مجلة الحوكمة والقانون الاقتصادي
المجلد: 03 العدد: 01 السنة: 2023 ص ص: 57 - 76

الجريمة الإلكترونية: بين حدود الخطر وضرورات المواجهة

(Cybercrime: Between the limits of danger and the necessities of confrontation)

تاريخ الإرسال: 2022/10/02 تاريخ القبول: 2022/10/23

مرابطي رميساء* *Roumaissa Merabti*
كلية الحقوق والعلوم السياسية سوسة/تونس
Univ Soussa - Tunis
merm44331@gmail.com

ملخص:

تعد الجريمة الإلكترونية، من الجرائم المستحدثة وهذا راجع إلى التطور التكنولوجي وعالم الاتصالات، والممارسة السيئة لهذه الأخيرة أدت إلى ظهور هذه الجريمة وهي بدورها تختلف عن الجريمة التقليدية في طبيعتها ومضمونها ونطاقها وحتى في خصوصية وتميز مرتكبيها والعقوبة المسلطة عليها، وقد ساهمت عوامل التحضر السريع وتكنولوجيا الاتصال دون أن ننسى عالم الانترنت الذي كان سباقا في ظهور هذه الجريمة، مما ساعد على سرعة انتشارها وارتفاع ضحاياها، خاصة مع قصور وسائل الرقابة، وقلة النصوص القانونية، وفرض العقوبات لتحجيم تأثيرات هذا النوع من الجرائم المستحدثة التي تستهدف الأفراد والدول، وبالتالي فهي تمثل حقيقة "الاستعمار الإلكتروني" في أبشع صوره.

الكلمات المفتاحية: الجريمة، العقوبة، الحاسب، المعلوماتية، الانترنت، القرصنة.

Abstract:

Cybercrime is one of the new crimes, and this is due to the technological development and the world of communications, and the bad practice of the latter led to the emergence of this crime, which in turn differs from the traditional crime in its nature, content, scope and even in the privacy and distinction of its perpetrators and the punishment imposed on them. The factors of rapid urbanization and communication technology have contributed Without forgetting the world of the Internet, which was a forerunner in the emergence of this crime, which helped in its rapid spread and the rise of its victims, especially with the shortcomings of the means of censorship, the lack of

*- مرابطي رميساء

legal texts, and the imposition of penalties to limit the effects of this type of new crimes targeting individuals and countries, and thus represent a reality. "Electronic Colonialism" in its ugliest form..

***Keywords**: (Crime, punishment, computer, informatics, internet, piracy .*

مقدمـة:

الجريمة ظاهرة قديمة، عرفتها المجتمعات البشرية منذ القدم، وظهرت في هذه المجتمعات السلطة الحاكمة انطلاقا من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لاستتباب الأمن لدى الفرد والمجتمع واعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله وسلامته الجسدية، فعل مجرم يستحق العقاب عليه.

لكن بعد ظهور فكرة الدولة تولت بنفسها سلطة تجريم الأفعال والعقاب عليها، حيث أصدرت تشريعات منها ماهو موضوعي "قانون العقوبات"، الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ماهو إجرائي "قانون الإجراءات الجزائية" الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان، قد حددت كليات خمس لا تستقيم الحياة إلا بها، وهي حفظ الدين، حفظ النفس، حفظ العقل، حفظ النسل، حفظ المال وبينت أن مسألة المجرم تكون استنادا لمبدأ حرية الاختيار.

غير أنه بتطور الإنسان في شتى الميادين، خصوصا في مجال التقنية إذ ظهر الحاسوب الآلي وشبكة الانترنت، وغزت هذه الوسيلتين جميع المجالات نظرا لما تتسم به من الدقة والسرعة، وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المجرمين، وهو الانعكاس السلبي لهذه الثروة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة المعلوماتية أو الجرائم السيبريالية Cyber Crimes وهي تلك الجرائم التي ترتكب عبر شبكة الانترنت أو بواسطتها وعادة ما يكون الفاعل إما فردا أو جماعة، ويصعب الكشف عن الجاني كما هو الشأن في الجرائم العادية فضلا عن كونه في أغلب الأحيان مخفيا.

وتمثل الجريمة السلوكيات والأفعال الخارجة على القانون أما الجرائم الإلكترونية فهي المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو إلحاق أذى مادي أو معنوي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنيت (البريد الإلكتروني- الهاتف الجوال).

وقد عرفت شبكة وسائل الاتصال تطورا تاريخيا نوعيا مطردا وهي ناتجة عموما عن الثورة

التكنولوجية التي شهدها العالم منذ بداية القرن السابع عشر والثامن عشر. ثم اختراع المطبعة وظهر البريد الجوي والتصوير الشمسي وتم تطوير أجهزة التصوير ثم ظهرت الوسائل الحديثة مثل الراديو والتلفزة.

وتعتمد تعاريف الجريمة الإلكترونية في الغالب على الغرض من استخدام هذا المصطلح وتشمل عددا من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة ويمثل جوهر الجريمة الإلكترونية أبعد من هذا الوصف، ومع ذلك فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر بما في ذلك أشكال الجرائم المتصلة بالهوية والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية".

وتظهر مدى خطورة جرائم الكمبيوتر والانترنت، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والاجتماعية والثقافية وكذا الأمنية ومن هنا تبرز إشكالية الدراسة والتي تتمحور على التساؤل التالي: إلى أي مدى صارت الجريمة الإلكترونية تجسد خطرا على مختلف نواحي المجتمع، وهل بالإمكان التصدي لها بكفاءة على نحو يحد من آثارها ويحمي المتضررين منها؟

تنبثق من هذه الإشكالية المحورية جملة من التساؤلات الفرعية تتمثل في ما يلي: ما المقصود بالجريمة الإلكترونية؟ ما هي خصائصها؟ وفيما تتجسد آليات مكافحة الجريمة الإلكترونية؟

للتعامل مع هذه الإشكالية والأسئلة المرتبطة بها سنعمل على تنظيم المادة العلمية المتصلة بالموضوع استنادا على المنهج الوصفي وذلك بالربط بين هدفي الشرح والتفسير للانتقال إلى حالة التوقع إزاء الآثار وآليات المواجهة للجريمة الإلكترونية، وهو انتقال يُدرج التحليل كغاية ووسيلة تُتيح لنا الإحاطة بالموضوع وربطه بإطاره القانوني.

استنادا إلى الإشكالية المشار إليها والمنهج المعتمد فإن العمل يتمحور حول مبحثين ضمن خطة ثنائية تنتقل من الإحاطة بالجريمة الإلكترونية إلى التعرف على آثارها السلبية ووصولا إلى ما يفرضه ذلك من ضرورة البحث عن الآليات الأكثر فعالية في التصدي لها وذلك بالربط دوما مع المنظومة التشريعية الجزائرية.

المحور الأول: الإطار المفاهيمي للجريمة الإلكترونية:

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، جرائم الكمبيوتر والانترنت، الجرائم المستحدثة، الجرائم الناعمة، إجرام ذوي الياقات البيضاء، وتجدر الإشارة إلى أن هناك فارق

بين ميدان جرائم الحاسب الآلي وميدان جرائم الانترنت فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الانترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات) وظهور مصطلح crime cyber. وسنحاول من خلال هذا المحور تحديد المقصود بالجريمة الإلكترونية، وتحديد طبيعتها القانونية وإبراز خصائصها وهذا ما سيكون محل معالجة من خلال عنصرين المواليين:

أولا- تعريف الجريمة الإلكترونية:

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك الاختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق والبعض الآخر ينظر إليها بمفهوم واسع وسنحاول إبراز هذين الاتجاهين وفقا لمايلي:

1- الاتجاه الضيق لمفهوم الجريمة الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وفقا لمعايير متعددة، سواء كانت وفقا لمعيار موضوع الجريمة أو من حيث توفر المعرفة والدراية بالتقنية، وسنسرد في هذا الإطار بعض التعريفات لفقهاء القانون الجنائي، فقد عرفتها الدكتورة هدى قشقوش بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل البيانات"، كما عرفها الفقيه الألماني Tièdement أنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب" فهو يرتكز في تعريفه على وسيلة ارتكاب الجريمة.

كما يرى الأستاذ Eslie D. Ball أنها: " فعل إجرامي يستخدم الكمبيوتر فيه كأداة رئيسية".[1]

وقد وجه لهذه التعريفات انتقادات ومنها أن تعريف الجريمة يستدعى الرجوع إلى العمل الأساسي المكون لها فحسب والوسائل المستخدمة في تحقيقه.

والجدير بالذكر، أن الدكتور سامي الشواء ينسب إلى الفقيه Tièdement تعريفه لجريمة الحاسوب بأنها: "كل جريمة ضد المال مرتبطة بالمعالجة الآلية للبيانات" وهو تعريف يختلف عن التعريف المشار إليه أعلاه، ولا عجب، إذ في ظل التباين الحاد حول المصطلحات الدالة على الجريمة وحول تعريفها يتوقع أن يبرز معيار موضوع الجريمة، وفي هذه الحالة يوجه له النقد بأن محل الجريمة ليس المال إلاّ في الأحوال التي يستخدم فيها الكمبيوتر وسيلة لارتكاب جرم استيلاء على مال، وحتى في هذه الحالة بمفهوم الداعين إلى اعتبار المعلومات مالا، فالجريمة توجه للمعلومات أساسا، وهي قد تكون مجردة عن تجسيد أية قيمة مالية وقد تجسد في الحقيقة أموالا أو أصولا.كما عرفت بانها المخالفات التي

ترتكب ضد الافراد او المجموعات من الافراد بدافع الجريمة بقصد ايداء سمعة الضحية او ادى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكة الاتصالات مثل الانترنت وغرف الدردشة والبريد الالكتروني والموبايل وهناك جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل، وهي تحديد سمة الدراسة والمعرفة التقنية، من هذه التعريفات، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت بأنها: "أيه جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها".[2]

ومن هذه التعريفات أيضا تعريف David Thompsan بأنها: "أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب". وتعريف آخر يذهب إلى أنها: "أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه التحقيق فيه وملاحقته قضائيا"[3]

2- الاتجاه الموسع لمفهوم الجريمة الإلكترونية

على عكس الاتجاه السابق يرى فريق آخر من الفقهاء ضرورة التوسع في مفهوم الجريمة الإلكترونية أو المعلوماتية، وعدم حصرها في الحاسوب وحده، أو في موضوع الجريمة أو في شخص مستخدميه، وأنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية فيعرفونها بأنها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال والأشياء المعنوية وأعطى الخبير Parker مفهوما واسعا للجريمة المعلوماتية أنها: كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الانترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي أو الاقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب.[4]

أما 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".

وعرفها الفقه الجزائري بتعاريف متعددة ومن هذه التعاريف ندكر 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 مظلة قانون العقوبات لحمايتها، أو أنها "استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع".[5]

من 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 وتمثل من الناحية المبدئية في جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

ومن أفضل التعاريف الأكاديمية: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ترتب عنه خسارة تلتحق بالضحية أو مكسب يحققه الجاني"، كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية:

1- على ما تكون المعلوماتية موضوعا الاعتداء عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية.

2- عندما تكون المعلوماتية أداة ووسيلة للاعتداء عندما يستخدم الجاني جهاز معلوماتي لتنفيذ جريمته.[6]

نتيجة لما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام لم يكن للمجتمع سابق عهد بها وعلى غرار كثير من الدول، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 [7] بإضافة قسم سابع مكرر تحت عنوان "جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المادة 394 مكرر 394 مكرر 7 حيث جاء في أسباب هذا التعديل: "إن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للأجرام مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وسوف يمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد.[8] في هذا الشأن اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية أو المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة (02)[9] من القانون رقم 09- 04 المؤرخ في 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنها: " جرائم المساس بأنظمة المعالجة الآلية

للمعطيات المحدد في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية..." فنص على جرائم المساس بأنظمة المعالجة الآلية للمعطيات بموجب المواد من (394 مكرر – 394 مكرر 7) من ق.ع.ج وإن كان استعمال هذا المصطلح ينصرف وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات، وهو بذلك يتوافق مع موقف المشرع الفرنسي في أن نظام المعالجة الآلية للمعطيات يشمل أيضا شبكة المعلومات وفقا للقانون الصادر سنة 1978، بمعنى أنه يشمل جميع العمليات التي تتم بواسطة الوسائل الإلكترونية. غير أن هذا المصطلح يقتصر على الجرائم التي تستهدف النظام فقط ليخرج بذلك من نطاقه ما دون ذلك من الجرائم التي تكون فيها نظام المعالجة الآلية للمعطيات وسيلة لارتكابها.[10]

وانطلاقا من فحوى هذه المادة نستنتج أن المشرع الجزائري قسم هذه الجرائم المستحدثة 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 الإلكترونية. [11]

ثانيا- الطبيعة القانونية للجريمة الإلكترونية:

رأينا في ما سبق أن المشرع الجزائري حاول إعطاء تعريف للجرائم الإلكترونية، فعرفها على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وعليه فهي تختلف في طبيعتها عن الجرائم التقليدية المعروفة.

ولفهم هذه الطبيعة الخاصة، لابد من التطرق أولا للطبيعة القانونية للمعلومات التي تعتبر أساس المعلوماتية، نظرا لقيمتها وطبيعتها من ناحيتي الاستئثار والانتشار في ظل تقنيات الحوسبة والاتصال (الفرع الأول)، ثم نتطرق للطبيعة الخاصة للجرائم الإلكترونية (الفرع الثاني).

1- **الطبيعة القانونية للمعلومات:**

تحتل المعلومة في وقتنا الحاضر أهمية بالغة، فمن يمتلك المعلومة يمتلك السلطة أو القوة فأصبحت المعلومات تمثل قيمة مالية واقتصادية كبيرة، وكسلعة تباع وتشترى وكمعطيات يمكن تبادلها باستعمال الحاسوب وشبكة الانترنت، حيث تعرف المعلومات على أنها: "مجموعة من الرموز أو الحقائق أو

المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها.

وعليه يثار التساؤل الآتي: هل المعلومة قابلة للاستئثار ومن ثمة تكون محلا للاعتداء عليها؟ في هذا الصدد[12] برز اتجاهان فقهيان، الأول اتجاه تقليدي يرى بأن المعلومة لا تعد قيمة في حد ذاتها لها طبيعة من نوع خاص، أما الثاني اتجاه حديث يرى بأن المعلومة عبارة عن مجموعة مستحدثة من القيم.

أ- المعلومة لها طبيعة من نوع خاص: يرى أنصار هذا الاتجاه التقليدي أن للمعلومة طبيعة خاصة بموجبها تضفي وصف القيمة على الأشياء المادية، حيث يركز هذا المبدأ على بديهية مسلم بها: "أن الأشياء التي توصف بالقيم، هي تلك الأشياء القابلة للاستحواذ، ومفاد ذلك ان الاشياء التي يمكن الاستئثار بها هي التي تكون لها قيم وبالتالي فمن غير المقبول أن تكون المعلومات قابلة للاستئثار وفق هذا الاتجاه، إلاّ عن طريق حق الملكية الأدبية أو الفكرية أو الصناعية. وعليه فإن المعلومات المختزنة التي لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، لا تندرج حتما في مجموعة القيم المحمية، كما لا يعني ذلك استبعاد الحماية القانونية لها، لأن الفقه والقضاء يعترفان بوجود اعتداء يعاقب عليه عند الاستيلاء على مال الغير، إذن فعدم مادية المعلومة هو الذي أدى بأصحاب هذا الاتجاه لاستبعادها من طائفة الأموال، فوصف القيمة لا ينطبق إلاّ على الأشياء المادية القابلة للاستحواذ، والمعلومات ذات طبيعة معنوية فإنها غير قابلة للاستئثار وبالتالي لا تندرج في مجموعة القيم.[13]

ب- المعلومات مجموعة مستحدثة من القيم:

يرى أصحاب هذا الاتجاه، أن المعلومات ما هي إلاّ مجموعة من القيم المستحدثة حيث يرى الأستاذ كاتالا (Catala) أن المعلومة المستقلة عن دعامتها المادية تكون لها قيمة قابلة للاستحواذ، وذلك لأنها تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا، كما وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها، كما أنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه وبذلك أضفى وصف القيمة على المعلومة بناءا أولا على قيمتها الاقتصادية وثانيا علاقة التبني التي تجمع بينها وبين مؤلفها مما يقودنا إلى الإقرار بوصفها قيمة مستحدثة.

من جانب آخر، تعتبر المادة في العلوم الطبيعية كل ما يشغل حيزا ماديا في فراغ معين يمكن قياسه، وبالتالي فبرامج الحاسوب تشغل حيزا ماديا يمكن قياسه بوحدات مثل: (البايت والكيلوبايت والميجابايت والجيجابايت ...) رغم أن هذه البيانات تأخذ شكل نبضات إلكترونية تمثل الرقمين (0- 1) فهي تشبه التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبل الأشياء المادية، وهو نفسه ما ذهب إليه المشرع الجزائري حينما اعتبر الكهرباء شيء ملموس يمكن أن يكون محلا للسرقة، وذلك بموجب نص المادة (2/350) من قانون العقوبات "وتطبق نفس العقوبات على اختلاس المياه

والغاز والكهرباء).[14]

2- الطبيعة الخاصة للجرائم الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة، والتي برزت نتيجة إساءة استخدام مجال تكنولوجيات الإعلام والاتصال، غير أن مكافحة هذا النوع من الجرائم يلقى صعوبات جمّة نتيجة الطبيعة الخاصة لها، ويرجع السبب في ذلك، كون المعلومات هي محور ارتكاز هذا النمط من الجرائم، ففي هذا المجال تقول الدكتورة (هدى قشقوش) في محاولتها تحديد الطبيعة القانونية الخاصة للجرائم الإلكترونية: "يجب أن نعترف بأننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، ففي معظم حالات ارتكاب الجريمة، تدخل في مجال المعالجة الإلكترونية للبيانات، كما تشير أيضا إلى أن تحديد هذه الطبيعة يستلزم "إضافة مجال معالجة الكلمات أو معالجة النصوص، إذ هي عملية وثيقة الصلة بارتكاب الجرائم وأن القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه، والتطور السريع في مجال المعلوماتية.[15]

من جانب آخر تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني إذ لم تكن النصوص التقليدية مخصصة لهذا النوع المستحدث من الجرائم وتطبيقها أدى إلى سلسلة من المشكلات كاعتبار المعلومات مالا يمكن الاعتداء عليه أو ما تعلق بمسألة الإثبات كالحصول على دليل مادي، لأن المجرم الإلكتروني يقوم بكل بساطة بمحو أدلة الإدانة في لحظات، كما تظهر الصعوبة أيضا في حالة إجراء التفتيش الواقع على المكونات المعنوية للحاسوب، أو في حالة اعتراض المراسلات فقد تكون البيانات المبحوث عنها مشفرة مما يثير مسألة مدى مشروعية إجبار الجاني على فك الشيفرة الخاصة به، إضافة إلى صعوبة ملاحقة مرتكبي الجرائم الإلكترونية الذين يقيمون في دولة أجنبية لا تربطها اتفاقية بالدولة التي نحقق فيها السلوك الإجرامي أو جزء منه، على اعتبار أن هذه الجرائم هي جرائم عابرة للحدود بسبب ما توفره شبكة الانترنت من حرية الإبحار في هذا العالم الافتراضي دون قيود أو حدود.

على ضوء الاعتبارات السابقة، يمكن القول بأن الجرائم الإلكترونية لها طبيعة خاصة، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود سواء ماتعلق بالجانب الموضوعي كتحديد أركان الجريمة بدقة واستحداث نصوص خاصة بها تتماشى وهذه الطبيعة، أو ما تعلق بإجراءات ملاحقة مرتكبها لأنها تتم في بيئة افتراضية يصعب معها تطبيق الإجراءات التقليدية كالتفتيش والحجز مثلا، وهذا ما عمل عليه المشرع الجزائري بمراعاته لهذه الطبيعة الخاصة أثناء سنه للنصوص القانونية المتعلقة بمكافحتها.

ثالثا: خصائص الجرائم الإلكترونية

نظرا للطبيعة المستحدثة للجرائم الإلكترونية فهي تنفرد بخصائص تميزها عن غيرها من الجرائم سواء بالنسبة للجريمة أو بالنسبة للمجرم الإلكتروني وهي في تصاعد مستمر نظرا لإساءة استدام تقنية المعلومات والفرص التي توفرها مثل: عدم إمكانية التعرف على شخصية المجرم الإلكتروني وقرصنة الأنظمة المعلوماتية وهذا ما سنتطرق إليه في الفرعين الآتيين.

1- السمات الخاصة بالجريمة الإلكترونية:

أدى ارتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الانترنت إلى إضفاء مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية، ويمكن إجمالها فيما يلي:

أ- الجريمة المعلوماتية عابرة للحدود:

إن الجريمة المعلوماتية لا تعترف بالقيود ولا بالحدود، فقد يكون الجاني في بلد بينما نتيجة الجريمة تكون في بلد آخر كما قد يمتد الضرر الحاصل إلى بلد ثالث أو أكثر في الوقت نفسه، فهذه الجريمة شكل من أشكال الجريمة العابرة للحدود ويستفيد مقترفوها من أثر التقنية في اختزال المسافات فهي جريمة عالمية إذ يمكن عن طريق الحاسب الآلي أو حتى هاتف نقال لشخص في الصين مثلا أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ضد شخص طبيعي أو معنوي في الو.م.أ أو العكس.(16)

ب- جريمة يصعب اكتشافها وإثباتها:

فيما يتعلق بصعوبة الكشف عن هوية الجاني، فهوية الجاني عادة ما تكون مخفية ساعة وقوع الجريمة وقد تبقى على تلك الحالة بعد وقوع الجريمة فضلا عن استعمال الجاني إما لحساب وهمي وإما من خلال اعتماده لبرنامج إلكتروني أو تطبيقه تسهل إخفاء هويته أو عنوانه أو المكان الذي ارتكبت من خلاله الجريمة، وعليه الهدف منه يسعى دائما إلى طمس معالم الجريمة كليا وذلك بمحو آثارها وأدلتها من الموقع الذي استعمله أو الوسيلة المستعملة لتحقيق غايته الإجرامية بصفة عامة وهو ما يجعل مسألة الكشف عنها أو إثباتها بالأمر شبه مستحيلاالا انه لايمكن اثبات الجريمة الالكترونية ومن الصعب جدا اثباتها نظرا لانهال اتترك اثرا حيث تعد مجرد ارقام يتم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها كما انها تفتقر للدليل المادي التقليدي كالبصمات مثلا.(17)

ج- ذاتية الجريمة المعلوماتية:

ذاتية الجريمة تبرز بوضوح في أسلوب ارتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر، وتقليد المفاتيح، كما هو الحال في جريمة السرقة وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الانترنت مع وجود مجرم يوظف

خبراته وقدراته على التعامل مع الشبكة، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغرير أو التغرير بالقاصرين، كل ذلك دون الحاجة لسفك الدماء.[18]

السمات الخاصة بالمجرم الإلكتروني2-

بالرجوع إلى تعريف الجريمة الإلكترونية بدلالة مرتكبها فهي: "قيام شخص ما مكنته معرفته واستخدامه لأجهزة الحاسوب والانترنت، أو معرفته لأحدهما من ارتكاب الجريمة المختارة، وانطلاقا من تفرد الجرائم الإلكترونية بخصائص عديدة، ينسحب ذلك أيضا على المجرم المعلوماتي الذي تتوفر فيه مميزات كالاحترافية، إضافة إلى الذكاء وعدم استعمال العنف.

أ- الاحترافية:

يتمت المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث يرتكبها بواسطة الكمبيوتر الأمر الذي يقتضي الخبرة والإدراك الواسعين والمهارة التقنية اللازمة لتحقيق أهدافه الإجرامية، إن المقصود بالمهارة في هذا المجال أن يكون المجرم على درجة من العلم والدراية في التعامل في مجال المعالجة الآلية للمعطيات، والتي قد يكتسبها من خلال الدراسة المخصصة أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، كاختراق نظم الكمبيوتر العائدة للشركات الصناعية والتجارية والقيام بعمليات[19] الاحتيال والتزوير عن طريق شبكة الانترنت بقصد تحقيق مكاسب مادية أو غيرها، كما تمكنهم احترافيتهم من التغلب على العقبات التي أوجدها المتخصصون في مجال البرمجيات لتوفير أنظمة لحماية الكمبيوتر من كافة أشكال القرصنة، كما في حالة البنوك والشركات والمؤسسات الصناعية والعسكرية.فهي تختلف عن الجريمة التقليدية كالقتل والسرقة فالجرائم الالكترونية لاتحتاج ادنى مجهود عضلي بل تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير او تعدل او تمحى من السجلات المخزنة في ذاكرة الحسابات

ب-الذكاء:

المجرم المعلوماتي ليس شخصية عادية، فهو يتصف بالذكاء وهو على قدر كبير من سرعة الفهم وسعة الإطلاع والنشاط الذهني المتقدم الذي يسعى إلى خداع الكمبيوتر وبرامجه، واستغلال شبكة الانترنت، فيستطيع التلاعب بالمعلومات أو الكيانات المنطقية للحاسوب كزرع فيروسات لنسخ البيانات أو تدميرها.[20]

ج- عدم استعمال العنف:

بمعنى أن المجرم لا يلجأ للمجهود العضلي كما في الجرائم التقليدية هي جرائم هادئة بطبيعتها (Soft

Crime) لا تحتاج للعنف، فهذه الجرائم تنتمي إلى إجرام الحيلة أو ما يعرف بجرام "الياقة البيضاء" كما يتمتع فيها المجرم بالتكيف الاجتماعي، أي لا يناصب أحد العداء كما أنه على درجة عالية من الثقافة.[21]

بين الأسطر: 1.0، المسافة البادئة للفقرات: 0.4 سم).

المحور الثاني: آليات مكافحة الجريمة الإلكترونية

سنحاول من خلال هذا المبحث بعد أن عرجنا في مبحث سابق إلى تحديد الإطار المفاهيمي والتشريعي للجريمة الإلكترونية توضيح آليات مكافحتها في التشريع الجزائري سواء كانت وفق القواعد العامة (أولا) أو وفق القواعد الخاصة (ثانيا).

أولا- آليات مكافحة الجريمة الإلكترونية وفق القواعد العامة

لم يبق المشرع الجزائري بمنأى عن التحولات الجارية في تكنولوجيا المعلومات وما صاحبها من أفعال مجرمة، فاستحدث نصوصا تجريمية للحد من الاعتداءات الصادرة ضد الأنظمة المعلوماتية، فقد تمم المشرع قانون العقوبات، الفصل الثالث من الباب الثاني من الكتاب الثالث بالقانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004، بقسم سابع مكرر 1 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" احتوى على أهم الجرائم التي تستهدف الأنظمة المعلوماتية، وذلك في المواد من 394 مكرر إلى 394 مكرر7، وضع من خلاله حماية فعالة لأنظمة المعالجة الآلية للمعطيات، فنص على مجموعة من الجرائم مقررا لها عقوبات مناسبة للحد من اقترافها، إلا انه تجدر الإشارة إلى أن المشرع الجزائري في هذا التعديل ركز على الاعتداءات الماسة بأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي وسنتطرق من خلال هذا المطلب إلى العقوبات الأصلية (الفرع الأول) والعقوبات التكميلية (الفرع الثاني).[22]

1- العقوبات الأصلية:

أ- العقوبات المقررة للشخص الطبيعي:

- عقوبة الدخول والبقاء غير المشروعان: (الصورة البسيطة للجريمة):

- عقوبة الدخول غير المرخص l'intrusion: يقصد بفعل الدخول هو ذلك الركن المادي لجريمة الاعتداء على نظام المعالجة الآلية للمعطيات أي بمعنى أخرى دخول معنوي أو إلكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا يعد فعل الدخول بحد ذاته سلوكا غير مشروع وإنما

يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص.[23] وهو ما يستشف من المادة 394 من قانون العقوبات الجزائري التي تنص على: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عم طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

ويلاحظ من خلال هذه المادة أن المشرع الجزائري اعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها تحقق مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بأكمله أو إلى جزء منه فقط، شرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو عن طريق الخطأ. كما لا تشترط المادة 394 مكرر لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق كالتشفير مثلا، بل جاءت عامة ومطلقة، أي تحمي كل الأنظمة المعلوماتية من الاعتداء سواء كانت محمية فنيا أم لا.

- **البقاء غير المرخص maintient:** ويقصد به حالات التواجد غير المصرح به في النظام المعلوماتي كربط الاتصال والإطلاع على البيانات أو القيام بعملية مختلفة أو هو: " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذه النظام"، كما يتسع فعل البقاء ليشمل أكثر من الوقت المحدد وذلك بقصد عدم أداء إتاوة، وعليه يجرم فعل البقاء حتى لو حصل بصفة عرضية. قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام كما قد يجتمعان. ويكون البقاء معاقب عليه استقلالا حينما يكون الدخول إلى النظام مشروعا مثل الدخول إلى النظام صدفة أو عن طريق الخطأ أو السهو، فهذه الصورة تحقق السلوك المجرم لفعل البقاء، وهي من جرائم النشاط الإيجابي الذي يتحقق بالامتناع أو الترك فيجب على الجاني في هذه الحالة قطع الاتصال الذي تحقق عن طريق الخطأ والانسحاب فورا.[24]

ويكون البقاء جريمة أيضا إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا فيه الرؤية والإطلاع فقط. وقد يجتمع الدخول غير المشروع والبقاء غر المشروع معا. حينما لا يكون للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة صاحبه.

اعتبر المشرع الجزائري على غرار المشرع الفرنسي البقاء غير المرخص به في نظام المعالجة الآلية للمعطيات جريمة مثلها مثل جريمة الدخول غير المرخص به وذلك بموجب المادة 394 مكرر من قانون العقوبات وحدد لهاتين الجريمتين نفس العقوبة وهي الحبس من 3 أشهر إلى سنة وغرامة مالية من 50000 دج إلى 100000 دج.[25]

- **الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات:**

تنص المادة 394 مكرر 3/2 ق.ع.ج على: " ... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) وغرامة من 50000 دج إلى 150000 دج.

وعليه تتحقق هذه الصورة عندما ينتج عن فعل الدخول أو البقاء إما حذف (محو) أو تغيير (تعديل) المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه، ففعل الحذف يشير إلى إزالة المعطيات داخل النظام، وهو أقصى أنواع الضرر مما جعل العقاب عليه مشددا، أما فعل التغيير هو إحداث تعديلات فحسب في المعطيات دون أن يصل الأمر إلى حد إزالتها، بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة أو لها معنى لكنه مغاير لما كانت عليه قبل التغيير. أما تخريب النظام فيقصد به كل فعل من شأنه جعل النظام مصابا بالشلل أو العجز وذلك باستعمال تقنيات كثيرة منها: برامج الفيروسات كبرنامج حصان طروادة والقنبلة الموقوتة وبرنامج الدودة، أو باستعمال [26] تقنية التشبع (Saturation)، أو باستعمال تقنية الفخ (trappe).

ولتوفر هذه الظروف المشددة، لا بد من وجود علاقة سببية بين الدول أو البقاء غير المشروع وتلك النتيجة الضارة، إلا إذا أثبت الجاني انتفاء تلك العلاقة أو أن حذف أو تغيير المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة ذاو الحادث المفاجئ فحينئذ يعاقب على أساس الصورة البسيطة لفعل الدخول أو البقاء.

ب: <u>العقوبات المقررة للشخص المعنوي:</u>

أقر المشرع الجزائري مبدأ مساءلة الشخص المعنوي في القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004، وذلك بموجب المادة 51 مكرر منه، كما حدد ثلاثة شروط لإمكانية مساءلة الشخص المعنوي جنائيا وتتمثل هذه الأخيرة في:

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا.
- أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي.
- أن ترتكب الجريمة لحساب الشخص المعنوي.

كما نصت المادة 18 مكرر من نفس القانون على: " العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات هي:

- الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة

واحدة أو أكثر من العقوبات التكميلية الأتية:

- حل الشخص المعنوي،

- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات،

- الاقصاء من الصفقات العمومية لمدة لاتتجاوز 5سنوات

- المنع من مزاولة نشاط أو عدة أنشطة معنية أو اجتماعية شكل مباشر أو غير مباشر نهائيا، أو لمدة 5 سنوات،

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها

- نشر وتعليق حكم الإدانة

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.[27]

2- **العقوبات التكميلية:**

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية يحكم بها إلى جانب العقوبات الأصلية وهي كالآتي:

- **المصادرة:** وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام، وذلك ببيعها أو حجزها مع مراعاة الغير حسن النية.

- **إغلاق المواقع:** إغلاق مواقع الانترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لارتكاب هذه الجرائم أو ساهمت في ارتكابها.

- **إغلاق المحل (المقهى الإلكتروني):** يكون في الحالة التي يكون فيها صاحب المحل مشاركا في الجريمة، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم،

ومن الملاحظ أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة، كما اشتملت على عقوبات تكميلية، وحتى عقوبات الشخص المعنوي.[28]

ثانيا- آليات مكافحة الجريمة الإلكترونية وفق القواعد الخاصة:

بالرغم من تبني المشرع نصوصا تشريعية حديثة لحماية المكونات المعنوية للنظام المعلوماتي إلا أنه لم يوفق بالإحاطة الشاملة لكل الجرائم المعلوماتية مثل جريمة التزوير المعلوماتي التي تكتسي أهمية خاص مع انتشار ثقافة استخدام الكمبيوتر فيما بين الأفراد بالإضافة إلى هذا يعاب كذلك على المشرع أنه بالرغم من وضعه لنصوص عقابية رادعة ووقائية إلا أنها تبقى غير قابلة للتطبيق كونها تحتاج إلى نصوص إجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية من خصوصية تختلف عن باقي الجرائم، وهو ما دفع المشرع إلى إصدار مجموعة من القوانين الخاصة لمواجهة الجريمة المعلوماتية.(29)

1- القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

يتميز القانون 09- 04 المؤرخ في 5 أوت 2009بأنه الإطار القانوني الأكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام والاتصال لاسيما الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، باستقراء فحوى هذا القانون يتبن لنا أن المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للتصدي لجرائم المعلوماتية، تتمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة، والتدخل السريع لتحديد مصدرها ورصد مرتكبيها

يعتبر القانون رقم 09- 04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الانترنت وعلى كل تقنية تظهر مستقبلا

وقد أورد المشرع في المادة 2 من القانون رقم 09- 04 أنه يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

كما تضمن القانون المذكور في الفصل الرابع منه القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في المادتين 10 و11، على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبحفظ المعطيات المتعلقة بحركة السير ووضعها تحت تصرف السلطات المذكورة.(30)

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير، مع الإشارة إلى قيام المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50000 دج إلى 500000دج، ويعاقب

الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.[31]

2- **القواعد الخاصة المتعلقة بحقوق المؤلف والحقوق المجاورة:**

أدت القفزة الرقمية التي حدثت في العالم إلى إحداث أثر بالغ على كافة جوانب الحياة وكان لها أثر بالغ على الملكية الفكرية خاصة في مجال حقوق المؤلف حيث أصبح نشر وتوزيع وعرض المصنفات غاية في السهولة والإتقان وبأقل التكاليف بظهور الحاسبات الآلية، مما أدى إلى مسايرة هذه التطورات لظهور ما يسمى بالملكية الرقمية والتي تشمل حقوق الملكية الفكرية على الانترنت والتي مضمونها يشمل كل مصنف إبداعي ينتمي إلى بيئة تقنية المعلومات يعد مصنفا رقميا.[32]

ولهذا سارع المشرع الجزائري على غرار التشريعات الأخرى إلى حماية هذه المصنفات بتطويع النصوص التقليدية الخاصة لحماية الملكية الفكرية الذي قام بإخضاع حماية المال المعلوماتي (برامج الحاسب الآلية) لقوانين الملكية الفكرية، حيث اعتبر برامج الحاسوب الآلي ضمن المصنفات الأدبية والفنية بموجب المادة 04 من الأمر رقم 03- 05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة والتي تنص على أنه تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:

أ- المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية والبحوث العلمية والتقنية، والروايات والقصص، والقصائد الشعرية، وبرامج الحاسوب.[33]

- ارتكاب جنحة التقليدية عن طريق الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان أو عازف، استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة، استيراد أو تصدير نسخ مقلدة من مصنف أو أداء، بيع نسخ مقلدة لمصنف أو أداء، تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء المادة 151 من الأمر 03- 05.

- ارتكاب جنحة التقليد عن طريق انتهاك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق أي منظومة معالجة معلوماتية (المادة 152) من نفس الأمر.

- الاشتراك بالعمل أو بالوسائل الحائز عليها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة (المادة 154 من نفس الأمر).

أما بالنسبة للعقوبات المقررة على مختلف هذه الاعتداءات فقد تضمنتها المواد 153، 156، 157، 158، 159 من الأمر السالف الذكر وتتمثل العقوبة لمرتكب جنحة التقليد لمصنف أو أداء فني كما هو وارد في المادتين 151 و152 من ذات الأمر بالحبس من 6 أشهر إلى ثلاثة سنوات، وبغرامة من خمسمائة آلاف 500000 دج إلى مليون دينار جزائري (1000000 دج)، سواء كان

النشر قد حصل في الجزائر أو خارجها طبقا للمادة 153 من نفس الأمر.

كما نصت المادة 154 من نفس الأمر على معاقبة الشريك في ارتكاب جريمة التقليد سواء سواء بأعماله أم بالوسائل التي يحوزها للمساس بحقوق المؤلف بنفس العقوبات المقررة في المادة 153 من الأمر السالف الذكر ونفس الشيء بالنسبة لكل من يمتنع عن دفع المكافأة المستحقة للمؤلف (المادة 155) من ذات الأمر.

وقد شدد المشرع العقوبة في حالة العود إلى ضعف العقوبة المقدرة في المادة 153 من الأمر 03-05 المشار إليه سابقا طبقا للمادة 156 من نفس الأمر.[34]

بالإضافة إلى هذه العقوبات الأصلية قرر المشرع كذلك لهذه الجرائم العقوبات التكميلية التي تتمثل في الغلق المؤقت لمؤسسة يستغلها المقلد أو شريكه، فالمصادرة سواء المصادرة المبالغ التي تمثل الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي طبقا للمادة 157 من الأمر 03-05، وكذلك نشر حكم الإدانة وفقا لأحكام المادة 158 من نفس الأمر.

خاتمة:

مما سبق يمكننا القول أن الجريمة الإلكترونية هي من أخطر الجرائم على المستوى العالمي، وذلك راجع إلى سوء استخدام التكنولوجيا والانترنت مما ساعد مجرمون أذكياء على اقترافها بواسطة وسائل وأدوات المعرفة التقنية وهذا ما يميزها على الجريمة التقليدية، لأن الجريمة الالكترونية في تطور مستمر ودون توقف وخاصة مع استخدام الكثير لمواقع التواصل الاجتماعي ومن خلال التطرق إلى تعريف الجريمة الإلكترونية وتبيان خصائصها، والإجراءات اللازمة للتصدي لها يمكننا التوصل إلى مجموعة من النتائج، نجملها وفقا لما يلي:

1- خصوصية الجريمة الإلكترونية عن الجرائم التقليدية وهذا راجع إلى التطور التكنولوجي على مستوى الإعلام والاتصال مما ساعد المجرمين على ارتكاب مثل هذه الجرائم المستحدثة.

2- نقص الخبرة والرقابة لدى العاملين في قطاع أمن المعلومات يتسبب في انتشار رهيب للجرائم الإلكترونية.

3- عدم وجود تعاون دولي للقضاء على الجرائم الإلكترونية والتصدي لها وردع مرتبطيها.

4- سوء استخدام التكنولوجيا على المستوى العالمي هو الأمر الذي انعكس بصفة سلبية على الأفراد وأدى إلى ظهور الجرائم الإلكترونية خاصة مع توفر الآليات والوسائل التقنية وذكاء واحترافية

مرتكبيها.

5- إن هذه الجريمة مع تعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه، فإنها تهدد أمن وسلامة الفرد والمجتمع، وهي تتسم بالغموض، حيث يصعب الكشف عنها وإثباتها والتحقيق فيها، مما يضع مسؤولية كبيرة من خلال هذه النتائج نتوصل إلى جملة من الاقتراحات نجملها كما يلي:

- لا يكفي مواكبة المشرع العقابي الجزائري لنصوص تشريعات المقارنة بدون تجسيدها من الناحية التطبيقية والاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة، مع توفير كافة الوسائل المادية والتقنية اللازمة لأداء عملها ومهامها على أحسن صورة.

- ضرورة تشديد الوصف الجنائي والعقوبات المقررة لتحقيق فكرة الردع وترسيخها على المجرمين.

- خلق سياسة توعوية تثقيفية لإعلام مرتكبيها بخطورة الجريمة والعقوبة المقررة لها، لأن التصريح بخطورتها يساعد على مكافحة الجريمة.

- ضرورة توفير الآليات والوسائل اللازمة لفرض الرقابة القضائية للتصدي للجريمة.

- العمل على إعادة النظر في المناهج الدراسية بالجامعات، وضرورة تضمينها مادة علمية عن الحاسب الآلي والشبكات المعلوماتية وكيفية التعامل مع الأجهزة الإلكترونية.

الهوامش:

(1)- سمير شعبان، الجريمة الإلكترونية: مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة الدراسات والأبحاث، العدد 01 سبتمبر «2009»، جامعة باتنة، ص 114.

(2)- راضية عميور، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، سنة 2022، ص92.

(3)- سمير شعبان، المرجع السابق، ص114.

(4)- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات، قانون الإجراءات الجزائية قوانين خاصة، دار الجامعة الجديدة، مصر، ص 48.

(5)- يزيد بوحليط، المرجع السابق، ص 49- 50.

(6)- مونة مقلاتني وراضية مشري، الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، جوان 2021. ص2.

(7)- الأمر 04- 15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66- 156 الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج.ر العدد 71.

(8)- مقلاتني مونة وراضية مشري، المرجع السابق، ص 2- 3.
(9)- انظر المادة 2 من الأمر 09- 04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر العدد 47.
(10)- يزيد بوحليط، المرجع السابق، ص 52- 53.
(11)- مقلاتني مونة وراضية مشري، المرجع السابق، ص 15.
(12)- يزيد بوحليط، المرجع السابق، ص 74.
(13)- يزيد بوحليط، المرجع السابق، 75.
(14)- انظر المادة 350 ف 2 من القانون 04- 15، السالف الذكر.
(15)- عبد الهادي بن زيطة، حمية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر ط 1، 2007، ص 12.
(16)- بن ملك إسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلةالبيان للدراسات القانونية والسياسة، عدد 01، 2019، ص: 116.
(17)- رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 01، 2018، ص 441.
(18)- نعيمة داودي، الجريمة الإلكترونية (خصائصها ومجلات استخدامها وأهم سبل مكافحتها، مجلة محمد اللغات، المجلد 02، العدد 01، 2020، ص 49.
(19)- يزيد بوحليط، المرجع السابق، ص 85.
(20)- رحموني محمد، المرجع السابق، ص 88.
(21)- زيد بوحليط، المرجع السابق، ص 88.
(22)- انظر المادة 394 مكرر 7 من القانون 04- 15، السالف الذكر.
(23)- راضية عميور، المرجع السابق، ص 99.
(24)- راضية عميور، المرجع السابق، ص 100.
(25)- انظر المادة 394 مكرر من القانون 04- 15 السالف الذكر.
(26)- انظر نص المادة 394 الفقرو 2 و3 من القانون 04- 15، السالف الذكر
(27)- انظر المادة 51 من القانون 04- 15، سالف الذكر.
(28)- أنظر المادة 394 مكرر 06 من القانون 04- 15 السالف الذكر.
(29)- راضية عميور، المرجع السايق، ص 104.
(30)- انظر المادة 2 و10 و11 من الأمر 09- 04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 47.
(31)- انظر المادة 394 مكرر من القانون رقم 04- 15 السالف الذكر.
(32)- راضية عميور، المرجع السابق، ص 103.
(33)- الأمر رقم 03- 05، المؤرخ في 19 جمادى الأولى عام 1424، الموافق لـ 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر العدد 44.
(34)- انظر المادة 151- 152- 153- 156 -157- 158-159- من الأمر 03- 05 السالف الذكر.