وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم
كلية الحقوق والعلوم السياسية
قسم: قانون خاص

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة الالكترونية على ضوء قانــون العقوبــات الجزائـــري

ميدان الحقوق والعلوم السياسية

الشعبة: حقوق
التخصص: قانون قضائي

من إعداد الطالبة:
داود وسيلة

تحت إشراف الأستاذ:
بن عديدة نبيل

أعضاء لجنة المناقشة

الأستاذ(ة)	عثماني محمد	رئيسا
الأستاذ(ة)	بن عديدة نبيل	مشرفا مقررا
الأستاذ(ة)	درعي العربي	مناقشا

السنة الجامعية: 2019/2018

نوقشت يوم:2019/06/25

الإهــداء

الحمد لله حمدا كثيرا مباركا وأشكره أن أكرمني بنعمته لإتمام هذا العمل المتواضع.

إلى من لا نبي بعده إلى البشير النذير وخاتم المرسلين من بلغ الرسالة نبيّ الرحمة سيّدنا محمد صلى الله عليه وسلم.

أهدي ثمرة جهدي إلى روح أبي الطاهرة وأدعو الله أن ينير قبره كما أنار حياتي والى الوالدة الكريمة أطال الله في عمرها.

إلى كل من شاركني أفراحي وأحزاني وكانوا لي رافدا في مشواري الدراسي زوجي، أبنائي والعائلة الكريمة من كبيرهم إلى صغيرهم حفظهم الله جميعا من كل مكروه.

كلمـة شكـر

أتقدم بالشكر الخالص للأستاذ المشرف الأستاذ بن عديدة نبيل الذي لم يبخل عليّ بنصائحه وتحفيزا ته التي تبث الثقة والاستمرار فكان خير عون بعون الله تعالى في هذا العمل، كما أتقدم بالشكر مسبقا لأعضاء لجنة المناقشة بقبولها مناقشة وإثراء هذا البحث.

قائمة المختصرات

أولا: بالعربية

1-ق ع ج: قانون العقوبات الجزائري

2-ق ع ف: قانون العقوبات الفرنسي

3-الخ: إلى آخره.

4-ص: صفحة.

5- ج ر: جريدة رسمية.

ثانيا: بالفرنسية

1-GRC : Gendarmerie Royal du Canada

مقدمـــــة

عرفت السنوات الأخيرة ثورة جديدة قلبت مناحي الحياة راسا على عقب وهي ثورة تكنولوجيا المعلومات وظهور ما يسمى بالمعلوماتية والتي حولت العالم الى وحدة سكنية واحدة، فالتطور وسائل الاتصال المرئية والمعلوماتية قد ترتب عليه اكتشاف انظمة تكنولوجية جديدة ادت الى ظهور استخدامات حديثة لوسائل الاتصال عن بعد.

وتعد العمليات الالكترونية محورا رئيسيا في تكنولوجيا المعلومات عن بعد وقد اثرت بشكل كبير على البنيان الاداري والاقتصادي من خلال استخدام تقنيات العمل بالأنترنت وذلك من اجل خلق أعمال وتطوير أنشطة، فقد خلقت هذه الثورة التكنولوجية حاجة ماسة لتطوير نظم المعلومات في جميع قطاعات الحياة وذلك لمسايرة التطورات التكنولوجية والاجتماعية والاقتصادية التي تتزايد يوما بعد يوم، وهذا كله من اجل هدف واحد هو الاستفادة بأكبر شكل ممكن من أثار هذه الثورة خاصة وان المستقبل سيشهد المزيد من التطور في نظم المعلومات بعد ان اتصلت هذه النظم بالأقمار الصناعية وبدا العالم يدخل عصرا جديدا هو عصر المعلوماتية ولكن الامر المؤكد ان هذه الثورة لها انعكاسات سلبية على مختلف مناحي الحياة واكبر انعكاس كان على الانسان بذاته والذي استغل هذه الثورة في خلق العديد من الاساليب الاجرامية التي سهلت له ارتكاب العديد من الجرائم ضد الاشخاص والاموال وكذا الدول فكلما زاد الاعتماد على الحاسبات في مختلف مجالات الحياة زادت مخاطر الغش والتزوير والاتلاف العمدي والتجسس وغيرها من الجرائم المرتكبة سواء عند ادخال البيانات الى الحاسب ،عند تبليغ البيانات الى مستخدميه، أو عند تخزين البيانات الى حين استخدامها، أو الاستخدام الغير المشروع لهذه الحاسبات عن طريق القرصنة والاختراق وعدة برامج خاصة بها والامر الذي يزيد من خطورة هذه الجرائم هو انها تتعدى حدود المكان كما ان محلها قد يتعدى القيم المادية ليكون قيما معنوية لا تلمسها الايدي ولا تبصرها الاعين.

ولعل اهم ما يميز التكنولوجيا الحديثة للمعلومات انها تعتمد على تحويل البيانات وهي غير ملموسة من شكل الى اخر وذلك اما بمعالجتها بواسطة الوسائل الالكترونية، او بنقلها من مكان أو من شخص الى اخر غير ان ملاحظ على هاته الوسائل انتهاكها للحياة الخاصة

والاسرار المهنية والاقتصادية فالتطور الهائل الذي عرفته شبكة الانترنت تسبب في تهديد الحريات الفردية من خلال الاعتداء عليها وهو ما يستوجب ايجاد اليات مناسبة للممارسة الرقابة عليها وتجنب الخطر خاصة وان النصوص العقابية المطبقة لم تعد كافية لحماية الحياة الخاصة من الاعتداء عليها باستعمال وسائل الكترونية مستحدثة وهذا ما يفسر عجز القوانين العقوبات الحالية التي وضعت في ظروف مختلفة عن تلك الى خلفتها ثورة المعلومات عن مواجهة هذا النوع الجديد من الجرائم واستيعابه .

وعلى ضوء ما سبق تبرز اهمية هذا البحث حيث يعتبر موضوع الجرائم الالكترونية من مواضيع المستحدثة وبالتالي فالجرائم المرتبطة به تعد حديثة كذلك وهي في تطور وتجدد مستمر وبأشكال خطيرة.

بالإضافة الى الفراغ القانوني المتعلق بهذا النوع من الجرائم وعدم قدرة النصوص العقابية على مسايرة التطور الغالب على هذا النوع من الجرائم وصعوبة اثباتها عن طريق الادلة المتحصل عليها من الوسائل الالكترونية مما يساهم بشكل كبير في فرار الجناة من العقاب.

ان الهدف من هذه الدراسة هو الرغبة في تسليط الضوء على ظاهرة اجرامية تزداد بمعدلات قياسية خاصة مع الانتشار الهائل لاستعمال جهاز الكمبيوتر واستعمال المتزايد لشبكة الانترنت والذي تنبه له المشرع الجزائري من خلال اصدار قانون 15/04 رغبة منه لمسايرة التشريعات العالمية الخاصة بالتصدي لهذه الظاهرة باعتبارها شكلا من اشكال الجريمة المنظمة والتي صادق على اتفاقية الامم المتحدة لمكافحتها سنة 2002 من خلال ارساء نصوص قانونية يجب فهمها.

إن البحث في هذا الموضوع كان بالرغم من الصعوبات العديدة التي واجهتها منها قلة المراجع التي تعالج هذا نوع من الجرائم على ضوء قانون الجزائري وبصفة ادق قانون العقوبات بالإضافة الى ضيق الوقت الذي لم يسمح لنا بتناول موضوع الجريمة الالكترونية بشكل مفصل في دراستنا له من خلال المنهج الدراسي وهو الامر الذي شدني الى الخوض فيه ومحاولة دراسته لكونه يتميز بكثرة المستجدات خاصة على الواقع العملي، وقد اعتمدت في دراستي هاته على المنهج التحليلي الوصفي الذي يعتمد على تحليل النصوص القانونية ووصفها.

ومن خلال ما سبق تتبلور الاشكالية في السؤال التالي:

ماهية الجريمة الالكترونية ومامدى معالجتها من قبل المشرع الجزائري ولتحليل هاته الاشكالية اتبعنا الخطة التالية، حيث تناولنا في الفصل الاول ماهية الجريمة الالكترونية من خلال مبحثين عالجنا في المبحث الاول مفهوم الجريمة الالكترونية والمبحث الثاني خصائص واسباب الجريمة الالكترونية.

وفي الفصل الثاني تطرقنا الى صور الجريمة الالكترونية المبحث الاول جريمة الاعتداء على نظام المعالجة الالية للمعطيات وجريمة التزوير الالكتروني وفي المبحث الثاني الجزاءات المقررة للجريمة الالكترونية.

لقد تغيرت أنماط الجريمة، فلم تعد الاعتداءات تستهدف النفس والمال فقط، بل طالت المعلومات، وهو ما أصبح يعرف على الساحة الدولية بإجرام ذوي الياقات البيضاء "White Collar Crime"، حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم، ليس فقط دون إراقة دماء ولكن أيضا بدون الانتقال من أماكنهم، بل ترتكب الجريمة في أمن وهدوء، وهو ما جعل البعض يصفها بالجرائم الناعمة (Soft Crime)، فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في اقتصاديات كبرى الشركات، وهذا النوع من الجرائم ليس مقصورا على منطقة، أو دولة معينة، لكنها مشكلة عالمية [1].

وما يشهده العالم في الوقت الراهن من ازدياد مخيف في استعمال تقنية المعلومات واعتماد كبير عليها في تسير شؤونه وهو الأمر الذي يزيد في المقابل من الإجرام ألمعلوماتي، وتعتبر الجريمة الالكترونية من الظواهر الإجرامية الحديثة التي لابد من تحديد مفهومها كخطوة أولى نحو تعرف على هاته الظاهرة من جميع جوانبها القانونية وتميزها عن غيرها من الجرائم التقليدية سواء في محلها أو خصائصها، وعلى إثر ما جاء سنتطرق في هذا الفصل إلى مبحثين:

المبحث الأول سنتطرق فيه لمفهوم الجريمة الالكترونية والمبحث الثاني إلى خصائص وأسباب هاته الجريمة.

[1]– سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، عدد 7، جامعة محمد خيضر، بسكرة، أفريل 2010، ص275 ،276 .

المبحث الأول: مفهوم الجريمة الالكترونية

تعتبر الجريمة الالكترونية من الظواهر الحديثة ودلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لهما، ولكن الفقه لم يتفق على تعريف محدد، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني.[1]

غير أن التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حتى الآن حال دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة الالكترونية، وما ورد من تعريفات في الفقه إنما اقتصر على ناحية محل بحث الفقيه.[2]

وفي غياب تعريف محدد وشامل للجريمة الالكترونية نجد أنفسنا في مواجهة مشكلات عملية أهمها صعوبة مواجهة هاته الجريمة وتعذر تقديم الحلول المناسبة لمكافحاتها.

وعليه سنتطرق في هذا المبحث إلى مطلبين، المطلب الأول سنتناول فيه تعريف الجريمة الالكترونية، وفي المطلب الثاني أطراف الجريمة الالكترونية.

المطلب الأول: تعريف الجريمة الالكترونية

سنتكلم فيه عن تعريف الجريمة الالكترونية من الجانب اللغوي والاصطلاحي كفرع أول أما الفرع الثاني سنبين فيه تعريف المشرع الجزائري لهاته الجريمة.

الفرع الأول: التعريف اللغوي والاصطلاحي للجريمة الالكترونية

أدت الحداثة التي تتميز بها الجريمة الالكترونية واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد لدلالة عليها، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وذلك خشية حصرها في مجال ضيق.

وترتيبا على ذلك اختلفت مصطلحات الجريمة الالكترونية فما المقصود بهذه المصطلحات؟ وما هو المصطلح المناسب لهذه الجريمة؟

وعليه سنحاول تعريف مصطلح الجريمة الالكترونية من الجانب اللغوي والاصطلاحي:

---

[1]– خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية، 2008، ص 41.

[2]– محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، طبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص41.

1- التعريف اللغوي للجريمة الالكترونية

لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم أو التسمية الدقيقة لهذا المصطلح، أي الجريمة الالكترونية لوجود مجموعة من المفاهيم المتقاربة والمنشقة من الإجرام الالكتروني والغش ألمعلوماتي، والانحراف الذي يقع بواسطة الجانب الآلي أو جرائم الانترنت حيث تطرح إشكالية التشابه والاختلاف مصطلحي الجريمة الالكترونية والجريمة المعلوماتية فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية أو العكس؟[1]

حيث ترى الدكتورة غنية باطلي في هذا الشأن: أن استعمال مصطلح الجريمة الالكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش ألمعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص.[2]

إن مصطلح الجريمة الالكترونية يعد أوسع من الجريمة المعلوماتية التي يقصد بها الجرائم المرتكبة على الكمبيوتر وجرائم الانترنت فالجريمة الالكترونية هي جريمة محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر أو أية وسيلة الكترونية أخرى، وهذا ما أكدته اتفاقية بودابست أو الاتفاقية المتعلقة بالجريمة الالكترونية والتي صادق عليها المجلس الأوربي في بودابست-المجر في 23 نوفمبر 2001.[3]

2- التعريف الاصطلاحي للجريمة الالكترونية

عرفت الجريمة بصفة عامة على أنها " كل فعل غير مشروع صادر عن إرادة آثمة يقرر لها القانون عقوبة أو تدبير احترازي " بينما تعتمد الجرائم الناشئة عن الاستخدام الغير المشروع

---

[1]- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 43.

[2]- غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية لنشر والتوزيع، الجزائر، 2015، ص 12،13.

[3]- نفس المرجع، ص 24.

اتفاقية بودابست :الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية تتكون من 48 مادة منها 35 مادة في مجال مكافحة الجرائم المعلوماتية.

شبكة الانترنت على المعلومة بشكل رئيسي وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[1].

وقد اختلفت التعريفات الفقهية والقانونية خاصة بهاته الجريمة نظرا لاختلاف الوسائل والنظم القانونية المتعلقة بها، حيث انقسم تعريف هذه الظاهرة الإجرامية إلى عدة اتجاهات تقوم على أسس مختلفة.

أ- على أساس وسيلة ارتكاب الجريمة

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما كان الحاسوب أو إحدى وسائل التقنية من وسائل ارتكابها حتى تعتبر من جرائم الانترنت حيث يعرف الفقيه Mawre الجريمة الالكترونية بأنها الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه.[2]

بينما يعرفها بعض الفقه أنها نشاط إجرامي تستخدم فيه التقنية الالكترونية -الحاسب الآلي وشبكة الانترنت -بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف.[3]

وترتيبا على هذه التعاريف، تعرف الجريمة الالكترونية على أنها الفعل الغير مشروع المرتكب بواسطة الكمبيوتر أو الانترنت أو أي وسيلة الالكترونية وقد لقي هذا التعريف عدة انتقادات أهمها اتسامه بالعمومية والاتساع لأنه يدخل كل سلوك ضار بالمجتمع يستخدم فيه الجانب الآلي في قائمة الجرائم الالكترونية.

ب-على أساس موضوع الجريمة

يعتمد هذا الاتجاه في تعريف الجريمة الالكترونية، على أساس أن موضوع الجريمة هو المعالجة الآلية للبيانات فكل تعريف أو تعديل أو نقل أو نسخ غير مشروع لها يعد جريمة الكترونية، وعليه فقد عرفت الجريمة الالكترونية وفقا لهذا الاتجاه بأنها: الجريمة المرتكبة عبر الانترنت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر[4].

---

[1]- غنية باطلي المرجع السابق، ص 5.

[2]- نفس المرجع، ص 15.

[3]- علي كحلوش، جرائم الحاسوب وأساليب مواجهتها، مجلة الشرطة، المديرية العامة الأمن الوطني، عدد 84، 13 جويلية 2007، ص 51، نقلا عن يوسف الصغير، الجرائم المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجيستر كلية الحقوق، جامعة مولود معمري، تيزي وزو الجزائر، ص9.

[4]- نفس المرجع.

كما عرفت الدكتورة هدى قشقوش الجريمة الالكترونية بأنها سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[1].

نستنتج من هذه التعريف أنها اعتمدت على محل الجريمة دون الوسيلة المرتكبة بها، وهذا ما يشكل أهم انتقاد موجه لها لأن ما يميز الجريمة الالكترونية أنها تتم في وسط افتراضي وتمس بمعطيات الحاسب الآلي.

ج –على أساس توفر المعرفة بتقنية المعلومات

تعتمد هذه التعاريف على أساس توافر المعرفة الفنية بتقنية المعلومات لدى الجاني في الجريمة الالكترونية، حيث عرفها الأستاذ David Thomson بأنها أية جريمة متطلبا لافتراضها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب[2].

كما عرفت الجرائم الالكترونية التي يتم ارتكابها إذا قام شخص ما معرفته بالحاسب الآلي بعمل غير قانوني[3].

ومستخلص من هذا التعريف أنه ارتكز في تعريفه للجريمة الالكترونية على معيار شخصي أي مدى معرفة الجاني بتقنية المعلومات وإتقانها وهو ما يعاب عليه لأنه حصر وربط شخصية الجاني في تعريفه للجريمة الالكترونية وهذا لا يكفي حيث من الممكن لأي شخص عادي حتى ولم يكن مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية.

د –على أساس الجمع بين عدة معايير

نظرا لعدم نجاعة التعاريف السابقة للجريمة الالكترونية، اعتمد أصحاب هذا الاتجاه إلى الجمع بين عدة معايير وعرفوا الجريمة عبر الانترنت بأنها الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو الجريمة التي يكون الحاسب نفسه ضحيتها[4]، وعرفت كذلك بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها[5].

---

[1]– يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ظبي 10–12–2012، ص 08 نقلا عن يوسف صغير، مرجع سابق ص 12.

[2]– هدى قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000، ص12.

[3]– هشام محمد فريد رستم، الجرائم المعلوماتية، الطبعة الثالثة، كلية الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت، من 01 إلى 05 ماي 2000 جامعة الإمارات العربية المتحدة، 2004، ص 407.

[4]– يوسف الصغير، المرجع السابق، ص11.

[5]– هشام محمد فريد رستم، المرجع السابق، ص 409.

ويعاب على هذا الاتجاه أنه جمع بين عدة تعاريف لتعريف جرائم الانترنت أو جرائم الكمبيوتر ومع هذا فان هذا التعريف يعد الناجح والراجح من الناحية العملية نظرا لتنوع الجرائم الالكترونية وتطورها.

كما أن للجريمة الالكترونية عدة مسميات نذكر منها:

1. جرائم الحاسوب والإنترنت.
2. جرائم التقنية العالية.
3. الجريمة الإلكترونية.
4. الجريمة السايْبِريّة.
5. جرائم أصحاب الياقات البيضاء.

ومثل تلك الجرائم قد تهدد أمن الدولة وسلامتها المالية والقضايا المحيطة بهذا النوع من الجرائم الكثيرة وأبرز أمثلتها الاختراق أو القرصنة وانتهاك حقوق التأليف ونشر الصور الإباحية للأطفال ومحاولات استمالتهم لاستغلالهم جنسيا والتجارة غير القانونية (كتجارة المخدرات) كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني[1].

ولا تقتصر الجرائم الإلكترونية على أفراد أو مجموعات وإنما قد تمتد إلى مستوى الدول لتشمل التجسس الإلكتروني (وأبرز أمثلته ما كشفته تسريبات المتعاقد السابق مع وكالة الأمن الوطني الأميركي إدوارد سنودن، الذي كشف مخططات أميركية عديدة للتجسس ليس على الأفراد فحسب بل على اتصالات دول أخرى) والسرقة المالية وغيرها من الجرائم العابرة للحدود[2].

وأحيانا توصف الأنشطة التي تتعلق بالدول وتُستهدف فيها دولة أخرى واحدة على الأقل بأنها تقع في إطار "الحرب الإلكترونية"، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية[3].

---

[1]– إسراء جبريل رشاد مرعي، الجرائم الإلكترونية" الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، 9 أوت 2016، انظر الرابط https-//democraticac.de/?p=35426 تاريخ الزيارة: 2019/05/17 بتوقيت الساعة 11سا، بدون صفحة.

[2]– نفس المرجع.

[3]– نفس المرجع.

الفرع الثاني: تعريف المشرع الجزائري للجريمة الالكترونية

سنتطرق في هذا الفرع إلى تعريف الجريمة الالكترونية في القانون الجزائري تعريفا فقهيا وأكاديميا وقانونيا، وسنوضح موقف المشرع منها.

1- التعريف الفقهي: إن الجريمة الالكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلا في الجرائم التقليدية، فلهذا ظهر اختلاف في تعريف قائما من هذه التعاريف ما يلي " : بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال. " وهناك من يعرفها على أنها " كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحث مظلة قانون العقوبات لحمايتها "أو أنها استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة و أمور غير أخلاقية لا يرتضيها المجتمع[1].

ومن خلال هذه التعاريف تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية [2].

2-التعريف الأكاديمي: كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ترتبت عنه خسارة تلتحق بالضحية أو مكسب يحققه الجاني، كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية على:

1. عندما تكون المعلوماتية موضوعا للاعتداء
2. عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية.
3. عندما تكون المعلوماتية أداة ووسيلة للاعتداء
4. عندما يستخدم الجاني أي جهاز معلوماتي لتنفيذ جريمته[3].

---

[1]- زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص43.

[2]- نفس المرجع، ص 44.

[3]- عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ملتقى حول الجرائم المعلوماتية، منظم من قبل كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، بتاريخ 2015/11/01، انظر الرابط: fdsp.univ.biskra.dz تاريخ الزيارة 2019/05/10 بتوقيت الساعة 10 سا.

3-التعريف القانوني: تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث [1].

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات[2].

حيث أنه عرف من خلال القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3].

مسميا إياه: " المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين[4].

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية وبأشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل هذا ما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في العاشر من نوفمبر 2004 المتمم لأمر رقم 66-156 المتضمن قانون العقوبات والذي افرد القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 07 .[5]

ووفقا للمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها، وركز

---

[1]- قانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج ر عدد 47، صادرة بتاريخ 2009/08/16، ص5.

[2]- نفس المرجع.

[3]- المادة 2 الفقرة ب، قانون رقم 09 -04، المرجع السابق، ص 5.

[4]- نشناش منية، مداخلة بعنوان الركن المفترض في الجريمة المعلوماتية، ملتقى منظم من قبل كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، بتاريخ 2015/11/16، ص 4.

[5]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، 2006، ص27.

على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات، أما فيما ينص الشرط الثاني لمجلس الشيوخ الفرنسي والمتعلق بضرورة توافر النظام على حماية فنية فيبدو أن النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية[1].

المطلب الثاني: أطراف وأدوات الجريمة الالكترونية

إن الجرائم الالكترونية كغيرها من الجرائم تحتاج إلى طرفين فاعل أو جاني، ومجني عليه، غير أن أطراف الجريمة الالكترونية يختلفون نوعا ما عن أطراف باقي الجرائم، وعليه فجوهر البحث بهذا الصدد ينصب على مصدر وجود الأفعال وتوجيهها، ومما لا شك فيه أن الشخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية، ولكن هل يعد كذلك أيضا حين ترتبط شبكة المعلومات عموماً بين حواسيب متعددة، يبدو أن الأمر يختلف بعض الشيء فالمؤسسات العامة والبنوك وغيرها، التي تحمل صفة الشخص المعنوي معرضة لاعتداءات عن طريق هذه الشبكة من المعلومات، فعلى الرغم من وسائل الحماية المتعددة، إلا انه تبت عدم فعاليتها أمام قرصنة شبكة المعلومات [2].

ومن بين أطراف الجريمة الالكترونية ما يدعى بالمجرم المعلوماتي وسنتطرق لتعريف هذا المجرم ونبين صفاته وخصائصه وكذا تصنيفه.

الفرع الأول: أطراف الجريمة الالكترونية

1- المجرم المعلوماتي

إن مظاهر الخطورة التي تتجلى بها الجريمة الالكترونية أن مرتكبيها يتسمون بالذكاء والدراية في التعامل في مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية ' وإذا كان الشخص الذي يرتكب العمل الغير مشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظم القانون مجرما ويتعرض للعقاب ' وكما هو معروف فانه لا يمكن للعقوبة أن تحقق هدفها ما لم تضع في الاعتبار شخصية المجرم ' وإذا كنا في مجال الإجرام

---

[1]– نشناش منية، المرجع السابق، ص4.

[2]– علي احمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، لبنان، 2006، ص244،248.

المعلوماتي فيجب أن ننظر إلى المجرم المعلوماتي من حيث صفاته وسماته وكذا من حيث أصنافه وأنماطه.[1]

2- خصائص المجرم المعلوماتي

يتميز المجرم المعلوماتي عن غيره من المجرمين بصفات وسمات معينة جعلت منه محل العديد من الأبحاث والدراسات، واختلف الباحثون في تحديد هذه الخصائص كما اختلفوا في مدى انطباق وصف جرائم ذوي الياقات البيضاء [2]على مجرمي المعلوماتية ذلك أن كلا من هؤلاء المجرمين قد يكون من ذوي الكفاءات، ولهم القدرة على التكيف الاجتماعي ومع ذلك يمكن أن نستخلص من هذه الأبحاث[3] مجموعة من السمات التي يتميز بها المجرم المعلوماتي والتي يساعد التعرف عليها في مواجهة هذا النمط الجديد من المجرمين ومن أهم هذه الصفات:

أ. الذكاء : يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف[4]، فهذا المجرم لا يمكن أن ينتمي إلى طائفة المجرمين الأغبياء، فمن يستعين بجهاز الحاسوب للاستلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع من الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته.

---

[1]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة 2012، 2013، ص50.

[2]– مصطلح المجرمين ذوي الياقات البيضاء مصطلح حديث نسبيا وأول من أطلقه هو عالم الاجتماع Sutherlanc أين وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع وذوي المناصب الإدارية الكبيرة وتشمل أنواعا مختلفة من الجرائم كغسيل الأموال، وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم.

[3]– يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة ويرى الأستاذ Parker بداءة أن المجرم المعلوماتي، وإن كان يتميز ببعض السمات الخاصة به إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يستوجب توقيع العقاب عليه .ويرمز الأستاذ Parker لهذه الصفات بكلمة Skram وهي تعني المهارة (Skills) –المعرفة –(Knowledg) الوسيلة، (Resources) السلطة (Autority) وأخيرا الباعث (Motives).

[4]– غنام محمد غنام، الحماية الجنائية لبطاقات الائتمان الممغنطة، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم من قبل اكاديمية الشرطة، دبي، مركز البحوث والدراسات، تاريخ الانعقاد 2003/04/26 الى 2003/04/28، ص 05.

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابه للجريمة، فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج.

ب. المهارة : تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين، ومستوى المهارة التي يكون عليها المجرم المعلوماتي هي التي تحدد الأسلوب الذي يرتكب به الجرائم، بحيث إذا كان الشخص مرتكب الجريمة المعلوماتية على قدر ضئيل من مستوى المهارة نجد أن الجرائم التي قد يرتكبها لا تتعد الإتلاف المعلوماتي أو نسخ البيانات والبرامج[1]، أما إذا كان المجرم المعلوماتي على درجة أعلى في المستوى المهاري فإن أسلوب ارتكابه للجرائم يختلف، إذ يمكنه عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي لسرقة الأموال وارتكاب جرائم تجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مهارة عالية في ارتكابها.

كما أن المهارة التي يتميز بها المجرم المعلوماتي تمكنه من تكوين تصور كامل لجريمته، إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى التمهيد لارتكاب جريمته بالتعرف على المحيط الذي تدور فيه، وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها[2].

ج. التنظيم والتخطيط :تتميز الجريمة المعلوماتية عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم المعلوماتية من عدة أشخاص يحدد لكل شخص منهم دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيمٍ سابق على ارتكاب الجريمة، فقد تحتاج جريمة نسخ برامج الحاسب الآلي مثلا إلى من يقوم بنسخ تلك البرامج وإلى من يقوم بعملية بيعها .كما أنه من الملاحظ أن الأشخاص الذين يقومون بخلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي، فجرائم المعلوماتية تتطلب عادة

---

[1]– خالد محمود إبراهيم، الجرائم المعلوماتية، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 135.

[2]– نائلة محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005، ص 58.

شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب[1]، وأحيانا أخرى يمكن تجنيد المجرم المعلوماتي القادر على اختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الإنترنت، ويمكن من خلال هذه الشبكة تبادل أفكار ومعلومات التطرف والإرهاب، كما يمكن الاتفاق معه على ارتكاب إحدى الجرائم الأخلاقية أو التلاعب في الحسابات أو بطاقات الائتمان[2] ...

د. المجرم المعلوماتي يبرر ارتكاب جريمته : أثبتت بعض الدراسات أنه لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقية ما يقوم به أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها بل لا يعتبر أن ما يقوم به يدخل في عداد الجرائم، خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، لذلك فإن كثيرا من العاملين في مجال المعلوماتية لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة، أو في نسخ البرامج بدلا من شرائها واستعمال الحاسبات الآلية للمؤسسات التابعين لها لأغراض شخصية، وما ساعد على نماء هذا الشعور هو عدم وجود احتكاك مباشر بين الجاني والمجني عليه، فالتباعد في العلاقة الثنائية هذه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل[3] إلا أن الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة من المجرمين المعلوماتيين لا ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم ودراية وإدراك بعدم مشروعية ولا أخلاقية هذا الفعل.

الفرع الثاني: أصناف المجرم المعلوماتي وادواته

إن مرتكبي الجرائم الالكترونية ليسوا على درجة واحدة من الخطورة أو الكفاءة، وعلى هذا الأساس يمكن تصنيفهم حسب إمكانياتهم ومقاصدهم من ارتكاب الجريمة إلى صنفين هما:

1- مجرمين مستخدمين: وهم من تتوافر لديهم معرفة كافية أو خبرة لا بأس بها في مجال المعلوماتية أو عمل الحاسب الآلي ومكوناته ووظائفه الأساسية، ومعرفة بعض البرامج التي

---

[1]- نائلة محمد فريد قورة، المرجع السابق، ص 58.

[2]- نفس المرجع، ص 61.

[3]-عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترانت، دار الكتب القانونية، مصر، 2007، ص105.

يجري العمل بها كالبرامج المحاسبية، ومع الإقرار بان المعلوماتية تكنولوجيا حديثة، ودخولها واقع الحياة اليومية حديث نسبياً، ونظراً إلى قلة المعرفة بهذه التكنولوجيا، ولما كان هؤلاء يمارسون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسة هواية اللهو، وهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي إلى أفعالهم غير المشروعة بالنسبة إلى نشاط معين[1]، لذا فان هذه الطائفة أو الفئة من المجرمين تعد اقل خطورة مقارنة بغيرها. ولكن مع ملاحظة ازدياد الأعداد المستخدمة لهذه التكنولوجيا (الانترنت)، وما سيتبعه بلا شك من ازدياد نسبة الجرائم في هذا المجال، فليس من المستبعد احتمال انزلاق هذه الفئة من مجرد هواة صغار للأفعال غير المشروعة إلى محترفين للإجرام[2]، وخصوصاً إذا ما تم احتضانهم من قبل منظمات إجرامية لتحقيق أغراض خطرة تؤثر بصورة أو بأخرى على معطيات التطور العلمي.

2- مجرمين مبرمجين

نظراً إلى المستوى المهارات الذي يتمتع به المبرمجون، من دخول واقتحام للأنظمة الحاسوبية بكل سهولة واقتدار، رغم احتياطات الأمن المتعددة ورغم قلة العناصر الخبيرة على كشفها، مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، إذ غالبا ما تكون جرائم التحويل والنسخ والإضافة للمعلومات على البرامج، وتغيير محتواها من هذه الفئة ضخمة[3]، علاوة على أن بمقدور هذه الفئة استخدام الإمكانيات والأساليب المعلوماتية ليس في ارتكاب الجريمة فقط، بل حتى في التهرب من محاولة كشف أمرهم، أو بالعمل كذلك على إعاقة ملاحقتهم من خلال تضييع الأدلة الموجودة[4] المؤدية إلى إدانتهم .

ومن خلال ما تقدم يتضح أن مرتكب الفعل الجرمي المعلوماتي، قد يكون فاعلا أصليا أو شريكاً في ارتكابه للجريمة، فصفة الفاعل الأصلي في الجريمة المعلوماتية غالباً ما تكون من أحد العاملين أو المستخدمين في منشأة تدار بالنظام المعلوماتي، بصرف النظر عن

---

[1]- أسامة احمد المناعسة، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، طبعة الأولى، دار وائل للنشر، عمان، 2001، ص 82.

[2]- إسماعيل رضا، الوقاية من الجرائم الناشئة عن استخدام الحاسب الآلي، بحث منشور في مجلة الاقتصاد الإسلامي، عدد 219، 1999، ص 34.

[3]- عبد الرحمن الشنيقي، المواجهة الأمنية لجرائم الحاسبات الآلية، مجلة الأمن والحياة، العدد 129، 1993، ص 46، وكذلك أسامة احمد المناعسة، المرجع السابق، ص84.

[4]- سعد الحاج بكري، شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، العدد 11، 1990، ص 210.

المستفيد من وراء ارتكاب مثل هذه الأفعال، ولما كان هذا النوع من الإجرام يستلزم الدقة والتنفيذ للعمليات غير المشروعة، فانه يستلزم كذلك مشاركة أو مساعدة أشخاص آخرين، سواء أكانوا فنيين أم مجرد وسطاء، وقد يكون هذا الاشتراك سلبياً، يترجم بالصمت أو السكوت، بيد انه في الغالب الأعم يتمثل بالمساعدة الفنية والمادية[1] وخصوصاً عندما تستلزم آليات الابتكار لمخادعة الحاسب الآلي الاستعانة بمجموعة من الوسطاء أو الشركاء والمؤتمنين على أسرار اسطوانات الحاسبات الآلية، إذ يؤدي هؤلاء الدور الرئيس في نجاح العملية غير المشروعة أو المستهدفة[2].

بقي أن نشير في هذا المقام إلى أن هناك بواعث رئيسة تدفع بهؤلاء المجرمين نحو الإقدام على ارتكاب جرائم المعلوماتية، منها الشغف بالإلكترونيات، ودوافع شخصية متعلقة بالعظمة واثبات القدرة والسعي إلى تحقيق الربح، ومؤثرات خارجية تمثل بدافع الإكراه والحقد، أو قد يكون ذلك لأسباب تتعلق بالمسؤول عن مركز معلوماتي معين، " أي أسباب خاصة بالمنشاة " [3].

3 – الضحية في الجريمة المعلوماتية

فكما يمكن أن يرتكب جرائم المعلوماتية شخص طبيعي أو معنوي، فان المجني عليه في تلك الجرائم قد يكون كذلك شخصاً طبيعياً أو معنوياً، مع أن الغالبية العظمى من هذه الجرائم تقع على شخص معنوي يتمثل بمؤسسات وقطاعات مالية وشركات ضخمة، بيد أن المعلومات المجردة تعد في الوقت الحاضر من أهم المصالح المستهدفة بعد الأموال، وخصوصاً إذا كانت هذه المعلومات ذات أهمية عالية، وكان هدف المجرم المعلوماتي هو الحصول على مقابل وعوض، عن طريق المقايضة غير المشروعة لهذه المعلومات أو بيعها لغير أصحابها الشرعيين، ويمكن تصور ذلك من المعلومات الآتية :

أ. **المعلومات المالية:** المرتبطة بالمركز المالي الحسابي والإداري وانتقال الأموال والاستثمارات[4]

---

[1]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص 45 وما بعدها.

[2]– نفس المرجع السابق، ص 46.

[3]– نفس المرجع السابق، ص 48 وما بعدها، و ينظر كذلك: أسامة احمد المناعسة، مرجع سابق، ص 88.

[4]– توفيق شمبور وآخرون، السرية المصرفية، أبحاث ومناقشات الندوة التي نظمها اتحاد المصارف العربية، لبنان 1993، ص82 وما بعدها، كما ضبطت في الأردن حديثاً جريمة عبر شبكة المعلومات العالمية (الانترنت)، مفادها قيام أحد الأشخاص بالدخول عبر كلمات السر إلى الحزمة الخاصة بأرقام بطاقات الائتمان، مما مكن الفاعل من استخدام أرقام هذه البطاقات في عمليات شراء واسعة على الشبكة العالمية، والقضية لا تزال قيد التحقيق، عن إدارة المختبرات والأدلة الجرمية، عمان، 2003.

ب. المعلومات التجارية: خصوصاً فيما يتعلق بالتجارة الإلكترونية وعمليات التجسس والقرصنة الحاصلة عليها[1].

ج. المعلومات الشخصية: المرتبطة بخصوصيات الأشخاص الطبيعية أو المعنوية كالشركات والمستشفيات وأقسام الشرطة، والأحزاب والنقابات وغيرها، سواء أكانت المعلومات مخزنة بذاكرة الحاسوب أم مدخلة في بنوك المعلومات، إذ يتم تشويشها وإظهارها على غير حقيقتها[2]، ويدخل في هذا النوع ما يتعلق بأسرار الدولة والمشاريع الصناعية المرتبطة بالتسليح الحربي، والتي تعد هذه الأخيرة أكثر عرضة للاعتداء من غيرها[3].

ومما تجدر الإشارة إليه بهذا الصدد هو دور المجني عليه في كبح الجريمة المعلوماتية، ففي الأغلب الأعم يكون دور المجني عليه ضئيلاً وسلبياً إلى حد كبير، إذ يفضل الكثير من المجني عليهم الإبقاء على ما لحقهم من اعتداء سراً، وبعبارة أخرى يميلون إلى التكتم عما لحقهم من أضرار ناتجة عن الجريمة المعلوماتية، ولعل مرد ذلك يكمن برغبتهم في الحفاظ عل مكانتهم الاجتماعية أو سمعتهم التجارية، حمايةً لمركزهم المالي وثقة العملاء بهم، لذا لا يرغبون بالكشف عن الاختراقات الحاصلة على أجهزتهم الحاسوبية، حتى لا ينظر إلى تدابير الحماية لديهم على أنها ضعيفة غير فعالة، فتسبب ضعف الثقة بالمؤسسة وبالتالي عزوف العملاء عنها[4].

فضلاً عن عجز المجني عليهم في الإثبات المادي للجريمة، فضلاً عن خشيتهم لاحتمالية المساءلة القانونية، في الوقت الذي يقع عليهم واجب الإشراف على المعلومات المستهدفة، وامتلاكهم السلطة اللازمة لإمكان التقدير ووضع الإجراءات الضرورية في حالة حدوث أضرار ناشئة من إفشاء معلومات على قدر من الحساسية والخطورة[5]، وعليه يكون

---

[1]– هدى حامد قشقوش، مرجع سابق، ص 6–18، وينظر كذلك: د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص10 وما بعدها وص 119.

[2]– طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الأولى، دار صادر للمنشورات الحقوقية، بيروت 2001، ص150 وما بعدها، وينظر كذلك: يونس خالد عرب، جرائم الحاسوب، رسالة ماجستير مقدمة إلى كلية الحقوق في الجامعة الأردنية، 1994، ص203 وما بعدها.

[3]– Pouvoir et libertes edition economica Paris1981, Andere vitalis informatique, p 135.

[4]– محمد سامي الشوا، مصدر سابق، ص 61.

[5]– محمد حسام لطفي، عقود وخدمات المعلومات، دراسة في القانون المصري والفرنسي، دار النهضة العربية للنشر و التوزيع القاهرة، 1994، ص 109.

للصدفة فقط دور كشف هذا النوع من الجرائم وملاحقتها، وبتقديري المتواضع أن هذا ينطبق إلى حد ما على بلادنا، أما في البلاد الغربية، فالوعي في هذا المجال اكبر، ولا يخشى أصحاب الشركات التي تم اختراقها الإعلان عن ذلك، بغية تحصيل حقوقهم، ومعاقبة المجرمين، وهو أمر يعود بالفائدة على الأجهزة القضائية، ومجموعة المعتدى عليهم على حدٍ سواء، فيما يتعلق بزيادة الخبرة . وتحديد أطر الجريمة، وبالتالي وضع أفضل الحلول لمكافحتها مستقبلاً.

ومن أبرز الأدوات التي يستعين بها القراصنة (Hackers) لتنفيذ جريمتهم الإلكترونية تتمثل في:

- الاتصال بشبكة الإنترنت وتعتبر أداة رئيسية لتنفيذ الجريمة.
- توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.
- وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي.
- البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز.
- طابعات (Printers) .
- هواتف رقمية ونقالة.
- برامج ضارة ومنها Trojan horse إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه[1].

[1]– إسراء جبريل رشاد مرعي، المركز الديمقراطي العربي، مرجع سابق، بدون صفحة.

المبحث الثاني: خصائص وأسباب الجريمة الالكترونية

من خصوصية الجريمة الالكترونية أن بعض حالات ارتكابها يعتمد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة منها المعالجة الالكترونية للبيانات، ومجال المعالجة الالكترونية للنصوص والكلمات الالكترونية.

في المجال الأول: يتدخل الجاني من خلال ارتكاب الجريمة الالكترونية في مجال المعالجة الالكترونية للبيانات، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسب الآلي، وذلك بغرض الحصول على المعلومات.

أما في المجال الثاني: يتدخل الجاني في مجال المعالجة الالكترونية للنصوص والكلمات، وهي طريقة أوتوماتيكية تمكن مستخدم الحاسب الآلي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات الموجودة تحت يده وبفضل إمكانيات الحاسب الآلي نتاج إمكانية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة، وهي بدلك علاقة وثيقة بارتكاب الجريمة[1].

وبالرغم من خصوصية التي تتميز بها هاته الجريمة إلا أن الدافع والقصد يشكلان أهم الركائز التي تحرك لارتكاب أفعال الاعتداء المختلفة تحت مفهوم الجريمة الالكترونية وهذا ما سنحاول توضيحه من خلال ذكر خصائص الجريمة الالكترونية في المطلب الأول وأسباب ودوافع هاته الجريمة في المطلب الثاني.

المطلب الأول: خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية بطبعة خاصة تميزها عن الجريمة التقليدية، ولدا أصبحت هذه الخاصية بهذا النوع من الجرائم عدة سمات وحقائق سواء تعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي[2].

وعليه سنحاول البحث خصائص الجريمة فيما يلي:

الفرع الأول: الجريمة الالكترونية جريمة عالمية الحدود

من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافيا لاتصالها بعالم الإنترنت وتقنية المعلومات، حيت قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، وبسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها، ومن أهم

---

[1]– محمد علي العريان، المرجع السابق، ص 37.

[2]– يونس عرب، المرجع السابق، ص 08.

القضايا التي أكدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة ايدز، وتتلخص وقائعها عام 1985 حيث قام أحد الأشخاص وهو " كوزيف بيب " بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الايدز، لكن في الحقيقة يحتوي هذا البرنامج على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الفاعل أو الجاني بطلب مبلغ مالي للحصول على عنوان الكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرسال البرنامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الانجليزي إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية[1].

فهذا النوع من الجرائم يمتاز بالنعومة وعدم استخدامه للعنف كما في جرائم التقليدية كجرائم الإرهاب والمخدرات والسرقة والسطو المسلح فالجريمة الالكترونية تعتمد بالصورة كبيرة على نقل البيانات من حاسب إلى آخر أو سطو الالكتروني على أرصدة البنك وهذا لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن[2].

ولعل من أهم أثار القانونية التي تميزها خاصية عالمية الحدود للجريمة الالكترونية القانون الواجب التطبيق عليها وكذا القضاء المختص بها فهل يكون قانون المطبق هو قانون الدولة التي وقع فيها النشاط الإجرامي، أم قانون الدولة التي يقيم فيها الجاني، أو قانون الدولة التي تضررت مصالحها من هذا التلاعب.

لهذا كان من الأجدر إيجاد الطرق والأساليب فعالة لتوفيق بين مختلف التشريعات الخاصة بهذه الجرائم من خلال إبرام اتفاقيات دولية خاصة بتسليم المجرمين والوسائل الناجمة لمكافحة هذا النوع من الجرائم.

الفرع الثاني: الجريمة الالكترونية سريعة التنفيذ

إن تنفيذ الجريمة الالكترونية لا يتطلب الوقت الكثير فبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى أخر وهدا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة بالإضافة الى ذلك فان الجريمة الالكترونية في اغلبها ما عدى جريمة سرقة معدات الحاسب لا تتطلب وجود الفاعل في مكان الجريمة بل يمكن

---

[1]– سويد سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان الجزائر، 2010، ص 12.

[2]– إسراء جبريل رشاد المرعي، مرجع سابق، بدون صفحة.

للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء من خلال الدخول لشبكة العنكبوتية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب الخ[1].

الفرع الثالث: صعوبة إثبات الجريمة الالكترونية

فالجرائم الالكترونية تتصف بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، وهي خطيرة وصعبة الاكتشاف، أو هي صعبة في تحديد موقعها، أو مكان التعامل معها، بسبب اتساع نطاقها المكاني، وضخامة البيانات ترجع صعوبة الجريمة الالكترونية إلى عدة أمور منها:

1. أنها كجريمة لا تترك أي آثار جانبية لها بعد ارتكابها، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية الغير مرئية ولا توجد مستندات ورقية.

2. فهذه الجرائم لا تترك أثرا لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فان معظم جرائم الانترنت ثم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، فالجريمة الالكترونية من الجرائم المستحدثة التي لا تترك شهودا يمكن استجوابهم ولا أدلة مادية يمكن فحصها، من هنا تأتى صعوبة الكشف عن هذه الجريمة.

3. تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها حيث تتطلب جرائم الكمبيوتر والانترنت المهام خاص بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو لملاحقتهم قضائيا[2].

4. قلة الإبلاغ عن الجريمة الالكترونية غالبا في الجرائم الالكترونية، المجني عليه يحجم عن طلب مساعدة السلطات المختصّة في إثبات الجريمة والكشف عنها، حتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرّة، وضياع ثقة المساهمين، في الحالة التي يكون فيها المجني عليه عادة بنكا أو مؤسسة مالية (شخصا معنويا) يهمّه المحافظة على سمعته وثقة عملائه، أكثر من اهتمامه بالكشف عن الجريمة ومرتكبيها، لذلك يفضل المجني عليه تقديم ترضية

---

[1]– اسراء جبريل رشاد المرعي، المرجع السابق، بدون صفحة.

[2]– خالد ممدوح إبراهيم، مرجع سابق، ص 45،46.

سريعة لعميله، وينهي الأمر داخليا، كما أن للمجني عليه دور مثير لريبة، قد يشارك بطريقة غير مباشرة في ارتكاب السلوك الإجرامي، ذلك في حالة التي يكون فيها مثلا المجني عليها امرأة، ثمّ التحرش بها وابتزازها عبر مواقع التواصل الاجتماعي Facebook فتضطر الضّحية للرضوخ لطلبات المجني خشية من، تشويه سمعتها[1].

لكن هناك حالات ضئيلة أين يتم الإبلاغ فيها عن الجرائم الالكترونية نسبة إلى شخصية المجني التي تلعب دور مهم في عملية الإبلاغ[2].

ولذا كان من الأحسن إيجاد صيغة عمل مشتركة بين مختلف أجهزة القضاء والأمن وحتى الخبراء وتنسيق بينهم عن طريق عقد دورات تدريبية بغرض تحقيق التعاون بين هذه الجهات والوصول إلى طرق وحلول قانونية كفيلة بمعالجة الجرائم الالكترونية.

المطلب الثاني: أسباب ودوافع الجريمة الالكترونية

مما لا شك فيه فان فئات مرتكبي الجريمة الالكترونية تختلف عن الأفعال الإجرامية التقليدية لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع فضلا عن ذلك تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماما عن الخصائص التي تتمتع بها الجرائم التقليدية[3].

ولابد من التأكيد على أن الجريمة مهما اختلفت وتنوعت تسميتها فهي في الأخير ستتشكل من عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

1. دافع معين لارتكاب العمل.
2. هدف الضحية.
3. الفرصة المواتية.

---

[1]– شهدت الجزائر في السنوات الأخيرة تضاعف مخيف للجرائم الإلكترونية، التي باتت تهدد كيان المجتمع، حيث تقول زهرة فاسي أستاذة في علم الاجتماع أن أكثر عرضة لهذا النوع من الجرائم هن النساء اللاتي لا يبلغن عن الفاعل خوفا من الفضيحة، مشيرة أن العديد من الفتيات رضخن للابتزاز وسلمن مبالغ مالية ضخمة مقابل عدم نشر صورهن على سبيل المثال ومنهم من هربت من بيوت الأهل خوفا من الفضيحة، أنظر إلى مقال صحفي، باسم خديجة بدومي، الجزائر www.dw. com

[2]– ماطلي غنية، المرجع السابق، ص35 .

[3]– مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، أنظر الرابط hrdoegypt.org/wp-content/uploads/2014/12 تقرير–الجريمة–الالكترونية. تاريخ الزيارة 2019/05/17 بتوقيت الساعة 11سا.

4. غياب عيون الأمن.[1]

بالإضافة الى جملة من الدوافع الشخصية والخارجية التي تقف في غالب الأحيان وراء الجريمة الالكترونية والتي سنتناولها بالشرح في الفرع الأول والثاني.

الفرع الأول: الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبو هذه الجرائم لديهم شغف الآلة يحاولون إيجاد – وغالباً ما يجدون–الوسيلة إلى تحطيمها بل والتفوق عليها ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتاً طويلا أمام 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 هو الدافع لارتكاب فعل الجريمة المعلوماتية، وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي هو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو النقص 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].

بالإضافة إلى دوافع أخرى نذكر منها على سبيل المثال:

1- حب التعلُّم

يعتبر حبُّ التعلم والاستطلاع من الأسباب الرئيسة التي تَدْفع إلى ارتكاب مثل هذه الْجرائم لأنَّ الْمُخترِق يعتقد أنَّ أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب ألاَّ تبقى المعلومات حكرًا على أيْ أحد: أنَّ للجميع الحقَّ في التعرُّف والاستفادة من هذه المعلومات.

---

[1]– أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، 2005، ص 126 وما بعدها.

[2]– مركز هردو لدعم التعبير الرقمي، مرجع سابق، ص 10.

2- المنفعة المادية

قد تكون مُحاولات الكسب السريع وجَنْي الأرباح الطائلة دون تعَب ولا رأس مال من الأسباب التي تَدْفع إلى اختراق أنظمة إلكترونيَّة كالتي تستخدمها الْمَصارف عن طريق الدُّخول إلى الحسابات المصرفيَّة والتلاعب فيها أو الاستخدام غَيْر المشروع لبطاقات الائْتِمان[1].

3- التسلية واللهو

عددٌ غير قليل من مُخترقي الأنظمة يتَّخِذون مِن عمَلِهم هذا وسيلة للمرح والتَّسلية وتقضية أكبر وقت مُمْكن في أنظمة وحواسيب الآخرين ويكون هذا الاختراق غالِبًا سِلْميًّا ودون أن يَحْدث تأثير يُذْكر.

الفرع الثاني: الدوافع الخارجية

إن تأثر الإنسان من بعض المواقف يجعله في حالة استسلام تام لكثير من المؤثرات والدوافع الخارجية التي تدفعه إلى ارتكاب بعض الجرائم الالكترونية، وذلك نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، ومع توافر هذه المؤثرات، فان الأمر حتما سيؤدي إلى ارتكابه للجريمة الكترونية، أما بدافع الانتقام أو جنون العظمة أو بدافع التعاون والتواطؤ على الأضرار والتهديد.

1- دافع الانتقام وإلحاق الضرر بالرب العمل

قد يكون الانتقام مؤثر في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشاة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشاة، ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من منشاة أو رب العمل[2].

2- دافع عقائدي

تتمثل في تلك القوى الداخلية المحركة لأشخاص حيث يبرر الكثير محاولاتهم لاختراق أجهزة الغير بحجة أنهم على مذاهب أو طوائف دينية معادية لمذاهبهم أو بحجة تكفيرهم وفضح أسرارهم.

---

[1]- موقع جزا يرس، جرائم الالكترونية تهدد امن الجزائريين، نشر في اخبار اليوم يوم 2018/04/10 من الرابط https-//www.djazairess.com/akhbarelyoum/240271 تاريخ الزيارة 2019/02/23 بتوقيت الساعة 09 سا20 د .

[2]- خالد دوادي، الجريمة المعلوماتية، دار الإعصار العلمي الجزائر، 2018، ص40.

3- دافع عنصري

والذي يكون وراء هذا النوع من الجرائم الالكترونية ويأتي عن طريق تميز بين عرق وأخر وقبيلة وأخرى فتجد مرتكبيها يسعون بكل الطرق إلى افتعال المشاكل وعمل أعمال تخريبية من شانها جر المشاكل عن طريق نشر شائعات وأكاذيب.

4- دافع سياسي وإيديولوجي

وهو الدافع الذي يلعب فيه الإرهاب الدور المركزي والأساسي وذلك من خلال لجوئه إلى الانترنت كوسيلة رئيسية لبث أفكاره العصرية المتمثلة في استخدام الوسائل الالكترونية التي جلبتها تقنية عصر المعلومات فبدلا من استخدام المتفجرات أصبحت الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمر البنية المعلوماتية وتغلق مواقع حيوية وتشل أنظمة القيادة والاتصالات أو حتى قطع شبكات الاتصال بين الوحدات والقيادات المركزية أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو تحكم في خطوط الملاحة الجوية والبرية والبحرية أو شل محطات إمداد الطاقة والماء أو اختراق النظام المصرفي مما يضر بأعمال البنوك والأسواق المالية العالمية [1].

وفي الأخير نجد أن الإرهاب الالكتروني مهما تعددت أسبابه وأنواعه فهي نفسها عموما أسباب ظاهرة الإرهاب حيث تتداخل الدوافع الشخصية مع الدوافع الفكرية والسياسية والاقتصادية والاجتماعية.

وفي نهاية هذا الفصل، يتضح لنا أن الجريمة الالكترونية هي جريمة وليدة التطور العلمي والتكنولوجي الذي وصلت إليه المجتمعات، فبرغم من الإيجابيات التي تطغى على هذا التقدم إلا أن الجانب السلبي له والذي يستعمل في أغراض سلبية يعرف انتشار كبيرا خاصة في أوساط الجيل الصاعد، فلمرتكبي هذا النوع من الجرائم أو ما يعرفون بالمجرمين

[1]- جميل عبد الباقي الصغير، مدى كفاية نصوص العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الانترنت، الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، ابوظبي من 15 الى 2008/11/19.

المعلوماتيين لهم قدرة كبيرة على تكيف بالمجتمعات الأخرى وكذا يتميزون بالذكاء والفطنة وهي أكبر مقومات ارتكاب هذا النوع من الجرائم.

كما أن صعوبة التي تحيط بالجريمة الالكترونية من حيث سرعة اكتشافها وكذا صعوبة إثباتها تشكل أكبر عوائق التي تواجهنا في مكافحة هذا النوع من الجرائم.

مع تطور المجتمع اتسع نطاق القانون حيث اضطر تدخل المشرع لتجريم صور سلوك تعبر عن مراحل التطور الجديد التي يعيشها المجتمع،[1] وإذا كانت الجريمة الالكترونية هي نتيجة طبيعية لهذا التطور فإن الفقهاء قد حاولوا تحديد أنماط جرائم الكمبيوتر والإنترنيت،[2] إذ أصبح البعض يستخدم اصطلاح جرائم الكمبيوتر للدلالة على الأفعال التي يكون الحاسوب فيها هدفا للجريمة، كالدخول غير المصرح به، وإتلاف البيانات المخزنة في النظم ونحو ذلك، أما اصطلاح الجرائم المرتبطة بالكمبيوتر فهي تلك الجرائم التي يكون فيها الكمبيوتر وسيلة لارتكاب الجريمة، كالاحتيال والتزوير ونحوهما، غير أن هذا الاستخدام ليس قاعدة ولا هو استخدام شائع، لكن مع ذلك بقي هذين الاصطلاحين الأكثر دقة للدلالة على هذه الظاهرة[3] المتعددة الجوانب، وتأخذ الجريمة الالكترونية عدة صور منها ما هو منصوص عليه في قانون العقوبات ومنها ما هو منصوص عليه في نصوص الجزائية الأخرى وبالنسبة للتشريع الجزائري، فقد تدارك المشرع الجزائري مؤخرا "ولو نسبيا" الفراغ القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص تجريميه لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 04-15 المؤرخ في 2004/11/10 والمعدل والمتمم لأمر 66-156 المؤرخ في 1966/06/08 المتضمن تعديل قانون العقوبات، ج ر عدد71 الصادرة في 2004/11/10، لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي[4]، ولذلك ارتأينا من خلال دراستنا أن نتعرض بصفة مفصلة للجرائم الواردة على المعلوماتية من خلال المبحثين التالين:

المبحث الأول: جريمة الاعتداء على نظام المعالجة الآلية للمعطيات وجريمة التزوير الالكتروني

المبحث الثاني: الجزاءات المقررة للجرائم الالكترونية

---

[1]- نور الدين العمراني، "شرح القانون الجنائي الخاص"، دار الامان للطبع والنشر والتوزيع، المغرب، 2005، ص8.

2- الموقع القانوني العربي على الإنترنيت، قوانين الجرائم الالكترونية على ضوء الشريعة، انظر الرابط www.islamonline.net، تاريخ الزيارة 2019/05/17، بتوقيت الساعة11 سا.

[3] - GRC. Criminalité informatique /http. rcmagrc.gc.ca en date 17/05/2019 à 12h

[4]- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم الى الملتقى المغاربي حول القانون والمعلوماتية المزعم عقده بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009، الرابط iefpedia.com arab uploads تاريخ الزيارة 2019/05/19 بتوقيت الساعة 15سا.

المبحث الأول:

جريمة الاعتداء على أنظمة المعالجة الآلية للمعطيات وجريمة التزوير الالكتروني

تعتبر الجريمة الالكترونية من الجرائم المستحدثة التي ترتكب في نطاق تقنية تكنولوجية متطورة ومتزايدة الاستخدام في مختلف مناهج الحياة الاقتصادية والاجتماعية وبناء على ذلك فان إضرارها تمتد وتتسع من خلال المس بأنظمة المعالجة الآلية للمعطيات ولقد كشف الاستخدام الكبير لأجهزة الكمبيوتر عن خطورة تتصل بهذا التصنيف من الاستعمال على عدة مصالح اجتماعية وفردية تهم المجتمع حمايتها ومع ذلك فان الصعوبة التي يمكن أن تظهر عند تصنيف هذا النوع من الجرائم المتصلة بالحاسب الآلي تتمثل في صعوبة حصر هذا نوع من الجرائم كون أن طبيعة وخصوصية هذه الجرائم تمنع ذلك باعتبارها جديدة ومتجددة وتختلف من مجتمع إلى أخر وتجدر الإشارة على أن المشرع الجزائري، قد وضع نصوص قانونية تعاقب على الأفعال التي تشكل جرائم معلوماتية وكان ذلك سنة2001 المادة 144مكرر ومكرر2 والمادة 146 من قانون العقوبات ثم أصدر نصا تشريعيا سنة 2004 يشمل سبعة مواد من المادة 394 مكرر إلى المادة 394 مكرر7 وهذا تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" القسم السابع مكرر من قانون العقوبات وأخيرا القانون رقم 09-04 المؤرخ 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

ستنصب دراستنا الآتية على دراسة جريمة الاعتداء على نظام المعالجة الآلية للمعطيات وجريمة التزوير الالكتروني من خلال المطلبين التالين:

المطلب الأول: مفهوم جريمة الاعتداء على نظام المعالجة الآلية للمعطيات

المطلب الثاني: مفهوم جريمة التزوير الالكتروني.

المطلب الأول: مفهوم جريمة الاعتداء على أنظمة المعالجة الآلية للمعطيات

لدراسة جرائم المساس بأنظمة المعالجة الآلية للمعطيات لابد أولا من الإلمام بالمصطلحات والمفاهيم المتعلقة بالمجال المعلوماتي حتى يمكن فهم أركان الجريمة وسبل تحقق نتائجها وبالرجوع لقانون العقوبات الجزائري في المواد 394 مكرر إلى 394 مكرر7فائنه لم يورد تعريفا لنظام المعالجة الآلية لمعطيات بأي نص، وكذا فعل المشرع الفرنسي رغم اقتراح البرلمان الفرنسي لتعريف مناقشة تعديل قانون تجريم هذا النوع من الاعتداءات ، الا انه لم يتم

[1]- القانون 09-04، ص05.

الموافقة على تضمين هذا التعريف بالنصوص التعديل بالحجة انه لا يمكن ربط التجريم في هذه الأنظمة بالحالة تقنية متغيرة قد لا يشملها التعريف الموضوع لاحقا.

في حين ورد بالقانون 09-04 المؤرخ في 2009/08/05 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تعريف للمنظومة المعلوماتية بالمادة 02 فقرة ب على أنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"

وعرفه الفقيه خالد ممدوح إبراهيم على انه[1]:

"مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها البعض والتي تعمل على جمع البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات والتنسيق وتامين السيطرة على المنظومة لتحليل المشكلات للموضوعات معقدة"

ومن خلال هذا التعريف نستخلص إن لنظام المعالجة أربعة نشاطات:

- **تامين مدخلات البيانات:** فكل أنواع المعطيات توضع في النظام بواسطة وسائل إدخال مناسبة
- **المعالجة:** أي تحويل البيانات المدخلة من شكلها الأولي إلى نتائج ومعلومات مفهومة وقابلة للاستخدام ومن هذا المنطلق فالجزء المعالج بالجهاز(Pocessing) يعتبر الأساس في نظام الكمبيوتر.
- **تامين المخرجات:** من المعلومات المطلوبة للمستخدمين لنقل المعلومات من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة.
- **التغذية الراجعة:** إذ أن العديد من البيانات المخرجة من الحاسوب هي مدخلات ثانية لإعادة معالجتها لأغراض أخرى[2].

وعرفه مجلس الشيوخ الفرنسي على انه:

"نظام المعالجة الآلية للمعطيات هو كل مركب يتكون من وحدة أو مجموعة من وحدات معالجة، والتي تكون كل منها الذاكرة، المعطيات، أجهزة الإدخال والإخراج، أجهزة الربط التي

---

[1]- خالد ممدوح ابراهيم، التقاضي الالكتروني، دار الفكر الجامعي، الاسكندرية، 2009، ص297.

[2]- نفس المرجع، ص 298.

تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نسخة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية[1].

وما يلاحظ على هذا التعريف انه أشار للعناصر المادية والمعنوية التي يتكون منها نظام المعالجة الآلية للمعطيات على سبيل المثال لا الحصر.

كما تعرفه المادة 01-14 من القانون العربي النموذجي الموحد بأنه:" كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة"[2].

ونصت المادة الأولى من الفصل الأول الفقرة الأولى من الاتفاقية الدولية للإجرام المعلوماتي على تعريف النظام المعلوماتي على انه:" أي جهاز أو مجموعة من أجهزة المتصلة ببعضها البعض، أو التي هي ذات صلة بذلك ويقوم احدها تنفيذا لبرنامج بعمل معالجة آلية للبيانات" وهو ذات المفهوم الذي أخذ به المشرع الجزائري السالف الذكر وجاء في المذكرة التفسيرية للاتفاقية أن المقصود بالنظام المعلوماتي هو جهاز يتكون من مكونات مادية ومنطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية وهو يشتمل على وسائل للإدخال وإخراج وتخزين البيانات، وهذا الجهاز قد يكون منفردا أو متصلا بمجموعة من أجهزة الموصولة عن طريق الشبكة[3].

ومن خلال هذا التعريف نستنتج أن لأنظمة المعالجة نوعين من مكونات مادية وغير مادية.

1- المكونات المادية

لا يمكن تصور أنظمة المعالجة الآلية للمعطيات دون وجود جهاز إعلام أو حاسوب بمكوناته المادية التي تتيح استعمال الأنظمة والمعطيات لإجراء معالجتها آليا ولغة علم الحاسب هو علم الإعداد وتعني كلمة الحاسب ناظمة آلية، ومن التعريفات التي أعطيت له انه مجموعة من أجهزة المتكاملة تعمل بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة وفقا

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة الاسكندرية، مصر، 2007، ص26.

[2]- جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للنشر والتوزيع الجزائر، 2012، ص109.

[3]- طارق إبراهيم الدسوقي عطية، الامن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة الإسكندرية، مصر، 2009، ص45.

لبرنامج موضوع مسبقا للحصول على نتائج معينة، ويعرف أيضا انه:" جهاز الكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعات كبيرة تصل إلى عشرات الملايين من العمليات في الثانية بدرجة عالية من الدقة ولديه القدرة على التعامل مع كم هائل من البيانات وتخزينها واسترجاعها عند الحاجة "[1].

ويعرف الحاسب الآلي على انه: «عبارة عن جهاز الكتروني يتكون من مجموعة متداخلة من الأجزاء تعمل فيما بينها لهدف مشترك وهو إخراج العمليات الحسابية والمنطقية طبقا لبرنامج يتم وضعه مسبقا من خلال عدة عمليات وهي الإدخال، المعالجة، الاسترجاع والإخراج"[2].

ويتكون الحاسب الآلي من:[3]

أ- وحدات الإدخال: وهي الوحدات التي يمكن من خلالها لشخص إدخال البيانات أو الأوامر التي لا يمكن للجاني ارتكاب جريمته دونها والتي يمكن بمقتضاها تغذية الحاسب الآلي بالمعلومات التي يريد تزويده بها أو تخزينها أو تعديل تلك المحفوظة على الجهاز ومنها الفارة، مشغل الأقراص، الماسح الضوئي، مشغل الاسطوانات ولوحة المفاتيح وغيرها.

ب- وحدات المعالجة المركزية: دور هذه الوحدات تلقي الأوامر عن طريق أجهزة الإدخال ثم معالجتها وإخراجها بالكيفية التي يرغبها مشغل الجهاز، وهذه الوحدات تتمثل في وحدة الذاكرة الرئيسية وهي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت، وحدة الحساب والمنطق ووحدات التحكم.

ج- وحدات الإخراج: هي الوحدة التي من خلالها يتم إخراج النتائج وإظهارها بأشكال مختلفة مرئية ومطبوعة ومنها الطابعات، الشاشات، مشغل الأقراص، وحدات الأصوات والسماعات وغيرها

د- وحدات التخزين: تعد من أهم الوحدات لاحتوائها على المعلومات والبرامج التي يستخدمها المستخدم في عمله وتمكنه من تخزين الملفات وبرامج التشغيل المختلفة ومنها الأقراص الصلبة، المرنة، أقراص الليزر.....

هـ- المودم: هي أجهزة تمكن الحاسبات من الاتصال ببعضها عبر خطوط معينة.

---

[1]- خالد ممدوح ابراهيم، المرجع السابق، ص 291،292

[2]- احمد خليفة الملط، مرجع سابق، ص27.

[3]- عبد الفتاح بيومي حجازي، مرجع سابق، ص100.

2- المكونات الغير مادية

تعتبر روح الحاسب الآلي وتتمثل في البرامج والمعطيات.

أ- **البرامج:** يقصد بالبرامج بالمفهوم الضيق مجموعة من التعليمات، فالبرنامج يرسل الأوامر إلى الجهاز لتنفيذها بناء على توجيهات المستخدم[1].

وبرامج نوعان:[2]

- **برامج التشغيل:** وتسمى كذلك برامج الاستغلال أو التنفيذ وهي التي تمكن الحاسب من أداء الوظيفة المحددة له، وهي لهذا السبب تعتبر جزءا من الحاسب نفسه ويتولى الإشراف عليها برنامج مشرف أو مراقب لتنظيم أداء هذه البرامج بدورها.
- **برامج التطبيق:** وتسمى برامج معالجة المعلومات وتقوم بتوجيه أقسام الحاسب الآلي ضمن النظام الذي وضع لها وفقا لأوامر البرامج التشغيلية المثبتة بالحاسب الآلي، أو بلوحات مستقلة يجري إدخالها في نظام الكمبيوتر فهي تجعل النظام يستخرج نتائج معينة مطلوبة من المستخدم.

ب- المعطيات: هي المعلومات والبيانات التي يتم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، والمعطيات عبارة عن نبضات الكترونية داخل الحاسب غير ملموسة[3]، والمعطيات عرفتها الاتفاقية الدولية للإجرام المعلوماتي في المادة الأولى من الفصل الأول فقرة ب على أنها: "عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر لما في ذلك البرنامج المناسب لجعل منظومة تؤدي وظائفها."

وعن المشرع الجزائري لم يورد في قانون العقوبات تعريفا إنما عرف المعلومة بالمادة الثانية من القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شانها جعل المنظومة معلوماتية تؤدي وظيفتها".

---

[1]- رشا علي الدين، النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين والقانون الدولي الاتفاقي، الطبعة الأولى، دار النهضة العربية، مصر، 2004، ص80.

[2]- امال قارة، مذكرة ماجيستر بعنوان الجريمة المعلوماتية، كلية الحقوق جامعة الجزائر، 2001، ص81.

[3]- محمد خليفة، مرجع سابق، ص25.

3- شبكات الاتصال

وهي ذات طابع مادي تنقل المحتوى الغير مادي من المعطيات ويعمل على ربط أجهزة والأنظمة المعلوماتية المختلفة على المستوى المحلي أو الدولي التي تخضع لسلطة وتسيير العنصر البشري ولعل أهمها حاليا هو شبكة الانترنت.

4- المقصود بالأنترنت

كلمة الانترنت (Internet) اختصار لمصطلحين Interconnecting-Network وتعني الشبكة التي تربط مجموعة من أجهزة الكمبيوتر ببعضها البعض لتستطيع تبادل المعلومات، وهي الشبكة التي أوجدها الجيش الأمريكي كوسيلة اتصال مستقلة وسريعة وانطلق العمل بها رسميا بتاريخ 1969/01/02 ثم انتشر هذا المشروع في منتصف السبعينيات وتبنته هيئات التدريس في الجامعات لتبادل البيانات العلمية والفنية وكان يسمى Arpa-Net وهو اختصار لـ "وكالة مشروعات البحوث المتقدمة"[1].

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات

من خلال تفحص المواد 394 مكرر وما بعدها المستحدثة لتجريم هذا النوع من الاعتداءات نلاحظ ان المشرع الجزائري ساير المشرع الفرنسي، إذ لم يعطي تعريفا دقيقا لنظام المعالجة الآلية للمعطيات عند نصه على جرائم المساس بأنظمة المعالجة الآلية للمعطيات في تعديله لقانون العقوبات سنة 2004، لكنه تطرق لهذا الموضوع في قانون 09-04 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتاها جاءت المادة الثانية من هذا القانون تحدد مفهوم بعض المصطلحات، ومنها مفهوم المنظومة المعلوماتية، بحيث عرفتها بأنها "اي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم الواحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[2].وعرفت الاتفاقية الدولية للإجرام المعلوماتي المبرمة بتاريخ 23 جوان2001 نظام المعالجة

---

[1]- صالح احمد البربري، بحث بعنوان دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 2001/11/23، أنظر الرابط www.mohamah.net، تاريخ الزيارة 2019/05/17، بتوقيت الساعة 12سا، بدون صفحة.

[2]- مجلة جيل الأبحاث القانونية المعمقة، العام الثالث، العدد25 ، ماي2018، من الرابط: jilrc-magazines.com، تاريخ الزيارة 2019/05/18، بتوقيت الساعة 10سا.

الآلية للمعطيات بأنه كل مركب يتكون من وحدة أو مجموعة من وحدات المعالجة مرتبطة فيما بينها أو مستقلة ليضمن فيها عنصر أو عدة عناصر لتنفيذ برنامج المعالجة الآلية للمعطيات[1].

ويتعين علينا أن نعرف بان نظام المعالجة الآلية للمعطيات هو علم قائم بذاته وبالمختصر فان كلمة معلوماتية هي مزج مختصر لكلمتين معلومة:Information وكلمة آلية Automatic ومعناها المعالجة الآلية للمعلومة ويفهم من المعطيات الفكرية المعالجة أليا هي عمل البرامج والبيانات الموجودة في الكمبيوتر وعلى شبكة الانترنت سواء كانت فنية أو أدبية أو علمية أو تجارية أو صناعية فهي تصنف كإنتاج ذهني لأصحابها ومعلوم ان حقوق الملكية الفكرية تعد أغلى السلع في العالم ومن هنا فهي تصبح محل حماية قانونية في مواجهة الانتهاكات التي تتم من جراء الدخول غير المشروع في أنظمة المعالجة الآلية للبيانات أو البقاء فيها [2] وهذا ما يستدعي ضرورة خضوع النظام لحماية فنية حيث يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الانترانت فهم يسعون لتامين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية.

وتنقسم أنظمة المعالجة الالية للمعطيات إلى ثلاثة أنواع:

- أنظمة مفتوحة للجمهور.
- أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

ومقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول والثاني فلا يتمتعان بتلك الحماية، وهناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية. فنيا لأنه من الطبيعي في نظرهم، أن ما يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وليس من يهمل منهم في توفير الحد

---

[1]– بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، مجلس قضاء قسنطينة، محاضرة في إطار التكوين المحلي المستمر للقضاة، سنة قضائية 2011/2010.

[2]– زبيخة زيدان، مرجع سابق، ص48.

الأدنى لحماية أمواله، ويكون دور القانون الجنائي في هذه الحالة دور وقائي وهذا أيضا هو ما يتفق وسياسة المشرع الجنائي وما نلاحظه من المفهوم العام للحماية الجزائية للملكية والرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات لا تتضمن شرط الحماية الفنية وخرجت تلك النصوص الخالية منه تماما. ومن المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك. ولا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، ولذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده. هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا.[1]

وتطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية ولكن إذا نظرنا للوقائع، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة وبصفة خاصة الركن المعنوي[2].

الفرع الثاني: أشكال جريمة الاعتداء على أنظمة المعالجة الآلية للمعطيات

لقد نص المشرع على مجموعة من الأفعال المجرمة من خلال المواد 394 مكرر، 394 مكرر 7 من قانون العقوبات والتي يمكن تلخيصها فيما يلي:

- الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

1- جريمة الدخول والبقاء الغير المشروع في أنظمة المعالجة الآلية للمعطيات

نصت المادة 394 مكرر الفقرة الأولى من قانون العقوبات على هذه الجريمة كما يلي:

---

[1]- أمال قارة، المرجع السابق، ص 103.

[2]- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، الطبعة الثالثة، بحث مقدم لمؤتمر والكمبيوتر والانترنت، منظم من قبل كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص 123.

"يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذ ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة 50000 دج إلى 150000 دج".

كما نصت المادة 2 من الاتفاقية الدولية للإجرام المعلوماتي: "الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب نظام أشغال المنظومة".

وفقا للمادة 394 مكرر السابق ذكرها في فقرتها الأولى أنها نصت على أركان الجريمة في صورتها البسيطة وعقوبتها، بينما تنص الفقرة الثانية منها على الصورة المشددة منها والتي شدد عقوبتها إلى الضعف من الجريمة البسيطة.

وتتجسد الصورة البسيطة للجريمة في مجرد الدخول أو البقاء غير المشروع، بينما الصورة المشددة تكون بتوافر الظرف المشدد لها والمتمثل في الدخول أو البقاء غير المشروع، إما حذف أو تغيير في المعطيات الموجودة في النظام وإما تخريب وظيفة تشغيل النظام.

وعليه سوف نتناول فيما سيأتي جريمة الدخول أو البقاء البسيطة، وجريمة الدخول أو البقاء المشددة.

أ- **جريمة الدخول أو البقاء البسيطة:** من المتفق عليه على أن الجريمة تقوم على ركنين مادي ومعنوي، ومن المبادئ المستقرة في القانون الجنائي ان كل جريمة يستلزم لقيامها تحقق ركن مادي يتمثل بواقعة ترتب ضررا أو تشكل خطرا على المصالح المحمية قانونا[1].

إلى جانب ذلك لا يكفي لقيام الجريمة وتقرير العقاب عنها مجرد تحقق ركنها المادي، بل لا بد من تحقق ركن معنوي يعكس اتجاها إراديا خاطئا يستدل منه على نفسية الجاني عند ارتكابه للفعل[2].

---

[1] – أحسن بوصقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني لأشغال التربوية، الجزائر، 2002، ص47.

[2] – محمد حماد مرهج الهيبتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2005، ص182.

بناء على نص المادة 394 مكرر، من قانون العقوبات الجزائري يتضح لنا ان جريمة الدخول تقوم كسائر الجرائم على ركنين الركن المادي والذي يشمل السلوك الإجرامي الذي يترتب عنه الدخول غير المشروع إلى النظام والركن المعنوي المتمثل في القصد الجنائي.

- **الركن المادي**

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي يتمثل أساسا في تحقق فعل الدخول، وحيث أن السلوك الإجرامي قد يأخذ صورة إيجابية أو سلبية، ويتطلب من الجاني مباشرة نشاط إيجابي ولا يمكن أن تتحقق الجريمة بنشاط سلبي[1].

وملاحظ على هذا النوع من الجرائم، أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة، مثل الرشوة أو الاختلاس أو الزنا، بل تقع وترتكب عن كل شخص أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا طريقة تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أم لا.[2]

- **فعل الدخول إلى النظام:** تجدر الإشارة إلى أن مدلول كلمة الدخول تنصرف إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي، أو سيطرة على المعطيات والمعلومات التي يتكون منها.[3] كما أن فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، وإنما يتخذ هذا الوصف انطلاقا من كونه قد تم دون وجه حق[4] ولا يقصد بالدخول هنا بمعناه المادي أي الدخول إلى مكان ما كالمحل أو المنزل، وفي نفس الاتجاه الدخول إلى جهاز الحاسب الآلي، وإنما يجب أن ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكر أو ملكة التفكير لدى إنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات .ولم يحدد المشرع الوسيلة التي يتم بها الدخول إلى النظام، ولذلك تقع الجريمة بأي وسيلة أو طريقة، فقد يلجا الجاني إلى التلاعب بعناصر النظام المادية لكي يصل إلى هدفه وهو الدخول أو يربط بجهاز تنصت يستطيع من خلاله اختراق النظام أو استقبال المعلومات، كما قد يكون عن

---

[1]– عبد القادر القهوجي، المرجع السابق، ص343.

[2]– قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية القاهرة، 2004، ص343.

[3]– محمد حماد مرهج الهيبتي، مرجع السابق، ص183.

[4]– نفس المرجع.

طريق فيروس مثل(فيروس حصان طروادة) [1] أو عن طريق استخدام الرقم السري لشخص أخر أو الدخول من خلال شخص أخر مسموح له بالدخول أو عن طريق الوصول إلى الرقم السري للدخول أو عن طريق تجاوز نظام الحماية الخاصة إذا كان ضعيفا في حالة وجود مثل هذا النظام، ويستوي أن يتم الدخول مباشرة أو بطريقة غير مباشرة، كما هو الحال في الدخول عن بعد من خلال شبكات الاتصال الهاتفية[2] ويكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع قيودا للدخول إليه ولم يحترم الجاني تلك القيود، ومثال ذلك الأنظمة المتعلقة بأسرار الدولة أو دفاعاتها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة، كما يكون الدخول أيضا غير مشروع إذ كان يتطلب ضرورة دفع مبلغ من النقود، وتم الدخول دون دفع ذلك المبلغ، وكذلك يتحقق إذا كان مسموحا للجاني بالدخول لجزء معين في البرنامج، ولكنه تجاوزه إلى جزء أخر غير مسموح له الدخول فيه[3]. ولذلك يخرج من نطاق الدخول غير المشروع، الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كما لا تتوافر الجريمة ان اقتصر دور الجاني على مجرد قراءة الشاشة دون الدخول إلى داخل النظام، اذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع للنظام المعلوماتي[4].

- **فعل البقاء داخل النظام:** يقصد به كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول والنظر فيه أي في المعطيات التي يتضمنها وغيرها من التصرفات الغير مسموح بها والتي تشكل بدورها بقاء احتياليا[5].

---

[1]– فيروس حصان طروادة، وهو برنامج فيروس لديه قدرة على الاختفاء في البرنامج الأصلي للمستخدم، وعندما يتم تشغيل البرنامج الأصلي ينشط هذا الفيروس وينتشر ليبدأ في نشاطه التدميري، وهو ما يؤدي إلى تعطيل البرنامج وتزوير المعلومات ومحو بعضها وقد يصل إلى تدمير النظام بأكمله.

[2]– علي عبد القادر القهوجي، مرجع السابق، ص121.

[3]– امال قارة، مرجع سابق، ص109.

[4]– عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي الاسكندرية، 2002، ص30.

[5]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية القاهرة، 2002، ص235.

ويقصد به كذلك بالبقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[1]. وللعلم يتحقق البقاء المعاقب عليه داخل النظام المعلوماتي مستقلا عن الدخول للنظام، أو قد يجتمعا ويكون البقاء معاقبا عليه استقلالا عندما يكون الدخول إلى النظام مصرحا به، والمثال على ذلك الدخول إلى النظام عن طريق الخطأ، أو الصدفة حيث يتوجب في هذه الحالة على المتدخل قطع الاتصال والانسحاب فورا من داخل النظام، ولكن إذا بقي رغم ذلك فانه يعاقب عن جريمة البقاء داخل النظام بعد المدة المحددة له للبقاء داخله[2]، أما في حالة دخول الجاني إلى النظام ضد إرادة من له حق في السيطرة عليه، وبقائه داخل النظام بعد ذلك فانه في هذا الفرض يجتمع الدخول غير المصرح به والبقاء غير المشروع معا[3] وهنا يتوجب عليه الخروج من النظام وهذا من خلال القيام بفعل إيجابي وقطع الاتصال وبالتالي يمكن القول بان هذه الجريمة تعد صورة من صور الجرائم الامتناع التي تتحقق بفعال ايجابي[4].

ويتحقق الركن المادي لجريمة الإبقاء على الاتصال الغير المشروع مع النظام الآلي، وهذا في الفرض الذي يجد فيه الشخص نفسه داخل النظام عن طريق الخطأ ومع ذلك يقرر البقاء داخل النظام، وعدم قطع الاتصال به[5].

وبكل بساطة هو مجرد البقاء الفعلي فيه حيث يقاس البقاء الغير المشروع بالمدة الزمنية التي يستعمل فيها الجاني النظام، وبالتالي تكتمل هذه الجريمة مع اكتمال البقاء لمدة زمنية بعكس ما هو عليه الحال بالنسبة للدخول غير المشروع.[6]

- **الركن المعنوي**

وفقا للتحديد السابق للقصد الجنائي، فان الركن المعنوي لا يتوافر متى كان دخول جاني أو بقاءه داخل النظام مسموح به، اي مشروعا كذلك لا يقوم القصد الجنائي ان وقع الجاني في

---

[1]– عبد القادر القهوجي، المرجع السابق، ص601.

[2]– نفس المرجع، ص 602.

[3]– محمد حماد مرهج الهيبتي، المرجع السابق، ص190.

[4]– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان، 2008، ص161.

[5]– دردور نسيم، الجرائم المعلوماتية على ضوء القانون الجزائري المقارن، مذكرة لنيل الماجستير، كلية الحقوق، جامعة منتوري قسنطينة، 2012–2013، ص 34.

[6]– نهلا عبد القادر المومني، المرجع السابق، ص 162.

خطا يتعلق بحقه في الدخول أو حقه في البقاء أو في مدى نطاق هذا الحق، كان يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطا انه مسموح له بالدخول، فمتى توافر القصد الجنائي بعنصريه العلم والإرادة، فانه لا محل للاعتداد بالباعث على ارتكاب الجريمة بوصف ان الباعث عليها لا اثر له في قيام هذه الجريمة على الدخول إلى النظام أو البقاء فيه، محاولة الفضول أو النزهة أو إثبات القدرة على الانتصار على النظام المعلوماتي[1].

ب- جريمة الدخول أو البقاء المشددة: تتحقق هذه الجريمة في صورتها المشددة متى ترتب على الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام ذاته ان يؤدي وظيفته[2] ويكفي لتوافر هذا الشرط المشدد أن هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع، وبين النتيجة التي تحققت، وهي محو أو عدم قدرته على أداء وظيفة المعالجة الآلية للمعطيات[3] ولقد نص المشرع في المادة 394مكرر الفقرة 3، 2 على ما يلي "تضاعف العقوبة إذ ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج، يلاحظ ان المادة المذكورة قد نصت على ظرفين تشدد بهما عقوبة الدخول أو البقاء داخل النظام .ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه، ويكفي لتوافر هذا الظرف المشدد ان تكون هناك علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة[4].

وطبيعة هذه الجريمة عمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصرية العلم والإرادة، فإذا اثبت الجاني انتفاء علاقة السببية بين السلوك الإجرامي المتمثل في الدخول أو البقاء غير المشروع، والنتيجة الإجرامية التي هي ذات الظرف المشدد في الجريمة، كان يثبت أن تعديـل أو محـو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص365-366.

[2]- علي عبد القادر القهوجي، مرجع سابق، ص137.

[3]- جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001، ص20.

[4]- خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010، ص119.

يرجع إلى القوة القاهرة أو الحادث المفاجئ، انتفى السلوك الإجرامي وكذلك القصد الجنائي لدى الجاني[1].

فإذا توافرت أركان جريمة الدخول أو البقاء غير المشروع في صورتها المشددة، فان عقوبة الجاني تكون بالعقوبة المقررة له.

2- جريمة الاعتداء العمدي على النظام

لم يتعرض المشرع لهذه الجريمة، بل اكتفي بالنص على جريمة الاعتداء على المعطيات فقط، بخلاف المشرع الفرنسي الذي نص عليها في المادة 2/323 ق.ع.ف: "يعاقب كل من عطل أو أفسد نشاط أو وظائف المعالجة الآلية للمعطيات بالحبس حتى ثلاث سنوات وبالغرامة حتى ثلاثمائة ألف فرنك". وتتعلق هذه الجريمة بتجريم كل فعل من شانه أن يؤدي إلى توقيف تشغيل نظام المعالجة الآلية للمعطيات أو عدم أدائه لوظائفه المعتادة، وان كان المشرع لم ينص صراحة على ضرورة توافر الركن المعنوي في هذه الجريمة، إلا أن يستفاد من الأعمال التحضرية ضرورة توافر هذا الركن، كما انه أصبح من المتفق عليه قضاءا وفقها ضرورة توافر هذا الركن وانه يتخذ صورة القصد الجرمي[2].

وسوف نتناول الركن المادي لجريمة الاعتداء العمدي على النظام (أولا)، وركنها المعنوي(ثانيا).

أ- الركن المادي: يتمثل السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي، والمنتظر منه القيام به، وأما في فعل إفساد نشاطه أو وظائف هذا النظام ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة واحدة، بل يكفي أن يؤثر على أحد العناصر فقط سواء المادية أو المعنوية[3].

وتتمثل الاعتداء العمدي على نظام المعالجة الآلية للمعطيات فيما يلي:

- **التعطيل أو التوقيف:** إن التعطيل أو التوقيف والذي يندرج ضمن إعاقة النظام المعلوماتي، يقع بأي وسيلة، فالمشرع لم يشترط طريقة معينة لحصول الإعاقة، فقد تكون بطريقة مادية أو

---

[1]- ومن الامثلة على الجرائم الدخول أو البقاء في النظام المعلوماتي، مما يؤدي إلى محو النظام أو تدميره اذكر ما يلي:

-قيام مجموعة ارهابية يطلق عليها action direct بإتلاف برامج وملفات تخص شركة كبرس متخصصة في بيع الحاسبات الآلية وتوثيق المعلومات الحسابية وكان ذلك لحساب مجموعة من الشركات المنافسة.

-استطاع مهندس متخصص في انظمة التشغيل من تغيير شفرة الدخول لبرنامج، مستغلا من ذلك العيوب الموجودة في هذا البرنامج، وبالتالي تمكن من الدخول إلى البرنامج وسرقة خمسة ملايين فرنك من أحد البنوك.

[2]- علي عبد القادر القهوجي، مرجع سابق، ص 139.

[3]- امال قارة، مرجع سابق، ص 115.

معنوية ومن أمثلة إعاقة النظام بطريق مادي، أعمال العنف المادية على أجهزة الحاسب وشبكة الاتصالات، وذلك عن طريق تخريبها بكسرها أو سكب سائل عليها أو أي مادة أخرى أو حتى منع العاملين من الوصول إلى النظام، أما الإعاقة أو التعطيل بوسيلة معنوية فقد يتمثل في إدخال فيروس على البرنامج أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة تؤدي على سبيل المثال، لان يتباطأ النظام عن أداء وظيفته المعلوماتية داخل النظام المعلوماتي[1].

يمكن القول كذلك إن إعاقة سير عمل نظام المعالجة الآلية للمعطيات هو فعل يتسبب في تباطؤ أو إرباك عمل نظام المعالجة، مما ينتج عنه تغيير في حالة عمل النظام[2].

وهذا الإرباك تتأثر به أجهزة الحاسب الآلي والبرامج على السواء، فهو يؤثر في نظام معالجة البيانات ككل بما فيها أدوات تشغيل ذلك النظام.

ويجب في التوقيف أو التعطيل أن يكون ايجابيا، وان يصدر عن الجاني نشاط ايجابي يؤدي إلى توقيف النظام، فإذا كان ما صدر عنه امتناع مجرد فلا يتوافر الركن المادي ولا تقوم الجريمة أما إذا كان على الجاني التدخل لتشغيل النظام بموجب يتوقف على تدخله، وامتنع بقصد تعطيل النظام، فهنا يتوافر الركن المادي وتقع بذلك الجريمة، والامتناع هنا هو امتناع مختلط بنشاط ايجابي يتمثل في رفض الجاني القيام بما يفرضه عليه القانون من واجب تشغيل النظام.

- **الإفساد أو التعييب:** يقصد بالإفساد أو التعييب كل فعل وان كان لا يؤدي إلى التعطيل لكنه يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم، وذلك بان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها ومن وسائل التعييـب أو الإفساد استخـدام

1- على عبد القادر القهوجي، مرجع سابق، ص139.

2- امال قارة، مرجع سابق، ص119

- القنبلة المعلوماتية[1] أو استخدام البرنامج الذي يحمل فيروسا يطلق عليه حصان طروادة[2] وغير ذلك من الفيروسات التي تجعل مخرجات النظام غير تلك التي كان يجب عليه أن يخرجها، بل أن الإفساد يمكن أن يتحقق عن طريق إتلاف أو تخريب العناصر المادية في النظام.[3]

مما سبق، فان السلوك الإجرامي في هذه الجريمة ينصرف إلى كل فعل من شانه إرباك عمل نظام معالجة البيانات، ويستوي أن يكون من شان نشاط الجاني إعاقة أو إفساد نظام التشغيل، ويستوي أن يؤدي نشاط الجاني إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة، أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شانها أن تعيق حسن سير النظام، كالاعتداء المادي على النظام أو نشر فيروس فيه، حيث يستوي لدى المشرع الوسيلة المستخدمة، ولا يشترط

---

[1]– القنبلة المعلوماتية :تنقسم إلى قنبلة منطقية وأخرى زمنية، والقنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محدّدة أو كل فترة زمنية منتظمة، و تّمّ وضعه في شبكة معلوماتية بهدف تحد يدّ ظروف أو حالة محو النظام بغرض تسهيل تنفيذ عمل غير مشروع، ومثال ذلك أن تسعى القنبلة المنطقية إلى البحث عن حرف وليكن حرف (أ) في أي سجل يتضمن أمرا بالدفع وعندما تكتشفه تتحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل، الأمر الذي يؤّدّي إلى تعييب ذلك النظام .أمّا القنبلة الزمنية فهي تثير حدثا في لحظة محدّدة بالساعة واليوم والثانية، يتم إدخالها في برنامج تنفذ من خلال جزء من الثانية أو عدة ثوان أو دقائق حسب التقدير اللازم.أكثر تفصيلا راجع: محمد سامي الشوا، مرجع سابق، ص195.

[2]– برنامج حصان طروادة :وهو برنامج يقوم بتغيير محسوس في البرامج أو المعطيات، وهو برنامج خادع يخفي ظاهره غرضا غير مشروع يضّمره، إذ يظّهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدمه بينما يكّون موجودا بطريقة خفية داخله بعض الأوامر أو المعلومات التي تؤدّي عند تشغيله مهامّا ضارّة غير متوقّعه تمثّل أغراضه الحقيقية المضرّة.أكثر تفصيلا راجع :جميل عبد الباقي الصغير، مرجع سابق، ص 27.

[3]– ومن الأمثلة العديدة والمتنوّعة لوضع قنابل زمنية ومنطقية ممّا أدى إلى التأثير على أنظمة الحاسب الآلي ونظم البيانات نذكر ما يلي:

أ. في فرنسا قام محاسب خبير في نظم المعلومات وبدافع الانتقام وعلى إثر فصله من المنشأة التي يعمل فيها، بوضع قنبلة زمنية في شبكات المعلومات الخاصة بالمنشأة، بحيث تنفجر بعد مضى ستة أشهر من رحيله من المنشأة وقد ترتّب على ذلك إتلاف كل البيانات المتعلّقة بها.

ب. في الدانمارك تمكّن خبير في نظم المعلومات من وضع قنبلة منطقية في نظام إحدى الحاسبات أدّت إلى محو أكثر من مائة برنامج، وقد تمّ كذلك محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليها، وتمّ ضبط الجاني حيث حُكم عليه بالحبس لمدّة سبعة أشهر.

ج. في ولاية لوس أنجلس الأمريكية تمكّن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها ممّا أدّى إلى تخريب ذلك النظام عدّة مرات .راجع :عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 373 وما بعدها.

أن تكون الإعاقة أو الإفساد بصورة كلية، بل يمكن أن يؤدي النشاط إلى إعاقة أو إفساد جزئي للنظام[1].

ب- الركن المعنوي: جريمة الاعتداء القصدي على النظام المعالجة الآلية للمعطيات جريمة قصدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة ويرى جانب من الفقه الجنائي انه إذا قام الشخص الذي يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطا في التشغيل أو التعامل مع البيانات، ينتفي القصد الجنائي لديه، ولا يسال عن هذه الجريمة[2] فإذا توافر الركن المعنوي بعنصريه السابقين إلى جانب الركن المادي قامت الجريمة واستحق مرتكبها العقوبة.

3- جريمة الاعتداء العمدي على سلامة المعطيات الموجودة داخل النظام

يتضح جليا مما سبق، إن المشرع لا يحمي نظام البيانات من الناحية المادية أو البرامج أو التطبيقات، لكنه يوفر الحماية الموجودة داخل النظام ذاته، وذلك ضد أي نشاط إجرامي، وهو ما يطلق عليه بالقرصنة المعلوماتية، علما بان هدف الجاني من هذه الجريمة هي ان يحقق النظام المعلوماتي نتائج أو معطيات غير تلك التي كان يجب أن يحققها، وذلك هو قصد الجاني ولذلك فهذه الجريمة تختلف عن الجريمة السابقة وهي الخاصة بإعاقة أو تحريف تشغيل نظام معالجة البيانات، فهذه الأخيرة تتعلق بالنظام ذاته، أما الجريمة التي نحن بصددها فهي خاصة بالمعطيات أو البيانات التي هي داخل النظام ولقد نصت عليها المواد 3.4.8 من الاتفاقية الدولية لإجرام المعلوماتي كما نص عليها المشرع في المادة 394 مكرر2 من قانون العقوبات "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من ادخل بطريقة الغش معطيات في نظام المعالجة الآلية أو ازل أو عدل بطريق الغش المعطيات التي يتضمنها.[3]

يتضح من خلال النص أعلاه، انه حتى تقوم الجريمة لابد من توافر ركنيها المادي والمعنوي.

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 375.

[2]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع السابق، ص43.

[3]- خيثر مسعود، مرجع سابق، ص123.

أ-الركن المادي: يتمثل النشاط الإجرامي في هذه الجريمة في أفعال الإدخال والمحو والتعديل، ويكفي توافر أحدهما لقيام الجريمة فلا يشترط اجتماعهما معا حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقوم الركن المادي في هذه الجريمة ولكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على تلاعب في المعطيات التي يتضمنها نظام المعالجة الآلية للبيانات، وذلك بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل اخرى قائمة[1].

وعليه فان السلوك الإجرامي في هذه الجريمة محدد ويتمثل في الاعتداء على معطيات في نظم المعالجة، أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز أو إشارات تمثل تلك المعلومات، أي بيانات تمت معالجتها فالجريمة في هذه الحالة تقع على المعطيات أي البيانات المعالجة، دون المعلومة ذاتها ولذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج بعد ولم تدخل إلى نظام معالجة البيانات، وكذلك البيانات التي أدخلت إلى النظام ولكن لم تبدأ بعد أي خطوة في معالجتها، وكذلك المعلومات التي انفصلت عن النظام وسجلت على شريط مضغوط أو قرص مدمج، وذلك لأنها أصبحت خارج النظام. فالنص يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بان اتخذت خطوة أو أكثر في مراحل معالجتها[2].

في هذا الصدد، يمكن القول بان الحماية الجنائية في هذه الجريمة مستمرة وقائمة طالما أن المعلومات المعالجة داخل النظام أو في طريقها للمعالجة حسب التحديد السابق، أو المعلومات المعالجة التي انفصلت عن النظام ثم أعيد إدخالها فيه، أما المعلومات غير المعالجة التي لم تدخل إلى النظام أو أدخلت ولم تبدأ مراحل معالجتها فقط، أو عولجت وانفصلت عن النظام فهي خارج نطاق الحماية المشمولة بهذا النص، وان كان يجوز حمايتها بنصوص جنائية أخرى[3].

وسأشرح فيما يلي ما المقصود بالأفعال المكونة لهذه الجريمة والتي تكون على إحدى الأشكال التالية:

- **فعل الإدخال:** يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في الفرض

---

[1]- علي عبد القادر القهوجي، مرجع سابق، ص 143.

[2]- امال قارة، مرجع سابق، ص 121.

[3]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 377.

الذي يستخدم فيه العامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها مبلغا من النقود من أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص والسري للدخول وسحب تلك النقود التي تفوق المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا (للتاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له، وبصفة عامة، يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان، سواء من صاحبها الشرعي أو من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب يضيف معطيات جديدة (فيروس، حصان طروادة، قنبلة معلوماتية زمنية)[1].

- **فعل المحو:** يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2].
- **فعل التعديل:** يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب بالمعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة (D'effacement Gomme) أو برنامج الفيروسات بصفة عامة[3].

ونستنتج مما سبق أن كل من فعل الإدخال، المحو والإدخال ذكرت على سبيل الحصر، مما يجعل أي فعل اخر غيرها لا يقع تحت طائلة التجريم، كالنقل المعطيات أو نسخها.

ب- الركن المعنوي: جريمة الاعتداء القصدي على المعطيات جريمة قصدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصرية العلم والإرادة. فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب ان يعلم الجاني بان نشاطه الجرمي يترتب عليه

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، ص 381.

[2]- قيام بعض المسؤولين بالاستيلاء على مبلغ قدره 61 ألف دولار كانت قد أرسلته إحدى شركات التامين لصالح إحدى المراكز الطبية، وقاموا بفتح حسابات وهمية ووضعوا المبلغ بها، وحتّى تتمّ هذه العملية بنجاح قاموا بمحو حسابات من سجلات الحاسب الآلي للمركز الطبّي، وهي حسابات المتوفين، وذلك ما جُعلها غير قابلة للتحصيل وإمّا بحذفها من الملفات.

[3]- امال قارة، مرجع سابق، ص 122.

التلاعب بالمعطيات، ويعلم أيضا انه ليس له الحق في القيام بذلك، وانه يعتدي على صاحب الحق والسيطرة على تلك المعطيات أو بدون موافقته، و لكن لا يشترط لتوافر الركن المعنوي بالإضافة إلى القصد العام، نية خاصة تتمثل في نية الإضرار أو قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وان كان الضرر قد يتحقق في الواقع نتيجة لنشاط الإجرامي إلا انه ليس عنصرا في الجريمة[1] فإذا كانت جريمة الاعتداء القصدي على المعطيات مثلها مثل جريمة الاعتداء القصدي على نظم المعالجة الآلية للمعطيات، تهدف إلى محاربة أفعال التخريب والقرصنة إلا أن التمييز بين تلك الجريمتين ليس أمرا سهلا ذلك أن جريمة الاعتداء القصدي على نظام المعالجة الآلية لمعطيات، وان كانت تقع بصفة أساسية على البرامج وشبكات الاتصال والنقل، إلا أنها قد تصيب المعطيات أيضا نتيجة لأفعال الاعتداء التي تقوم بها تلك الجريمة، وبالمقابل فان الاعتداء على المعطيات الذي تقوم به جريمة الاعتداء القصدي على المعطيات قد يؤثر على صلاحية نظام المعالجة الآلية للمعطيات للقيام بوظائفه سواء على البرامج أو على شبكات الاتصال والنقل.[2]

المطلب الثاني: مفهوم جريمة التزوير الالكتروني

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شانه ان يشكل جريمة التزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير ويلاحظ إن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة 1988 وصدور قانون العقوبات لسنة 1994 عدل المادة 441/1 لكي تستوعب جانب التزوير العادي جريمة التزوير الالكتروني حيث نصت بعد تعديلها على" ان كل تغيير للحقيقة بطريق الغش..... في محرر أو في دعامة أخرى تحتوي تعبير عن الفكر" فالمشرع فصل بذلك التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات حيث افرد نص خاص، لصورة الأولى بينما احتوت الصورة الثانية في النص العام لجريمة التزوير[3].

---

[1]– علي عبد القادر القهوجي، مرجع السابق، ص 150.

[2]– نفس المرجع، ص 149.

[3]– عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، 2009، ص 104.

ونجد أن المشرع الجزائري لم يتكلم عن التزوير المعلوماتي لذلك سنتطرق لتحديد وتعريف التزوير الالكتروني في الفرع الأول وموقف المشرع الجزائري من التزوير الالكتروني في الفرع الثاني.

الفرع الأول: تعريف التزوير الالكتروني

عرف التزوير الالكتروني على انه تغيير الحقيقة في المستندات المعالجة اليا والمستندات المعلوماتية وذلك بغية استعمالها.[1] ويختلف التزوير الالكتروني عن التزوير التقليدي، كون أن تزوير الالكتروني يتضمن إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو بالإضافة، إضافة إلى انه قد يتعلق بالكيان المادي للحاسب الآلي، أو البرامج ذاتها، وهو يندرج بصفة عامة تحت نطاق التزوير الالكتروني كسلوك غير مشروع يتعلق بمعالجة المعلومات ونقلها، فهو سلوك غير قانوني وغير مسموح به يتعلق بالتعامل الفوري مع المعلومات والبيانات أو انتقالها[2] وتزوير يتضمن نسخ الأقراص المدمجة على أقراص أخرى، وتغيير المعلومات والبيانات واستخدامها كوسيلة لتدليس، سواء تم استخدامها في ارتكاب عمل إجرامي أو لا، لان تغيير الحقيقة في المحررات أو تغيير التوقيعات والصور من قبيل التزوير[3] ومهما تعددت التعريفات الخاصة بالتزوير الالكتروني فإنها لا تكاد تخرج على إن التزوير الالكتروني يعتبر نسخا للأقراص أو دخول غير مشروع للشبكة مع تعديل بيانات وغيرها من الوسائل المختلفة.

1- جريمة التزوير الالكتروني

نقصد بها ارتكاب جريمة التزوير الالكتروني سواء بالدخول المشروع أو غير المشروع على النظام المعلوماتي والتعامل مع بياناته بطرق التزوير المادية أو المعنوية وباستخدام الحاسب الآلي وملحقاته للحصول على المحرر أو وثيقة الكترونية مزورة و تعد جريمة التزوير في المجال المعلوماتي من اخطر صور غش المعلوماتية نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات وأصبحت تجري من خلال كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف "

---

[1]- على عبد القادر قهوجي، المرجع السابق، ص 152.

[2]- الهيتي محمد حماد مرهج، مرجع سابق، ص 76.

[3]- النجيمي محمد بن يحي بن حسن، الجرائم الالكترونية من جهة النظر اسلامية والقانونية، الدورة الخامسة، المجتمع والأمن، كلية الملك فهد الامنية، الرياض، أفريل 2008، ص 76.

المكتوب" في القانونين المدني والجنائي، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة.[1]

فان موضوع التزوير هو المحرر الذي لابد من توافر شروط فيه تتمثل في الكتابة من قبل شخص وان ينتج أثار القانونية هذه من الناحية التقليدية لجريمة التزوير لكن في مجال المعلوماتية فالأمر يختلف فالجريمة التزوير الالكتروني تقع على المستندات الالكترونية[2].

تجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، ربما اقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا، الفرق أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير تجعل التزوير يرد على محرر وعليه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير كما هو عليه الحال في التشريع الفرنسي مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي[3].

2- النشاط الإجرامي لجريمة التزوير الالكتروني

النشاط الإجرامي لجريمة التزوير يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير والمقصود هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير، أو مراكزهم القانونية الثابتة في تلك المحررات، وعليه يمكن تصور تغيير الحقيقة في نطاق المعالجة المعلوماتية بالتلاعب في المعطيات مما يؤثر على أصالتها.[4]

وتجدر الإشارة إلى أن تحويل البرامج أو قواعد البيانات لا يعد تزوير وإنما يقع تحت طائلة نصوص التقليد الواردة في قانون حق المؤلف والحقوق المجاورة.

---

[1]- فشار عطاء الله، المرجع السابق، بدون صفحة.

[2]- نفس المرجع.

[3]- نفس المرجع.

[4]- أمال قارة، المرجع السابق، ص 139.

لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية –والتي كما هو معروف– لا تتحقق إلا أثناء تكوين المستند بالنسبة إلى للجريمة محل البحث التزوير العادية[1].

الفرع الثاني: طرق التزوير قانونا وعلاقتها بالتزوير الالكتروني

1- التزوير المادي

ذكرت صور التزوير في قانون العقوبات الجزائري على سبيل الحصر، وعليه لا يمكن اعتبار تغيير الحقيقة تزوير إلا أذا حصلت بأحدي الطرق النى نصت عليها المواد 214 و215 بالنسبة لغير الموظف العام، ولقد حصرت المادة 214 عقوبات أفعال التزوير المادي بقولها[2] "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومي المحررات العمومية أو الرسمية أثناء تأدية وظيفته".

أ- **أما بوضع توقيعات مزورة:** يتحقق هذا النوع من التزوير عندما يمضي المزور محررا باسم شخص أخر أو باسم شخص خيالي أو باسم شخص يشاركه في الاسم ولكن بدون تكليف منه، فلا يشترط في الإنشاء أن يكون مقلدا تقليدا مزورا بل يقوم التزوير كيفما كان التقليد لان القانون يكتفي لقيام الجريمة بوضع المزور إمضاء غير إمضائه على المحرر، وكذلك لا يجد تزويرا في توقيع المرأة المتزوجة بالاسم الذي كانت تحمله قبل الزواج، ولا في توقيع الشريك في مصالحة الشخصية بتوقيع الشركة لان كلتا الحالتين يكون الإمضاء قد صدر عمن له الحق في التوقيع به[3].

ب- **التقليد في الكتابة:** تقليد الكتابة يعني صنع كتابة مشابهة لها، هنا أيضا لا يشترط في التقليد أن يكون متقنا وإنما يكفي فيه أن يكون على درجة من التشابه بحيث يحمل القارئ عن الاعتقاد أن المحرر صدر عن الشخص الذي قلدت كتابته، وكثيرا ما يختتم التقليد في الكتابة بوضع إمضاء مزور إذ المحرر الخالي من إمضاء لا قيمة له قانونا وبالتالي لا يرتب ضررا بالغير، إلا أن هذا القول ليس مطلقا، وقد نجد محررا مقلدا خاليا من كل إمضاء ورغم ذلك له قيمة قانونية ما لم يكشف تزويره وقد يضر بالغير كتقليد تذاكر السكة الحديدية.[4]

---

[1]- د. علي عبد القادر القهوجي، المرجع السابق، ص 155.

[2]- بلحاج العربي، ابحاث ومذكرات في قانون الفقه الاسلامي، ديوان المطبوعات الجامعية، بن عكنون الجزائر، 1996، ص518.

[3]- دردروس مكي، القانون الجنائي الخاص في التشريع الجزائري، ديوان المطبوعات الجزائرية، قسنطينة، 2007، ص 70.

[4]- دردروس مكي، المرجع السابقّ، ص 71.

ج- التغيير في الكتابة : يكتسي هذا النوع من التزوير عدة أشكال، فقد يقع التزوير بحذف جزء من المحرر، وقد يحصل بشطب كلمة أو جملة من المحرر أو محوها بممحاة أو بمادة كيميائية وقد يحصل بإضافة شيء إلى المحرر كان يكتب المزور كلمات بين السطور أو في البياض المتروك في المحرر وفي هذه الحالة لا يشترط التقليد في الكتابة المضافة، فالتغيير المقصود هنا هو التزوير الذي يقع على المحرر بعد تمامه وإمضائه، أما إذا وقع التزوير أثناء كتابة المحرر وقبل التوقيع عليه فان العملية تدخل في حكم التزوير المعنوي، وقد يقع التزوير بالإنقاص كان يمحو المزور عبارة من المحرر ثم لا يعوضها بشيء، وقد يقع أخيرا باستبدال اسم أو تبديل تاريخ أو طمس كلمة ببقعة حبر[1].

د- اصطناع المحرر: يتم هذا النوع من التزوير بإنشاء اتفاقات أو نصوص أو التزامات أو مخالصات بالمعنى المشار إليه في المادة 2/216 فهو فعل من يصنع لنفسه سندا لأنه لا يملك سندا أو للاستعاضة به عن سند اقل منه نفعا، وهذا الفعل يتبعه عادة توقيع مزور ولكن ليس بالضرورة لان عقوبة المادة 216 تطبق على فعل الاصطناع قبل إتمام المحرر والتوقيع عليه[2].

2- التزوير المعنوي

إن صور التزوير المعنوي تناولتها بالحصر المادة 215 من قانون العقوبات الجزائري والمتعلقة بتزييف جوهر المحررات الرسمية او ظروفها بطريق الغش، وكتابة الاتفاقات خلاف التي أمليت أو دونت من قبل الأطراف ، وتقرير وقائع كاذبة بصورة وقائع صحيحة ، والشهادة كذبا بوقائع غير معترف بها في صورة وقائع معترف بها وإسقاط أو تغيير الإقرارات عمدا والتي تنص " يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية قام أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريق الغش وذلك إما بكتابة اتفاقات خلاف التي دونت أو أمليت من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبا بان وقائع قد اعترف بها أو وقعت في حضوره أو بإسقاطه أو بتغييره عمدا القرارات التي تلقها. ويقع التزوير المعنوي عن طريق استبدال الأشخاص كانتحال شخصية الغير بالتصريح شخص في محرر ما أمام موثق انه يحمل اسم غير اسمه الحقيقي ويكون تزوير معنويا إذا اثبت الموثق كذبا في محرر رسمي أن شخص حضر أمامه والواقع لم

---

[1]- نفس المرجع.

[2]- نفس المرجع، ص 72.

يحضركما يمكن أن يقع عن طريق استبدال اتفاقات ووقائع أو تزييف الإقرارات وهي من أشكال التزوير المنصوص عليها في نص المادة 216 ق.ع.ج ، ومن المؤكد عليه انه لا يتم المعاقبة على التزوير المعنوي إلا إذا ارتكب في السندات رسمية إذ أن الكذب وحده لا يؤبه به ما لم يتجسد في عقد أو سند رسمي على عكس التزوير المادي فان القضاء يعاقب عليه إذا كان واقع على المحررات مهما كانت طبيعتها على شرط أن يقع عمدا ومن شانه إلحاق ضررا بالغير.[1]

3- التزوير بالكمبيوتر

يمكن عن طريق استعمال الكمبيوتر وملحقاته، نقل صورة من أصل ذاكرة الكمبيوتر ثم عرضها على الشاشة وطبعها بطابعة وتتلخص طرق التزوير الالكتروني فيما يلي:

- استخدام جهاز يعرف بالماسح الضوئي "Scanner" في أخد صورة لمحرر المراد تزويره وذلك ليسجل في ذاكرة الكمبيوتر باستخدام برنامج معين يسمى بالملف"Fille".
- يتم عرض المستندات التي سجلت باستخدام سكانر على شاشة عرض الجهاز "Monitor".
- يتم ضبط لصورة المحرر لإحداث تغييرات أو إدخال مستجدات عليه.
- يتم إعطاء أمر بالطبع "Print" للطابعة لتطبع المحرر المزور.
- يتم إخراج المحرر المزور من الورقة.
- يتم فحص المحرر المزور بالمساحات المتناسبة مع الأصل.

كما يمكن أن يتم التزوير بالآلة الناسخة[2] وذلك بواسطة استخدام الكمبيوتر وملحقاته، يمكن نقل مستند أو صورة من أصل ذاكرة الكمبيوتر ثم استعراضها على الشاشة ثم طبعها بطابعة وتتلخص طريقة تزييف العملات بالكمبيوتر فيما يلي:

- استخدام جهاز يعرف بالماسح الضوئي"Scanner" في اخذ صورة لوجه وظهر العملة المراد تزييفها وذلك لتسجل في ذاكرة الكمبيوتر باستخدام برنامج معين يسمى بالملف "File".

---

[1] – المادة 215، 216، من الأمر رقم 156/66 المؤرخ في18 صفر عام 1386 الموافق لـ 08 جوان 1966، الذي يتضمن قانون العقوبات، المعدل والمتمم، ص 65.

[2]– هلال محمد رضوان، بحوث واراء جديدة في مجال كشف التزييف والتزوير، عالم الكتب، مصر،1993 ص 79،81.

- يتم عرض العملات التي تم تسجيلها باستخدام السكانر على الشاشة عرض الجهاز "Monitor"
- يتم عمل ضبط لصورة العملة المسجلة أو إحداث تحسينات أو إدخال مستجدات عليها.
- يتم إعطاء أمر بالطبع "Print" للطابعة لتطبع العملات المزيفة.
- يتم إخراج العملات المزيفة على هيئة مجموعات على ورقة عن طريق تنسيق ومقابلة كل من الوجه والظهر مثل العملة الصحيحة.
- يتم فص العملات بالمساحات المناسبة لكل فئة من العملة الورقية التي وقع عليها التزييف
- يتم تجهيز العملات الزائفة لدفعها للتداول.[1]

وتكمن خطورة التزوير بالكمبيوتر وملحقاته في توفره وشيوع استخدامه في الوقت الحاضر كما تكمن خطورة التزوير بهذا الجهاز في إنتاج نسخ مزورة في زمن قياسي، وقد شجع على التزوير الالكتروني وجود الطابعات كوسائل إخراج توصل بالكمبيوتر حيث تتفاعل معه وتحول ما هو مسجل في ذاكرته أو ما هو معروض على الشاشة إلى طبعات تزداد في حسنها يوما تلو الأخر، مع ازدياد التقدم التكنولوجي التنافسي بين الشركات المنتجة[2]. وعليه فان وقت الحالي يعرف انتشار واسع للحاسب الآلي وشبكة المعلومات الدولية بالخصوص وتأثيرها الكبير على حياة الناس وهذا يستلزم علينا إعادة نظر وتفسير لطرق التزوير الحالية والتي لا تعالجها النصوص العقابية الحالية فما تحمله الجريمة الالكترونية من أنماط يستلزم علينا تجريمه ومواجهته حتى تطاله النصوص العقابية.

---

[1]– هلال محمد رضوان، مرجع السابق، ص83.

[2]– نفس المرجع، ص82

المبحث الثاني: الجزاءات المقررة للجريمة الالكترونية

لقد نص المشرع الجزائري على جملة من العقوبات الخاصة بالجرائم الالكترونية منها عقوبات أصلية وأخرى تكميلية، بالإضافة إلى عقوبة خاصة بالأشخاص المعنوية والأشخاص الطبيعية سنوضح أكثر من خلال المطلب الأول الذي سنخصه بالدراسة حول الجزاء المقررة لشخص الطبيعي والمطلب الثاني بالجزاء المقرر لشخص المعنوي.

المطلب الأول: الجزاء المقرر لشخص الطبيعي

لقد أورد المشرع الجزائري جملة من الجزاءات على الشخص الطبيعي والتي تختلف باختلاف الفعل المرتكب.

الفرع الأول: العقوبات الأصلية

إن الملاحظ من نصوص الخاصة بالجرائم الماسة بالأنظمة المعلوماتية وجود تدرج داخل النظام العقابي، وهذا يؤكد الخطورة الإجرامية لهاته التصرفات، ويتجلى هذا التدرج الهرمي على حسب الخطورة.

1- الجزاء المقرر لجرائم الاعتداء على سير النظام

سنتناول الجزاء المقرر لكل من جريمتي الدخول والبقاء غير المشروع سواء في صورها البسيطة أو المشددة.

❖ **بالنسبة لجريمة الدخول أو البقاء غير المشروع**

نص المشرع الجزائري من خلال نص المادة 394 مكرر من ق.ع.ج على عقوبة هاته الجريمة سواء في صورتها البسيطة أو المشددة.

- **في صورتها البسيطة:** يعاقب المشرع الجزائري طبقا لنص المادة سالفة الذكر بالحبس من 3 أشهر إلى سنة وغرامة من 50000 دج إلى 200000 دج[1] ونجد هنا ان المشرع الجزائري ترك للقاضي السلطة التقديرية بان جعل له حد أدنى وحد أقصى في تقدير العقوبة بحسب الوقائع المعروضة أمامه، حيث يختلف الباعث من شخص لأخر، فليس باعث الفضول والاكتشاف كباعث الجوسسة والربح، وعلى هذا وجب اختلاف التقدير.

[1]- حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني، كلية الحقوق، جامعة اكلي محند أولحاج، العدد الثاني، 2016، ص 73،74.

- **في صورتها المشددة: ان** المشرع الجزائري في نص المادة 394 مكرر فقرة الثانية والثالثة ضاعف من عقوبة جريمة الدخول والبقاء غير المشروع إذا ترتب عن هذا الأخير إما حذف أو تغيير المعطيات، سواء في حدها الأدنى الذي أصبح ستة أشهر بعدما كان ثلاثة أشهر، أو في حدها الأقصى إلى سنتين بعدما كانت سنة واحدة. وبالنسبة للغرامة تكون من 50000 دج إلى 300000 دج[1].

2- الجزاء المقرر لجرائم الاعتداء العمدي على المعطيات

سنتناول فيه العقوبات الأصلية إلى نص عليها المشرع الجزائري بالنسبة لجريمتي الاعتداء العمدي على المعطيات الموجودة داخل النظام ثم العقوبات الأصلية لجريمة التعامل غير المشروع في المعطيات.

- **بالنسبة لجريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام**

نصت المادة 394 مكرر1 من ق ع ج على العقوبة الأصلية لمرتكب جريمة الاعتداء العمدي على المعطيات بالحبس لمدة تمتد من 6 أشهر إلى ثلاث سنوات وغرامة من 500000دج إلى 4000000 دج.

- **بالنسبة لجريمة التعامل غير المشروع بالمعطيات**

تكون العقوبة عن طريق تقرير عقوبتان أصليتان هما الحبس والغرامة.

- **بالنسبة لتعامل في معلومات صالحة لارتكاب الجريمة**

إن التعامل في المعطيات ينطوي على العديد من الأفعال والأعمال والعمليات السابقة على استعمال المعلومات كبحثها وتجميعها، وصولا إلى توفيرها ونشرها أو الاتجار فيها حيث يعاقب المشرع على القيام العمدي أو عن طريق الغش بالأفعال السابقة الذكر بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000دج إلى 10000000دج[2].

---

[1]- المادة 394 مكرر2 من قانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق لـ 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر 1386 الموافق لـ 08 جوان 1966، والمتضمن قانون العقوبات، ج ر العدد 71، الصادرة بتاريخ 2004/11/10، ص 11.

[2]- حمود ناصر، المرجع السابق، ص 81-83.

- بالنسبة لجريمة التعامل في معلومات متحصله من الجريمة

أضاف المشرع الجزائري صورة ثانية من صور التعامل في معلومات غير المشروعة، تتمثل في التعامل في معلومات متحصلة من جريمة وذلك في حالة ارتكاب فعل من الأفعال التي حصرتها الفقرة الثانية من المادة 394 مكرر2 وهي الحيازة أو الإفشاء أو النشر أو الاستعمال والتي يعاقب عليها بنفس العقوبة المقررة في الصورة الأولى من جريمة التعامل غير المشروع في المعطيات.[1]

- بالنسبة لجريمة التزوير الالكتروني

فنجد ان القوانين الجنائية لم تفرض عقوبة الإعدام على مرتكبي هذا نوع من الجرائم ولكنها شملت في قوانينها عقوبات أخرى كالسجن والحبس والغرامة وغيرها من العقوبات كما جاء في المواد 214 ق ع 215ق ع و 216 ق ع 217 ق ع 218 ق ع الخاصة بالتزوير التقليدي وكذلك المواد 394 مكرر1 الى مكرر7 الخاصة بالجرائم المعلوماتية وتعتبر الغرامة في جرائم التزوير المعلوماتي عقوبة مالية توقع على المجرم المعلوماتي قد تكون اصلية وقد تكون اختيارية لوجود عقوبة أخرى معها، فالقضاء هو الذي يحدد اما ان يحكم بها مع العقوبة الاصلية او لا يحكم.

الفرع الثاني: العقوبات التكميلية

إلى جانب العقوبات الأصلية المطبقة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، اقر المشرع عقوبات تكميلية التي تطبق على كافة صور المساس بأنظمة المعالجة الآلية للمعطيات وهي العقوبات المنصوص عليها بالمادة 394 مكرر6 على النحو التالي:

مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها" ومن نص هذه المادة يمكن حصر العقوبات التكميلية في:

1- المصادرة

كما عرفتها المادة 15 فقرتها الأولى من قانون العقوبات هي: الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء.

[1]- باطلي غنية، المرجع السابق، ص 221.

وتشمل المصادرة فيما يتعلق بهذه الجرائم أجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة مع مراعاة حقوق الغير حسن النية. وبذلك تكون المصادرة بالنسبة لهذه الجرائم عقوبة وجوبية.

2- إغلاق الموقع

يتعلق الأمر بالواقع التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

3- إغلاق المحل أو مكان الاستغلال

شرط أن تكون الجريمة قد ارتكبت بعلم مالك المكان الذي سمح من خلاله بالدخول غير المصرح به لمختلف الأنظمة وسمح بالتلاعب بالمعطيات مثل مقاهي الانترنت وهنا وجب التأكد واثبات ركن العلم لدى الأخير اذ يمكن أن يكون غير مرتكب الجريمة وعليه لا تطبق عليه العقوبة التكميلية بعد إدانة الجاني.

وبالنسبة لمدة الغلق لم تحددها المادة 394مكرر6 من ق ع ج، وعليه يمكن أن تكون مؤبدة أو مؤقتة[1].

وفيما يخص العقوبات التكميلية الخاصة بالجريمة التزوير تتمثل في حرمان مرتكب التزوير من تولي بعض الوظائف وغيرها من العقوبات المذكورة في المادة 9مكرر و9مكرر1 من القانون 06-23 المتضمن قانون العقوبات اما فيما يخص تطبيق عقوبة المصادرة على هذا النوع من الاجرام فتتم بالمصادرة الأجهزة التي استعملت في ارتكاب جريمة التزوير كجهاز الحاسب الالي وغيره من المعدات المستعملة في الجريمة او كانت معدة للاستعمال وهذا ما ذكرته المادة 394 مكرر3[2].

المطلب الثاني: الجزاء المقرر لشخص المعنوي

نص المشرع الجزائري على مسالة الشخص المعنوي وتطبيق عقوبات خاصة به تطبيقا لتوصية الواردة بالمادة 12 والتي نصت على وجوب أن يسال الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما يسال عن الجريمة التامة أو الشروع

[1] – المادة 394 مكرر6، قانون 04-15، ص 11.

[2] –فشار عطاء الله، مرجع السابق، ص 33.

فيها شرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي وبواسطة أحد أعضائه أو ممثليه[1].

ويجب الإشارة إلى أن المسؤولية الجزائية لشخص المعنوي لا تستبعد المسؤولية الجزائية لأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

الفرع الأول: العقوبات الأصلية

أخذ المشرع الجزائري بمبدأ مسؤولية الشخص المعنوي عامة مستقلة عن مسؤولية الشخص الطبيعي بعد تعديل قانون العقوبات بموجب القانون 23/06 المؤرخ في 2006/12/20 في المادة 18 مكرر والتي نص فيها على العقوبات المطبقة على الشخص المعنوي فيما يخص الجنايات والجنح وهي كالاتي:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر لمدة 5 سنوات.
- مصادرة الشيء المستعمل في ارتكاب الجريمة.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته[2].

وبالنسبة للعقوبات المطبقة على الشخص المعنوي في حال ارتكابه أحد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فقد نصت عليها المادة 394مكرر4 من ق ع ج على النحو الاتي:

- يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة لشخص الطبيعي.
- ويشترط تبعا لذلك لتقرير مسؤولية الشخص المعنوي ثلاث شروط:

---

[1] – المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي.

[2] –المادة 18 مكرر، قانون 06–23 المؤرخ في 2006/12/20 يعدل ويتمم الامر رقم 156/66 المؤرخ في 18 صفر 1386 الموافق ل 08 جوان 1966 والمتضمن قانون العقوبات الجزائري، ج ر العدد 71، الصادرة بتاريخ 2004/11/10، ص 08.

- يشترط في الشخص المعنوي أن يكون عاما أو خاصا باستثناء الدولة
- يجب أن ترتكب الجريمة لصالح الشخص المعنوي.
- يجب أن ترتكب الجريمة من طرف عضو أو ممثل الشخص المعنوي دون ان تؤثر على مسؤولية الشخص الطبيعي بالإضافة إلى هاته العقوبات هناك عقوبات أخرى مقررة في حالة الاعتداء على الجهات العامة والتي نصت عليها المادة 394 مكرر3 من ق ع ج والتي تنص "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق العقوبات اشد"[1].

الفرع الثاني: العقوبات التكميلية

وهي نفس العقوبات التكميلية المطبقة على الشخص الطبيعي والمنصوص عليها بالمادة 394 مكرر6 التي جاءت شاملة والتي سبق أن تناولنها بالشرح بالمطلب الأول الخاص بالجزاءات المطبقة على الشخص الطبيعي التي "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالك كما انه لابد من الإشارة إلى عقوبة الشروع والاشتراك في الجريمة الالكترونية باعتبار أن المشرع يعاقب على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد".[2]

وقد المادة 394 مكرر5 من قانون العقوبات نصت على شروط للعقاب على الاتفاق الجنائي وهي كالاتي:

- مجموعة أو اتفاق.
- بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.
- القصد الجنائي.

---

[1]- المادة 394 مكرر3 من قانون 04-15، ص 11.

[2]- امال قارة، مرجع السابق، ص 131.

فمن خلال استقراء المادة السابقة فان المشرع لم يخرج عن القواعد العامة لمعاقبة الشريك، حيث رصد لها نفس عقوبة الفاعل الأصلي، ذلك ان جرائم الاعتداء على نظم المعالجة الآلية للمعطيات اغلبها تتم في شكل جماعات، وان كان لم يسبق اتفاق بينها على ارتكاب هذه الجريمة. ولكن النتيجة الجريمة تبين اتفاق ضمني بين أفراد المجموعة، إذ أن هذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر، وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص الأخر وان لم يكن هناك بينهما معرفة سابقة، كما يستوي أن يكون أفراد الاتفاق مجموعة أشخاص طبيعية أو معنوية[1].

أما عن عقوبة الشروع فقد نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع في المادة 394مكرر7 من قانون العقوبات يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة لجنحة ذاتها."

الملاحظ من قراءة نص المادة حرص المشرع على توسيع نطاق العقوبة وجعلها تشمل أكبر عدد من الأفعال الماسة بالأنظمة المعلوماتية، وذلك من خلال جعل فعل الشروع معاقب عليه بنفس عقوبة الجريمة التامة.

ومع هذا فالنصوص القانونية في هذا المجال تعد غير كافية لمواجهة هذا نوع من الجرائم بل يجب الإسراع في وضع استراتيجية وطنية لتعريف وتحديد مخاطر هذه الجرائم وهذا يكون عن طريق توعية الأفراد داخل المجتمع بإضرارها وابعادها وتخصيص دورات تكوينية وملتقيات علمية لتوعية كل القائمين على مكافحة هذا نوع من الجرائم وهذا كله يهدف إلى احتواء كل مظاهر الإساءة للمعلومات وتحدي صعوبة اكتشاف هذا نوع من الجرائم وسعي لإيجاد سبل جديدة لتعامل مع مرتكبي هذا نوع من الجرائم وإيجاد الوسائل الفعالة ونصوص رادعة لمكافحة هذه الجريمة ومواكبة تطورها المستمر.

[1]– خيثر مسعود، مرجع السابق، ص 129.

خاتمـــة

في ختام هذه الدراسة الخاصة بالجريمة الالكترونية استخلصنا أن هذه الجريمة تختلف من حيث طبيعتها وتعريفها عن باقي الجرائم التي عهدناها بالإضافة إلى صعوبة وضع تعريف جامع وموحد لها وذلك مما أدى إلى اختلاف المفاهيم وتعاريف حولها فهناك من عرفها على أساس وسيلة ارتكاب الجريمة وهناك من عرفها على أساس محل أو موضوع الجريمة، والبعض الاخر على أساس شخصية الجاني، والأخر جمع بين عدة تعاريف.

كما أن طبيعتها الخاصة تجسدت في خصائصها المتميزة والمتمثلة في أنها جريمة عابرة للحدود لكونها ترتكب بواسطة الحاسوب وفي مجال الحاسب الآلي، كما انها تتميز بالسرعة في تنفيذ ويغلب عليها التطور المستمر ومتسارع من حيث ارتكابها وإلى جانب هذا هناك الخصوصية التي يتميز بها المجرم المعلوماتي وصفاته، باعتباره لا يلجا إلى العنف كما هو الحال في المجرم التقليدي، بل يتميز بالذكاء والمهارة والسلطة والمعرفة وهذا ما جعل القوانين الحالية عاجزة عن مكافحة هذا النوع من الجرائم نظرا لتطور الحاصل بالمجال تقنية المعلومات حيث لم يعد مبدأ "لا جريمة ولا عقوبة إلا بالنص كافيا لمواجهة هذا النوع من الجرائم هذا ما استدعى ضرورة التعاون الدولي والعمل على إيجاد قوانين وعقد مؤتمرات وإبرام اتفاقيات لتصدي لهذه الجرائم ذات البعد العالمي، غير أن اهتمام المشرع الجزائري بالجريمة الالكترونية وبالعقوبات المقررة لها من خلال النصوص القانونية لا يعد كافيا لمواجهة الانتشار المخيف والتطور السريع لهذه الجريمة بل يجب إصدار قانون خاص بها يتضمن المصطلحات الخاصة بهذه الجريمة وأنواعها والعقوبات المقررة لها، مع وجوب تشديد العقوبات نظرا لأثار السلبية التي تخلفها على مؤسسات العامة والأشخاص وبصفة كبيرة على امن الدولة.

ومن خلال دراستنا هذه توصلنا إلى جملة من النتائج التالية:

- نظرا لحداثة الجريمة الالكترونية استحال وجود اجماع موحد على تعريفها.

- بالرغم من تدارك المشرع الجزائري للفراغ القانوني في مجال الإجرام المعلوماتي من خلال وضعه لعديد من نصوص القانونية التي تجرم الاعتداءات الماسة بالنظام المعالجة الآلية للمعطيات إلا انه لم يستحدث نصوص خاصة بالتزوير المعلوماتي.
- تعد الخطوة التي تبنها المشرع الجزائري في تعديله الأخير لقانون العقوبات في عام 2006 بموجب قانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 إيجابية وتهدف إلى توعية بالخطورة هذا النوع من الإجرام وأثاره سلبية على الاقتصاد الوطني وانتشاره بين أوساط المجتمع باختلاف فئاته.
- إن المشرع الجزائري لم يضع قانون خاص بالجريمة الالكترونية.
- التزايد الكمي في إعداد الجريمة الالكترونية.
- التطور النوعي في أساليب ارتكابها.
- صعوبة الكشف عن الشروع في الجرائم الالكترونية.

وعلى ضوء دراستنا هذه ارتأينا بعض التوصيات والاقتراحات تتمثل في:

1. العمل على إيجاد تعريف شامل وجامع للجريمة الالكترونية باختلاف أنواعها.
2. خلق ثقافة اجتماعية جديدة عن جريمة الالكترونية باعتبارها سلوك غير مشروع يترتب عنه عقوبات جزائية.
3. ضرورة وضع قانون جديد خاص بالجريمة الالكترونية باختلاف أنواعها وطرق مكافحتها.
4. استحداث نصوص قانونية جديدة تخص التزوير الالكتروني.
5. ضرورة تدريس السلوكيات الإجرامية المتعلقة بالجريمة الالكترونية في كليات الحقوق والمعاهد القضائية ونشر الوعي القانوني.

قائمـــة المراجـــع

1/ النصوص القانونية

أ-الأمر رقم 156/66 المؤرخ في18 صفر عام 1386 الموافق لـ 08 جوان 1966، الذي يتضمن قانون العقوبات، المعدل والمتمم.

ب-القانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق لـ 10 نوفمبر 2004. الجريدة الرسمية العدد 71، صادرة بتاريخ 2004/11/10.

ج-القانون 06-23 المؤرخ في 2006/12/20، جريدة رسمية عدد 71 صادرة بتاريخ 2004/11/10.

د-قانون رقم 09-04 المؤرخ في 14 شعبان1430 الموافق لـ 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47، صادرة بتاريخ 2009/08/16.

2/ المراجع باللغة العربية

أ-مراجع عامة

1-أحسن بوصقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني لأشغال التربوية، الجزائر،2002.

2-نور الدين العمراني، "شرح القانون الجنائي الخاص"، دار الامان للطبع والنشر والتوزيع، المغرب، 2005.

3-علي احمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، لبنان، 2006.

4-دردروس مكي، القانون الجنائي الخاص في التشريع الجزائري، ديوان المطبوعات الجزائرية، قسنطينة، 2007 .

5-جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للنشر والتوزيع الجزائر، 2012.

ب-مراجع خاصة

1-محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.

2-محمد حسام لطفي، عقود وخدمات المعلومات، دراسة في القانون المصري والفرنسي، دار النهضة العربية للنشر والتوزيع ،القاهرة، 1994.

3-هدى قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، 2000.

4-أسامة احمد المناعسة، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، طبعة الأولى، دار وائل للنشر، عمان، 2001.

5-مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة،2001.

6-طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، الطبعة الأولى، دار صادر للمنشورات الحقوقية، بيروت 2001.

7-عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي الاسكندرية، 2002.

8-عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية القاهرة، 2002.

9-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

10-رشا علي الدين، النظام القانوني لحماية البرمجيات بين نظرية تنازع القوانين والقانون الدولي الاتفاقي، الطبعة الأولى، دار النهضة العربية، مصر، 2004.

11-قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية القاهرة، 2004.

12-محمد حماد مرهج الهيبتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2005.

13-نائلة محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005.

14-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، 2005.

15-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، 2006.

16-عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والانترانت، دار الكتب القانونية، مصر، 2007.

17-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة الاسكندرية، مصر، 2007.

18-خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية، 2008.

19-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2008.

20-خالد محمود إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009.

21-خالد ممدوح ابراهيم، التقاضي الالكتروني، دار الفكر الجامعي، الاسكندرية، 2009.

22-طارق إبراهيم الدسوقي عطية، الامن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة الإسكندرية، مصر،2009.

23-عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، القاهرة، دار النهضة العربية، 2009.

24-خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010 .

25-زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى، عين مليلة، الجزائر، 2011.

26-محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، طبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014.

27-غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، الدار الجزائرية لنشر والتوزيع، الجزائر، 2015.

28-خالد دوادي، الجريمة المعلوماتية، دار الإعصار العلمي، الجزائر، 2018.

3/ المراجع باللغة الأجنبية

1-Pouvoir et libertesediteconomica Paris1981, Anderevitalis informatique.

4/ مذكرات ورسائل جامعية

1-يونس خالد عرب، جرائم الحاسوب، رسالة ماجستير مقدمة إلى كلية الحقوق في الجامعة الأردنية، 1994.

2-امال قارة، مذكرة ماجيستر بعنوان الجريمة المعلوماتية، كلية الحقوق جامعة الجزائر، 2001.

3-سويد سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان الجزائر، 2010.

4-دردور نسيم، الجرائم المعلوماتية على ضوء القانون الجزائري المقارن، مذكرة لنيل الماجستير، كلية الحقوق، جامعة منتوري قسنطينة، 2012-2013.

5-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة 2012، 2013.

6-يوسف الصغير، الجرائم المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجيستر كلية الحقوق، جامعة مولود معمري، تيزي وزو الجزائر،2013.

5/ مجلات

1-سعد الحاج بكري، شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، العدد 11، 1990.

2-عبد الرحمن الشنيقي، المواجهة الأمنية لجرائم الحاسبات الآلية، مجلة الأمن والحياة، العدد 129، 1993.

3-توفيق شمبور وآخرون، السرية المصرفية، أبحاث ومناقشات الندوة التي نظمها اتحاد المصارف العربية، لبنان 1993.

4-هلال محمد رضوان، بحوث واراء جديدة في مجال كشف التزييف والتزوير، عالم الكتب، مصر، 1993.

5-بلحاج العربي، ابحاث ومذكرات في قانون الفقه الاسلامي، ديوان المطبوعات الجامعية، بن عكنون الجزائر، 1996.

6-إسماعيل رضا، الوقاية من الجرائم الناشئة عن استخدام الحاسب الآلي، بحث منشور في مجلة الاقتصاد الإسلامي، عدد 219، 1999.

7-هشام محمد فريد رستم، الجرائم المعلوماتية، الطبعة الثالثة، كلية الشريعة والقانون،مؤتمر القانون والكمبيوتر والانترنت، من 01 إلى 05 ماي 2000 جامعة الإمارات العربية المتحدة

8-اتفاقية بودابست :الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني بمعنى الإجرام المعلوماتي أو الجرائم المعلوماتية تتكون من 48 مادة منها 35 مادة في مجال مكافحة الجرائم المعلوماتية.

9-غنام محمد غنام، الحماية الجنائية لبطاقات الائتمان الممغنطة، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم من قبل اكاديمية الشرطة، دبي، مركز البحوث والدراسات، تاريخ الانعقاد 2003/04/26 الى 2003/04/28.

10-علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، الطبعة الثالثة، بحث مقدم لمؤتمر والكمبيوتر والانترنت، منظم من قبل كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004.

11-علي كحلوش، جرائم الحاسوب وأساليب مواجهتها، مجلة الشرطة، المديرية العامة الأمن الوطني، عدد 84، 13 جويلية 2007.

12-جميل عبد الباقي الصغير، مدى كفاية نصوص العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الانترنت، الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية، بالتعاون مع جامعة عين الشمس، ابوظبي من 15 إلى 2008/11/19.

13-النجيمي محمد بن يحي بن حسن، الجرائم الالكترونية من جهة النظر إسلامية والقانونية، المجتمع والأمن، افريل2008، كلية الملك فهد الامنية، الرياض.

14-سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، عدد 7، جامعة محمد خيضر، بسكرة، أفريل 2010.

15-بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، مجلس قضاء قسنطينة، محاضرة في إطار التكوين المحلي المستمر للقضاة، سنة قضائية 2011/2010.

16-يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ظبي 2012/12/10.

17-نشناش منية، مداخلة بعنوان الركن المفترض في الجريمة المعلوماتية، ملتقى منظم من قبل كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، بتاريخ 2015/11/16.

18-حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الاكاديمية للبحث القانوني، كلية الحقوق، جامعة اكلي محند أولحاج، العدد الثاني، 2016.

6/ مواقع الانترنت

1-إسراء جبريل رشاد مرعي، الجرائمالإلكترونية" الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، 9 أوت 2016، انظر الرابط:
https//democraticac.de

2-عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ملتقى حول الجرائم المعلوماتية، منظم من قبل كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، بتاريخ 2015/11/01، انظر الرابط: fdsp.univ.biskra.dz

3- مركز هردو لدعم التعبير الرقمي، الجريمة الالكترونية وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، أنظر الرابط: hrdoegypt.org/wp-content/uploads/2014/12 تقرير الجريمة الالكترونية.

4- موقع جزا يرس، جرائم الالكترونية تهدد امن الجزائريين، نشر في إخبار اليوم يوم 2018/04/10 من الرابط: https-//www.djazairess.com/akhbarelyoum/240271.

5- الموقع القانوني العربي على الإنترنيت، قوانين الجرائم الالكترونية على ضوء الشريعة، انظر الرابط: www.islamonline.net

6- GRC. Criminalité informatique /http. rcmagrc.gc.caen -

7–فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المزعم عقده بأكاديمية الدراسات العلي بليبيا في أكتوبر 2009، الرابط iefpedia.comarabuploads

8–صالح احمد البربري، بحث بعنوان دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 2001/11/23، أنظر الرابط: www.mohamah.net

9–مجلة جيل الأبحاث القانونية المعمقة، العام الثالث، العدد 25، ماي 2018، من الرابط: jilrc-magazines.com

الفهـــرس

العنـــــوان **الصفحة**

مـلخص المذكرة

تعد الجريمة الإلكترونية ظاهرة بالغة الخطورة واحتمال تعرض الأشخاص لها أصبح على درجة مرتفعة جدا نظرا لتزايدها المستمر وتأثيرها السلبي ولقد أثار هذا النوع من الجرائم عدة تساؤلات في أوساط المجتمع باعتبار كل فرد معني بأخطار والعواقب التي يخلفها هذا السلوك الإجرامي وبالرغم من النصوص القانونية التي تجرم هذه الأفعال الا انها لا تعد كافية ولا تلم بجميع أنواع الجرائم الالكترونية.

الكلمات المفتاحية:

- الجريمة الإلكترونية.
- التزوير الإلكتروني.
- الأنترنت.
- ذوي الياقات البيضاء.
- المجرم المعلوماتي.
- القرصنة.