الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية

Cybercrime: indication of the concept and effectiveness of the legal treatment

مونة مقلاتي*
مخبر الدراسات القانونية البيئية
جامعة 8 ماي 1945 قالمة
meguellati.mouna@univ-guelma.dz

راضية مشري
مخبر الدراسات القانونية البيئية
جامعة 8 ماي 1945 قالمة
mecheri.radia@univ-guelma.dz

تاريخ الاستلام: 2021/01/03 تاريخ القبول: 2021/05/16 تاريخ النشر: 2021/06/08

ملخص: تعتبر الجرائم الإلكترونية من الأشكال الحديثة للإجرام، نظرا لارتباطها بالتطورات التقنية التي يعرفها العالم، والتي قوامها تكنولوجيا المعلومات والاتصالات، حيث ثبت من خلال أساليب وقوعها وطرق ارتكابها، وتتبع حيثياتها ونتائجها؛ أنها تختلف عن الجرائم التقليدية سواء من حيث نطاقها أو المتضررين منها، أو تقنيات الكشف عنها، مع تسجيل التوظيف السيء للتكنولوجيا في الرفع من احترافية مرتكبي تلك الجرائم، وصعوبة ضبطهم.

إنّ دخول المجتمعات إلى عالم الرفاه والسرعة، وتوفر الأدوات المعلوماتية وأجهزة الاتصال، قد ساهم في رفع تعداد تلك الجرائم، وتضاعف أعداد ضحاياها، ويمكن تسجيل حقيقة أنها جرائم عابرة للحدود، بحيث لا تقتصر على اقليم دولة واحدة، بل إنها تضم أفرادا وخبرات وأساليب مبتكرة ومستحدثة، تقتضي التفكير بشأن ضبط مفهوم تلك الجرائم، وتحديد مسبباتها، وآليات التعامل القانوني معها.

كلمات مفتاحية: الجريمة الالكترونية. الحاسوب. القرصنة. التزوير. القانون الجنائي. المعلومات.

Abstract: Cybercrime is considered to be a new form of crime, due to its correlation with technological developments in the world, which are based on information and communication technology. Cybercrime differ from traditional crimes, whether in terms of their scope or those affected by them, and through the methods of their occurrence and the methods of their commission, tracking of their results. It differs from traditional crimes, whether in terms of their scope or those affected by them, or the techniques of their detection, with bad and illegal use of technology in raising perpetrators professionalism of these crimes, also the difficulty of controlling those criminals, or prevent from damages and losses that they cause. The transformation of societies into a world of well-being and speed, and the availability of information tools and communication devices has contributed to increasing the number of these crimes, and doubling the number of their victims.

Keywords : Electronic crime ; computer ; Piracy ; Counterfeiting; Criminal Law; information.

* المؤلف المرسل

مقدمة

تتجه الجهود الدولية والوطنية الرسمية في الدفع بالتشريعات القانونية لأن تكون مواكبة للاستعمالات السلبية للتكنولوجيا وأدوات الاتصال والمعلوماتية، وأن تمتلك تلك التشريعات من النجاعة والفعالية ما يؤهلها للاستجابة بسرعة وحزم مع هذا النوع المستجد من الجرائم، وأن يجري تظافر تلك الجهود المشار إليها في التصدي للجريمة الإلكترونية، والمشرّع الجزائري معني قبل غيره بضرورة تسريع إجراءات تعديل القوانين للإحاطة بكل جوانب الجريمة الالكترونية، والقدرة على مواكبة دخول مؤسسات الدولة الجزائرية واقتصادها، عالم المعلوماتية والتبادل الالكتروني، وأسواق الخدمات وحركات الأفراد ورؤوس الأموال، وأن يجري تخفيض المخاطر وإزالة المخاوف بشأن الصفة الردعية للقانون الجزائري إزاء تلك الجرائم ومرتكبيها.

إن تعدد الاتجاهات الفقهية في تعريف الجريمة الإلكترونية، والاختلاف بشأن أرضية تلك الجرائم، وسرعة الاستجابة في مواجهتها ، يحتم أن يتم إعطاء تحليل واف بخصوص تعريف الجريمة الالكترونية، وعماد الفعل والنشاط ضمنها، وهو الحاسوب وأنظمة المعلوماتية، وما تكفله من اطلع على عمليات رصد وتخزين المعطيات، مع ما يشير له هذا المسار من احتمالات القرصنة والاختراق، وانتحال شخصية الأفراد أو التحكم في الأرصدة، أو ممارسة التضليل والاحتيال، ومختلف أنشطة الدعاية غير القانونية والتحريض ونشر قيم الكراهية والعنصرية، وهي كلها جوانب تفترض الإرادة القوية في مواجهتها بحزم، وهو ما توفره قوانين أكثر إلماما بجوانب هذا النمط من الإجرام، ولها من صفة الردع، ما يحبط الأنشطة المتزايدة ذات المضمون الاجرامي في عالم المعلوماتية.

تتمثل الإشكالية التي تعمل هذه الورقة على مناقشتها في الصيغة التالية:

كيف يمكن استيضاح الجانب المفهومي والقانوني لظاهرة الجريمة الإلكترونية، بشكل يستوعب ويواكب التطور المستمر والمتسارع لتكنولوجيا الاتصالات والمعلوماتية؟

سيتم التعامل مع هذه الإشكالية بإتباع المنهج الوصفي لوصف ظاهرة الجريمة الإلكترونية وأصنافها، وفقا للخطة المفصلة أدناه.

المبحث الأول: الإطار المفاهيمي للجرائم الإلكترونية:

أصبحت التقنية خاصة في جانب المعلوماتية من أساسيات الحياة في عصرنا الحالي، لكن البعض من مستخدمي هذه التقنية الحديثة استغلها في أهداف غير مشروعة طبقا لمصالحه، أين أصبح الإعلام الألي بشكل عام وشبكة الأنترنت على وجه الخصوص؛ أدوات أو محلا لارتكاب الجريمة بمفهومها الحديث، مع احتراف بعض الجناة عديد الجرائم، بواسطة الحاسب الألي أو شبكة الانترنيت[1]، وبذلك أصبحت الجريمة الإلكترونية من الظواهر الرائجة حديثا، نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصالات، بناء على هذا التقديم، يجب تحديد المقصود من هذا النمط الإجرامي.

المطلب الأول: تعريف الجريمة الإلكترونية:

تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم، حيث لا يوجد إجماع على تعريف الجريمة الإلكترونية؛ من حيث تحديدها والجرائم التي تشملها، وهناك غياب لتعريف عام، أو إطار نظري متسق في هذا الحقل بشأنها، وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية والسيبرانية للدلالة عليها، وكلها تعكس فجوات مهمة في التعريف[2] .

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية:

إزاء المساعي الموجهة نحو التصدي لظاهرة الإجرام المعلوماتي، فإنّ المصطلحات التي تناولت هذه الظاهرة، قد اختلفت فيما بينها، حيث لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فالبعض أطلق عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، والبعض يسميها جرائم الكمبيوتر والأنترنت، وهناك من يطلق عليها الجرائم المستحدثة؛ إضافة إلى عدم الاتفاق على تعريف تشريعي شامل لهذا النوع من الجرائم، وقد ذهب الفقهاء في تعريف الجريمة الإلكترونية مذاهبا مختلفة، ونتيجة للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، فإنّ ذلك حال دون وضع تعريف فقهي جامع وشامل، إذ تباينت في هذا السياق الاتجاهات الفقهية، بين موسّع لمفهوم الجريمة الإلكترونية، وبين مضيّق لمفهومه[3]، وسنحاول إبراز هذين الاتجاهين وفقا لما يلي :

أولا: الاتجاه الضيّق لمفهوم الجريمة الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وفقا لمعايير متعددة، سواءا كانت وفقا لمعيار شخصي من حيث توفر المعرفة والدراية بالتقنية، أو وفقا لمعيار موضوع الجريمة، والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وسنسرد في هذا الإطار بعض التعريفات لفقهاء القانون الجنائي، فقد عرفتها الدكتور هدى قشقوش بأنها:" كل سلوك غير مشروع أو غير مسموح به، فيما يتعلق بالمعالجة الألية للبيانات أو نقل البيانات"؛ وعرّفها الأستاذ Rosen Blat بأنها:" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تُحوّل عن طريقه[4]؛

يعاب على هذا التعريف أنه يخرج من نطاق الجريمة الإلكترونية، عدد كبير من الأفعال غير المشروعة، والتي يستخدم فيها الحاسب الآلي، كأداة لارتكابها كالاحتيال المعلوماتي، وقد أخذت وزارة العدل الأمريكية بتعريف للجريمة الالكترونية في تقرير صادر عنها عام 1989 المتعلق بجرائم المعلوماتية بكونها:

"كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الألية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى".[5]

يتبيّن لنا من خلال هذا التعريف أنه لا يكف فقط أن تتوافر معرفة تكنولوجيا الحاسبات الألية، بدرجة كبيرة من أجل ارتكاب الجريمة الإلكترونية، ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها، بمعنى لابد من توافر قدر كبير من العلم بهذه التكنولوجيا، لدى الجناة والقائمين على معاينة وملاحقة مرتكبيها.

ثانيا: الاتجاه الموسّع لمفهوم الجريمة الإلكترونية:

على عكس الاتجاه السابق يرى فريق أخر من الفقهاء، ضرورة التوسّع في مفهوم الجريمة الإلكترونية أو المعلوماتية، وعدم حصرها في الحاسوب وحده، أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية؛ فيعرّفونها بأنّها:" كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"؛

كما عرّفتها منظمة التعاون الاقتصادي والتنمية بأنّها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخّل التقنية المعلوماتية[6]؛

أمّا مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فقد تبنى التعريف التالي للجريمة الإلكترونية:"هي أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[7]؛

نحن من جانبنا نتفق مع هذا التعريف، إذ أنّه التعريف الذي استطاع الإحاطة –قدر الإمكان– بجميع الأشكال الإجرامية للجريمة الإلكترونية، سواء التي قد تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف الجرائم التي من الممكن أن تقع في بيئة إلكترونية، فهذا التعريف لم يركز على فاعل الجريمة ومقدراته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة الإلكترونية، بل إنّه حاول عدم حصر الجريمة الإلكترونية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

نستشف من خلال عرضنا للتعاريف الفقهية سالفة الذكر، حول مفهوم الجريمة الإلكترونية أنّها اقتصرت على مفاهيم عامة مرتبطة بجهاز الحاسوب من جهة، وبالبيانات من جهة أخرى، فالفقهاء الذين تبنوا الاتجاه الموسع لتعريف الجريمة الإلكترونية، كانوا أكثر حكمة لأنّ هذا العالم الافتراضي سريع التطور، وأي تضييق في مفهوم الجريمة الإلكترونية سوف يقنّن مفهوم الجريمة الإلكترونية، كما أنّه باستقرائنا لمختلف التعاريف، نجد أن تعريف منظمة التعاون الاقتصادي والتنمية سالف الذكر، يتسم بالوضوح والشمول للأسباب التالية:

*تحديده لماهية السلوك الإجرامي، للجريمة التي قد تقع به، إذ شمل كل من الفعل الإيجابي والسلوك السلبي، المتمثل في الامتناع؛

*تعريف واسع يتيح الإحاطة الشاملة، قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة؛

*يعبر عن الطابع التقني المميّز، الذي تنطوي تحته أبرز صور الجريمة الإلكترونية؛

*يتيح إمكانية التعامل مع التطورات المستقبلية التقنية[8].

إنّ تعريف الجريمة الإلكترونية على العموم يقوم على ثلاث عناصر، السلوك ووصفه والنص القانوني على تجريم السلوك وإيقاع العقوبة، ثم محل الاعتداء في الظاهرة الإجرامية المستحدثة متمثلا في معطيات الحاسوب، خلافا للجريمة عموما، إذا هي سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله،

معطيات الحاسب الألي فالسلوك يشمل الفعل الإيجابي والامتناع عن العمل ، مع الاعتبار أنّ إسباغ الصفة الجرمية لا يتحقق في الميدان الجنائي إلا بإرادة المشرع، ومن خلال النص القانوني ومحل الجريمة ذاتها دائما هو معطيات الكومبيوتر بدلالاتها الواسعة[9].

الفرع الثاني: موقف المشرع الجزائري من الجريمة الإلكترونية:

أدّت الحداثة التي تتميز بها الجريمة الإلكترونية، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، ممّا انجرّ عنه عدم وضع تعريف موحّد لهذه الظاهرة الإجرامية، والمشرّع الجزائري وللدلالة على الجريمة الإلكترونية؛ اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال[10]وكخطوة أولى لمواجهة ما يعرف بجرائم تكنولوجيات الإعلام والاتصال، أجرت الحكومة الجزائرية بعض التعديلات على قانون العقوبات، بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل، والمتمم للأمر رقم 66-156، المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات، حيث استحدثت عقوبات تتعلق بالمساس بأنظمة المعالجة الألية للمعطيات، وهو ما نصت عليه المواد 394 و394مكرر1 إلى 7 من القسم السابع مكرر، وتراوحت هذه العقوبات من شهرين إلى ثلاث سنوات، مع دفع غرامة مالية من 50000دج إلى 5000000 دج، وذلك حسب حجم ودرجة خطورة الجريمة الالكترونية المرتكبة، كما قام المشرّع الجزائري بتجريم الأفعال الماسة بأنظمة الحاسب الآلي بسبب ما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، وهو ما دفعه إلى تعديل قانون العقوبات 15/04؛ تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.[11]

يعدّ قانون 04/09 أول قانون في الجزائر اهتّم بكيفية تبادل المعلومات الرقمية، وتجري فيه كل أنواع المعاملات والخدمات الالكترونية، وقد عرّفت المادة 02 منه الجريمة الالكترونية على أنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية.[12]

توّضح هذه المادة نية المشرع الجزائري في تبنّي مبدأ المرونة في الصياغة التشريعية، للتمكن من استيعاب الأنشطة الاجرامية الالكترونية التي يتعذر حصرها وتحديدها، نظرا لسرعة وتطور أساليبها، تبعا للتطور التقني، وهو ما يتيح للقاضي حرية واسعة في التقدير، وانطلاقا من فحوى هذه المادة، يتبيّن أنّ المشرع الجزائري قسّم هذه الجرائم إلى ثلاثة أنواع:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الالكترونية. [13]

يتضح لنا من موقف المشرع الجزائري بشأن تعريف هذه الجريمة، أنّه أعطى لها مفهوما واسعا؛ بالرغم من تحديده لمجالها من خلال كونها متصلة بتكنولوجيات الاعلام والاتصال، إلا أنّه ترك فيما بعد المجال واسعا لتضم إليها أي نوع من الجرائم التي قد يسفر عنها التطور التكنولوجي، خاصة وأنّ هذا الميدان شهد تطورا

وتسارعا كبيرين، وقد نصت المادة السابقة على العبارة التالية: "...أو أي جريمة أخرى ترتكب، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية"[14].

من خلال استعمال المشرع الجزائري لمصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، للدلالة على الجرائم الالكترونية، فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فالأولى تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما تكنولوجيات الاتصال فتقوم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، ولذلك فقد وُفّق المشرع الجزائري–في نظرنا– باختياره مصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال التي تتوافق مع مصطلح الجرائم الالكترونية بالمفهوم الواسع، وهذا للأسباب التالية:

– الجرائم الناشئة في البيئة الرقمية هي جرائم حديثة، يرتبط مفهومها بظهور التكنولوجيا الحديثة، وما يواكبها من تطور مستمر في تشغيل ونقل وتخزين المعطيات في شكل إلكتروني؛

– استعمال هذا المصطلح له مفهوم واسع، فهو يشمل كل الاعتداءات التي تتم في بيئة افتراضية، بما فيها الجرائم التي تقع على نظم المعالجة الآلية للمعطيات، وتكون وسيلة لارتكابها؛

– يعبّر هذا المصطلح عن الطابع التقني والمميز للجرائم الالكترونية.[15]

– لم يحدد المشرّع صور السلوك المجرّم الذي يرتكب أو يسهل ارتكابه ضمن منظومة معلوماتية، أو نظام للاتصالات الالكترونية؛

– تضمّن هذا التعريف التكرار، كون أنّ مفهوم نظام الاتصالات الالكترونية يندرج تحت مصطلح المنظومة المعلوماتية، ذلك أنّ المشرّع الجزائري عرّف هذه الأخيرة بموجب أحكام المادة 02، على انّها نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات، تنفيذا لبرنامج معيّن"، ومن وجهة نظرنا؛ فإن تعريف الجريمة الالكترونية الأقرب للصواب هو أنّها تمثّل كل اعتداء يتم باستخدام النظام المعلوماتي، وكان له دور رئيسي في السلوك المجرّم.

المطلب الثاني: خصائص الجريمة الإلكترونية:

تتميّز الجريمة الالكترونية بطبيعة خاصة، تجعلها تختلف عن غيرها من الجرائم؛ وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي، مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم، عددا من السمات التي انعكست بدورها على مرتكبي هذه الجريمة، الذين أصبح الواحد منهم يُعرف بالمجرم المعلوماتي، نظرا لتميّزه في أفعاله عن الأشكال التقليدية للإجرام.

الفرع الأول: خصائص الجريمة الالكترونية المشتركة مع بعض الجرائم الاخرى

تتسم الجريمة الالكترونية بدرجة من الخطورة البالغة، والحجم الكبير للأضرار التي تنشأ عنها، وهي بذلك تشترك مع بعض الجرائم كالإرهاب والاتجار بالمخدرات، ومن هذه الخصائص يمكن تفصيل ما يلي:

أولا–خطورة الجرائم الالكترونية:

تنطوي الجريمة الالكترونية على قدر كبير من الخطورة، وذلك لوقوعها على الانسان في فكره وحياته الخاصة، كما تمس المؤسسات في نشاطها الاقتصادي خاصة، ويقع ضررها على أمن البلاد الوطني، مع ما في ذلك من خطر المساس بالمعلومات والأسرار السياسية والعسكرية والاقتصادية، وفي جانب آخر فإنّها جرائم تنتهك حرمة الحياة الخاصة، فالاطلاع على خصوصيات الأفراد يظل جريمة يعاقب عليها القانون، كونها تنتهك حقا أساسيا للأفراد في حماية خصوصياتهم، وهو حق كفلته مختلف التشريعات.

إنّ الاختراقات المتكررة التي تتم لأنظمة الحواسيب في الهيئات الرسمية لعديد الدول، أثبتت كيف أنه مهما بلغ تقدم الدول فإنها تبقى معرّضة لتلك الاختراقات، وهو ما واجهته مثلا وزارة الدفاع الأمريكية من تسريبات للبيانات، واختراق لأنظمتها المعلوماتية وقرصنة لبياناته[16]، ولم يسلم من ذلك أرشيف وزارة الخارجية وكذا ملفات المخابرات وهويات العملاء، وأصبح من المعتاد ورود أخبار عن تعرض أعداد كبيرة من الملفات للاختراق والاطلاع والنشر غير القانونيين.

ثانيا-الجرائم الالكترونية باعتبارها جرائما عابرة للحدود

إنّ البيئة الافتراضية لا تعترف بالقيود ولا بالحدود، فقد يكون الجاني في بلد؛ في حين أنّ جريمته وضحاياها قد يكونون في بلد آخر، كما قد يمتد الضرر الحاصل إلى بلد ثالث أو أكثر في الوقت نفسه، فالجريمة الالكترونية شكل من الجريمة العابرة للحدود، يستفيد مقترفوها من أثر التقنية في اختزال المسافات، وإخفاء الأثر الالكتروني، وكذا السرعة الزمنية الهائلة في تداول المعلومات والحصول عليها، ووقوع كثير من العمليات الالكترونية في نفس الوقت، ضمن ما يعرف باللحظية المعلوماتية، والعمل عن بعد الذي يعدم التواجد المادي للمجرم المعلوماتي، ويُصعّب عملية البحث بشأنه، ويقتضي تتبع المعاملات الالكترونية التي تتجاوز حدود الدولة الواحد، في حرص على الربط بين الفعل والنتيجة الاجرامية له، من خلال المعطيات محل الجريمة.

يستوجب الشكل العابر للحدود للجريمة الالكترونية تظافر الجهود التشريعية، وعمليات التنسيق الأمني والمعلوماتي من أجل التصدي لهذا النمط من الإجرام، والإيقاع بالمجرمين وتقديمهم للقضاء[17]، كما يستلزم هذا الوضع تطوير الأنشطة الوقائية والإجراءات الردعية التي تحول دون تنامي هذا الشكل الخطير من الجرائم، كما أنّه من الوسائل المجدية في هذا الإطار تفعيل اتفاقيات الملاحقة القانونية وتسليم المجرمين، ووضع نشرات بشأنهم، وتجميد مدخراتهم والعوائد المالية التي يجنونها من الأفعال الاجرامية المقترنة بالأنظمة المعلوماتية.

الفرع الثاني: الخصائص التي تنفرد بها الجريمة الالكترونية عن الجرائم الأخرى:

تنفرد الجريمة الإلكترونية عن سواها من الجرائم الأخرى، بسمات تضفي عليها طابعا مميزا ومنها والتي يمكن إجمالها على النحو التالي:

أولا: يتطلب ارتكابها وجود حاسب ألي ومعرفة تقنية:

يعدّ الكومبيوتر الأداة الأساسية لارتكاب كافة الجرائم الإلكترونية، والمقصود من وجوده هنا أن يستعان به كوسيلة لتنفيذ هذه الجرائم، ذلك أن الحاسب الألي وإن كان موضوعا للاعتداء كإتلاف أو سرقة الجهاز نفسه، أو

شاشته فلا تثور لدينا أية مشكلة، ذلك لأنّ نصوص قانون العقوبات التقليدية كفيلة بردع الجاني لأن الحاسب هنا لا يتعدى كونه من الأموال المادية المنقولة، ولكن تثور المشكلة عندما يطال الاعتداء على ما يمكن أن يسمى بفن الحاسب الألي، كتدمير برامجه وسرقتها وتقليدها، أو العبث ببيانات الحاسب أو المعلومات المختزنة، وهذا هو المقصود من جرائم الحاسب الألي، والتي يصلح فيها الحاسب أن يكون موضوع الاعتداء فيها. [18]

إضافة إلى ما سبق؛ فإنّ الجريمة الإلكترونية تتطلب الإلمام بتقنيات الكومبيوتر ونظم المعلومات، سواء لارتكابها أو التحقيق فيها أو ملاحقتها قضائيا، لذلك يجد مأموري الضبط القضائي أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية، على هذا النوعية من الجرائم، فضلا عن صعوبة إجراءات التحريات السرية، وتتبع مسار العمليات الإلكترونية العابرة للحدود، فقد يتسبب المحقق بدون قصد، أو بطريق الخطأ في إتلاف الدليل الإلكتروني، أو تدميره كما في حالة محو البيانات الموجودة في الأسطوانة الصلبة، كما قد يتجاهل المحقق الدليل الإلكتروني ظنا منه أنه غير مهم، أو لا يقوم بمصادرة جهاز الكومبيوتر المستعمل في الجريمة، أو ملحقاته من طابعة أو ماسح ضوئي.[19]

ثانيا: صعوبة اكتشاف الجريمة وإثباتها:

توصف الجرائم الإلكترونية بأنّها خفية ومستترة في أغلبها، بحكم أنّ الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنّه من تنفيذ جريمته بدقة واحترافية، كإرسال فيروسات وسرقة الأموال والبيانات الخاصة، وإتلافها والتجسس وسرقة المكالمات... إلخ[20]، ويمكن رد الأسباب التي تقف وراء صعوبة اكتشافها، إلى عدم تركها لأثار خارجية، كما في الجرائم التقليدية فهي تتم في بيئة افتراضية، كما تُوفّر التقنية المعلوماتية للمجرم إخفاء أثار الجريمة، عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية، وبالتالي محو أثاره مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته، وضمان عدم إفلاته من العقاب، خاصة وأنّ تنفيذها لا يتطلب وجود الفاعل في مكان الجريمة، بل يمكنه تنفيذ جريمته وفي دولة بعيدة ، كل البعد عن الفاعل[21]، كما أنّ معظم الجرائم الإلكترونية تم اكتشافها بمحض الصدفة، وبعد مرور وقت طويل، إضافة إلى أنه لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية، إما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به، لذلك ما يرتكب فعلا من جرائم إلكترونية أكبر بكثير مما يصرح به[22].

ثالثا: جرائم هادئة وصعبة الإثبات:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها، كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم على معرفة تقنية للكومبيوتر، وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغيّر أو تُعدّل، أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أنّ البعض يشبهها بجرائم العنف؛ مثلما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية، نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف. [23]

في جانب آخر فإنّ تلك الجرائم صعبة الإثبات، وذلك عائد لصبغتها اللامادية التي تجعل من محو الأدلة الجزائية أمرا سهلا، إذ يمكن للمجرم الإلكتروني أن يمحو مئات الألاف من البيانات من الحاسب الألي بضغطة زر واحدة، وبإمكانه عدم تخزينها أصلا وعدم معالجتها على حسابه الشخصي، كما قد يعمد بعض الجناة إلى تشفير المعطيات المجرّمة، بحيث يستحيل فك رموزها من طرف السلطات الأمنية، ويمكن أن يكون ذلك على مستوى التخزين أو على مستوى تبادل المعلومات بين مجرمي الأنترنت على الشبكة العنكبوتية، حيث تطورت تقنيات التشفير بشكل يسمح بتشفير رسائل إلكترونية، ثم تبادلها في شكل صور فوتوغرافية عادية؛ وهي تقنية تحمل اسم Steganography، وتُشكّل الفضاءات العامة والمقاهي، التي يمكن فيها استغلال خدمة الأنترنت بدون تحديد مسبق لهوية المستفيد من الخدمة صعوبة إضافية، تقف أمام تحديد الجاني في صورة ارتكابه لجريمة عن طريق الأنترنت المخصصة للعموم[24]، وفي هذه الحالة يصعب كثيرا إثبات أنّه ارتكب الجريمة.

نخلص إلى القول بأنّ الجريمة الإلكترونية أصبحت ظاهرة إجرامية جديدة، وسمة بارزة في بداية القرن 21م، وتميّزها بهذه الخصائص يجعلها تختلف عن الجرائم التقليدية، إذ أنّ المجرمين في هذا المجال أو كما يُسمّون " **الهاكرز**" يتميزون بالذكاء في استخدام وسائل تقنية متطورة، وتنفيذ جرائمهم سواء في عمليات إرسال الفيروسات المخرّبة للمواقع والأنظمة، أو سرقة الأموال والسطو على أرصدة المصارف، وتحويل الأموال أو سرقة البيانات المهمة أو إتلافها، كما تتميّز الجريمة بالسرعة في التخطيط والتنفيذ، وبجهد وتكاليف أقل بكثير من الجهد والأموال الكبيرة، التي كانت تنفق في تنفيذ الجرائم التقليدية.[25]

المبحث الثاني: تقسيم الجرائم الإلكترونية

لقد اختلف الفقه في تقسيم الجرائم المعلوماتية؛ وذلك حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم تركب على نظم الحاسوب، وأخرى بواسطته، وبعضهم يصنّفها ضمن فئات بالاستناد إلى الأسلوب المتّبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، فيما هناك من يسند تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه، فتوزّع جرائم الكومبيوتر وفق هذا التقسيم إلى: جرائم تقع على الأموال بواسطة الحاسوب، وتلك التي تقع على الحياة الخاصة[26]، ومن الملاحظ أنّ هذه التقسيمات أو بعضها، لم تراع بعض أو كل خصائص الجريمة الإلكترونية وموضوعها، والحق المعتدى عليه لدى وضعها كأساس أو معيار التقسيم.

المطلب الأول: الجرائم الإلكترونية الواقعة على النظام المعلوماتي

يتمثّل هذا الصنف في الجرائم الموجهة ضد النظام المعلوماتي، من خلال ما يقع على المكونات المادية لنظام المعلومات أو البرامج التي تحتوي عليها نظام المعلوماتية، أو المعلومات المسجلة على نظام المعلوماتية، وقد تناول المشرع الجزائري بعضا من هذه الجرائم بموجب تعديل قانون العقوبات في 2004م، وعنونها تحت ما يسمى بجرائم المعالجة الآلية لنظم المعطيات، وتشمل: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي،

والجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي، وكذا الجرائم الواقعة على المعلومات المسجلة بالنظام المعلوماتي.

الفرع الأول: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يُقصدُ بالمكونات المادية للنظام المعلوماتي مجموع الأجهزة والمعدات الملحقة به، والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات[27]، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية، ضمن الجرائم التي تستهدف المال، باعتبار مكونات الحاسوب المادية أموالا منقولة، تصلح محلا للاعتداء عليه بالجرائم الموصوفة كجرائم الإتلاف والتخريب، ولا يربطها بالمعلوماتية سوى أنّ الأجهزة المادية محل الجريمة؛ تستخدم لتشغيل النظام المعلوماتي[28]، ولا تثير الجرائم الواقعة على المكونات المادية للحاسب الآلي أي إشكال، لأنها تخضع للقواعد العامة في قانون العقوبات باعتبارها مالا ماديا، ومن بين هذه الجرائم جريمة السرقة والإتلاف.

الفرع الثاني: الجرائم الواقعة على المكونات المعنوية أو المعلومات المسجلة بالنظام المعلوماتي

تتحقق هذه الجريمة عندما تكون مكونات الكومبيوتر غير المادية محلا أو موضوعا للجريمة، كما ينصبّ على المعلومات باعتبارها المحور الأساسي الذي تدور حوله المعلوماتية، وقد قسّم الفقه تلك الجرائم إلى:

أولا: جريمة الدخول والبقاء عن طريق الغش المعلوماتي:

تضمّن قانون العقوبات الجزائري هذه الصورة من الجرائم في نص المادة 394مكرر، والواقع أنّ أي جريمة تقوم على ركنين مادي ومعنوي، وبالرجوع إلى المادة سالفة الذكر يتضح بأن هذه الجريمة تقوم على ركنين: مادي ومعنوي، حيث يتمثل الركن المادي لهذه الجريمة في نشاط يتمثل في تحقق الدخول، ويأخذ هذا السلوك صورة ايجابية أو سلبية، ويتطلب من الجاني مباشرة نشاط ايجابي لا يمكن أن يكون بنشاط سلبي. [29]

يتحقق فعل الدخول بكل فعل يسمح الولوج إلى النظام المعلوماتي، أو السيطرة على المعطيات التي يتكون منها، وفعل الدخول إلى النظام المعلوماتي لا يعتبر في حد ذاته سلوكا غير مشروعا، وإنما يتخذ هذا الوصف انطلاقا من كونه قد تم دون وجه حق[30].

إنّ المعيار الذي يتم من خلاله تبيان أنّ الاتصال قد تم بطريقة الغش، وبالتالي تحديده بأنّه تم بطريقة غير مشروعة أو بواسطة الغش، وهو انعدام حق الشخص في الاتصال بهذا النظام، سواء كان هذا الانعدام يتعلق بكل النظام أو جزء منه، طالما ظلّ يُستغل بطريقة مشروعة[31]، وتُعد هذه الجريمة جريمة شكلية لا تتطلب نتيجة، كما أنّها من الجرائم المستمرة، لأنّ السلوك الإجرامي يمتد فيها، طالما ظل يستغل النظام بطريقة غير مشروعة، أمّا الركن المعنوي لهذه الجريمة فيتحقق إذا كان دخول الجاني مسموحا به، أو وقع في خطأ في الواقع سواء تعلق بمبدأ الحق في الدخول في نطاق هذا الحق، كأن يجهل بوجود خطأ للدخول، أو كان يعتقد انه اخطأ أنه مسموح له بالدخول، أي لا يُعتد بالباعث في الدخول في هذه الجريمة، بل يبقى القصد الجنائي قائم[32].

ثانيا: جريمة التلاعب غير المصرح به بالمعلومات

لقد نصّت المادة 04 من اتفاقية بودابست لمكافحة جرائم الانترنيت لسنة 2001م على هذه الجريمة، ولقد نصّ عليها المشرع الجزائري في المادة 394 مكرر 1 ق ع، وبيّن ثلاث صور لهذا السلوك؛ وهي الإدخال أو التعديل أو الإزالة، والمقصود بالإدخال هو تغذية النظام بالمعلومات أو إضافة خصائص ممغنطة جديدة، وبالتالي الإدخال يكون بالفعل، عندما يتحقق بكل حالات تغذية النظام المعلوماتي بمعلومات مغلوطة وخبيثة الفيروسات أو غير صحيحة، أو إدخال معلومات صحيحة غير مصرّح بإدخالها، أمّا فعل التعديل يتعيّن أن يكون بطريق الغش، ويعني تغيير المعلومات داخل النظام واستبدالها بمعلومات أخرى[33]، في حين أنّ فعل الإزالة يعني التدمير والمحو والإتلاف، وكلها تعني اقتطاع خصائص البيانات والمعطيات عن طريق محوها، أو عن طريق طمسها أو ضغط خصائص أخرى فوقها، وهي مرحلة لاحقة على مرحلة الإدخال المعلومات.[34]

تعد هذه الجريمة من الجرائم المادية ذات نتيجة، وهو وقوع ضرر فعلي على هذه المعلومات، كما أنّ هذه العمدية تتطلب قصدا جنائيا عاما، وان كانت هناك بعض التشريعات تتطلب قصدا جنائيا خاصا، وهو نية تحقيق الربح[35]، وهذا ما لم يشترطه المشرع الجزائري.

ثالثا: التزوير الإلكتروني

انتشر استخدام الحاسب الآلي في شتى مجالات التعامل بين الأفراد، وحلّ محل الأوراق في أغلب المعالجة الآلية للمعلومات، غيرا أنّه حمل معه قدرا من تزايد الاعتداءات الواقعة على البيانات والمعلومات والمعطيات، وذلك بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس بمراكز الأفراد[36]، ولقد عرّف عبد الفتاح بيومي حجازي التزوير الإلكتروني على أنه:

> " **تغيير للحقيقة يرد على مخرجات الحاسوب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تم عن طريق الطابعة أو كانت مرسومة عن طريق الرسّام، ويستوي في المحرر الإلكتروني أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات لا ورقية، شرط أن تكون محفوظة على دعامة، كبرنامج منسوخ على أسطوانة، وشرط أن يكون المحرر الإلكتروني ذا أثر في إثبات حق أو أثر قانوني معين**[37].

يتضمن التزوير الإلكتروني نسخ الأقراص المدمجة على أقراص أخرى، وتغيير المعلومات والبيانات واستخدامها كوسيلة للتدليس، كما أنّ تزوير البيانات يكون بالدخول بطريقة مشروعة أو غير مشروعة على قاعدة بيانات في نظم المعلومات، وتعديل البيانات سواء بإلغاء بيانات موجودة بالفعل، أو بإضافة بيانات لم تكن مجودة من قبل، مما يضع عراقيلا أمام تنفيذ مشاريع التجارة الإلكترونية، نتيجة إمكانية تزوير البيانات، وصعوبة القبض على مرتكبيها أو تحديدهم[38]، وجوهر جريمة التزوير يتمثل في الكذب المكتوب الذي يمس بالثقة العامة في المحررات واستقرارها، حيث يتمثل ركنها المادي في تغيير الحقيقة بإحدى الطرق المحددة قانونا، وأن يكون هذا التغيير في محرر سواء كان رسميا أو عرفيا، وأن يترتب على هذا التغيير ضررا، أما الركن المعنوي فيتمثل

في القصد الجنائي العام، بالإضافة إلى الخاص[39]، والمشرع الجزائري –على غرار عدد من التشريعات العربية– لم ينص على جريمة التزوير المعلوماتي، بالرغم من توالي التعديلات لنصوص قانون العقوبات.

رابعا: جريمة التعامل في معطيات غير مشروعة

نظرا لأهمية المعطيات الالكترونية؛ فقد حرص المشرع في خطته لمكافحة الجريمة الإلكترونية، والتصدي لها قبل وقوعها، وذلك بمنع كل الأفعال التي تُشكّل مقدمة لها، فقام بتجريم مجموعة من الأفعال تنصبّ كلها في التعامل مع معطيات صالحة، لأن ترتكب بها إحدى جرائم المعطيات، وتناول المشرع هذه الجريمة في نص المادة 384 مكرر 2 ق ع، وجرّم التعامل بالمعطيات غير المشروعة، لمنع وقوع الجريمة، أو التخفيف من أثارها إن وقعت، كما يسعى إلى إيقاف العدوان في مصدره وبدايته.

تقوم هذه الجريمة كباقي الجرائم على ركن مادي، يتمثل أساسا في النشاط الإجرامي، حيث تأخذ صورتين: صورة التعامل في معلومات صالحة لارتكاب جريمة، وصورة التعامل في معلومات متحصلة من جريمة، وبالنسبة للصورة الأولى فتنطوي على عدة أفعال مثل التصميم، البحث والتجميع، والتوفير والنشر والإتجار، أما الصورة الثانية فقد حصرت المادة 394 مكرر2 من قانون العقوبات الأفعال التي تشكل هذه الصورة، وهي الحيازة، الإفشاء، النشر، الاستعمال، ولقد استعمل مصطلح " عن طريق الغش"؛ مما يوحي أنّ هذه الجريمة تتطلب قصدا عاما وكذا قصد خاصا، وتُعدّ هذه الجريمة من الجرائم الشكلية التي لا تتطلب نتيجة، رغبة من المشرع في وقف هذه الجرائم عند مرحلة الخطر، دون انتظار ترتيب الضرر، أمّا بالنسبة للركن المعنوي للجريمة الإلكترونية، فهي تتكون من عنصريها أي العلم والارادة، فالعلم: هو إدراك الفاعل للأمور، أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة[40].

المطلب الثاني: الجرائم الإلكترونية الواقعة بواسطة النظام المعلوماتي

تُجسّد الاستعمالات الواسعة للنظم المعلوماتية خاصية للحياة اليومية للأفراد ونشاط المؤسسات، وإزاء ما يعرقل السير الحسن لتلك الأنظمة أو يحوّلها عن الغرض منها، تقف الجرائم الالكترونية التي وسيلتها النظام المعلوماتي، حيث تتنوع هذه الجرائم ما بين الجرائم الاقتصادية، أو قرصنة المعلومات أو ذات طابع سياسي، أو المتعلقة بأمن الدولة، وقد تقع هذه الجرائم على أشخاص طبيعية وأخرى معنوية، ويمكن تقسيمها إلى: الجرائم الواقعة على الأموال والجرائم الواقعة على الأشخاص.

الفرع الأول: الجرائم الالكترونية الواقعة على الأموال

في ظل التحوّل من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية؛ وما انجرّ عنه من تطور وسائل الدفع والوفاء، وفي خضم التداول المالي الكثيف والواسع عبر الأنترنيت، أصبحت هذه المعاملات عرضة لشتى انواع الجرائم، التي نذكر منها:

أولا: جرائم التجارة الإلكترونية

أدى الاستعمال الواسع لشبكة الأنترنت والاستفادة من مكتسبات العصر الرقمي، إلى رواج التجارة الإلكترونية، والتي أتاحت العديد من المزايا، وفي نفس الوقت ازداد معها حجم الجرائم المرتكبة في سياق معاملات تلك التجارة، في ظلّ تخلف الآليات القانونية التقليدية وعجزها عن التعامل معها، وقصور تلك القوانين التي وضعت للتجارة التقليدية، خاصة وأن التجارة الإلكترونية تعتمد الطابع الافتراضي، أين تسلّم المنتجات وتؤدى الخدمات إلكترونيا، كما أنّ عدم وجود مستندات ورقية بخط اليد، يحدث مشكلة عدم التمييز بين الرسالة الأصلية والرسالة المستنسخة، مما يزيد من حجم جرائم التزوير، كما لا يعيق عديد الجرائم من قبيل عمليات السطو وقرصنة البيانات الشخصية عبر الأنترنت، والجرائم التي يكون ضحيتها المستهلك، خاصة عندما يلجأ المنتج إلى توظيف أساليب دعائية، تنطوي على قدر كبير من الغش والخداع والتضليل[41]، حيث يكون هدفه دفع المستهلك إلى التعاقد، دون احترام لعديد شروط السلامة أو المطابقة بشأن ما يعلنه بشأن السلعة أو الخدمة، وما هي عليه في الواقع.

ثانيا: جرائم غسيل الأموال إلكترونيا

يعد غسيل الأموال إحدى صور الجرائم الاقتصادية؛ وهو ظاهرة ترتبط بالجريمة العالمية المنظمة وبالأخص متاجرة بالمخدرات، والإرهاب الدولي، وكذا تهريب الأسلحة والتزييف، وأيضا الفساد السياسي والفساد الإداري والمالي، وتعد جريمة غسيل الأموال اليوم من المشاكل العالمية التي تحظى باهتمام الدول المتقدمة والنامية، وتراهن على مواجهتها المنظمات الدولية الحكومية وغير الحكومية.

يقدّر صندوق النقد الدولي حجم الأموال التي يتم غسلها وإضفاء الشرعية عليها سنويا؛ ما بين 620 الى 1600مليار دولار، ولأن الجهاز المصرفي هو الوسيلة الأكثر فعالية لإضفاء صفة المشروعية على الأموال القذرة، فإنّه صار من المعتاد أن توجّه أنشطة غاسلي الأموال الى المصارف، على أمل إجراء سلسلة من العمليات المصرفية المعقدة، يتم فيها إدخال وسطاء وشركات وهمية، والبحث عن ملاذات أمنة، يصعب فيها تتبع الأصول والودائع المالية، لتندمج في الأخير ضمن العمليات المالية، وأنشطة البورصات والمبادلات المالية، ولا يمكن لذلك أن يتم بسرعة واحترافية، إلا إذا جرت الاستعانة بما تكفله الأنظمة المعلوماتية التي تزيد من نسبة نجاح تلك العمليات، والواقع يشير إلى أنّ الأضرار عن هذه الجرائم لا تنحصر في الجوانب الاقتصادية فقط، بل تمتد إلى الجوانب الاجتماعية والسياسية، وحتى الأمنية، باعتبارها جريمة مركّبة تأتي لاحقة لجريمة أخرى[42].

تأتي خطورة غسيل الأموال عبر الأنظمة المالية الالكترونية في كونها تظل حافزا لاستمرار الأعمال الإجرامية، وزيادة عوائدها، كما أنها تدفع نحو سهولة التجنيد والتنفيذ لتلك الأعمال، وهي في جانب آخر تعوق عمل العدالة في الوصول إلى الأرصدة المالية والتثبت من مدى احترام طرق تحصيلها وانفاقها، وكذا تسهل الملاذات الأمنة للتهرب الضريبي، ويمكن لتلك الأموال القذرة أن تستمر في تنمية تجارة المخدرات والسلاح، ودعم الفساد وعرقلة الديمقراطية وانتهاك حقوق الانسان.

الفرع الثاني: الجرائم الالكترونية الواقعة على الأشخاص

حملت التطورات العلمية التي عرفها العالم خلال النصف الثاني من القرن العشرين؛ جملة من التحولات العميقة في بنية ونشاط المجتمعات الانسانية، واتضح أنّه مع ظهور الكومبيوتر ثم شبكة الانترنت، أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، ما جعلها عرضة للانتهاك والاستعمال غير المشروع، كما أنّ سمعة وشرف الأفراد صارت مهددة بأن تصير مستباحة بقدر كبير، وعلى أساس هذا الوضع، يمكن الإشارة إلى جملة من الجرائم في هذا السياق، وهي على النحو التالي:

أولا –جرائم السب والقذف عبر الانترنت

تعدّ جرائم القذف والسب من أكثر الجرائم انتشارا عبر شبكة الانترنت، ولقد عرّفتها المادتين 296–297 من قانون العقوبات بالقول:

"يعدّ سبا؛ كل تعبير مشين، أو عبارة تتضمن تحقيرا أو قدحا، لا ينطوي على اسناد أية واقعة."

"يعد قذفا؛ كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئات المدّعى عليها بها، أو إسنادها إليهم، أو إلى تلك الهيئة، ويعاقب على نشر هذا الادعاء، أو ذلك الاسناد مباشرة، أو بطريق إعادة النشر، حتى ولو تمّ ذلك على وجه التشكيك، أو إذا قُصد به شخص أو هيئة، دون ذكر الاسم، ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصيّاح أو التهديد، أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة."

لقد اشترط المشرّع في كلتا الجريمتين العلانية، لأنّ المادة 296 نصت على أن تكون بأية وسيلة من وسائل العلانية، وهذا ما يعني بان جريمة القذف والسب عبر شبكة الانترنت، تتحقق بالعلانية.

ثانيا: الجرائم المخلة بالآداب العامة عبر الانترنت

وفّرت شبكة الأنترنت أكثر الوسائل فعالية وجاذبية في صناعة ونشر الإباحية، حيث وجد العاملون في مجال الرذيلة والإباحية في تلك الشبكة؛ وسيلة حديثة ذات كفاءة عالية في الدعوة إلى ممارسة البغاء وبربحية غير مسبوقة، وساهم هذا التوجه في الترويج للانحلال والفجور، الذي تقع ضحيته الفئات الهشة من المجتمع، وفي مقدمتهم الأطفال والمراهقون، خصوصا وأنّه يجري الاستفادة من مزايا سرعة التراسل الالكتروني وكذا التسويق التجاري الالكتروني الذي أداته الأساسية هو الإعلانات الإلكترونية، والمحتويات المغرية ضمن مواقع الويب الإباحية، والتي تعد ملايين المواقع على الشبكة العالمية، وقد استطاعت تلك الأطراف تطوير أساليبها في الوصول إلى جمهور واسع من المتابعين، كما أنّها طوّرت طرقا في تفادي الحظر والحجب، وأيضا في التحايل على القوانين الوطنية والدولية، ولعلّه من المفيد الإشارة إلى قدرات الشبكات الإجرامية في استغلال التقنية في إنشاء شبكات الدعارة، واستغلال الأطفال جنسيا، ويقع ضحية لذلك الملايين من الأفراد مقابل عوائد ضخمة للجناة الناشطين على الشبكة الالكترونية العالمية، وعلى الشبكات البديلة، والمواقع السوداء. [43]

إنّه من الواضح أنّ الجريمة الالكترونية من هذا الصنف، قد قطعت شوطا طويلا من التقدّم، يقتضي جهودا جادة في التصدي لها، وتقف المنظومة القانونية ضعيفة في التعامل بكفاءة وبشكل استباقي مع ارتكاب تلك الجريمة، وتزداد صعوبة اكتشاف هذه الأنماط من الجرائم وتحديد مصدرها وإقامة الدليل عليها، بالإضافة الى عدم وجود تشريعات حديثة فعّالة تواجه الجرائم الأخلاقية التي ترتكب عبر الإنترنت، وكلما بذلت الدول جهودا في محاصرتها، طوّر الجناة أساليب بديلة في استمرار نشاطهم، الذي يغذيه الفقر والحرمان والتفكك الأسري، والأمية وانتشار المخدرات والعنف المجتمعي.

ثالثا–جرائم التعدي الالكتروني على الحياة الخاصة

صُمِّمت الإنترنت كشبكة مفتوحة تتدفق خلالها المعلومات في صيغة صريحة، لذا فكل ما ينساب عبرها يمكن اعتراضه والاطلاع عليه بسهولة، إذا لم يتم تحصين الحسابات الشخصية، وإيجاد آليات تأمين فعّال للمعلومات والبيانات المهمة، لذا فإن أكثر ما يشغل مستخدمي هذه الشبكة؛ هو حماية الخصوصية والهوية الرقمية والبيانات الشخصية والمعاملات المالية، خصوصا وأنّ التقاعس أو التفريط في ذلك قد يؤدي إلى آثار سلبية، أقلّها اطلاع الآخرين على كل ما يخص المتضرر، فيما يسعى هو إلى جعل معلوماته غير متاحة لغيره، ووصولا إل الخسارة المالية وتراجع مستويات الثقة والارتباط؛ إذا كان المتضرر شركة أو مؤسسة مالية أو مؤسسة خدمات، يفترض فيها ممارسة الحد الأقصى من الانضباط والدقة وحماية بيانات المتعاملين.[44]

إنّ من صور الاعتداء على الحياة الخاصة بالوسائط الالكترونية؛ نذكر منها جمع البيانات وتخزينها على نحو غير مشروع، وإساءة استعمال البيانات أو المعلومات الإسمية، والخطأ في المعلومات أو البيانات الإسمية، الإفشاء غير المشروع للبيانات والمعلومات الإسمية، وجريمة الاعتداء على سرية الاتصالات والمرسلات، وجريمة إتلاف معلومات البرمجة ألليا بواسطة الفيروسات، وانتهاك الحق في الخصوصية على شبكة الإنترنت لا يخرج عن أربع صور، وهي :اقتحام عزلة الشخص، والكشف عن أسرار الشخص، وادعاء الأكاذيب، والاستخدام غير المصرح به لاسم الشخص أو لصورته.[45]

الفرع الثالث: الجرائم الالكترونية الواقعة على أمن الدولة

من أهم الجرائم الإلكترونية التي تهدد أمن الدولة ومجتمعاتها، يمكن الإشارة إلى:

أولا: الإرهاب الإلكتروني

يُعرّف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية، الصادر من الدول والجماعات أو الأفراد على الإنسان، في دينه أو عرضه أو عقله أو ماله بغير حق، بشتى أصناف وصور الفساد في الأرض[46]، حيث يقوم الإرهابيون بإنشاء أو تصميم مواقع لهم على شبكة المعلومات لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، حيث تتضمن شبكة الانترنيت معلومات ذات صلة بدعم الأنشطة الإرهابية، وكذا مواقعا لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع وتعطيلها، وأيضا طرق اختراق البريد الإلكتروني، وكيفية

الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات ، وغير ذلك من الممارسات التي تقع في صميم الإرهاب الالكتروني، الذي يواجهه العالم بشدة خاصة في العقدين الأخيرين.[47]

إنّ من بين محاسن التفاوت في امتلاك التكنولوجيا، هو أنّ الدولة المتخلفة وغير المندمجة كلية في المنظومة المعلوماتية العالمية هي أكثر تحصينا بحكم أساليبها التقليدية، في مجال الأمن الالكتروني، في حين تزداد مخاطر الإرهاب الإلكتروني على الدول المتقدمة؛ التي تملك بنية تحتية بالحواسيب وتدير أنشطتها الاقتصادية والإدارية عبر شبكة من المعلومات والعمليات الالكترونية، وهو ما يفرض على تلك الدول تحديات كبرى، باعتبار هذا النوع من الإرهاب إرهابا متصلا بالتقنية التي تمتد وتتطور باستمرار في الحاضر، ومن المتوقع أن تكون لها أشكال أكثر تعقيدا في المستقبل.

ثانيا: جرائم التجسس الإلكتروني:

تواجه الدول باستمرار مخاطر وقوعها ضحية لأنشطة التجسس الإلكتروني، وهو النمط الذي يتم فيه الوصول إلى المعلومات السرية في الميدان العسكري وكذا القطاعات الحساسة في الدولة، عبر أشكال تتجاوز الشكل التقليدي في الحصول على المعلومة، حيث يتم اختراق الأجهزة الالكترونية للمؤسسات العسكرية والأمنية وكذا القطاعات الاقتصادية الحيوية، وتتم عملية قرصنة البيانات أو اتلافها، وتشمل أيضا عمليات التجسس الالكترونية الوصول إلى الأطقم البشرية المسيرة لتلك القطاعات، وسرقة معلوماتهم لاستغلالها في الدخول غير المشروع للبيانات السرية، وقد يكون التجسس الالكتروني ذا بعد اقتصادي، يهدف ممارسوه إلى معرفة معلومات تتعلق بالجانب المادي، أو ممارسة أنشطة الابتزاز والضغط وبيع المعلومات المهمة، وتندرج في هذا الاطار أيضا أنشطة التجسس الصناعي، التي هي مجرّمة طبقا للقوانين الجنائية القائمة، فعلى سبيل المثال قد يتم تنزيل الأسرار الصناعية من كومبيوتر في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافسين، بل قد تكون تكنولوجيا المعلومات نفسها هدفا مهما لهذه الجريمة، فقد تتم سرقة اختراع جديد في تكنولوجيا الكومبيوتر، وبيعه بمبلغ كبير من المال يعادل ملايين الدولارات[48]، والواقع يشير إلى أنه لم تعد هناك سرية مطلقة، تتيح الاحتفاظ بالمعلومات، دون أن تتعرض لمخاطر وتهديدات عمليات التجسس أو الهاكرز.

خاتمة:

نخلص في نهاية هذه الورقة البحثية إلى القول أنّ الجريمة الإلكترونية بمثابة الشكل الحديث للجرائم ذات الطبيعة المالية والاقتصادية والأخلاقية، والتي ظهرت وتعددت أساليب ارتكابها مستفيدة من التسهيلات والامتيازات التي وفّرتها العولمة في بعدها التكنولوجي والاتصالية، وبناءا على هذا التصور نتوصل إلى جملة من النتائج، بخصوص مفهوم وتقسيمات تلك الجريمة، نجملها وفقا لما يلي:

أولا: النتائج:

1- عدم وجود اتفاق على تعريف شامل وموحد للجريمة الإلكترونية، باعتبار أنها تحدث في بيئة افتراضية تتسم بالتغيير والانتشار الجغرافي العابر للحدود، وهو الأمر الذي انعكس أيضا عند محاولة وضع

تصنيف لها، إذ لم تتحل بتصنيف واحد بل تعددت التصنيفات بشأنها وهو ما ولد صعوبات في التصدي لها على مختلف الأصعدة، كما أن واقع هذه الجريمة يجعلها تحظى بخصوصيات تختلف عن الجريمة التقليدية؛

2-أدى الانتشار الواسع لهذا النمط الإجرامي المتطور جدا، والذي تستخدم فيه أحدث التقنيات التكنولوجية العالية والمتطورة وسرعة وبداهة وحيلة مرتكبيها، والتي تجعلهم دائما يفلتون من العقاب، في ظل غياب الدليل المادي للجريمة؛

3-تعتبر الجريمة الإلكترونية من أكثر الجرائم، التي تثير مسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، لأن الجريمة قد تقع في مكان وتنتج أثارها في مكان أخر؛

4-في إطار السياسة الجنائية الرامية لمواجهة مخاطر الجريمة الإلكترونية، سلك المشرع الجزائري خطوة مهمة تجسدت في تعديل قانون العقوبات بموجب القانون رقم 04-15 بإضافة قسم سابع مكرر عنوانه:

" جرائم المساس بأنظمة المعالجة الألية للمعطيات " ضمن المواد 394 إلى 394 مكرر 7 كجريمة الدخول والبقاء غير المشروع في نظام المعالجة الألية للمعطيات، كما نسجل ضمن هذا الإطار إغفال المشرع لبعض الجرائم رغم أهميتها كجريمة التزوير المعلوماتي، وهو ما يجدر على المشرع أن يضعه في الاعتبار.

ثانيا: التوصيات:

1-تطوير التشريعات القانونية باستمرار لمواكبة التطور المستمر لهذه الجرائم، والتحديث المستمر لبرامج حماية الحواسيب من الفيروسات؛

2-إن مواجهة هذه الجريمة يتطلب خلق سياسات أمنية تقوم على التعليم والتدبير، وإعداد عناصر بشرية مؤهلة للتمكن من مواجهة الجريمة الإلكترونية، بطرق أكثر احترافية قادرة على احتوائها والحد من تداعياتها وخطورتها؛

3-خلق سياسة توعوية تثقيفية للتصريح بخطورة هذه الجريمة، وعقوباتها وتعزيز التعاون الوطني والدولي للوقاية منها؛

4-تبادل الخبرات والزيارات والدراسات المشتركة مع الجهات المعنية بمكافحة الجريمة الإلكترونية، والعمل على إعداد العديد من النشرات والمطويات، والمقالات والدراسات والبحوث، التي تتناول موضوع الجرائم الإلكترونية والمستجدات التي تتناول الموضوع، والعمل على نشر البحوث والدراسات على النحو الذي يحقق أفضل استفادة على الجانب الأمني؛

5-إنشاء قاعدة بيانات لجرائم المعلومات، من حيث أساليبها وأنواعها، تكون سندا وإطارا يمكن اعتماده في صياغة العقوبات اللازمة لمجابهة هذه الجريمة.

الهوامش:

([1])–أمينة بوشعرة ، سهام موساوي، **الإطار القانوني للجريمة الإلكترونية** ، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية، 2018 ، ص:04.

([2])–ذياب موسى البداينة، **الجرائم الإلكترونية: المفهوم والأسباب**، ورقة علمية مقدمة للملتقى العلمي حول **الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**، خلال الفترة من 02 إلى 04 سبتمبر2014، كلية العلوم الاستراتيجية، عمّان، الأردن، ص: 08.

([3])–نداء نائل فايز المصري، **خصوصية الجرائم المعلوماتية**، مذكرة مقدمة لنيل درجة الماجيستر ، في القانون العام ، بكلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2017 ، ص: 03.

([4])– محمد علي قطب، **الجرائم المعلوماتية وطرق مواجهتها** ، مركز الإعلام الأمني ، وزارة الداخلية ، الأكاديمية الملكية للشرطة ، مملكة البحرين ، 2010 ، ص: 09.

([5])–سفيان سوير، **جرائم المعلوماتية** ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، وعلوم الإجرام ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011، ص:12.

([6])–يزيد بوحليط، **الجرائم الإلكترونية والوقاية منها في القانون الجزائري ، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات ، ق إ ج ، قوانين خاصة** ، دار الجامعة الجديدة ، الإسكندرية ، 2019 ، ص: 50.

([7])– نداء المصري، مرجع سابق، ص05

([8])– سفيان سوير، مرجع سابق، ص15.

([9])–إدريس النوازلي، **موقف القضاء من الجريمة الإلكترونية** ، سلسلة الندوات والأيام الدراسية ، **التجارة الإلكترونية أية حماية ؟** أشغال الندوة الوطنية التي نظمها مكتب الدراسات الجنائية وهيئة المحامين بمراكش، المغرب، أيام 29، 30 ماي2009، ص:91.

([10])– أمينة بوشعرة، سهام موساوي، مرجع سابق، ص12.

([11])–سعيداني سلامي وطارق طراد، **التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة: عرض تشريعي قانوني**، مجلة الحقوق والعلوم السياسية، العدد 12، جوان 2019، ص ص245–257.

([12])–قانون 04/09 المؤرخ في 2009/08/05، المتضمن **القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها**، ج ر 74، الصادرة في 2009/08/16.

([13])– يزيد بوحليط، مرجع سابق، ص55.

([14])–محمد السعيد زناتي،" **الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية**"، مجلة إيليزا للبحوث والدراسات، المجلد 02، العدد01، ديسمبر 2017، ص ص 28–40.

([15])– بوحليط، مرجع سابق، ص ص59، 60.

([16])–محمود أحمد عبابنة ومعمر الرازقي، **جرائم الحاسوب وأبعادها الدولية**، (الأردن: عمّان، دار الثقافة للنشر والتوزيع، 2005)، ص33.

([17])– سميرة معاشي، **الجريمة المعلوماتية: دراسة تحليلية** ، مجلة المفكر، العدد 17، جوان 2018، ص ص 397–417.

([18])–محمود أحمد عبابنة ومعمر الرازقي، مرجع سابق ، ص36.

([19])–سميرة معاشي، مرجع سابق، ص ص397–417.

([20])–سعيداني سلامي وطارق طراد، مرجع سابق، ص249.

([21])– يزيد بوحليط، مرجع سابق، ص82.

([22])–المرجع نفسه.

([23])– رحموني أحمد ، "**خصائص الجريمة الإلكترونية ومجالات استخدامها** "، مجلة الحقيقة ، العدد 41 ، 2018 ، ص ص 432–451.

([24])– أنيس العذار، "**مكافحة الجريمة الإلكترونية** "، المجلة الأكاديمية للبحث القانوني ، المجلد 17 ، العدد 01 ، 2018، ص ص721–744.

([25])–نصير لعرباوي، فاتح النور رحموني ، "**الجريمة الإرهابية الإلكترونية** ،" المعيار ، العدد 43 ، جانفي ، 2018 ، ، ص ص367–377.

([26])– خالد ممدوح إبراهيم ، **أمن الجريمة الإلكترونية** ، الدار الجامعية للطباعة والنشر والتوزيع ، القاهرة، مصر ، 2008، ص61.

([27])–نمديلي رحيمة ، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة** ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية – الجزائر ، 24–25 مارس 2017، ص104.

([28])–خالد ممدوح إبراهيم، مرجع سابق، ص65.

([29])–عزيزة رابحي، **العنصر المفترض في جريمة الدخول او البقاء غير المصرح به للنظام المعلوماتي**، المجلة الجزائرية للدراسات التاريخية والقانونية، المركز الجامعي تندوف، المجلد 01، العدد 02، جوان 2016، ص ص262–281.

([30])– محمد حماد مرهج الهيتي، **الجريمة الالكترونية: نماذج من تطبيقاتها(دراسة مقارنة)**، القاهرة، دار الكتب القانونية 2014، ص 187.

([31])– عزيزة رابحي، مرجع سابق، ص ص262–281.

([32])–أمال قارة، **الجريمة المعلوماتية** ، مذكرة ماجستير ، كلية الحقوق بن عكنون ، الجزائر ، سنة 2002 ، ص06.

([33])– رشيدة بوكرا، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، بيروت، منشورات الحلبي الحقوقية، 2011، ص ص185،186.

([34])–عبد الفتاح بيومي حجازي، **مكافحة جرائم الكومبيوتر والانترنيت في القانون النموذجي العربي**، القاهرة، دار الكتب القانونية، 2007، ص49.

([35])–نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، بيروت، منشورات الحلبي الحقوقية ، 2005، ص223.

([36])–غانم مرضي الشمري، **الجرائم المعلوماتية – ماهيتها – خصائصها – كيفية التصدي لها قانونيا**، الأردن:عمّان، الدار العلمية الدولية للنشر والتوزيع و دار الثقافة للنشر والتوزيع ، 2016، ص60.

([37])– حجازي، الدليل الجنائي، والتزوير في جرائم الكومبيوتر والانترنيت، 2002، ص170.

([38])–منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية ، 2005 ، ص 90–91

([39])– يزيد بوحليط، مرجع سابق، ص276.

([40])– ناصر حمودي، **الحماية الجنائية لنظم الآلية المعطيات في التشريع الجزائري**، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 06 ، 2016 ، ص ص67–91.

([41])–خالد ممدوح إبراهيم، مرجع سابق، ص ص70،71.

([42])– المرجع السابق، ص78.

([43])- سليم حميداني وعباسي سهام، "**اختراق الخصوصية في العالم الرقمي: حدود الظاهرة ومطالب الحماية القانونية**"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، المجلد 04، العدد 02، ماي 2019، ص ص 33-46.

([44])- المرجع نفسه.

([45])- يعقوب عبد العزيز الصانع، **انتهاك الحق في الخصوصية عبر الإنترنت**، جريدة القبس، الكويت، العدد 16022، 2017/01/08، ص12.

([46])-ايهاب ماهر السنباطي : **الجرائم الإلكترونية: قضية جديدة أم فئة مختلفة ؟**، عمل الندوة الإقليمية حول **الجرائم المتصلة بالكومبيوتر** ، المملكة المغربية 19-0 جوان 2007 ، ص 21.

([47])- أيسر محمد عطية، "**دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته** "، ورقة علمية مقدمة في الملتقى العلمي : **الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية**، خلال الفترة 02-4 سبتمبر 2014 ، عمان الأردن ، ص 16 .

([48])- إيهاب ماهر السنباطي، مرجع سابق، ص21.