرات الصيدلانية، عبر الإنترنت[2].

[1]–فاروق خلف، المرجع السابق، ص11.

[2]- المرجع نفسه، ص12.

سادسا: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر: يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990 و قد حث في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز و بتجريم تلك الأفعال جنائيا واتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

ضمان أن الجزاءات و القوانين الراهنة بشأن سلطات التحقيق و الأدلة في الإجراءات القضائية تتطبق على نحو ملائم ، و إدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك. النص على جرائم و جزاءات وإجراءات تتعلق بالتحقيق و الأدلة حيث تدعو الضرورة

للتصدي لهذا الشكل الجديد و المعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم، كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتر، بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة ، و نصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين و تبادل المساعدة في المسائل الجنائية تنطبق بكل تام على الأشكال الجديدة للإجرام مثل الجرائم الإلكترونية ، وأن تتخذ خطوات محددة نحو تحقيق هذا الهدف، كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أوتطوير:

أ معايير دولية لأمن المعالجة الآلية للبيانات.

ب اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابر للحدود أوذات الطبيعة الدولية.

ت إبرام اتفاقيات دولية تنطوي على نصوص تنظيم و إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها و الأشكال

الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد و حرياتهم و سيادة الدول[1].

الفرع الثاني: دور المجلس الأروبي في مواجهة الجريمة الإلكترونية

كان للمجلس الاوربي دور هام في مكافحة الجريمة الإلكترونية خصوصا في الحفاظ على المعطيات الشخصية وكل ما يتعلق بالحياة الخاصة ، كون أن دول الأعضاء متقدمة علميا وتقنيا الأمر الذي دفعها لوضع التوصيات وعمل الاتفاقيات ترمي لحمايتها من كل اعتداء على منظومتها ، ومن أهم أعمال المجلس :

أولا: اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية

لم تكن إتفاقية بودابست بداية الإهتمام بالجريمة المعلوماتية، ذلك أن هذا الاهتمام سبقها بكثير مما يجعلها كنتيجة لجهود سبقتها، حيث نوقش موضوع ارتباط الحاسب الآلي بالجريمة أول مرة سنة 1976 وذلك في المؤتمر الثاني عشر لمديري معاهد البحوث في علم الإجرام تحت رقابة رعاية المجلس الأوروبي، وفي عام 1983 عقدت هيئة التعاون الاقتصادي OECD مجلسا لدراسة إمكانية التطبيقات الدولية لقوانين الجريمة التي تحدد مشاكل الجرائم المعلوماتية ، كما قامت اللجنة الأوروبية المشكلة لدراسة مشاكل الجريمة من عام 1985 إلى 1989 و صدرت التوصية رقم 89 التي تضمنت الإرشادات الموجهة للمشرعين في الدول الأعضاء بالنص لديهم على مكافحة الجريمة المعلوماتية وقد حددت هذه اللجنة مجموعتين من الأفعال المجرمة المعلوماتيا.

المجموعة الأولى: إعتبرتها إلزامية وتشمل كل من جرائم

أ الإحتيال المعلوماتي.

ب التزوير المعلوماتي.

[1]– ليندة شرا بشة، السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الإلكترونية–الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة الدراسات والأبحاث، العدد01، جامعة عاشور زيان، الجلفة، الجزائر،2009،ص 244.

ت الإتلاف المعلوماتي.

ث الإعتراض غير المصرح به لنظام الحاسب.

ج إعاقة النظام المعلوماتي عن وظيفته.

ح الدخول غير المشروع لبرامج الحاسب.

خ النسخ غير المشروع للتصميمات الخاصة برقائق الحاسبات الآلية.

د أما المجموعة الثانية: فتضم قائمة إختيارية من الأفعال المجرمة وهي كالتالي:

ذ التعديل في البيانات المخزنة بالحاسب أوبرامجه.

ر التجسس المعلوماتي.

ز الإستعمال غير المصرح به لنظام الحاسب.

س الإستعمال غير المصرح به لبرامج الحاسب التي تشملها الحماية القانونية .

وفي إطار التصـــدي أكثر لمكافحة الجريمة المعلوماتية عقد المجلس الأوروبي في 11 سبتمبر 1995 مؤتمرا لوزراء الدول الأعضاء لبحث مشاكل صياغة إتفاقيات لمكافحة الجريمة المعلوماتية بعقد إتفاقية بودابست في 23 نوفمبر 2001[1].

ففي 08 نوفمبر 2001 قامت لجنة الوزراء للمجلس الأوروبي بإعتماد اتفاقية بودابســـت وتقريرها التفسيري خلال دورتها 109.

ولقد وقع عليها في 23 نوفمبر 2001 في بودابســـت بمناســـبة المؤتمر الدولي عن جرائم الحاســـب الآلي، وقد بينت المذكرة التفســـيرية لهذه الاتفاقية أن تحديد الجرائم المعلوماتية فيها هدفه تحســين وإصـــلاح وســـائل منع وقمع الجريمة المعلوماتية، من خلال تحديد معيار بالحد الأدنى المشـــترك، الذي يســـمح باعتبار بعض التصـــرفات من قبيل الجرائم المعلوماتية، وأنه بـالإمكـان أن يتم اســـتكمـال هذه القـائمـة في القوانين الـداخليـة، كمـا أنـه يـأخـذ في الاعتبـار الممارسات غير المشروعة الأكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن

[1]- طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي، جامعة الجزائر 01،الجزائر، 2011-2012، ص69.

بعد، وقد حددت الاتفاقية اتفاقية بودابست الجرائم المعلوماتية وصنفتها في خمسة عناوين في القسم الأول من الإتفاقية.

العنوان الأول: ويضم جوهر جرائم الحاسب أوالجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات و النظم.

العنوان الثاني: ويضم الإنتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.

العنوان الثالث: ويشمل الإنتهاكات والجرائم المرتبطة بالمحتوى، وهي التي تخص الإنتاج والنشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، في المادة التاسعة من الإتفاقية.

العنوان الرابع: ويشمل الجرائم المتعلقة بالإعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة العاشرة من الإتفاقية.

العنوان الخامس: وهو يشتمل على أحكام إضافية بخصوص الشروع والإشتراك وأيضا الجزاءات والإجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية.

وقد أوجبت إتفاقية بودابست مجموعة من الشروط حتى تأخذ الأفعال السابقة وصف الجريمة وهذه الشروط هي:

أ أن ترتكب الجرائم المذكورة في الاتفاقية دون وجه حق.

ب أن ترتكب الجرائم المذكورة بطريقة عمدية من اجل إقرار المسؤولية الجنائية[1].

[1]- طرشي نورة، المرجع السابق، ص70.

الفرع الثالث: دور الجامعة العربية في مواجهة الجريمة الإلكترونية

إن المجتمعات العربية على غرار بقية المجتمعات الدولية ليست في منأى عن تهديدات الجريمة الإلكترونية، تكون هذه الأخيرة جريمة متعدية الحدود ولقد صدر القانون العربي النموذجي الإسترشادي بخصوص مكافحة الجرائم الإلكترونية، أو بالأحرى جرائم الكمبيوتر و أنترنيت كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعاً بخصوص مكافحة الجريمة المعلوماتية.

ولقد حرصت جامعة الدول العربية، منذ إنشائها على تعزيز روابط التعاون القانوني والقضائي والأمني بين أعضائها، في مجال مكافحة الجريمة وتحقيق العدالة الجنائية من خلال تنسيق سياساتها الجنائية وإرساء آليات قانونية لتنظيم هذا التعاون، كما شاركت بفاعلية جدية في جهود المنتظم الدولي لمكافحة الجريمة المنظمة عبر الوطن، حيث كان لها إسهام ملحوظ في جميع مراحل صياغة اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها، وذلك من خلال الاقتراحات التي قدمتها في اجتماعات الخبراء الحكوميين.

لقد إعتمدت جامعة الدول العربية ما سمي بقانون الإمارات الاسترشادي لمكافحة جرائم تقنية المعلومات وما فيه حكمها، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات المتحدة، وتم إعتماد هذا القانون النموذجي من قبل مجلس الوزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 495 الدورة 19، بتاريخ 8 أكتوبر 2003، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين.

إن قانون دولة الإمارات العربية المتحدة يمنع نسخ برامج الكمبيوتر بدون إذن وكل من يقبض عليه متلبسا بقرصنة البرامج سيخضع هو وشركته للمحاكمة، بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب قانون الغرامة المالية بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل 3 سنوات.

ونصت المادة السابقة من القانون العربي النموذجي الموحد في شأن مكافحة الجرائم إساءة استخدام تقنية المعلومات على معاقبة كل من زورا المستندات المعالجة آليا أوالبيانات المخزنة في ذاكرة الحاسب الآلي أوعلى شريط أوأسطوانة ممغنطة أوغيرها من الوسائل[1].

نجد من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد ، كقانون عربي نموذجي، أين نجد الباب السابع الخاص بالجرائم ضد الأشخاص، قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص، الناتج عن المعالجات المعلوماتية، وذلك في المواد 461-464 التي أشارت على وجوب حماية الحياة الخاصة، وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الإسمية وكيفية الإطلاع عليها، والعقاب المطبق في حال ارتكاب هذه الجرائم.

تم في مجال الملكية الفكرية إبرام الإتفاقية العربية لحماية حقوق المؤلف حيث نصت في مجال المعلوماتية، على توفير الحماية القانونية للبرامج المعلوماتية (برام الحاسب الآلي)، بالإضافة إلى حث وتشجيع الدول الأعضاء على ضرورة تطوير تشريعاتها الجزائية لمواجهة الجرائم المرتكبة عبر الإنترنت.

غير أن الملاحظ في هذه المحاولات على المستوى العربي هو إعتمادها على علاج نقص التشريعات والأنظمة الخاصة بموضوع جرائم الإنترنت، وذلك بوضع أطر عامة حول ضوابط استخدام وأمن الإنترنت عن طريق تحديد بعض النشاطات الإجرامية التي يمكن أن توظف الشبكة والحاسبات عموما فيها، كما تشمل هذه المحاولات على العديد من تعليمات أمن المنشئات الحاسوبية، البرامج، وبعض القواعد العامة المنظمة لإرتباط المنشئات الحكومية بالشبكة العالمية[2].

---

[1]-فريد ناشف، آليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد01، جامعة بليدة 02، الجزائر،2022، ص445.

[2]-صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم سياسية، تيزي وزو، الجزائر،2013 ص101.

المطلب الثاني: مواجهة الجريمة الإلكترونية على مستوى الوطني

سنحاول من خلال هذا المطلب إلى التطرق إلى الجهود الرامية لمواجهة الجريمة الإلكترونية على الصعيد الوطني في تشريع الجزائري(الفرع الأول)، ثم التطرق إلى التشريعات العربية الرامية لمواجهة هذه الجريمة(الفرع الثاني).

الفرع الأول: مواجهة الجريمة الإلكترونية في التشريع الجزائري

نتيجة لتأثر الجزائر بما أفرزته ثورة تقنية المعلومات من أشكال جديدة للجرائم طالت مصالح جديدة غير تلك التي يحميها قانون العقوبات، فقد تطرق المشرع الجزائري إلى تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات[1] من خلال جملة من القوانين الرامية للحد وردع مثل هذه الجرائم وهذا من خلال التالي:

البند الأول: القوانين الجزائرية العامة المنظمة للجريمة الإلكترونية

قامت الجزائر بسن قوانين خاصة بالجريمة المعلوماتية، وهي تعتبر متأخرة مقارنة ببعض الدول العربية، بالرغم من إحتلالها المراتب الأولى عربيا وإفريقيا، ومن بين التشريعات نذكر منها:

أولا: الدستورالجزائري

كفل الدستور الجزائري حماية الحقوق الأساسية والحريات الفردية، والسهر على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى، تحذر كل مساس بهذه الحقوق ، ومن بين المبادئ الدستورية نجد بحسب المواد التالية:

المادة 38 التي تنص على مايلي: ((الحريات الأساسية وحقوق الإنسان و المواطن مضمونة))، بالتالي المشرع الجزائري سعى لحماية الحقوق من جميع أشكال الانتهاكات.

[1]–سعيداني النعيم، المرجع السابق، ص79.

بينما نصـــت المادة 44 على مايلي: ((حرية الابتكار الفكري و الفني و العلمي مضـــمونة للمواطن، حقوق المؤلف يحميها القانون ، لا يجوز حجز أي مطبوع أوتســـجيل أو أية وســـيلة أخرى من وســـائل التبليغ و الإعلام إلا بمقتضـــى أمر قضـــائي، الحريات الأكاديمية و حرية البحث العلمي مضـــمونة وتمارس في إطار القانون، تعمل الدولة على ترقية البحث العلمي و تثمينه خدمة للتنمية المستدامة للأمة.

لا يجوز انتهاك حرمة حياة المواطن الخاصـــة ، وحرمة شـــرفه و يحميها القانون ، ســـرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة.))

يفهم من سـياق نص المادة ، أن المشـرع سـعى لحماية حق المؤلف، من جهة لايجوز حجز أي مطبوع أو تسجيل أوأية وسيلة أخرى من وسائل التبليغ و الإعلام، إلا بمقتضى أمر قضائي ، وحماية الحياة الخاصة من كل أشكال الإعتداءات[1].

ثانيا: قانون العقوبات الجزائري

قـامـت الجزائر بتعـديـل قـانون العقوبـات بموجـب القـانون رقم 04-15 المؤرخ في 10 نوفمبر2004، والذي أدخل عليه تعديل في 20ديسـمبر2006، والذي يتضـمن قانون العقوبات الجزائري القسـم السـابع 394 إلى 394 مكرر 6، و التي تناولت تحت عنوان المسـاس بأنظمة المعالجة الآلية للمعطيات ضمن المواد من 394 إلى 394 مكرر6، والتي تناولت أنواع الجرائم الإلكترونية و عقوبتها والتي تناول بعضها من قبل[2].

ثالثا: قانون الإجراءات الجزائية الجزائري

لقد قام المشـــرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بـالجريمـة المعلومـاتيـة، محـاولـة منـه تطوقهـا و القضـــــاء عليهـا، أوعلى الأقل الحد من

[1]– بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية–دراسة مقارنة، مذكرة لنيل شهادة ماستر في الحقوق، تخصص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم سياسة، بجاية ، الجزائر، 2017،2018 ، ص66.

[2]- بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، مجلد 14، العدد04، جامعة قسنطينة02، الجزائر، 2021، ص56.

انتشـــارها، حيث وضـــع قواعد و أحكام خاصـــة لســـلطة التحري والمتابعة، الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون الإجراءات الجزائية[1].

متابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة، والضبط ...إلخ.

البند الثاني: القوانين الجزائرية الخاصة المنظمة للجريمة الإلكترونية

نطاق الجريمة الإلكترونية، التي أصبحت لا تقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم، وعلى أســـاس أن القانون الجنائي التقليدي غير قادر على إســـتيعاب الجرائم الإلكترونية الحديثة مما دفع بالمشـرع الجزائري إلى إسـتحداث قوانين خاصـة لمواكبة هذا النوع المسـتحدث من الجرائم.

أولا: قانون البريد والمواصلات السلكية واللاسلكية

ســـعى قانون البريد والإتصـــالات لمواجهة هذه الظاهرة الإجرامية ، من خلال المواد التي تضـمنها لهذا الغرض، بات من السـهولة إجراء التحويلات المالية عن الطريق الإلكتروني نظرا لتطور تكنولوجيا الإعلام والاتصال.

كما نص القانون السالف الذكر إلى استخدام حوالات دفع عادية أو إلكترونية أو برقية.

بينما نصـت المادة 23 منه على مايلي : ((يجوز إنشـاء و/أو اسـتغلال شـبكات المواصـلات السـلكية اللاسـلكية مهما كان نوع الخدمات المقدمة، وفق الشـروط المحددة في هذا القانون وفي النصوص التنظيمية المتخذة لتطبيقه.

ولا تشـــمل أحكام هذه المادة منشـــآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي))، بحسـب هذه المادة يجوز كأصـل عام إنشـاء اسـتخدام شـبكات الإتصـال السـلكية واللاسـلكية، بإختلاف نوع الخدمة المقدمة، لكن وفقا لشـروط المحددة قانون، بإسـتثناء منشـآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي.

[1]- بوشعرة أمينة، موساوي سهام، المرجع السابق، ص69.

كما نصت المادة 93 الفقرة الأخيرة كمايلي: ((لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات[1])) .

بمعنى أنه يجب إحترام سرية المراسلات ، تطرق أيضا القانون السالف الذكر إلى معاقبة كل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب فيه الجاني بالحرمان من ممارسة كل نشاط أومهنة في قطاع المواصلات السلكية و لاسلكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس سنوات.

ثانيا: قانون التأمينات

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا، بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أونسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا أوفي المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93مكرر2[2].

-مقتضى أحكام قانون التأمينات الإجتماعية رقم (08/01) المؤرخ في 23/01/2008 شدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الإلكترونية للمؤمن له إجتماعيا، وعاقب المشرع الجزائري كل من يسلك أو يستسلم بهدف الإستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة طبقا للمادة (93مكرر 2) من نفس القانون، كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية أو نسخ البرمجيات المتعلقة

[1]- بوشعرة أمينة، موساوي سهام، المرجع السابق، 71.

[2]– فضيلة عاقلي، الجريمة الإكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإكترونية»، طرابلس، بتاريخ 24-25 مارس 2017 ،ص 118.

بإستعمال البطاقة الإلكترونية، أوالمحاولة على إرتكاب الفعل طبقا لنص المادة (93 مكرر 3) منه، كما أقر المشرع أيضا عقوبة للشخص المعنوي تتمثل في الغرامة ضعف المقررة للشخص الطبيعي طبقا لنص المادة (93 مكرر 5) من ذات القانون، ومصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح[1].

ثالثا: قانون الخاص المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

قانون رقم 09-04 المؤرخ في 16/8/2009، وهو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها، صدر هذا القانون في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16/8/2009، يحتوي على 6 فصول تناولت التعريف بالجريمة مراقبة الإتصالات الإلكترونية، القواعد الإجرائية، الهيئة الوطنية للوقاية من الجرائم المعلوماتية و الإختصاص القضائي و هذا في 19 مادة[2].

من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها رقم (09/04)، تبرز أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للإعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الإتصال عامة وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا، وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أوفي حالة توفر معلومات عن إحتمال الإعتداء على المنظومة المعلوماتية.

وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الإتصالات الإلكترونية، والفصل الرابع تعرض إلى القواعد

[1]-فاروق خلف، المرجع السابق، ص17.

[2]- بوهرين فتيحة، المرجع السابق، ص56.

الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والفصل الرابع تعرض إلى تحديد الإلتزامات التي تقع على المتعاملين في الإتصالات الإلكترونية، ثم الفصل الخامس نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السابع فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها بالمساعدة وتبادل المعلومات[1].

الفرع الثاني: جهود بعض التشريعات العربية في مواجهة الجريمة الإلكترونية

لقد ساهمت التشريعات العربية في مواجهة الجريمة الإلكترونية وهذا ما سوف نوضحه من خلال الآتي ذكره:

البند الأول: دور التشريع المصري في مواجهة الجريمة الإلكترونية

فيما يتعلق بآليات مواجهة الجريمة المعلوماتية، فلا أحد ينكر الجهود الحكومية والأهلية في مجال مكافحة، فقد أنشأت وزارة داخلية المصرية، عام 2002 آلية فى هذا الاطار تحت مسمى " إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للإدارة العامة للمعلومات والتوثيق، بالقرار الوزاري رقم 13507 لسنة 2002 .

وقد تحددت مهام الإدارة فى رصد ومتابعة جرائم التطور التكنولوجي، وتتبع مرتكبيها من خلال أحدث النظم الفنية والتقنية الحديثة وتتم الإجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة التى تتعامل معها الإدارة تتمثل فى الأنشطة غير القانونية، التي يكون فيها الكمبيوتر وسيلة أوغاية أوكليهما، وتتخذ أشكالا متعددة بما فيها الإحتيال بإستخدام البطاقات الائتمانية، وبيع المواد الإلكترونية، وإنتهاك حقوق الملكية الفكرية في مصر، وسرقة البريد الإلكتروني، والتزوير بإستخدام الماسحات الضوئية والطابعات، وجرائم الشبكات وإختراقها والدخول على أجهزة الحاسب الآلي

[1]–فاروق خلف، المرجع السابق، ص18.

للغير، وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أوالمؤسسات أوالشركات، وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أوتسيء لشكل ومظهر الدولة، ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات وإختراق المواقع الرسمية أو الشخصية أو إختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم الصناعي، وجرائم الأموال مثل السطو والإحتيال والنصب والجريمة المنظمة، وجرائم المخدرات وغسيل الأموال، وجرائم الآداب، وتجارة السلاح، وجرائم الإبتزاز الإلكتروني، وجرائم الغش الإلكتروني.

والجدير بالملاحظة أن إدارة مكافحة جرائم الحاسوب بوزارة الداخلية، تستطيع الوصول لشخص الذي يرتكب جريمة الكترونية عن طريق (I.P)، وهو العنوان الإلكتروني لهذا الشخص، فبمجرد دخول أي شخص على الأنترنت يحصل على رقم خاص به، وعن طريق هذا الرقم يتم تحديد موقعه.

وتشير مصادر بوزارة الداخلية إلى أن جرائم إنتهاك حقوق الملكية الفكرية خاصة قرصنة البرمجيات، أدت إلى خسائر كبيرة في منطقة الشرق الأوسط وإفريقيا، وهاتين المنطقتين تعدان من المناطق التى شهدت إرتفاعا كبيرا في معدل قرصنة المعلومات بين عامي 2005 ، 2006، حيث وصلت نسبة إنتشار البرمجيات المقلدة إلي 60% في منطقة الشرق الأوسط. ومن مظاهر الجهود المبذولة من الإدارة الجديدة تشكيل مجموعات عمل لمتابعة شبكة الإنترنت يوميا على مدى اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أوأعمال تمثل خروجا على القانون والشرعية أوتهديد أمن واستقرار الوطن يتم التدخل فورا بالتنسيق مع الأجهزة النوعية الأخرى.

ويأتى فى إطار الآليات الخاصة بمواجهة الجرائم الإلكترونية فى مصر، الإبلاغ عن الجرائم، حيث بإمكان المواطنين الإبلاغ عن الجرائم الإلكترونية عبر الوسائل الآتية:

أ- الموقع الإلكتروني لوزارة الداخلية علي شبكة الانترنت:(WWW.Moicgypt.gov.eg)

ب- إخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بشارع الشيخ ريحان سواء بالحضور الشخصى أو الإتصال.

ت- يمكن تلقي البلاغات من خلال الخط الساخن (108) والذى تم إنشاؤه مؤخرا لهذا الغرض.

ولا يمكن إنكار الدور الذى تمارسه الجمعية المصرية لمكافحة جرائم الإنترنت في مجال التصدى لهذا النوع من الجرائم بإعتبارها إحدى الآليات الأهلية التي بذلت من جهود فنية وبحثية من أجل الحد من جرائم المعلوماتية والانترنت، ويمكن رصد بعضا من هذه الجهود في النقاط التالية:

أ- وقعت الجمعية بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق والآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة وأعضاء النيابة العامة، والسادة المحاميين والعاملين في القطاعات القانونية في المؤسسات، وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة، بارتباط المعلوماتية والإتصالات بتخصصاتهم ومدى تأثير إستخدام تكنولوجيا المعلومات في إنجاز مهام أعمالهم، والتعريف بماهية التعامل مع الإشكاليات القانونية في حقل المعاملات الإلكترونية حول موضوعات تشمل كيفية إثبات الشخصية، كيفية التوقيع الإلكتروني، أنظمة الدفع النقدي (المال الرقمي، أو الإلكتروني)، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسؤولية عن الأخطاء و المخاطر، حجية المراسلات الإلكترونية، التعاقدات المصرفية الإلكترونية، مسائل الملكية الفكري لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها علاقات وتعاقدات البنك مع الجهات المزودة

للتقنية أو الموردة لخدماتها أو مع المواقع الحليفة، مشاريع الإندماج والمشاركة و التعاون المعلوماتي[1].

ب- مبادرة انطلقت من القاهرة كمبادرة دولية تبنتها الجمعية الدولية لمكافحة الإجرام السيبيرى بفرنسا، بالتعاون مع الجمعية المصرية لمكافحة جرائم الإنترنت تحمل بارقة أمل لسن قوانين رادعة تحمي رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومرورا بالسطو على الحقوق الفكرية، وإنتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية، وماهية التنظيم القانوني للعالم الإفتراضي بأقسامه من المعاملات القانونية الرقمية، وعقود التجارة الإلكترونية، وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت، وماهية الدليل الرقمي وحجيته في الإثبات وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم.

ت- وغنى عن البيان أن الكثير من أهل الاختصاص فى مجال جرائم المعلوماتية والإنترنت، قد إقرحوا آلية متخصصة تماما فى هذا المجال هي الشرطة الأنترنت كجهة مسؤولة عن مكافحة جرائم الانترنت

ويجب التأكيد على أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق بوزارة الداخلية، إنما هي تعمل علي تطبيق القوانين الحالية ومنها قانون العقوبات رقم 58 لسنة 1937 وقانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002، وقانون تنظيم الإتصالات رقم 10 لسنة 2003، وقانون تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، والقانون رقم 126 لسنة 2008 بتعديل قانون الطفل رقم12سنة 1996، فضلا عن قوانين أخرى من المقرر الإنتهاء منها، وتشمل قانون الجريمة الإلكترونية، وإجراءاتها الجنائية، وقانون التجارة الإلكترونية، وقانون حماية البيانات الشخصية، وتأمين الفضاء الإلكتروني، ويتم إعداد وصياغة تلك القوانين من خلال تعاون وثيق بين أجهزة الدولة التشريعية والتنفيذية والفنية.

[1]- عبد العال الدريبي، محمد صادق اسماعيل، المرجع السابق، ص119.

ومن المؤكد أنه باكتمال صـدور تلك التشـريعات تكتمل منظومة مكافحة الجرائم الإلكترونية فى مصر[1].

البند الثاني: دور التشريع السعودي في مواجهة الجريمة الإلكترونية

تعتبر المملكة العربية السـعودية من أبرز الدول المتقدمة عالمياً في توفير الخدمات الحكومية الإلكترونية من خلال البوابات والمنصـــات الحكومية؛ وهي أيضـــا من أكثر الدول عرضـــة للتهديدات الإجرامية والهجمات الإلكترونية"، لذلك إتخذت المملكة العديد من الإجراءات والآليات مكافحة الجرائم المعلوماتية وتتمثل فيما يلي:

أ- إصدار تشريع خاص بمكافحة الجرائم المعلوماتية :" نظام مكافحة جرائم المعلوماتية " لمكافحة أي جريمة من الجرائم لابد أن يكون هناك بنية قانونية عقابية تحكمها، وأن يكون هناك جهة قضائية تطبق الجزاء على من يقوم بإرتكابها.

لذلك وعلى الرغم من أن المملكة تعتمد على القوانين الشـرعية والتي تسـتمد أصـولها من كتاب الله والسنة النبوية، فإنها سبقت نظيراتها من الدول العربية في إصدار قانون خـاص بمكـافحـة جرائم المعلومـاتيـة، بمقتضـــى المرســـوم الملكي رقم م/17في 08/03/1428هـ بناء على قرار مجلس الوزراء رقم 79 بتاريخ 08/03/1428هـ . ويتألف النظام من 16 مادة، تشـمل المادة الأولى بعض التعريفات الرئيسـة، وتوضـح المادة الثانية الهدف من القانون، وتضـــمنت المواد من 3-13 الجرائم والعقوبات، وتبين المادتين 14 و 15 دور الهيئات المختصة، أما المادة 16، فقد أوضحت تاريخ دخول القانون حيز النفاذ وقد حددته في مائة وعشرين يوما من تاريخ نشره.

والجـدير بـالـذكر، أن للقـانون العـديـد من نقـاط القوة حيـث نص على الإلتزام بمـدأ الشرعية الجنائية الذي يقضـي بأن لا جريمة ولا عقوبة إلا بنص، وإشتمل على غالبية

[1]- عبد العال الدريبي، محمد صادق اسماعيل، المرجع السابق، ص121.

الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة منها[1].

ويهدف إلى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة عن الإستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الإقتصاد الوطني.

ب- المصادقة والإنضمام إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: صادقت السعودية على هذه الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة سنة 2010، التي تضم العديد من الجرائم المعلوماتية مثل سرقة بطاقات الإئتمان، وجرائم الإنترنت والإرهاب الإلكتروني، وتصنيع الفيروسات أونشرها، والقرصنة وإختراق الأنظمة والوصول والإختراق غير المشروع، وغير ذلك، وتأتي هذه الإتفاقية ضمن الجهود العربية الحثيثة التي تقوم بها جامعة الدول العربية لوضع التدابير الأمنية اللازمة لمكافحة الجرائم في شتى أشكالها وصورها ومنها جرائم تقنية المعلومات عبر إيجاد الأسس النظامية والبيئة القانونية، وتعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وترسيخ الهدف النبيل والغاية في المحافظة على الأمن والمصير المشترك الذي يتطلب تضافر الجهود للحفاظ على أمن واستقرار المجتمعات الإنسانية، وتعد هذه الإتفاقية نقطة تحول في التعاون العربي لمكافحة الجرائم السيبرانية، حيث نصت الإتفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها: التعاون القضائي، تبادل المعلومات، تبادل الخبرات، الإختصاص القضائي، تسليم المجرمين، المساعدة القضائية وغيرها من الموضوعات ذات الصلة"، و أوضحت المادة الثالثة من الإتفاقية مجالات تطبيقها على

[1]-حمزة بن فهم السليمي، الجرائم المعلوماتية والضوابط القانونية لمكافحتها على الصعيدين الوطني والدولي، مجلة الجامعة العربية، العدد59، جامعة العراق، العراق، 2023، ص585.

النحو التالي: " تنطبق الإتفاقية على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها[1]".

ت- الجهود الحكومية في مكافحة جرائم المعلوماتية : لا شك أن القوانين لا يكفي في حد ذاتها ولا يتحقق الهدف منها إلا بإحداث أجهزة ومؤسسات حكومية لتنفيذها، وفي هذا الإطار تقوم الوزارات والهيئات الحكومية السعودية المختلفة بجهود جبارة في مكافحة الإجرام الإلكتروني بمختلف أشكاله، ونذكر منها على سبيل المثال:

1. وزارة الإتصالات وتقنية المعلومات السعودية : هي الوزارة المسؤولة عن جميع وسائل الإتصال وتقنية المعلومات في المملكة، ولها سلطة إقتراح مشاريع الأنظمة المتعلقة بالإتصالات وتقنية المعلومات ورفعها إلى مجلس الوزراء، وقد قامت الوزارة بإصدار العديد من القرارات المنظمة للتعاملات الإلكترونية منها: القرار رقم 7 /ب/33181 لسنة 2003 المتضمن وضع خطة لتقديم الخدمات والمعاملات الحكومية، والقرار رقم م/ب/8189 لسنة 2005، الخاص بتشكيل لجنة داخل كل جهة حكومية للتعاملات الإلكترونية .

وقد أسهمت الوزارة بصورة كبيرة في الجهود التي بذلها الدولة لمكافحة الجرائم المعلوماتية، من خلال إقتراحها للإستراتيجية الوطنية لأمن المعلومات الخاصة بالمملكة العربية السعودية في عام 2011 التي تقدم رؤية واضحة للمملكة هدفها توفير بيئة رقمية آمنة وقوية، من خلال العمل على:

1-1 تطوير بنية تحتية للتكنولوجيا المعلومات آمنة ومرنة وموثوق فيها.

1-2 توفير موارد بشرية قادرة على تحقيق الأمن المعلوماتي بأعلى درجاته.

1-3 تهيئة بيئة الأمن المعلومات ملهمة قائمة على الثقة والشفافية والتعاون.

[1]- حمزة بن فهم السليمي، المرجع السابق، ص585.

1-4 دعم خدمات الحكومة الإلكترونية ودعم البنية التحتية للمملكة من أجل الإيفاء بأهداف الأمن المعلوماتي وخطط واستراتيجيات تكنولوجيا المعلومات والإتصالات[1].

1-5 تعزيز النمو الاقتصادي من خلال البحث والتطوير

2.وزارة الداخلية السعودية : تعتبر وزارة الداخلية الوزارة المسؤولة عن مراقبة شؤون الأمن الداخلي، وفي هذا الصدد تسعى الوزارة إلى الصدي للجرائم المعلوماتية، وتقوم بعمل إجماعات لبحث إستعداداتها لمباشرة إستقبال بلاغات هذه الجرائم، وأسلوب تحريز الأدلة الرقمية "، وتحديد هوية المجرمين الرقميين، ومراقبة الانترنت للأعراض الجنائية، وقد تصدت الوزارة إلى العديد الأنشطة الإجرامية الإلكترونية الخطيرة .

3.وزارة العدل السعودية: تختص وزارة العدل بالإشراف على النظام القضائي في المملكة، كما لها سلطة ضمان الإمتثال لمطلبات مكافحة غسل الأموال وتمويل الإرهاب، ولقد شهدت المحاكم السعودية زيادة هائلة في عدد القضايا المتعلقة بالجرائم المعلوماتية؛ حيث تعمل المحاكم على مكافحة هذه الجرائم وذلك بمعاقبة مرتكبيها والجدير بالذكر، أن مكافحة الجرائم المعلوماتية لم تقتصر على الوزارات المذكورة، بل إن هناك الكثير من الجهود التي بذلها الوزارات والأجهزة الأخرى، من بينها وزارة التعليم، من خلال ما تقوم به من مجهودات في التوعية بخطورة هذه الجرائم وذلك بعظيمها للعديد من المؤتمرات في الغرض.

4. الهيئة الوطنية للأمن السيبراني : استشعارا لأهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة وإرتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أومخاطر يشهدها القصاء المعلوماتي، أنشأت السعودية الهيئة الوطنية للأمن السيبراني التي تربط بالملك حفظه الله، وتمت الموافقة على تأسيسها وتنظيمها بمقصى الأمر الملكي بتاريخ 11/02/1439هـ الموافق ل 11/02/2017م، لتكون " الجهة المختصة في المملكة بالأمن السيراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حماية للمصالح الحيوية للدولة

[1]- حمزة بن فهم السليمي، المرجع السابق، ص 586.

وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية[1].

الفرع الثالث: جهود بعض التشريعات الغربية في مواجهة الجريمة الإلكترونية

لم تسلم الدول الغربية من هذه الجريمة المستحذثة وهذا ما سوف نوضحه من خلال التي:

البند الأول: دور المشرع الأمريكي في مواجهة الجريمة الإلكترونية

بدأ إهتمام الولايات المتحدة الأمريكية بمكافحة الجريمة المعلوماتية في 1966 في أول قضية هي قضية HANCOCKE V STATE تعرضت لموضوع إساءة استخدام الحاسبات الآلية وتتلخص وقائع هذه القضية في إتفاق مبرمج لحاسبات آلية بإحدى الشركات بالإتفاق مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 59 برنامجا ملكا للشركة التي يعمل بها والتي هي ذات أهمية كبيرة وتسليمها للشركة الأخرى في مقابل تلقيه 5 ملايين دولار وأثناء التسليم تم القبض على المتهم وقدم للمحاكمة بتهمة السرقة.

وقد تنوعت القوانين والتشريعات الخاصة بمكافحة الجريمة المعلوماتية في الولايات المتحدة الأمريكية بين ولاياتها وبين حكومتها الفدرالية بحيث صدرت عدة قوانين في هذا المجال من كلا الطرفين لذلك سنتعرض لها كما يلي:

-إستحداث نصوص عقابية خاصة فدرالية و نصوص صادرة عن ولايتها:

بالنسبة للقوانين الفدرالية الصادرة في مكافحة الجريمة المعلوماتية يمكن الاشارة للقوانين التالية :

-القانون الفدرالي الصادر في 1984 : وهو من أهم القوانين الفدرالية الخاصة بمكافحة الجريمة المعلوماتية، صدر عام 1984 وتم تعديله بشكل جوهري عام 1986 ثم عام 1994 ثم عام 1996 حيث أصبح يسمى بقانون حماية المعلومات القومية، وقد تناول هذا القانون

[1]- حمزة بن فهم السليمي، المرجع السابق، ص 586.

سـبعة نصـوص جوهرية متعلقة بمكافحة الجرائم المعلوماتية تضـمنتها المادة A1/1030 إلى A7/1030 المتعلقة بالدخول غير المصرح به إلى الحاسب الآلي.

كما جرمت المادة A4/1030 من هذا القانون أي القانون الفدرالي لجرائم الحاسـبات الآلية لعام 1996 الدخول غير المصرح به إلى نظام الحاسب الآلي متى كان بنية الحصول على أي شيء له قيمة، ومن ثم فقد حل هذا القانون مسألة اعتبار سرقة المعلومات محلا لجريمة السرقة لكي تنطبق عليها النصـوص الخاصـة بهذه الجريمة وحتى يوفر حماية ولو جزئية للمعطيات المعلوماتية بعدما تباينت أحكام الولايات في اعتبارها محلا لجريمة السرقة أم لا.

ثم جاءت المادة a5/1030 تجرم الأفعال الخاصة بإتلاف الحاسب الآلي ونظامه وما يحتوي عليه من معلومات بعدما كانت هذه المادة في نفس القانون السـابق لسـنة 1984 في فقرتها الثالثة تجرم فقط إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن إسـتعمال أنظمة الحاسبات، لذلك عدل هذا القانون بإضافة الفقرة A5 للمادة 1030 التي تتناول جريمة الإتلاف العمدي وغير المصـرح به المعلومات يحتوي عليها حاسـب آلي تابع لحكومة الولايات المتحدة الأمريكية وإدارتها أوحاسب آلي غير تابع لهذه الحكومة.

-القانون الفدرالي الصادر في 03 جانفي 1984: اهتم هذا القانون بمكافحة ناشري فيروسات الحاسبات الآلية حيث بمقتضاه يعاقب على الأعمال الخاصة بإعداد البرامج الخبيثة وإدخالها إلى أنظمة الحاسبات الآلية بهدف نشرها، بشرط أن تتم عملية إعداد الفيروس بواسطة الفاعل تم القيام بإدخاله إلى نظام الحاسب الآلي.

-القانون الفدرالي الصادر في 13 سبتمبر 1994: جرم هذا القانون نقل الفيروسات أومعلومات أورموز أو أوامر إلى الحاسب الآلي أونظام للحاسبات الآلية[1].

متى تم هذا النقل بنية إلحاق الضـرر أوإتلاف بحاسـب آلي أونظام معلوماتي أو بشـبكة للمعلومات بحيث يتمثل هذا الضرر في عدم إمكان إستخدام أي من العناصر السابقة.

[1]- طرشي نورة، المرجع السابق، ص 29.

-القانون الفدرالي الصادر في 28 فبراير 2005: قانون مكافحة إصطياد الضحايا عبر البريد الإلكتروني الصادر في 28/02/2005، والذي يجرم إستعمال طرق النصب والإحتيال عبر استخدام البريد الالكتروني، دائما وفي إطار المكافحة الموضوعية للجريمة المعلوماتية في الولايات المتحدة الأمريكية يجب الإشارة إلى التشريعات والقوانين الموضوعة من قبل ولايات هذه الدولة حيث نذكر الأهم منها على سبيل المثال:

-القانون الخاص بجرائم الحاسبات الآلية في ولاية فرجينيا الصادر سنة 1986 والذي بخص جريمة الإستعمال غير المصرح به للنظام الحاسب الآلي، حيث ينص هذا القانون على أن كل من يستخدم عمدا وبسوء نية حاسبا آليا أوشبكة للحاسبات الآلية بغرض الحصول على الخدمات التي يقدمها الحاسب أو الشبكة دون أن يكون مصرحا له بذلك يعد مرتكبا لجريمة سرقة خدمات الحاسب الآلي"، كذلك القانون الخاص بجرائم الحاسبات الآلية في ولاية كاليفورنيا لعام 1985 جرم الإستعمال غير المصرح به النظام الحاسب الآلي بالدخول في هذا النظام بغرض الحصول على أموال أوممتلكات أو خدمات، واشترط ضرورة توافر العلم بكون الدخول غير مصرح به في المادة 502 فقرة (د) من هذا القانون أو أن يكون الدخول إلى نظام الحاسب قد تم بقصد الإضرار بالغير في المادة 502 فقرة (د).

- قانون جرائم الحاسبات الآلية في ولاية "مين" الصادر عام 1998 الذي يعاقب في الفقرة الثالثة من المادة 433 منه كل من يقوم عمدا بإدخال فيروس إلى نظام الحاسبالآلي،هذا ويعاقب القانون الصادر عام 1976 والمعدل في 1996 في ولاية ميتشجان كل من يقوم بإدخال أوخلق الظروف الملائمة لدخول فيروس إلى أي من مكونات نظام الحاسب الآلي[1].

كما يعاقب قانون جرائم الحاسبات الآلية في ولاية نبراسكا الصادر في 1991 كل من يقوم بتوزيع برنامج مدمر ويعد هذا الفعل جناية وفقا لهذا القانون.

[1]- طرشي نورة، المرجع السابق، ص.29

البند الثاني: جهود المشرع الفرنسي في مواجهة الجريمة الإلكترونية

يعتبر القانون الخاص بالمعلوماتية و ملفات البيانات و الحريات رقم 78-17 ، المؤرخ في 6 جانفي 1978 ، أول قانون فرنسي ينظم الجوانب القانونية المتصلة بالمعلوماتية و أثرها على الخصوصية و أنشأت من خلاله اللجنة الوطنية للمعلوماتية و الحريات التي تختص بمراقبة سلامة تنفيذ هذا القانون.

قامت فرنسا بتطوير منظومتها القانونية لتتماشى مع مستجدات الإجرام المعلوماتي حيث تضمن قانون العقوبات الفرنسي من خلال التعديلات المتلاحقة عليه نصوصا خاصة بتجريم المساس بنظام المعالجة الآلية للمعطيات بمختلف أشكال الاعتداء حيث أدرجها في الفصل الثالث تحت عنوان :

Des atteintes aux systèmes de traitement automatisé de donnés

حيث تنص المادة 3233-1 من قانون العقوبات الفرنسي على ما يلي:

(Le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système automatisé de données est puni de deux ans d'emprisonnement et de d'un système de traitement 6000euros d'amende.)

L'ors qu'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 100000euro d'amende.

Lorsque les infractions prévues au deux premiers alinéas ont été commises a l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat. La peine est portée a cinq ans d'emprisonnement et à 150000 d'amende).

نجد أن المشرع الفرنسي طبقا لنص هذه المادة قد جرم بعض الأفعال المساهمة في حدوث الجريمة الإلكترونية من فعل الدخول أو البقاء بطريق الغش داخل كل أوجزء من نظام المعالجة الآلية للمعطيات، ويعاقب على ذلك بالحبس لمدة سنتين وغرامة مقدارها 60000 أورو[1]، أما إذا نتج عن ذلك حذف أوتعديل للمعطيات الموجودة في النظام أوتحريف لمجريات النظام،

[1]- بوشعرة أمينة، موساوي سهام، المرجع السابق، ص61.

فتكون العقوبة الحبس لمدة 3 سنوات وغرامة تقدر ب 100000أورو، وفي حالة إرتكاب الجرائم المنصوص عليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة يتم رفع العقوبة إلى السجن لمدة خمس سنوات وغرامة 150000 أورو، بينما في المادة 323_3 من نفس القانون من نفس القانون فقد جرمت إدخال بطريقة إحتيالية معطيات إلى النظام المعالجة الآلية من إستخراج ونسخ وإرسال وحذف أوتعديل البيانات التي يحتوي عليها ويعاقب عليها بالسجن لمدة خمسة سنوات وغرامة قدرها 150000 أورو، كما تطرق قانون العقوبات الفرنسي إلى ذكر حالة إستخدام أداة أو برنامج معلوماتي أو أية معطيات يمكن أن ترتكب بها أي جريمة من الجرائم المذكورة في المواد 1-323 إلى 323-3، ويعاقب على ذلك بنفس العقوبة المقررة للجريمة نفسها أو بالعقوبة أشد.

وبالخصوص العقوبات المقررة للأشخاص الطبيعيين الذين إرتكبوا الجرائم المنصوص عليها في المواد السالفة الذكر، إلى جانب العقوبات الأصلية عقوبات تكميلية تتمثل في:

المنع من الحصول على الحقوق المدنية و العائلية حسب اجراءات المادة 131-26 من قانون العقوبات الفرنسي.

المنع من ممارسة الوظائف العامة، أوأي نشاط مهني أو إجتماعي، ومصادرة المواد التي إستخدمت في إرتكاب الجريمة أو المعدة لذلك، وإذا كان الفعل مرتكبا من طرف إحدى المؤسسات فيكون العقاب بالإغلاق و الطرد من الصفقات العامة و نشر الحكم حسب شروط المادة 131-35 من قانون السالف الذكر.

إلى جانب العقوبات المقررة للشخص الطبيعي هناك عقوبات أخرى للشخص المعنوي وفقا للشروط المنصوص عليها في المادة 121-2 من قانون العقوبات الفرنسي ،حيث يعاقب بالغرامة المنصوص عليها في المادة 131-39 ، والمنع المنصوص عليه في البند الثاني من المادة السالفة الذكر، كما نص كذلك هذا القانون على معاقبة الشروع في إرتكاب أي من الجرائم المنصوص عليها سابقا بنفس العقوبة التامة، و نجد أن المشرع الفرنسي قد بذل مجهودات

معتبرة في مجال التصـدي لهذا النوع المسـتحدث من الجرائم من خلال تطوير بنيتها التشـريعية لمواجهة هذه الجريمة التي أصبحت تهدد كيان المجتمعات على حد سواء[1].

المبحث الثاني: القواعد الإجرائية للتحقيق في الجريمة الإلكترونية

إن أنشـطة مكافحة جرائم المعلوماتية أبرزت تحديات ومشـكلات جمة تغاير في جوانب كثيرة التحديات والمشكلات التي ترتبط بالجرائم التقليدية الأخرى.

فهذه الجرائم لا تترك أثرا ماديا في مسـرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على إتلاف أوتشويه أوإضاعة الدليل في فترة قصيرة[2].

فكان لزاما على المشرع الجزائري أن يساير هذه التحديات من خلال إجراءات تتوافق والجريمة الإلكترونية وهذا ما سوف نتطرق إليه من خلال الأتي:

المطلب الأول: القواعد الإجرائية الكلاسيكية و المستحدثة للتحقيق في الجريمة الإلكترونية

سنتطرق في هذا المطلب إلى القواعد الإجرائية الكلاسيكية (الفرع الأول)، والقواعد الإجرائية المستحدثة (الفرع الثاني).

الفرع الأول: القواعد الإجرائية الكلاسيكية للتحقيق في الجريمة الإلكترونية

سنتطرق من خلال هذا الفرع الى الإجراءات المادية المتمثلة في:

البند الأول: المعاينة

أولا: تعريف المعاينة تعددت التعريفات الفقهية للمعاينة، حيث أن المشـرع لم يتصـدى لتعريفها، وإنما نظم إجراءات القيام بها، وترك مجال تعريفها للفقه كالتالي:

يقصد بالمعاينة: الإنتقال إلى محل الجريمة، واثبات حالتها، وضبط الأشياء التي قد تفيد في إثبات وقوعها، ونسـبتها إلى مرتكبها، وعليه فإن كل من يترك في مكان الجريمة من أدوات وبصمات وغير ذلك من الظواهر المادية فهو في الحقيقة مساعدة لرجال الضبطية القضائية في

[1]- بوشعرة أمينة، موساوي سهام، المرجع السابق، ص63.

[2]– سامي على حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، د.ط، دار الفكر الجامعي، مصر، 2007، ص 101.

معرفة المشـتبه فيه"، وتعرف أيضـا أنها:" عرض حال عن المكان والأشـياء التي تلتقطها العين واليد"،وهي أيضـا "مشـاهدة لمكان وقوع الجريمة أو الأمكنة التي وقعت فيها أطوار الجريمة في حالة تعدد الأفعال ، ومكان الجريمة هو الشـاهد الصـامت عليها و لكي يتكلم يجب الإنتباه إلى كل شيء ذي علاقة بالجريمة و قد يكون ظاهر أوغير ظاهر كالبصمة..".

من خلال التعريفات السـابقة للمعاينة نجدها أنها تصـب في قالب واحد مع إختلاف الصـياغة، فهي تعني الفحص الشـامل والدقيق لمكان إرتكاب الجريمة بمختلف مراحلها وأدواتها... الخ، و بالتالي إعطاء صـورة حقيقية وكاملة عن كل ما يدور في فلك الجريمة المرتكبة في مكان أو أمكنة معينة، فمسرح الجريمة هو مستودع سرها لذلك يعتبر إجراء المعاينة مفتاح مسـتودع السـر الجرمي، وبالتالي معرفة الكثير من الحقائق بضـبط الأدلة وكل الآثار المادية والظروف المحيطة بالجريمة، فهي تنصب على حالة الأماكن والأشخاص والأشياء.

ومما سبق فإن الجريمة محل إجراء المعاينة هي الجريمة التقليدية والمسـتحدثة أي الجريمة المعلوماتية فيكون مسـرحيين هما مادي لضـبط الأدلة المادية ومعنوي، فالآثار المترتبة عن الجريمة المعلوماتية و التي يتم معاينتها هي المعلومات سـواء كانت كتابة أوصـورة...الخ الموجودة و المخزنة في الحواسيب و الهواتف ...فيتم فحص الرسائل المرسلة و المستقبلة و كذا الإتصلات المتبادلة[1].

ثانيا: الشـروط القانونية للمعاينة المعلوماتية: يخضـع إجراء المعاينة المعلوماتية لجملة من الشروط والأحكام القانونية نسردها كاتالي:

أ- إذن أو أمر المعاينة المعلوماتية: لا يجوز إجراء المعاينة إلا برضـا صـريح من الشـخص الذي سـتتخذ لديه هذه الإجراءات المادة 64 من قانون الإجراءات الجزائية الجزائري، لكن هذا يعتبر شـرط موقف لإجراء المعاينة في حال رفض الشـخص، وللإجابة عن هذا الإشـكال قال رئيس خلية مكافحة الجرائم الإلكترونية بأمن ولاية

[1]- حاحة عبد العالي، قلات سومية، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد01، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، 2023،ص523.

بســـكرة : " أن معاينة مثلا هاتف شـــخص تكون برضـــاه، فإذا رفض نعلم وكيل الجمهورية الذي يعطي أمر بحجز الهاتف أي تعليمة: عمل على حجز الهاتف النقال وهي تعليمة شفوية أكتبها في التقرير الإجمالي، كما ندون في المحضر أن الشخص المشـتبه فيه رفض تسـليم الهاتف وهي قرينة ضـده، وبعد إجراء المعاينة نكون أمام خيارين إرجاع الهاتف لصـاحبه أوتشـميعه مع محضـر المعاينة،" وبالنسـبة لمعاينة المساكن فيكون ذلك أيضا برضا الشخص صاحب المسكن هذا في حال عدم وجود إذن مســبق، لكن مع وجود الإذن تتم المعاينة حتى وإن رفض صـــاحب المســـكن، وخلاصـة القول أن الإذن أو الأمر ضـروري لإجراء المعاينة سواء في الميعاد المحدد أوخارجه إلا في حالة رضا الشخص الذي يكون إجراء المعاينة بصدده.

ب- وقت إجراء المعاينة المعلوماتية بما أننا بصـــدد جريمة معلوماتية فإن إجرائها يكون في كل ســاعة من ســاعات النهار أوالليل بناء على إذن مســبق من وكيل الجمهورية حســـب نص المادة 47 فقرة 3 قانون إجراءات جزائية ، على عكس الجرائم التقليدية لها وقت محدد من الساعة الخامسة صباحا إلى غاية الساعة الثامنة مساءا.

ت- مكان إجراء المعاينة المعلوماتية تجرى في أي مكان ارتكبت فيه الجريمة- مراعاة مبدأ الشخصية والعينية من خلال نصوص المواد من 582 إلى 591 قانون إجراءات جزائية والمادة 15 من القانون 09/04 الســـابق بيانه على غرار مبدأ الإقليمية[1] – ماعدا السفارات فلا يجوز معاينتها إلا بوجود إتفاقية ترفع الحصانة وبحضور السفير شخصيا.... وأيضا الثكنات العسكرية لا يجوز معاينتها إلا بواسطة وكيل الجمهورية لدى القضـــاء العســكري، حيث يمكن إختراق منظومة معلوماتية والتجســس عليها أو التلاعب في معطياتها الهامة و الســـرية أوتخريبها... الخ داخل نطاق الســـفارة أو الثكنات العسكرية.

[1]- حاحة عبد العالي، قلات سومية، المرجع السابق، ص528.

ث- الأشخاص الذين يحق لهم حضور المعاينة المعلوماتية: المتهم والضحية ومحامهم ووكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية، كما يجوز لأطراف القضية و هما المتهم و الضحية أومحاميهم في أي مرحلة من مراحل التحقيق أن يطلبوا من قاضي التحقيق إجراء المعاينة لإظهار الحقيقة وإذا رأى قاضي التحقيق أنه لا موجب لإتخاذ هذا الإجراء عليه أن يصدر أمرا مسببا خلال 20 يوم التالية لطلب الأطراف و محاميهم، وإذا لم يبت قاضي التحقيق في الطلب خلال الأجل المحدد جاز للطرف المدني أوالمتهم أووكيله الطعن أمام غرفة الاتهام وفقا لأحكام المادتين 69 مكرر و 172 من قانون الإجراءات الجزائية.

كما يستعين ضباط الشرطة القضائية أوقاضي التحقيق بأشخاص مؤهلين ونقصد في هذا المقام بالضبط المتخصصين في المجال المعلوماتي و هذا ما نصت عليه المادة 49 الأنفة الذكر.

ولقاضي التحقيق أن يخطر وكيل الجمهورية عند رغبته في إجراء المعاينة، كما أنه يستعين بكاتب التحقيق ويحرر محضر بما يقوم به من إجراءات المادة 79 قانون إجراءات الجزائية، ويقوم قاضي التحقيق أيضا بجمع الآثار التي يعثر عليها في مكان الجريمة يقوم بجردها وحفظها في إحراز ويمكن رسم مكان الجريمة وأخذ صور شمسية وإستماع إلى أقوال الأشخاص الحاضرين بعين المكان وهذا ما يقوم به ضباط الشرطة القضائية[1].

ج-محضر المعاينة المعلوماتية هو ثمرة مجهود ما قامت به الهيئات المكلفة بها، حيث أوجب قانون الإجراءات الجزائية على ضباط الشرطة القضائية تحرير محاضر عن أعمالهم التي يقومون بها ويضمن مجموع ما قام به من إجراءات وهذا ما نصت عليه المادتين 18 و 54 من قانون الإجراءات الجزائية، كما أن ضابط الشرطة القضائية ليس ملزما قانونا أن يصطحب معه كاتبا، وإن كان له الحق في الاستعانة بأعوانه في تحرير المحاضر طبقا للمادة 20 من قانون الإجراءات الجزائية وهي

[1]- حاحة عبد العالي، قلات سومية، المرجع السابق،529.

قاعدة عامة ويتضمن محضر المعاينة مجموعة من البيانات تتعلق بالجريمة والمشتبه فيه وبمحرر المحضر وصفته ورتبته وتوقيعه وختمه وتاريخ تحرير المحضر.

ح-كما أوجبت المادة 79 من قانون الإجراءات الجزائية على قاضي التحقيق تحرير محضر بما يقوم به من معاينات عند انتقاله إلى مكان الجريمة بصحبة كاتب التحقيق وعادة ما يقوم قاضي التحقيق بإعداد مسودة أثناء خروجه للمعاينة وعند عودته إلى مكتبه، يحرر الكاتب محضر المعاينة يتضمن تاريخ الخروج لإجراء المعاينة ووسيلة التنقل وتاريخ الوصول إلى الأماكن محل المعاينة ثم يتم سرد جميع العمليات التي قام بها... ووقت إنتهاء المعاينة والعودة إلى المكتب ويوقع كل من قاضي التحقيق والكاتب والمترجم عند الاقتضاء، هنا يمكن القول الخبير المعلوماتي ويرفق بمحضر المعاينة رسم تخطيطي لمكان الجريمة و كذلك الصور، إلا أن الانتقال للمعاينة في الجريمة المعلوماتية يختزل كل المسافات والوقت كونه افتراضيا، بالإضافة إلى تدوين أقوال الحاضرين وأي شخص له معلومات عن الجريمة مع التوقيع على المحضر وإن امتنعوا يصرح بذلك في المحضر.

من خلال ما سبق نجد أن محضر المعاينة في الجريمة المعلوماتية لا يختلف عن المحاضر التقليدية شكلا... وإنما الاختلاف يكون في موضوع الجريمة من ناحية سرد سلوكها الإجرامي، فنموذج محضر المعاينة نفسه ،[1] ومثال عن ذلك يمكن القول ونحن بصدد جريمة معلوماتية فيما يخص عنصر موضوع الجريمة تم معاينة مقطع فيديو مدته 10 دقائق، باللغة العربية تم التلفظ بعبارات القذف والسب من قبل المدعو..... المعروف على مستوى مصالحنا... الخ. بعد أن تم تناول مختلف النصوص القانونية التي تحكم المعاينة المعلوماتية.

[1]- حاحة عبد العالي، قلات سومية، المرجع السابق، ص530.

البند الثاني: التفتيش

أولا: تعريف التفتيش

التفتيش بمعناه القانوني هو إجراء من إجراءات التحقيق، ووظيفته البحث عن أدلة الجريمة. فهو ليس دليلا بذاته وإنما هو وسيلة للحصول على دليل، ولم تتضمن مختلف التشريعات تعريفا للتفتيش مما يترك المجال للفقه والقضاء للتطرق إلى هذه المسألة.

وقد وضـــع الفقه عدة تعريفات لعملية التفتيش، فقد عرفه البعض بأنه إجراء من إجراءات التحقيق، تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أوجنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه.

كما عرفه البعض الآخر بأنه: " إجراء من إجراءات التحقيق فهو ليس عملا إداريا من أعمال الضبط الإداري، وإنما هو عمل من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين "

وهناك من يعرفه: " التفتيش هو البحث عن مكنون ســـر الأفراد على دليل للجريمة المرتكبة أوالبحث عن الدليل، وهو إجراء من إجراءات التحقيق الإبتدائي الذي يخوله القانون لقاضـــي التحقيق أصلا وإستثناء لضباط الشرطة القضائية "

ومنهم من عرفه بأنه البحث والتحري داخل ســـر الأفراد عن أدلة تفيد لإثبات جريمة معنية إرتكبت فعلا، وهو الإجراء من الإجراءات التحقيق.

أما تفتيش الأنظمة المعلوماتية، فقد عرفه بعض الفقهاء بأنه البحث في مســتودع ســر المتهم عن أشياء مادية أومعنوية تفيد في كشف الحقيقة ونسبتها إليه[1].

أوهو البحث الدقيق والإطلاع على محل منحه القانون حماية خاصــة باعتباره مســتودع ســر صاحبه سواء كان مسكناً أوجهاز حاسوب أوأنظمة أو الانترنت.

[1]- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد05، جامعة الوادي، الجزائر، 2012، ص160.

وتفتيش النظم المعلوماتية هو إجراء يسمح بجمع الأدلة المخزنة أوالمسجلة بشكل إلكتروني، ويستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب والمعطيات المعلوماتية والإتصالات الإلكترونية.

ويقصد بالمنظومة المعلوماتية في التشريع الجزائري" أي نظام منفصل أومجموعة من الأنظمة المتصلة ببعضها البعض أوالمرتبطة، يقوم واحد منها أوأكثر بمعالجة آلية للمعطيات تنفيذ برنامج معين "

وإجمالا فإن التفتيش، سواء أكان في شكله التقليدي أوالحديث، هو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة، وعن أشياء تفيد في معرفتها ونسبتها إلى المتهم.

البند الثالث: الضبط الدليل الرقمي

اولا : تعريف الدليل الرقمي

تنوعت التعريفات التي قيلت في شأن الدليل الرقمي أو الإلكتروني وتباينت بين التوسع في مفهومه والتضييق فيه، فقد عرفته المنظمة العالمية لدليل الكمبيوتر CE10 في أكتوبر 2001 بأنه" المعلومات ذات القيمة المحتملة والمخزنة أوالمنقولة في صورة رقمية" .

كما عرفه البعض على أنه" الدليل المأخوذ من أجهزة الحاسب الآلي يكون في شكل مجلات أونبضات مغناطيسية أوكهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء[1].

وعرفه الدكتور عمر محمد بن يونس على أنه: "الدليل الذي يجد له أساسا في العالم الإفتراضي، ويقود إلى الجريمة.

[1]– بن فردية محمد، الدليل الجنائي الرقمي وجحيته أمام القضاء الجزائي–دراسة مقارنه، المجلة الأكاديمية للبحث القانوني، العدد01، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، 2014، ص278.

أما الدكتور مصـــطفى محمد موســـى فعرفه بأنه: " المعلومات المخزنة أو المنقولة بصـــفة رقمية، ويُعتمد عليها في التحقيقات وأمام المحكمة إما بالإدانة أوالبراءة .

وعليه يمكن القول أن الدليل الرقمي هو ذلك الدليل الذي ينشأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة[1].

يتمثل الضبط في العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها التحفظ عليها ،و يعتبر الضـبط هو الهدف من التفتيش والنتيجة المباشـرة و المسـتهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيـه نفس القواعـد التي تطبق بشـــــأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط[2].

ثانيا: خصائص الدليل الجنائي الرقمي

للدليل الجنائي الرقمي عدة مزايا يتصف بها دون غيره من الأدلة الجنائية، فهو دليل علمي غير مرئي ذو طبيعة تقنية يصعب التخلص منه، ويكون قابلا للنسخ وفقا للتفصيل الآتي:

أ- دليل غير مرئي: أي يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسـة، بل إدراكها يتم باســـتخدام أجهزة ومعدات الحاســـب الآلي (Hardware) ونظم برمجيات الحاسوب (Software).

ب- الدليل الرقعي دليل علمي وبالتالي يســتبعد تعارضـــه مع القواعد العلمية الســلمية وفقا لقاعدة في القضاء المقارن مفادها " إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة".

ت- الدليل الرقمي من طبيعة تقنية حيث أن التقنية تنتج نبضـــات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصـــلبة التي يتكون منها الحاســـب الآلي، فهي ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان إلى آخر عن طريق شبكات الإتصال.

---

[1]- بن فردية محمد، المرجع السابق، ص278.

[2]- بوشعرة أمينة، موساوي سهام، المرجع السابق، ص78.

ث- قابلية الدليل الرقمي للنسخ: حيث أن هذه الخاصية تقلل أو تعدم مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد والتلف، عن طريق نسخ طبق الأصل من الدليل.

ج-صعوبة التخلص من الدليل الرقمي حتى في حالة إصدار أمر من الجاني بإزالته فيمكن إسترجاعه[1].

الفرع الثاني : القواعد الإجرائية المستحدثة للتحقيق في الجريمة الإلكترونية

نظرا لعجز وسائل التحقيق الكلاسيكية عن مواجهة الجرائم الإلكترونية ، إستحدثت التشريعات وسائل إجرائية مستحدثة تتمثل في:

البند الأول: إعتراض المراسلات

واستحدث المشرع الجزائري هذه الإجراءات في قانون الإجراءات الجزائية بموجب التعديل 06/22 المؤرخ في 20 ديسمبر 2006 في الفصل الرابع من المادة 65 مكرر 5 إلى 65 مكرر 10 حيث أجاز لوكيل الجمهورية أوقاضي التحقيق أن يأذن بهذا الإجراء عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5.

ولصحة هذا الإجراء لابد من شروط شكلية وموضوعية

أولا: الشروط الشكلية لإعتراض المراسلات

أ- الإذن القضائي : جعل المشرع الجزائري بموجب المادة 65 مكرر 5 من ق إج الاختصاص بالإذن بإجراء هذه العمليات لوكيل الجمهورية, وفي حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناءا على إذن من قاضي التحقيق وتحت مراقبته المباشرة، ويمكن تعريف الإذن بأنه عبارة عن تفويض يصدر من السلطة المختصة إلى أحد ضباط الشرطة القضائية مخولا إياه إجراء تلك العمليات .

[1]- بن فردية محمد، المرجع السابق، ص278.

ويشترط القانون بالمادة 65 مكرر 7 من ق إج في الإذن الشروط التالية :

أ- أن يتضـــمن كل العناصـــر التي تســـمح بالتعرف على الإتصـــالات المطلوب التقاطها والأماكن الســـكنية المقصـــودة أوغيرها, والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

ب- أن يكون مكتوبا تحت طائلة البطلان ذلك أن الأصل في العمل الإجرائي الكتابة.

ت- أن يسلم لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أوالتحقيق ضمن نفس الشروط الشكلية والزمنية.

ث- أن يكون مصـــدره مختصـــا نوعيا ومكانيا أصـــلا بالبحث أوالتحقيق في الجريمة التي صـــدر الإذن بشـــأنها، ووفقا للقواعد العامة يتحدد الاختصـــاص النوعي بحســـب نوعية الجريمة أما الاختصاص المكاني بمحل الواقعة أوضبط المتهم, أومحل إقامته.

ب- محضـــر العمليات : إســـتوجب المشـــرع الجزائري على في المادة 65 مكرر 9 على ضـــابط الشـــرطة القضـــائية المأذون له أوالمناب من طرف القاضـــي المختص أن يحرر محضرا عن كل عملية إعتراض وتسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الإلتقاط والتثبيت والتســـجيل الصـــوتي أو الســـمعي البصـــري و يذكر بالمحضـــر أيضـــا بتاريخ وســـاعة بداية هذه العمليات والانتهاء منها، كما أوجب عليه في المادة 65 مكرر 10 وصف أونسخ المراسلات والصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة كمرفقات تودع بالملف, وتنســـخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الإقتضاء بمساعدة مترجم يسخر لهذا الغرض[1].

[1]- صالح شنين، اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور في قانون الإجراءات الجزائية الجزائري،، المجلة الأكاديمية للبحث القانوني، العدد01، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، 2010، ص68.

ولا يكون لهذه المحاضر قوة في الإثبات إلا إذا كانت صحيحة في الشكل طبقا للمادة 214 من ق إج و الأدلة الواردة بها لها حجة نسبية أي صحيحة ما لم يقدم ما يخالفها, على خلاف الأدلة الواردة بالمحاضر المنصوص عليها بالمادة 216 من ق إج.

ج-صفة القائم بالعمليات : وفقا للمواد 65 مكرر 8 9 10 يقوم بعمليات الإعتراض والإلتقاط والتسجيل ضابط الشرطة القضائية, ويجوز لوكيل الجمهورية أوضابط الشرطة القضائية المناب أن يسخر كل عون مؤهل لدى مصلحة أو وحدة عمومية أوخاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5.

ثانيا: الشروط الموضوعية لإعتراض المراسلات

بالإضافة إلى الشروط الشكلية يشترط القانون الشروط الموضوعية التالية

أ- التسبيب : يعتبر التسبيب أساس العمل القضائي, ومن ثم كان لزاما عند إصدار الإذن بإجراء عمليات الإعتراض أو الإلتقاط والتسجيل, سواء من طرف وكيل الجمهورية أوقاضي التحقيق إظهار الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية .

ب- نوع الجرائم :حصرت المادة 65 مكرر 5 من ق ا ج الإذن بإجراءات الإعتراض والإلتقاط والتسجيل في جرائم المخدرات أوالجريمة المنظمة العابرة للحدود أوالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أوجرائم تبييض الأموال أوالإرهاب أوجرائم الصرف أوجرائم الفساد.

وتجدر الإشارة إلى أنه يترتب على تخلف احد شروط عمليات الإعتراض والإلتقاط والتسجيل بطلان الإجراء وعدم الاعتماد بما قد يتمخض عنه من دليل جرمي[1].

[1]- صالح شنين، المرجع السابق، ص69.

البند الثاني: التسرب

أولا: تعريف التسرب

يعد التسرب أو الإختراق تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري أوالتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 05، كما يجوز لوكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة، ويعتبر أسلوب التسرب أو الإختراق تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أوعون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقة، ويقدم المتسرب نفسه على أنه فاعل أوشريك.

أما فيما يخص التعريف القانوني للتسرب فقد تناوله المشرع الجزائري في المادة 65 مكرر 12 من القانون رقم 06-222 المؤرخ في 20 ديسمبر 2006 بقوله : "يقصد بالتسرب قيام ضباط أوعون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أوجنحة بإيهامهم أنه فاعل معهم أوشريك لهم أوخاف، هذا ويلاحظ أن المشرع سمى هذه العملية بالتسرب في قانون الإجراءات الجزائية في حين إستخدم مصطلح الإختراق في المادة 56 من القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته ، وهما مسميان لمسمى واحد ولهما نفس المدلول.

من خلال التعريف السابق يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم[1].

[1]- زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد11، جامعة قاصدي مرباح ورقلة، 2014 ،ص 117.

ثانيا: شروط وإجراءات التسرب

أ- شروط التسرب

إشترط المشرع في المادة 65 مكرر 11 من قانون الإجراءات الجزائية وجوب أن تقتضي ضرورات التحري أو التحقيق إجراء عملية التسرب، وبمفهوم المخالفة فإن أدلة كافية تعزز الإشتباه أوتدعم الإتهام فإنه لا داعي للمخاطرة بإجراء عمليات تسرب وعليه فإن هذه الأخيرة تجرى عند الضرورة فقط المتمثلة في قلة أوصعوبة الحصول على أدلة وبراهين كافية لتحريك دعاوى العمومية.

كما إشترط المشرع في اللجوء إلى هذا الأسلوب ضرورة إرتكاب أنواع محددة من الجرائم التي تقسم بالخطورة والتعقيد، من ثم فإن الأمر بإجراء عمليات التسرب ليس مفتوحا لكل الجرائم بل هو خاص بمجموعة محددة من الجرائم المذكورة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية هذه الجرائم هي: جرائم المخدرات أوالجريمة المنظمة العابرة للحدود الوطنية أو**الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** أوجرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، إذن فيما عدا هذه الأنواع المذكورة على سبيل الحصر لا يجوز إستخدام هذا الأسلوب.

فما يلاحظ هنا أن المشرع الجزائري عند هذه الجرائم على سبيل الحصر، وقد يرجع هذا للخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة وإقتصادها، أما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل.

ب- إجراءات التسرب

هناك عدة إجراءات تطلبها المشرع لصحة عمليات التسرب، وهذا لإضفاء طابع الشرعية في الحصول على الدليل تطبيقا لمبدأ المشروعية الذي يمثل أساسا لكل إجراء صحيح، سواء من حيث الجهات صاحبة السطة في الإذن بإجراء عمليات تسرب أومن حيث الجهات المختصة بمباشرة هذا الإجراء.

ضـمانا لمشـروعية الدليل المسـتمد من إجراء عملية التسـرب إشـترط المشـرع ضـرورة حصـول المتسـرب على إذن من وكيل الجمهورية المختص وأن تتم عملية التسـرب تحت إشـرافه ومراقبته فإن قرر قاضـي التحقيق مباشـرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح إذن مكتوب لضـابط الشـرطة القضـائية الذي تتم العملية تحت مسـؤوليته، على أن يتم ذكر هويته فيه.

كما يجب أن يكون الإذن مكتوبا ومسـببا، حيث يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضـابط الشـرطة القضـائية الذي تتم العملية تحت مسـؤوليته، ولا بد أن يحدد الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر .

ويمكن أن تجدد العملية حسب مقتضيات التحري أوالتحقيق ضمن نفس الشروط الشكلية، غير يجوز للقاضـي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل إنقضـاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الإنتهاء من عملية التسرب .

يجوز لوكيل الجمهورية أوقاضـي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب إذا إقتضت ضرورات التحري في الجريمـة المتلبس بهـا أو التحقيق الابتدائي في جرائم المخدرات أوالجريمة المنظمة العابرة للحدود الوطنية أوالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أوجرائم تبييض الأموال أو الإرهاب أوالجرائم المتعلقة بالتشريع الخاص بالصـرف و كذا جرائم الفسـاد وهذا ما تناولته المادة 65 مكرر 11 ، التي اشـترطت ضرورة أن تتم العملية تحت رقابة قاضـي يقدر هذه العملية ويراقبها خطوة بخطوة لتلافي حدوث تجاوزات للقانون، ويكون هذا الإذن القضـائي مكتوبا ومسـببا تحت طائلة البطلان طبقا لأحكام المادة 65 مكرر 15[1].

وكما هو معلوم فإن بطلان الإذن يرتب بطلان كافة الإجراءات المتخذة بناء عليه، إذ يشـترط أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضـابط الشـرطة القضـائية

[1]– زوزو هدى، المرجع السابق، ص 119.

التي تتم العملية تحت مسـؤوليته، و يحرر بهذا الإذن مدة عملية التسـرب، والتي لايمكن أن تتجاوز أربعة (04) أشـهر و يمكن تجديدها حسـب مقتضـيات التحري والتحقيق كما يجوز للقاضـي الذي رخص بها أن يأمر في أي وقت بوقفها قبل انقضـاء المدة المحددة و تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب .

يسمح القانون طبقا لأحكام المادة 65 مكرر 14 لضابط أولعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأعمال التالية إقتناء أوحيازة أونقل أوتسليم أوإعطاء مواد أو أموال أومنتوجات أو وثائق أومعلومات متحصـل عليها من إرتكاب الجرائم أو المستعملة في إرتكابها، وإستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي و كذا وسائل النقل والتخزين أوالإيداع أوالحفظ أو الإتصال.

هناك من الفقهاء من يرى في هذه الأعمال خروجا عن مبدأ نزاهة ومشـروعية الدليل الجنائي للوصـول لغاية أسـمى هي ضـرورة حماية المجتمع عندما تعجز الأسـاليب التقليدية للتحري والتحقيق عن مواجهة بعض الجرائم.

يحرر ضابط الشرطة القضائية المكلف بالتنسيق تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضـابط العون المتسـرب، و كذا الأشـخاص المسخرين لهذا الغرض وهذا ما تناولته المادة 65 مكرر 13.

إذا تقرر وقف العملية أو عند إنقضـاء المهلة المحددة في رخصـة التسـرب و في حالة عدم تمديديها يمكن للعون المتسرب مواصلة المهمة للوقت الضروري الباقي لتوقيف عمليات المراقبة فـي ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن يتجاوز ذلك مدة أربعة 04 أشهر و إذا انقضـت مدة أربعة أشـهر دون أن يتمكن العون المتسـرب من توقيف نشـاطه في ظروف تضمن أمنـــــه يجب إخبار القاضي المرخص الذي يستطيع أن يرخص بتمديدها لمدة أربعة أشهر أخرى على الأكثر، للإشارة فإنه يجوز سماع ضابط الشرطة القضائية الذي تجري العملية تحت مسؤوليته دون سواه لوضعه شاهد عن العملية ، كما يرتب القانون عقوبات جزائية على

كل من يكشف هوية ضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحـل الإجراءات (المادة 65 مكرر 16).

أما عن الجهات المخولة بإجراء عمليات تسـرب فهم ضـباط الشـرطة القضـائية المذكورون في المادة 15 من قانون الإجراءات الجزائية الجزائري، ويسـتثنى من هؤلاء لإعتبارات ميدانية الولاة ورؤساء المجالس الشعبية البلدية بالإضافة إلى مساعدي ضباط الشرطة القضائية وهم الأعوان الذين جاء ذكرهم في المادة 19 من نفس القانون، فالأعوان يمارسـون مهامهم تحت مسـؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية وتصدر باسمهم.

كما أضافت المادة 65 مكرر 13 مصطلح المسخرين ويقصد بهم كل الأشخاص من الجنسين يراه ضـابط الشرطة القضـائية القائم بتنسيق عملية التسرب مفيدا لإنجاز مهمته،وهذا دائما تحت رقابة القضائية[1].

البند الثالث: مراقبة الإتصالات الإلكترونية

يقصد بمراقبة المحادثات التليفونية وتسجيلها أنها تعد إجراء من إجراءات التحقيق، يباشر في جناية أو جنحة وقعت للبحث عن أدلتها ضـد شـخص قامت تحريات جدية على أنه ضـالع في إرتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه التليفونية ما يفيد في إظهار الحقيقة، بعد أن صـعب الوصـول إليها بوسـائل البحث العادية، وكانت الجريمة على درجة من الجسامة تستأهل إتخاذ هذا الإجراء الإستثنائي[2].

ينصـــب إجراء المراقبة على الإتصـــالات الإلكترونية وفقا لما نص عليه القانون 09-04 ويقصـد بالإتصـالات الإلكترونية في مفهوم هذا القانون ووفقا لما ذهبت إليه المادة 2 بند (و): "كل تراسل أو إرسال أو إستقبال علامات أو إشارات أوكتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

---

[1]- زوزو هدى، المرجع السابق، ص ص 119، 120.

[2]-عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية-دراسة مقارنة، ط01، مكتبة القانون والإقتصاد، السعودية، 2012، ص345.

وتعرف الإتصالات الإلكترونية في الفقه المقارن، بأنها الإتصالات التي تتم عن طريق جهاز الحاسب الآلي، والتي تتخذ شكل البريد الالكتروني (E.Mail) أوشكل محادثة فورية(Instant message) والتي تتم عن طريق شبكة الانترنت.

وتبعا لذلك تأخذ الإتصالات الإلكترونية شكل مراسلات مكتوبة أومحادثات شفوية أوصور ملتقطة وهي تشكل بذلك أهم العناصر الأساسية التي يقوم عليها الحق في حرمة الحياة الخاصة.

ولهذا يعد هذا الإجراء من أخطر الإجراءات الحديثة التي تمس الإنسان في حقه في الخصوصية.

بينما يقصد بالمراقبة تجميع وتسجيل محتوى الإتصالات الإلكترونية ومن ثم الإطلاع عليها والكشف عنها وفي ذلك أيضا تهديد للحق في حرمة الحياة الخاصة، ففي كثير من الأحيان تحوي هذه الإتصالات الإلكترونية على ما يمس حياة الشخص الخاصة بوصفها مستودع سر لصاحبها، والملاحظ أن المشرع الجزائري لم يحدد وسائل المراقبة الإلكترونية ما عدا ما ذكره أنه يتوجب وضع الترتيبات التقنية الخاصة بالمراقبة، وبالرجوع إلى الفقه المقارن فقد ذهب البعض إلى تحديد أشكال المراقبة الإلكترونية في:

أ- استخدام وسائل فنية من خلال ما يسمى بقلم التسجيل أوما يسمى بالفخ والمتابعة، في هذه الحالة يتم تسجيل أسماء المتراسلين مع متهم معين أي مع بريده الإلكتروني أومع من يقوم بالمحادثة الفورية معه[1].

ب- إستخدام وسائل التنصت على محتوى الرسالة الإلكترونية أو المحادثة الفورية الإلكترونية بوسائل للإعتراض و التنصت.

[1]- دنيازاد ثابث، مراقبة الإتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسانية، العدد06، جامعة تبسة، الجزائر، 2012، ص207.

أقر المشـــرع الجزائري إجراء اللجوء إلى مراقبة الإتصـــالات الإلكترونية وتفتيش المنظومة المعلوماتية في حالات إســتثنائية فقط لما لها من إعتداء على حق الإنســان في ســرية حياته الخاصــة وإتصــالاته الشــخصــية لغرض معين، وهو الوصــول إلى حقيقة الجريمة والكشــف عن مرتكبيها خلال مرحلتي جمع الإســتدلالات والتحقيق الإبتدائي، ولم يتم التوصـــل إلى ذلك عن طريق اللجوء إلى الإجراءات التقليدية.

وهو ما قال به المشـــرع الجزائري في نص المادة 3 من القانون 09-04 بأن يتم اللجوء إلى هذا الإجراء متى تطلبت مستلزمات التحريات أوالتحقيقات القضائية الجارية.

والملاحظ أن المشـــرع الجزائري لم ينص على إمكانيـة اللجوء إلى المراقبـة بعد إرتكـاب الجريمة والبحث عن حقيقة الوصـول إلى مرتكبيها فقط، بل أقر أيضـا اللجوء إلى استعمال هذه التدابير كوســيلة وقائية للحماية من وقوع جرائم معينة هي الأفعال الموصـــوفة بجرائم الإرهاب والتخريب أوالجرائم الماســـة بأمن الدولة أو الإعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أومؤســسـات الدولة أو الإقتصــاد الوطني وفقا لما نصــت عليه المادة 4 فقرة (أ) و(ب).

ومن جهة ثالثة تهدف هذه الإجراءات إلى تعزيز التعاون الدولي في مجال مكافحة الإجرام المنظم في مجال المعلوماتية، ذلك أن هذه الجرائم تعد من الجرائم العابرة للحدود الوطنية ولا ترتبط في كثير من الأحيان بمكان معين، ويكون ذلك في إطار المســاعدة الدولية المتبادلة وفقا لما نص عليه القانون والاتفاقيات الدولية في هذا الشأن.

في حين نجد أن المشــرع الفرنســي إشــترط في نص المادة 100-1 من قانون الإجراءات الجزائية الفرنســـي بأن يكون اللجوء إلى المراقبة ضـــروري لمصـــلحة التحقيق وتتحقق حالة الضــرورة حين يكون من الصــعب معرفة الجناة وضــبط أدلة الجريمة بوســائل البحث والتحري العادية[1].

[1]- دنيازاد ثابث، المرجع السابق، ص210.

المطلب الثاني: الجزاءات المقررة للجريمة الإلكترونية في التشريع الجزائري

أجرت الحكومة الجزائرية بعض التعديلات على قانون العقوبات بموجب القانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، حيث إستحدثت عقوبات تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، وهو ما نصت عليه المواد 394 مكرر و 394 مكرر 1 ، و 394 مكرر 2 ، و 394 مكرر 3 ، و 394 مكرر 4 و 394 مكرر 5 و 364 مكرر ،6 و 395 مكرر 7 ، من القسم السابع مكرر ، وتراوحت هذه العقوبات ما بين الحبس من شهرين إلى ثلاثة سنوات مع دفع غرامة مالية من 50000.00 دج إلى 5000000.00 دج ، وذلك حسب حجم ودرجة خطورة الجريمة الإلكترونية المرتكبة .

وبعد قانون 09-04 المؤرخ في 5 أوت 2009 أول قانون في الجزائر إهتم بكيفية تبادل المعلومات الرقمية وتجري فيه كل أنواع المعاملات والخدمات الإلكترونية، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويحتوي القانون على 19 مادة موزعة على 6 فصول نوردها كالاتي:

– الفصل الأول يحتوي على أحكام عامة تبين أهداف القانون وتحدد مفهوم التقنية الواردة فيه، فضلا عن مجال تطبيق أحكامه.

– الفصل الثاني نصت مواده على ضرورة مراقبة الإتصالات الإلكترونية.

– الفصل الثالث يحتوي القواعد الإجرائية التي تخص الحجز والتفتيش في مجال جرائم تكنولوجيات الإعلام والاتصال وفقا للمعايير الدولية المعمول بها.

– الفصل الرابع تضمن التزامات المتعاملين في مجال الإتصالات الإلكترونية.

– الفصل الخامس أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته[1].

[1]– اسعيداني سلامي، طارق طراد، التجربة الجزائرية لمواجهة الجريمة الإلكترونية في ظل البيئة التفاعلية الجديدة(عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، العدد 12، جامعة عباس لغرور، خنشلة، الجزائر، 2019، ص251.

– الفصل السادس نص على التعاون والمساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضـــائي والتعاون الدولي، إلا أن تجســـيد بنود هذا القانون على أرض الواقع يبقى ضـــعيف ويرجع ذلك لإهمال المشـــرع الجزائري للجوانب التقنية الكفيلة بتصـــنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبها واقتصرت العقوبات في أغلب الأحيان على الغرامة المالية[1].

الفرع الأول: الجزاء المقرر للشخص الطبيعي المرتكب الجريمة المعلوماتية في التشريع الجزائري

أولا: الجرائم المعلوماتية المرتكبة من طرف الشخص طبيعي

أ– جريمة الدخول غير المشـــروع في المنظومة المعلوماتية في قانون العقوبات الجزائري: تنص المادة 394 مكرر عليها ، حيث جرم هذا الفعل فبمجرد إختراق جهاز كمبيوتر ســـواء كان ذلك بقصـــد الوصـــول إلى البيانات أولمجرد التســـلية ، فيعد إنتهاكا للنظام المعلوماتي بطريقة غير مشروعة .

ب– جريمة البقاء في المنظومة المعلوماتية وفقا لقانون العقوبات الجزائري: إن نص المادة 394 مكرر يجرم الدخول والبقاء فيها دون وجه قانوني أومصلحة قانونية

ت– إدخال معطيات في نظام المعالجة الآلية أو إزالتها بطرق تدليسية: نصت عليها المادة 394 مكرر 1 من قانون العقوبات.

ث– جرائم نشر المعطيات المحزنة أوالمعالجة أوالمرسلة بواسطة منظومة معلوماتية وحيازتها والإتجار فيها ، تخزين معالجة و إرسال المعطيات : طبقا للمادة 394 مكرر 2

ج–جريمة تجميع أو توفير بيانات المحزنة أومعالجتها آليا: حســـب المادة 394 مكرر 2 فالمشرع وسع نطاق الحماية لما أسماه المعالجة الآلية للمعطيات ، إذ بسط هذه الحماية ليشـمل المتصـل بالمعلومات أو البيانات فضـلا عن تحريمه الدخول غير المشـروع في المنظومة أوفي جزء منها أوالبقاء فيها.

ح–جريمة نشـر المعطيات و إفشـاءها: نصـت على هذه الجريمة المادة 394 مكرر 2 فقرة 1 من قانون العقوبات الجزائري[2].

[1]– اسعيداني سلامي، طارق طراد، المرجع السابق ، ص252.

[2]– إيمان بغدادي، المرجع السابق، ص 186.

ن- جريمة إعاقة سير المعلومات المرسلة عن طريق منظومة معلوماتية: ويكون الغرض منها القرصنة و الإتجار فيها.

و – جريمة حيازة البيانات أو المعطيات: وتتحقق الجريمة هته بتوافر أركانها

البند الأول: العقوبات الأصلية المقررة للشخص الطبيعي المرتكب الجريمة الإلكترونية في التشريع الجزائري

من خلال إستقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي، هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، و يمكن تقسيم هذه العقوبات إلى ثلاث فئات كالتالي:

أولا: جريمة الدخول أوالبقاء غير الشرعي في صورتها البسيطة

نص المشرع في قانون العقوبات بالمادة 394 مكرر فقرة 1 على عقوبة الحبس من ثلاث أشهر إلى سنة و بغرامة مالية من 50.000 دج إلى 200.000دج.

ثانيا – جريمة الدخول أوالبقاء غير الشرعي في صورتها المشددة

طبقا لنص المادة 394 مكرر 2ضاعف المشرع الجزائري العقوبة الواردة في الفقرة الأولى إذا ترتب عن الدخول أو البقاء غير الشرعي حذف أو تغيير للمعطيات، كما نصت المادة 394 مكرر 3 أنه إذا أدى الدخول أوالبقاء إلى تخريب نظام إشتغال المنظومة، فالعقوبة المقررة تكون من ستة أشهر إلى سنتين حبس وغرامة من 50000 دج إلى 300000 دج.

ثالثا: جريمة المساس العمدي بالمعطيات والتعامل بمعطيات غير مشروعة

كما ذكرنا سابقا فهذه الجريمة تتمثل في فعل الإدخال الإزالة أوالتعديل حيث نصت المادة 394 مكرر 1 من ق ع ج أن العقوبة المقررة لهذه الأفعال هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 4000000 دج.

أما جريمة التعامل في معطيات صالحة لإرتكاب الجريمة المتمثلة في الحيازة أو الإنشاء أو نشر أو إستعمال المعطيات المتحصل عليها من إحدى الجرائم[1].

[1]-رزيقة بونار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر تخصص قانون عام داخلي، كلية الحقوق والعلوم السياسية، جيجل، الجزائر، 2020، 2021، ص34.

فالعقوبة المقررة لها بنص المادة 394 مكرر 2 من ق ع ج هي الحبس من شـهرين إلى ثلاث سنوات وغرامة 1000000 دج إلى 10000000دج.

البند الثاني: العقوبات التكميلية المقرر للشـــخص الطبيعي المرتكب الجريمة الإلكترونية في التشريع الجزائري

نصـــت المادة 394 مكرر 6 من ق ع ج على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصـلية، والتي عددت محل المصـادرة على سـبيل المثال وليس الحصـر إذ ورد بها عبارة "... والوسـائل المسـتخدمة ... التي تسـتوعب أي شـيء وتجعله قابل للمصـادرة، وتتمثل في:

أولا:المصادرة

ويشـمل الأجهزة والبرامج والوسـائل المسـتخدمة في إرتكاب جريمة من الجرائم الماسـة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسـن النية الذي يجهل أن وسـائله إسـتعملت في إرتكاب الجريمة.

ثانيا:إغلاق المواقع

والأمر يتعلق بـالمواقع (les sites) التي تكون محلا الجريمـة من الجرائم المـاســـة بـالأنظمـة المعلوماتية.

ثالثا:إغلاق المحل أومكان الاستغلال

شـرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي يسـمح من خلاله بالدخول غير المصـرح به لمختلف الأنظمة وسـمح بالتلاعب بالمعطيات مثل مقاهي الأنترنت، وهنا وجب التأكد و إثبات ركن العلم لدى هذا الأخير إذ يمكن أن يكون غير مرتكب الجريمة، وعليه لا تطبق عليه العقوبة التكميلية بعد إدانة الجاني، وبالنسـبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من ق ع ج وعليه يمكن أن يكون الغلق مؤبدا أومؤقتا.

-الظروف المشدّدة

نصـت المادة 394 مكرر في فقرتيها الثانية والثالثة على تشـديد العقوبة في جريمتي الدخول أو البقاء غير شرعي إذا ما تحقق ما يلي:

إذا ترتب حذف أوتغيير في المعطيات فتضاعف العقوبة المنصوص عليها بالفقرة الأولى.

إذا ما ترتب عليه تخريب نظام إشـتغال المنظومة توقع العقوبة من سـتة أشـهر إلى سـنتين وغرامة من 50000 دج إلى 300000 دج.

والظرف المشـدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأسـاسـية، وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره.

كما نصت المادة 394 مكرر 3 على ظرف تشديد آخر وهو: تضاعف العقوبات المنصوص عليها في هذا القسـم إذ إسـتهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسـسـات الخاضـعة للقانون العام دون الاخلال بتطبيق عقوبات أشد".

وهنا ظرف التشـــديد يتعلق بمركز المجني عليه، فمتى كانت الضـــحية المســـتهدفة إحدى الهيئات المنصـوص عليها بالمادة تكون العقوبة المقررة هي ضـعف العقوبة المنصـوص عليها لكل جريمة طبقا للمواد السالفة الذكر[1].

الفرع الثاني: الجزاء المقرر للشخص المعنوي في التشريع الجزائري

جرائم المعلوماتية المرتكبة من طرف الشـخص المعنوي حسـب المادة 394 مكرر 4 ق ع ج حيث أن للشـخص المعنوي المسؤولية الجزائية ، وذلك من خلال تعديل قانون العقوبات بموجب القانون 06 – 23 المؤرخ في 20 ديسمبر 2006.

جرائم تكوين جمعية الأشرار المعلوماتيين لغرض التحضير للجرائم الماسة بالأنظمة المعالجة الآلية حسب المادة 394 مكرر 5 من قانون العقوبات الجزائري .

[1]- رزيقة بونار، المرجع السابق، ص ص 35،36.

حيث حرص المشـرع على توافر شـروط معينة بعد حصـول الإتفاق أوالإجماع أي تشـكيل فريق أومجموعة بأن يجسـد التحضـير للجريمة فعل مادي أوعدة أفعال تسـتهدف سـرقة البيانات أوتعطيل شبكة الإنترنت وعرقلة سير المعلومات أوبث الفيروسات[1].

البند الأول: العقوبات المقررة للشـــخص المعنوي المرتكب الجريمة الإلكترونية في التشـــريع الجزائري

يسـأل الشـخص المعنوي عن هذه الجرائم سـواء بصـفته فاعلا أصـليا أوشـريكا أومتدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد إرتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

وبالتالي عقوبة الشـخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصـى المقررللشخص الطبيعي .

علما أن نص المادة 18 مكرر من القانون 15/04 المتضـــمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات المقررة.

عقوبة الإتفاق الجنائي:

تبنى المشـرع الجزائري مبدأ معاقبة الإتفاق الجنائي بنص المادة 394 مكرر 5 ، بغرض التحضـير للجرائم الماسـة بالأنظمة المعلوماتية ،وعقوبة الإشـتراك في الإتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد.[2]

[1]- إيمان بغدادي، المرجع السابق، ص 187.

[2]–فضيلة عاقلي، المرجع السابق، ص130.

خاتمة

خاتمة:

من خلال طرح موضــوع آليات مكافحة الجريمة الإلكترونية على مســتويين الدولي والوطني كان الهدف الأساسي منه معرفة هذه الجريمة المستحذثة، ومدى اهتمام المشرع بها على مستوى الدولي والوطني من خلال طرح وتحليل النصوص القانونية، وعرض آليات مجابهتها .

حيث حرص المشرع على صيانة حق الفرد والمجتمع من كافة أشكال الإعتداءات التي قد تقع على حرياته الفردية خاصــة ، وكل من تسـول نفســه بأن يرتكب فعل من شــأنه أن يهدد المجتمع أو أحد أفرادها أو يلحق بمؤسساته الضرر من داخل أوخارج الوطن، فحرص المشرع على حماية من كافة الإعتداءات التي تهدد إستقراره سواء كان من داخل الوطن أومن خارجه، فعمل على تجريم كافة الأفعال التي تهدد الفرد وتمس أمنه وســـلامته من أي تعرض يمس البيئته الرقمية.

أجرى المشـــرع الجزائري التعديلات على قانون العقوبات بموجب القانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004 المعـدل والمتمم للأمر رقم 66 - 156 المؤرخ في 8 يونيو 1966 والمتضـمن قانون العقوبات، حيث اسـتحدثت عقوبات تتعلق بالمسـاس بأنظمة المعالجة الآلية للمعطيات، وهو ما نصــت عليه المواد 394 مكرر و 394 مكرر 1 ، و 394 مكرر 2 ، و 394 مكرر 3 ، و 394 مكرر 4 و 394 مكرر 5 و 364 مكرر ،6 و 395 مكرر 7 ، من القسم السابع مكرر.

وفي الأخير وبعد دراستنا لهذا الموضوع إرتئينا تقديم بعض النتائج و الإقتراحات التي تساهم في حل بعض المشكلات منها:

أ-النتائج

1. واقع الجريمة الإلكترونية يختلف عن الجريمة التقليدية.
2. إن الأفعال الإجرامية للمجرم المعلوماتي تتطور وتأخذ سلوك اجرامي جديد، الذي يقابله تطور وتعديل النصوص الناصة والرادعة.
3. صعوبة إثبات الجريمة الإلكترونية لانها لاتترك أثر مادي ملموس.

4. توحيد و تظافر الجهود الدولية منها والوطنية في مجال الأمن الإلكتروني من خلال آليات ونصوص قانونية تهدف للتعاون الأمني في المجال.

ب-الإقتراحات

1. إنشاء دورات تدريبة وخبراء في مجال معلوماتية.
2. تطوير معارف القاضي و إنشاء تخصصات في مجال الجريمة الإلكترونية.
3. ضرورة مراجعة التشريعات الوطنية لمواكبة تطور الجريمة الإلكتروني.

قائمة المصادر و المراجع

قائمة المصادر و المراجع:

أولا-المصادر:

النصوص التشريعية:

1-الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386الموافق 8يونيو 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

2-الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386الموافق 8يونيو 1966المتضمن قانون العقوبات، المعدل والمتمم.

ثانيا: مراجع

أ-الكتب متخصصة

1. جلال محمد الزغبي، أسامة أحمد مناعسة، جرائم تقنية نظم المعلومات الإلكترونية-دراسة مقارنة، ط01، دار الثقافة للنشر والتوزيع، 2010.
2. سامي على حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، د.ط، دار الفكر الجامعي، مصر، 2007.
3. عبد الصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية-دراسة مقارنة، ط01، مكتبة القانون والإقتصاد، السعودية، 2012.
4. عبد العال الدريبي، محمد صادق اسماعيل، الجرائم الإلكترونية -دراسة قانونية قضائية مقارنة، ط01، المركز القومي للإصدارات القانونية، 2012.
5. عبد الفتاح البيومي حجازي، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النمودجي، د،ط، دار الكتب القانونية، مصر، 2007.
6. لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية-دراسة مقارنة، ط،01 دار الحامد للنشر و التوزيع، عمان، 2015.
7. محمد أمين شوابكة، جرائم الحاسوب والأنترنت -الجريمة المعلوماتية، ط01، دار الثقافة للنشر والتوزيع، الأردن، 2009.
8. يعيش تمام شوقي،الجريمة المعلوماتية-دراسة تأصيلية،ط01، مطبعة الرمال ، الجزائر، 2019.

قائمة المصادر و المراجع

ثالثا: مقالات علمية و مداخلات

1. أحمد بن خليفة، حفوظة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصـــدي لها،مجلة الإمتياز لبحوث الإقتصاد والإدارة،العدد03، جامعة الأغواط، الجزائر،2017.
2. اســعيداني ســلامي، طارق طراد، التجربة الجزائرية لمواجهة الجريمة الإلكترونية في ظل البيئة التفاعلية الجديدة(عرض تشريعي قانوني)، مجلة الحقوق والعلوم السياسية، العدد 12، جامعة عباس لغرور، خنشلة، الجزائر، 2019.
3. إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصـــدي للجريمة الإلكترونية، مجلة الآفاق للبحوث و الدراسات،العدد04، المركز الجامعي إليزي، الجزائر.
4. بن فردية محمد، الدليل الجنائي الرقمي وجحيته أمام القضـــاء الجزائي–دراســة مقارنه، المجلة الأكاديمية للبحث القانوني، العدد01، كلية الحقوق والعلوم الســياســية، جامعة بجاية، الجزائر، 2014.
5. بن مالك اسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها،مجلة البيبان للدراسات القانونية والسياسية، العدد 04، كلية الحقوق والعلوم السياسية، برج بوعريريج، الجزائر، 2019.
6. بوضـياف اسـمهان، الجريمة الإلكترونية و الإجراءات التشـريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، مسيلة، الجزائر، 2018.
7. بوهرين فتيحـة، الجريمـة المعلومـاتيـة في التشـــريع الجزائري، مجلـة الحقوق والعلوم الإنسانية، مجلد 14، العدد04، جامعة قسنطينة02، الجزائر، 2021.
8. جعود ســعاد،الحماية الجزائية لتكنولوجيات الإعلام و الإتصــال في التشــريع الجزائري– دراســة مقارنة،مجلة الرســالة للدراســات والبحوث الإنســانية، العدد04،جامعة العربي التبسي، الجزائري،2022.
9. حاحة عبد العالي، قلات سومية، مقتضيات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد01، كلية الحقوق والعلوم الســياســية، جامعة بسكرة، الجزائر، 2023.

قائمة المصادر و المراجع

10. حمزة بن فهم السـليمي، الجرائم المعلوماتية والضـوابط القانونية لمكافحتها على الصـعيدين الوطني والدولي، مجلة الجامعة العربية، العدد59، جامعة العراق، العراق، 2023.
11. دنيازاد ثابث، مراقبة الاتصـالات الالكترونية والحق في حرمة الحياة الخاصـة في القانون الجزائري، مجلة العلوم الإجتماعية والإنسـانية، العدد06، جامعة تبسـة، الجزائر، 2012.
12. ربيعي حسين،المجرم المعلوماتي–شخصيته وأنواعه، مجلة العلوم الإنسانية، العدد40، جامعة محمد خيضر بسكرة، 2015.
13. صـالح شـنين، اعتراض المراسـلات وتسـجيل الأصـوات والتقاط الصـور في قانون الإجراءات الجزائية الجزائري،، المجلة الأكاديمية للبحث القانوني، العدد01، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، 2010.
14. –فاروق خلف،الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد02،كلية الحقوق جامعة حمة لخضر، الوادي، الجزائر، 2015.
15. فريد ناشـف، آليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد01، جامعة بليدة 02، الجزائر،2022.
16. قزران مصـطفى، زرقين عبد القادر،الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن، العدد 02،جامعة خميس مليانة، الجزائر،2022.
17. ليندة شـرا بشـة، السـياسـة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية– الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة الدراسات والأبحاث، العدد01، جامعة عاشور زيان، الجلفة، الجزائر،2009.
18. محمد خليفة، خصـوصـية الجريمة الإلكترونية وجهود المشـرع الجزائري في مواجهتها، العدد 01، مجلة الدراسات و الأبحاث،جامعة زيان عاشور، الجلفة،الجزائر، 2009.
19. محمد علي سـالم، حسـون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، العدد14،كلية القانون، جامعة بابل،العراق، 2007.
20. ياسـمينة بونعارة، الجريمة الإلكترونية، مجلة المعيار، العدد39، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة،الجزائر، 2015.

قائمة المصادر و المراجع

البحوث العلمية:

أ-رسائل الدكتوراه

1. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية باتنة، 2015،2016.

ب-رسائل الماجستير:

1. أمال قارة، الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي و علوم جنائية، كلية الحقوق والعلوم السياسية، الجزائر، 2005.
2. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق ، باتنة،الجزائر،2012،2013.
3. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، تلمسان،2010 ،2011.
4. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة ماجستير تخصص قانون دولي للأعمال، كلية الحقوق والعلوم سياسية، تيزي وزون الجزائر،2013 .
5. طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة ماجستير تخصص قانون جنائي، جامعة الجزائر 01، 2011-2012
6. عبد الله دغش العجمي،المشكلات العلمية والقانونية للجرائم الإلكترونية-دراسة مقارنة، رسالة مقدمة للحصول على شهادة ماجستير، تخصص قانون العام، جامعة الشرق الأوسط، الأردن، 2014.
7. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة لنيل شهادة ماجستير في العلوم القانونية، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، باتنة، 2011،2012.

قائمة المصادر و المراجع

ج-رسائل الماستر

1-بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية-دراسة مقارنة، مذكرة لنيل شـــهادة ماســـتر في الحقوق، تخصـــص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم سياسة، بجاية ، الجزائر، 2017،2018.

2-رزيقة بونار، الجريمة المعلوماتية في التشـــريع الجزائري، مذكرة لنيل شـــهادة ماســـتر تخصـص قانون عام داخلي، كلية الحقوق والعلوم السـياسـية، جيجل، الجزائر، 2020، 2021.

الفهرس

الفهرس

كلمة شكر .....

إهداء .....

قائمة المختصرات .....

مقدمة..... 1

الفصل الأول: ماهية الجريمة الإلكترونية 4

المبحث الأول: مفهوم الجريمة الإلكترونية 5

المطلب الأول: تعريف الجريمة الإلكترونية 5

الفرع الأول: تعريف الجريمة الإلكترونية 5

الفرع الثاني: أركان الجريمة الإلكترونية..... 10

البند الأول: الركن القانوني للجريمة الإلكترونية..... 10

البند الثاني: الركن المادي للجريمة الإلكترونية..... 13

البند الثالث: الركن المعنوي للجريمة الإلكترونية 18

المطلب الثاني: أطراف ودوافع إرتكاب الجريمة الإلكترونية 18

الفرع الأول: أطراف الجريمة الإلكترونية..... 19

البند الأول: الفاعل في الجريمة الإلكترونية 19

البند الثاني : المجني عليه في الجرائم التقنية..... 22

الفرع الثاني: دوافع ارتكاب الجريمة الإلكترونية 23

البند الأول:الدوافع الشخصية 23

البند الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية 26

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية 27

الفهرس

المطلب الأول: خصائص الجريمة الإلكترونية وطبيعتها 27

الفرع الأول: خصائص الجريمة الإلكترونية..... 27

البند الأول:الجريمة الإلكترونية جريمة عابرة للحدود 27

البند الثاني:الجريمة الإلكترونية جريمة صعبة الإثبات..... 28

البند الثالث: الجريمة الإلكترونية جريمة سهلة الإرتكاب..... 29

البند الرابع: الجريمة الإلكترونية جريمة مغرية للمجرمين 30

الفرع الثاني: طبيعة الجريمة الإلكترونية 30

البند الأول: جرائم التقنية جرائم أموال 30

البند الثاني: جرائم التقنية جرائم أشخاص 31

البند الثالث: جرائم التقنية جرائم أمن دولة وجرائم مخلة بالثقة العامة والآداب العامة. 32

الفرع الرابع: جرائم التقنية جرائم اقتصادية..... 33

المطلب الثاني: أنواع الجرائم الإلكترونية 34

الفرع الأول: الجريمة الإلكترونية باستخدام النظام المعلوماتي 34

البند الأول: الجرائم المعلوماتية الواقعة على الأشخاص الطبيعية 34

البند الثاني: الجرائم المعلوماتية الواقعة على أسرار 36

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي..... 37

البند الأول: جريمة الإعتداء على مكونات المادية لنظام المعلوماتي 38

البند الثاني: جرائم الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي 38

البند الثالث: الأفعال الإجرامية الأخرى 41

الفهرس

الفصل الثاني: آليات مكافحة الجريمة الإلكترونية..... 42

المبحث الأول: المواجهة الدولية و الوطنية للجريمة الإلكترونية 43

المطلب الأول: مواجهة الجريمة الإلكترونية على المستوى الدولي 43

الفرع الأول: دور الأمم المتحدة في مواجهة الجريمة الإلكترونية 44

البند الأول: قرارات وتوصيات الجمعية العامة للأمم المتحدة : 45

الفرع الثاني: دور المجلس الأروبي في مواجهة الجريمة الإلكترونية..... 47

الفرع الثالث: دور الجامعة العربية في مواجهة الجريمة الإلكترونية..... 50

المطلب الثاني: مواجهة الجريمة الإلكترونية على مستوى الوطني 52

الفرع الأول: مواجهة الجريمة الإلكترونية في التشريع الجزائري..... 52

البند الأول: القوانين الجزائرية العامة المنظمة للجريمة الإلكترونية 52

البند الثاني: القوانين الجزائرية الخاصة المنظمة للجريمة الإلكترونية..... 54

الفرع الثاني: جهود بعض التشريعات العربية في مواجهة الجريمة الإلكترونية 57

البند الأول: دور التشريع المصري في مواجهة الجريمة الإلكترونية 57

البند الثاني: دور التشريع السعودي في مواجهة الجريمة الإلكترونية..... 61

الفرع الثالث: جهود بعض التشريعات الغربية في مواجهة الجريمة الإلكترونية 65

البند الأول: دور المشرع الأمريكي في مواجهة الجريمة الإلكترونية 65

البند الثاني: جهود المشرع الفرنسي في مواجهة الجريمة الإلكترونية..... 68

المبحث الثاني: القواعد الإجرائية للتحقيق في الجريمة الإلكترونية 70

المطلب الأول: القواعد الإجرائية الكلاسيكية و المستحدثة للتحقيق في الجريمة الإلكترونية..... 70

الفرع الأول: القواعد الإجرائية الكلاسيكية للتحقيق في الجريمة الإلكترونية 70

الفهرس

البند الأول: المعاينة 70

البند الثاني: التفتيش 75

البند الثالث: الضبط الدليل الرقمي 76

الفرع الثاني : القواعد الإجرائية المستحدثة للتحقيق في الجريمة الإلكترونية..... 78

البند الأول: إعتراض المراسلات 78

البند الثاني: التسرب 81

البند الثالث: مراقبة الإتصالات الإلكترونية 85

المطلب الثاني: الجزاءات المقررة للجريمة الإلكترونية في التشريع الجزائري 88

الفرع الأول: الجزاء المقرر للشخص الطبيعي المرتكب الجريمة المعلوماتية في التشريع الجزائري 89

البند الأول: العقوبات الأصلية المقررة للشخص الطبيعي المرتكب الجريمة الإلكترونية في التشريع الجزائري 90

البند الثاني: العقوبات التكميلية المقرر للشخص الطبيعي المرتكب الجريمة الإلكترونية في التشريع الجزائري 91

الفرع الثاني: الجزاء المقرر للشخص المعنوي في التشريع الجزائري 92

البند الأول: العقوبات المقررة للشخص المعنوي المرتكب الجريمة الإلكترونية في التشريع الجزائري 93

خاتمة:..... 94

قائمة المصادر و المراجع: 96

الفهرس 101

ملخص مذكرة الماستر

من خلال دراســـتنا لموضـــوع آليات مكافحة الجريمة الإلكترونية على المســـتويين الدولي و الوطني ، إســـــتنادا إلى الإتفاقيات الدولية و الوطنية المنعقدة لمجابهة هذه الأخيرة ، حاولنا تبيان جريمـة الإلكترونيـة ، من خلال تطرق إلى موضـــــوعها و الجهود الدوليـة و الوطنيـة لمكافحتها و العقوبات المقررة لها.

الكلمات المفتاحية:

الجريمـة الإلكترونيـة؛ المجرم المعلومـاتي؛ المعلومـاتيـة؛ التعاون الدولي؛ تكنولوجيا؛ الفضـــــاء الإلكتروني.

Abstract of Master's Thesis

Through our study of the issue of mechanisms to combat cybercrime at the International and national levels, based on the International and national agreements held to counter the latter, we tried to identify cybercrime, by touching on its subject and international and national efforts to combat it and the penalties prescribed for it.

Keywords:

Cybercrime; information criminal; Informatics; International Cooperation; technology; cyberspace.