مجلة الدراسات القانونية المقارنة

EISSN:2600-6154 المجلد 07/ العـــدد01 (2021)، ص.ص. 2526-2543 ISSN:2478-0022

الإطار المفاهيمي للجريمة المعلوماتية

Conceptual Framework For Cyber Crime

صليحة بوجادي

Saliha Boudjadi

أستاذة محاضرة "ب"، جامعة محمد البشير الإبراهيمي برج بوعريريج

Lecture Professor B, MuhamedElBachir El Ibrahimi University, BBA.

saliha.boudjadi@univ-bba.dz

تاريخ إرسال المقال:2020/12/02 تاريخ القبول:2021/04/10 تاريخ النشر:2021/06/28

ملخص:

تعد الجريمة المعلوماتية من الجرائم المستحدثة في الوقت الراهن التي ظهرت كرد فعل متوقع للتطور السريع الحاصل في مجال الثورة التكنولوجية والمعلوماتية التي عهدنا أنها تعمل على تغيير مجالات الحياة إلى الأفضل فقط، وتهدف هذه الدراسة إلى بيان ماهية الجريمة المعلوماتية من حيث تعريفها وتبيان خصائصها والسمات التي تكتسي مجرمها المعلوماتي. ويعد الإلمام بهذه الجريمة أمرا مهما كونها تنتشر بسرعة الوسيلة المستعملة فيها(الانترنت)، لذا وجب فهمها واستيعاب كيفية حدوثها، حتى يتسنى لنا فيما بعد التوصل إلى مجرميها والتصدي لهم.

وقد خلصت الدراسة إلى عدم وجود مصطلح قانوني موحد للدلالة على هذه الجريمة إلا أن بعضها يفضل تسميتها بالجريمة المعلوماتية أو "الجريمة الالكترونية"، كما قد اختلف الفقهاء في تعريفها بين موسع ومضيق. وانتهت الدراسة بضرورة تدخل المشرع الجزائري لأجل العمل على تعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية والتي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.

كلمات مفتاحية:

جريمة معلوماتية، جريمة الكترونية، مفهوم، قانون، مشرع جزائري.

Abstract:

Cyber Crime is one of the modern crimes nowadays. It came as a feedback to the very development in Technology that did huge good changes to the world. Therefore this research paper was submitted to deal with the definition of Cyber Crime from the perception of its meaning, its characteristics, and the features of the cyber criminal. It is important to learn about this crime for it will help to understand it, and how it happens. Thus, we can reach the criminal, and stop them.

المؤلف المرسل: د/ بوجادي صليحة Email : saliha.boudjadi@univ-bba.dz

Through out this paper, It is by any means not oblivious that there were not a united legal term for this crime in the Arabic language, thus countries. Despite that fact, there were many definitions to it.To conclude,it is important tomake new legal efforts to enhance the Algerian Law acts to contain the modern version of crimes including cyber crimes.

Keywords:
Cyber crimes; Laws; Definition; Modern crimes.

مقدمة:

عرف العالم في السنوات الأخيرة تطورا مذهلا في تكنولوجيا الإعلام والاتصال، وذلك بسبب ظهور الانترنت والمواقع الالكترونية المختلفة كمواقع التواصل الاجتماعي وكذا التزايد المستمر في استخدام الحاسب الآلي وغير ذلك... فبالرغم من الإيجابيات التي تكتسي الثورة المعلوماتية وقدرتها على تغيير أوجه الحياة للأحسن والأفضل إلا أنها تحمل في طياتها العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسوب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجية المعلومات، مما أدى إلى ظهور نوع جديد من الجرائم الخطيرة التي تعرف بـ"الجرائم المعلوماتية" أو "الجرائم الالكترونية"، وتعتبر كنتيجة حتمية للانفتاح على العالم ولكل تقدم علمي أو تقني مستحدث.

وقد بدأت في الانتشار بشكل واسع حتى أنها تخطت في بعض الأحيان حدود الدول، إذ أضحت ظاهرة عالمية تهدد كيان المجتمعات نظرا لخطورتها.

لذلك فإن الإشكالية المطروحة في هذه الدراسة هي: ما هي الجريمة المعلوماتية؟ و للإجابة عن هذه الإشكالية وما يتعلق بها، انتهجت المنهج الوصفي والتحليلي حيث عمدت إلى جمع المعلومات المتعلقة بهذه الظاهرة "الجريمة المعلوماتية" ثم تحليلها وفقا للخطة الآتية:

أولا: تعريف الجريمة المعلوماتية والطبيعة القانونية لها

ثانيا: خصائص الجريمة المعلوماتية وأنواعها

ثانيا: صفات المجرم المعلوماتي وأنماطه

أولا: تعريف الجريمة المعلوماتية والطبيعة القانونية لها

1- تعريف الجريمة المعلوماتية

تتكون عبارة الجريمة المعلوماتية من مقطعين هما: الجريمة والمعلوماتية؛ حيث يستخدم مصطلح **الجريمة** للتعبير عن السلوكيات و الأفعال الخارجة عن القانون.

أما مصطلح **المعلوماتية** أو ما يسمى أيضا بـ**علم المعلومات**: هو ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها وتخزينها واسترجاعها وتغييرها وكذا تحويلها واستخدامها[1].

كما يهتم هذا العلم بدراسة أساليب معالجة المعلومات كالأنظمة المعلوماتية ونظم البرمجة، وبهذا المفهوم تعتبر المعلوماتية علما متصلا بالعديد من العلوم الأخرى.

إذن مفهوم المعلوماتية يقوم أساسا على "العلاقة بين المعلومات وبين التقنية الحديثة التي تستخدم في معالجة هذه المعلومات"[2].

و لعل أهم مشكل يصادفنا في تعريف الجريمة المعلوماتية هو عدم وجود مصطلح قانوني موحد للدلالة على هذه العبارة " الجريمة المعلوماتية"؛ وهو اختلاف رافق مسيرة النشأة والتطور اللامتناهي لظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات.

إذ أن هناك من يطلق عليها مصطلح جرائم الكمبيوتر، إلى جرائم الهاكرز أو الاختراقات فجرائم الانترنت وأخيرا السيبركرايم[3].

كما يطلق عليها أيضا مصطلح الغش المعلوماتي أو الاحتيال المعلوماتي، والبعض الآخر يطلق عليها الاختلاس المعلوماتي أو جرائم الحسابات أو حتى الجريمة الالكترونية وهي الأكثر شيوعا. وآخرون يفضلون تسميتها بالجريمة المعلوماتية[4].

كما يتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية، وبناء على ذلك تعرّف الجرائم الالكترونية على أنها: " الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال"[5]، أي الجرائم التي ترتكب بأساليب ووسائل الكترونية وآليات الاتصال عن بعد télécommunicationمن التلفون والفاكس والحاسوب وغيرها.

وقد تعددت التعريفات الفقهية للجريمة المعلوماتية أو كما تسمى جرائم الحاسبات الالكترونية لارتباطها بنظم المعالجة الآلية للمعطيات، وتباينت هذه التعريفات فيما بينها بين موسع ومضيق، وقد أسفر ذلك عن تعذر إيجاد مفهوم مشترك لظاهرة الجريمة المعلوماتية.

أ- أنصار الاتجاه الضيق لمفهوم الجريمة المعلوماتية

وضع أنصار هذا الاتجاه عدّة تعريفات للجريمة المعلوماتية، تختلف عن بعضها البعض من حيث المعيار المعتمد، ومن بين هذه التعريفات: أن الجريمة المعلوماتية هي" كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية ولملاحقته من ناحية أخرى"[6]. فقد أخذ هذا التعريف بمعيار وسيلة ارتكاب هذه الجريمة ألا وهي الكومبيوتر معتبرا إياها بأنها فعل غير مشروع. كما عرفت بأنها "هي التي تقع على جهاز الكومبيوتر أو داخل نظامه فقط"[7]. كذلك اعتمد هذا التعريف على معيار وسيلة الارتكاب وهي الكومبيوتر. وعرفها الفقيه الألماني تيدمان بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[8]. وعرفها الأستاذ جون فورستر بأنها:" فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية "[9]. إذن تشترك هذه التعريفات جميعها التي تخص الجريمة المعلوماتية في المعيار المعتمد ألا وهو وسيلة ارتكابها المتمثلة في "الكومبيوتر".

أما البعض الآخر من أنصار هذا الاتجاه فقد أخذ بمعيار النتيجة، ومن ذلك تعريف الأستاذ الفرنسي ماس للجريمة المعلوماتية بأنها " تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[10]. بيّن هذا التعريف أن الغاية من الجريمة المعلوماتية مادية وهي تحقيق الربح، وبذلك يكون قد ركز على معيار النتيجة.

كما عرفها الفقيه روزملات على أنها: " نشاط غير مشروع موجه للنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحل عن طريقه"[11]. فقد أخذ هذا التعريف بمعيارين: معيار موضوع الجريمة ألا وهو محاولة الوصول إلى المعلومات بطريقة غير مشروعة، وكذا معيار وسيلة ارتكاب هذه الجريمة ألا وهي الحاسوب.

كما عرفت بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب"، وقريبا من ذلك عُرّفت بأنها: " أي فعل غير مشروع تكون المعرفة بتقنية أساسية لمرتكبه"[12].

يتضح من هذين التعريفين أن الجريمة المعلوماتية جريمة مرتبطة بالمعرفة الفينة أو التقنية باستخدام الحاسب الآلي.

إن الشيء الملاحظ على هذه التعريفات الفقهية لأنصار الاتجاه الضيق لمفهوم الجريمة المعلوماتية:

– أنه حصر الجريمة في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وهو إن تحقق في بعض الأحوال فقد لا تتوفر في كثير منها، إذ قد يرتكب الفعل غير المشروع في البيئة الرقمية دون أن يكون فاعله بحاجة إلى هذا القدر من المعرفة،و رغم ذلك فإنه لا يمكن إنكار أن هذه الأفعال تدخل في عداد جرائم المعلوماتية. فالقيام مثلا بإتلاف البيانات المخزنة داخل نظام الكومبيوتر لا يتطلب من فاعله قدرا كبيرا من العلم بتكنولوجيا الحاسبات الآلية؛ وعلى الرغم من ذلك فقد جرمته الكثير من التشريعات العقابية.

– أنها جاءت قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي؛ فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة، و البعض الآخر ركز على وسيلة ارتكابها، أما البعض الآخر فقد ركز على معيار النتيجة.

ب– أنصار الاتجاه الموسع لمفهوم الجريمة المعلوماتية

نظرا للانتقادات التي وجهت للاتجاه الأول المضيق لتعريف الجريمة المعلوماتية، حاول بعض الفقه تعريفها على نحو أوسع من الأول؛ تفاديا لأوجه القصور التي شابت تعريفات الاتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

لقد تباينت مواقف أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية بحسب المعايير التي اعتمد عليها كل فريق في تعريفها، و بحسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية، فتجدهم يعرفونها بأنها " كل سلوك إجرامي يتم بمساعدة الكومبيوتر". أو هي " كل جريمة تتم في محيط أجهزة الكومبيوتر"[13]. يستشف من هذين التعريفين أن الجريمة المعلوماتية في نظر هذا الاتجاه هي كل سلوك إجرامي يتم بمجرد مشاركة الكومبيوتر له، معتمدان في تعريفها على معيار وسيلة الارتكاب.

ويعرفها البعض الآخر بأنها " كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية أو المعنوية"[14]، وقد جاء هذا التعريف موافقا للتعريف الذي جاءت به منظمة التعاون الاقتصادي و التنمية في أوروبا التي عرّفت الجريمة المعلوماتية بأنها " كل فعل أو امتناع عن فعل من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[15]. أضاف هذا

التعريف الهدف من الجريمة المعلوماتية والمتمثل في الاعتداء على الأموال المادية أو المعنوية سواء أكان ذلك بطريق مباشر أو غير مباشر.

وعرفها الفقيه ستين سكيولبيرغ على أنها: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه و التحقق فيه و ملاحقته قضائيا"[16]. اشترط هذا التعريف أن يكون مرتكب الجريمة المعلوماتية على قدر كبير من المعرفة بتقنية المعلومات، وبالتالي يستحق جزاءه وهو الملاحقة القضائية.

مما سبق يتضح أن هذا الاتجاه قد توسع كثيرا في مفهوم الجريمة المعلوماتية؛ حيث بمجرد مشاركة الحاسب الآلي في النشاط الإجرامي بصفة مباشرة أو غير مباشرة يصبغ عليه وصف الجريمة المعلوماتية.

أما التعريف الدولي للجريمة المعلوماتية فهو يعتمد في الغالب على الغرض من استخدام المصطلح؛ فهناك عدد محدود من الأفعال التي تمس السرية و النزاهة و بيانات الكمبيوتر و أنظمة تمثل جوهر الجريمة الالكترونية، كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر[17].

ج- موقف المشرع الجزائري من تعريف الجريمة المعلوماتية

تبنى المشرع الجزائري حديثا للدلالة على الجريمة المعلوماتية مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"[18]. إذ اعتبر أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية "محلا للجريمة"، و يمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لا بد من تحققه حتى يمكن توافر أركان الجريمة. وبالرجوع إلى قانون العقوبات الجزائري نجده لم يعرف جرائم الانترنت بل اكتفى بالعقاب على بعض الأفعال تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات" وذلك في المواد: من المادة 394 مكرر إلى المادة 394 مكرر 7 منه.

وبذلك يكون المشرع الجزائري قد أعطى تعريفا موسعا للجرائم المعلوماتية في القانون رقم 04/09 معتبرا إياها أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات -المواد المشار إليها سابقا- "أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية".

بذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء فقط، بل توسع نطاقها لتشمل إضافة إلى ذلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.

ويجب التنويه هنا إلى أن المشرع الجزائري قد تطرق أيضا للجرائم الالكترونية والعقوبات المقررة لها من خلال قانون التجارة الالكترونية رقم 05/18،[19] وذلك في الفصل الثاني من الباب الثالث منه تحت عنوان "الجرائم والعقوبات، وشملتها المواد من 37 إلى 48، غير أن هذا القانون لم يتطرق لتعريف الجريمة الالكترونية.

و عليه يتبين مما سبق:

- أنّ المشرع الجزائري قد اعتمد على عدة معايير للدلالة على الجريمة الإلكترونية كمعيار وسيلة ارتكاب الجريمة من جهة وهو نظام الاتصالات الإلكتروني، ومن جهة ثانية معيار موضوع الجريمة ألا وهو المساس بأنظمة المعالجة الآلية

للمعطيات، أما المعيار الثالث فهو القانون واجب التطبيق أو الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات. كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية باعتبار أنها ترتكب في نظام معلوماتي أو نظام الاتصالات الالكترونية[20].

– إن نص المادة 2 من القانون رقم 04/09 –السابق ذكرها– غير كاف وحده لتجريم الأفعال التي ترتكب بواسطة المنظومة المعلوماتية و يسهل ارتكابها عن طريق هذه المنظومة، طالما أنه لا توجد نصوص قانونية موضوعية تجرّم كل فعل بعينه و تحدد أركانه و العقوبة المقررة له، وهو الأمر الذي يخالف مبدأ شرعية التجريم والعقاب، فعبارة "أي جريمة أخرى" التي استعملها المشرع الجزائري في المادة 2 من القانون رقم 04/09 يعتقد أنه لا يمكن القياس عليها لمتابعة أي شخص جزائيا حتى لو ارتكب جريمة تقليدية بواسطة منظومة معلوماتية في ظل غياب النص الجزائي الذي يجرّم هذا الفعل إذا ارتكب بواسطة منظومة معلوماتية صراحة.

– يستحسن بالمشرع الجزائري أن يعمل على تعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية التي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.

2– الطبيعة القانونية الخاصة للجريمة المعلوماتية

تقوم الجرائم المعلوماتية على تقنية المعلومات و ترتبط بها، وهذا ما أكسبها طابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية. فإذا كانت الجريمة بصفة عامة محل تطبيق القانون الجنائي، فإن الطبيعة المتميزة للجريمة المعلوماتية تتعلق غالبا بما يسمى بالقانون الجنائي المعلوماتي[21]. ومن ثم فإن للجريمة المعلوماتية طبيعة قانونية خاصة تكمن في الخصائص التي تتميز بها هذه الجريمة من جهة، وبخصوصية المحل الذي يقع عليه الاعتداء في ارتكاب هذه الجريمة المعلوماتية.

و للإشارة فإن الجريمة المعلوماتية كأي جريمة أخرى لها أركانها، و التي تتمثل في: الركن المادي، الركن المعنوي، والركن الشرعي. و يقصد بالركن المادي سوء استخدام الجرائم الأنظمة الالكترونية بطريقة غير مشروعة، واقتحام آثار مادية ملموسة تساهم في التدمير للمعلومات، أو السرقة لبطاقات الائتمان أو التزوير والتلاعب في البيانات المرتبطة بالحواسب الآلية. أما الركن المعنوي فهو الحالة النفسية والمزاجية لمرتكبي الجرائم الإلكترونية، مع أهمية التركيز على العلاقات التي تكون مرتبطة ما بين ماديات الجريمة وشخصية الجاني. و يبقى الركن الشرعي الذي يمثل الصفات غير المشروعة للفعل، حيث يكون هنالك قاعدة تجريم وعقوبات مفروضة على الجرائم الإلكترونية المرتبطة بأنظمة المعلومات.

و عليه فإن عدم وجود مفهوم مشترك للجريمة المعلوماتية هو موطن ضعف و نقص، حبذا لو تم تداركه لأن مشروعية الفعل من عدمه تنطلق من فكرة تحديد مفهوم له.

ثانيا: خصائص الجريمة المعلوماتية وأنواعها

1– خصائص الجريمة المعلوماتية

ترتبط الجريمة المعلوماتية ارتباطا كاملا بجهاز الكمبيوتر وشبكة الانترنت، هذا ما ميزها عن الجريمة التقليدية بمجموعة من الخصائص و السمات أهمها:

أ- محل الجريمة

تعد الجرائم المعلوماتية جرائم افتراضية لا تحدث على ارض الواقع و رغم هذا فإن نتائجها تظهر فيه، حيث تستهدف معنويات لا ماديات، فالجريمة المعلوماتية تستهدف المعلومات، وهي أشياء معنوية غير محسوسة.[22]

ب- جريمة عابرة للحدود

لقد ساهمت شبكة الاتصالات ومالها من وسائل كالأقمار الصناعية و الفضائيات و الإنترنت في انتشار الثقافة وعولمتها، كما كان لها يد – ولو عن غير قصد- في انتشار الجريمة و بثها عالميا دون قيود الحدود الإقليمية للدول، وكذا المكان والزمان، وأصبح العالم ككل ساحتها التي تمارس فيها شتى نشاطاتها.

إن أغلب الجرائم الالكترونية يختلف فيها الجاني والمجني عليه في مقر السكن، فنجد مثلا الجاني من روسيا والمجني عليه مواطن أمريكي؛ وفي هذا حماية للجاني نظرا لكونه جارح إقليم المجني عليه، ما يعني تعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف الاجتماعي والنظام الأخلاقي والسياسي للدولة[23]، وهذا يعني وجود تعقيدات بخصوص الملاحقة القضائية. ومن أمثلة هذه الخاصية قضية عرفت باسم مرض فقدان المناعة المكتسبة "الإيدز" المرتكبة من قبل الأمريكي جوزيف بيب، و الذي قام بإرسال فيروس إلى أشخاص من المملكة المتحدة. وقد ألقي القبض عليه في أوهايو وعُرِض أما القضاء الإنجليزي الذي أطلق سراحه نظرا لتدهور حالته العقلية.

وعليه فإن هذه الحماية غير المقصودة تستدعي ضرورة التعاون الدولي لمواجهة هته الجرائم ووضع المجرمين عند حدهم أسوة بأنواع الجرائم العابرة للحدود الأخرى من تهريب للرق والمخدرات. ومثل هذه الجرائم أيضا يمكن ارتكابها في البيئة الرقمية.

ج- صعوبة اكتشاف الجريمة المعلوماتية

إن إحدى أهم مميزات الجريمة المعلوماتية وأكثر ما يجعلها جريمة محنكة هي صعوبة اكتشافها باعتبارها نادرا ما يتم الكشف عنها ولو حدث الكشف فإنه يعد صدفة بحتة. والسبب وراء اكتشافها عادة يرجع إلى تمييزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف، كما أنها لا تترك أثرا خارجيا ملموسا أو مرئيا[24].

وليس من العسير بحكم توافر المعرفة و الخبرة في مجال الكمبيوترات غالبا لدى مرتكبها أن لا يدري المجني عليه بوقوع الجريمة ضده، ذلك لقيام الجاني بحجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في الذبذبات الالكترونية المسجلة للبيانات، وكذلك لقدرته على التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة. ثم إنه و رغم إمكانية محو كل آثار الجريمة في جزء من الثانية و معه كل أدلة الإدانة، إلا أنها لا تمحى كليا، و ما يبقى في مقبرة العالم الافتراضي مستحيل الوصول إليه، ناهيك عن استرجاعه.

تعتبر طبيعة الجريمة المعلوماتية كونها عابرة للحدود واحدة من التحديات أمام محاولة كشفها، إذ أنها بسبب هته الأخيرة يصعب تعقبها و بالتالي كشفها، و ملاحقتها قانونيا نظرا لاختلاف الإجراءات من بلد إلى آخر.

هناك من يشير إلى أن هذه الجرائم لم يكشف منها إلا ما نسبته واحد بالمائة فقط و ما تم الإبلاغ عنه إلى السلطات المختصة لم يتعدى خمسة عشر بالمائة من النسبة السابقة، و حتى ما طرح أمام القضاء من هذه الجرائم فإن أدلة الإدانة فيه لم تكن كافية إلا في حدود 5/1. [25]

د- صعوبة إثبات الجريمة المعلوماتية

في حالة اكتشاف الجريمة المعلوماتية - هذا إن اكتشفت كما سبق وذكرنا- فإنه تواجهنا صعوبة أخرى هي صعوبة إثباتها لأنها تقع خارج الإطار المادي الملموس التقليدي المتعارف عليه، فقيام أركانها في بيئة الحاسوب و الانترنت يجعل الأمور تزداد تعقيدا لدى سلطات الأمن المتخصصة؛ لأن الإجرام يتعلق بكل سلوك غير مشروع بخصوص المعالجة الآلية لبيانات وإدخال المعلومات ونقلها[26].

إن طبيعة البيانات المتمثلة في نبضات الكترونية غير مرئية تجعل أمر طمس الدليل ومحوه طليا من قبل الفاعل أمرا غاية في السهولة[27].

يرجع عدم تبني إثبات الجريمة المعلوماتية لوسائل المعاينة والطرق التقليدية نظرا للطبيعة الخاصة التي تمتاز بها إلى:

أ- الجريمة المعلوماتية لا تخلف آثارا مادية تقوم عليها الأدلة كون للجريمة المستحدثة طبيعة خاصة من حيث أنها تخضع لقواعد غير القواعد التقليدية، وتتم في بيئة رقمية غير تقليدية؛ بيئة افتراضية يغيب فيها المادي الملموس.

ب- قد تكون المعلومات التي قام الجاني بالسطو عليها مشفرة في حد ذاتها بشفرة معقدة ما يصّعب لعناصر الأمن مسألة فكها لأمرين: هته الشفرة تحمي معلومات لا يجوز لعناصر الأمن معرفتها و بالتالي فكها و تعقب الجاني، أو أن الجاني قد قام بتغيير الشفرة إلى أخرى أكثر تعقيدا تتطلب وقتا يسمح له بمحو آثار جريمته.

ج- صعوبة إثبات الجريمة لصعوبة ملاحقتها في حالة غياب الاتفاقية بين دولتي الجاني و المجني عليه.

د- تعاقب العديد من الأشخاص على مسرح الجريمة، ما يعطي فرصا لا محدودة للجاني في الفرار متوجها في ذلك إلى تغيير أو إتلاف أو العبث بالآثار المادية إن وجدت. وهو الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية[28].

من خلال كل هذا نستخلص أن صعوبة إثبات الجريمة المعلوماتية يقوم على أنها جريمة غير تقليدية كونها لا تترك أثرا ماديا ملموسا حيث يصعب فهم حدودها الإجرامية خاصة مع أنها تتطلب ذكاء و حنكة و احترافية كبيرة عند ارتكابها.

هـ- تعاون عدة أشخاص في الجريمة المعلوماتية

يتعاون عادة في ارتكاب الجريمة الالكترونية عدة أشخاص حيث يتقاسمون المهام فيما بينهم على النحو الآتي:

- شخص متخصص في تقنيات الكمبيوتر ذو مهارات وخبرة كبيرة في مجال البرمجة والاختراق والأنظمة...

– شخص يهتم بالجانب الفني للجريمة؛ وهو الذي يحدد طبيعة الجريمة وهدفها ويضع الخطة. وفي غالب الأحيان يكون هو العقل المدبر ورابطة الوصل بين الشخصين الآخرين.

– شخص من محيط الضحية لتغطية الجريمة والتخفيف من حدة الآراء حولها في الوسط، وكذا إخفاء وتسريب النواقص ليتم استدراكها إذا تطلب الأمر ذلك.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يأتي على هيئة اشتراك سلبي يترجم بالصمت من جانب من يعلم بوقوع الجريمة لتسهيل إتمامها وقد يأتي على هيئة اشتراك آخر ايجابي يتمثل في تقديم المساعدة الفنية والمادية.

و– أسلوب ارتكاب الجريمة

إن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم المعلوماتي عادة ما يكون ذو مهارات تقنية عالية و إلمام بتكنولوجيا المعلوماتية. [29]

على عكس الجريمة التقليدية التي تستدعي نوعا من الجهد العضلي وممارسة العنف والإيذاء الجسدي، فإن الجرائم المعلوماتية هي جرائم هادئة لا يسمع حسيسها تعرف بصفة الناعمة لأنها في مجملها تقع بمجرد الضغط على أزرار و اجتياز الحاجز الأمني، فهي لا تحتاج إلى العنف بل إلى خبرة وذكاء في التعامل مع الكمبيوتر المتصل بشبكة الانترنت وتوظيفه في الجرائم المختلفة من تجسس واختراق وسطو وغيرها، مع وجود الإرادة في تحقيق الغرض الإجرامي.

ز– قلة الإبلاغ عن الجرائم المعلوماتية

يحجم المجني عليه طلب تدخل الجهات المختصة في حالات تعرضه لجريمة ما خوفاً من دعاية مضرة، وضياع ثقة المساهمين خاصة في حالة كان المجني عليه صاحب مؤسسة مالية فإنه لا يهمه المجرم وتعقبه ومعاقبته أكثر من عملائه وثقتهم. فنجد يعتبر الأمر مسألة أمن داخلي ويوظف له مختصين لحله والحلول دون التعرض لجريمة الكترونية أخرى ويدع الأمر طي الكتمان.

لكن هته الحالات ضئيلة جدا وهناك حالات كثيرة أين يتم الإبلاغ عن الجرائم المعلوماتية نسبة إلى شخصية المجني عليه التي تلعب دورا مهما في الإبلاغ[30].

مما سبق نجد أن الجريمة المعلوماتية نوع مستحدث من الجرائم، لا يرتبط أي ارتباط مباشر أو غير مباشر بالجريمة التقليدية، لهذا السبب فإنه يتطلب تعاونا دوليا وجهدا تشريعيا.

2- أنواع الجريمة المعلوماتية

تتمثل أنواع الجريمة المعلوماتية في الأنواع الآتية:

إن جرائم المعلوماتية تنقسم إلى فئتين هما: النشاط الإجرامي الذي يستهدف أجهزة الكمبيوتر (فيروسات وبرامج ضارة لإلحاق الضرر بالأجهزة و الأنظمة أو إيقافها عن العمل، أو حتى حذف البيانات أو سرقتها.)، و النشاط الإجرامي الذي يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى (أين يستخدم الكمبيوتر لنشر البرامج الضارة أو

المعلومات أو الصور غير المشروعة، أو حتى إدخال جرائم حقيقية كما يحدث في الويب العميق)، وتأتي أغلب الجرائم المعلوماتية في أشكال متنوعة، نجد منها:

-الاحتيال عبر البريد الالكتروني و الانترنت.

- سرقة البيانات المالية أو بيانات الدفع بالبطاقة.

- هجمات برامج الفدية.

- التجسس الالكتروني.

- تزوير الهوية.

-سرقات بيانات الشركات و بيعها.

- السرقة المشفرة.

و هناك أنواع أخرى للجريمة المعلوماتية ويمكن بيانها في ما يأتي:

- الجرائم ضد الأفراد و تسمى بجرائم الانترنت الشخصية مثل: سرقة الهوية، أو سرقة الاشتراك في موقع شبكة الانترنت.

- الجرائم ضد الملكية وهو انتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية لتدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك.

- الجرائم ضد الحكومات وتتمثل في مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت. وهي ترتكز على تدمير الخدمات والبنية التحتية ومهاجمة شبكات الكومبيوتر وغالبا ما يكون هدفها سياسي بحت[31].

- جرائم الابتزاز الالكتروني و هي أن يتعرض نظام حاسوبي أو موقع الكتروني ما لهجمات حرمان من خدمات معينة ، حيث يشن هذه الهجمات ويكررها قراصنة محترفون بهدف تحصيل مقابل مادي لوقف هذه الهجمات.[32]

- الجرائم السياسية الالكترونية التي تستهدف المواقع العسكرية للدول بهدف سرقة معلومات تتعلق بالدولة و أمنها.

-الإرهاب الالكتروني الذي يتمثل في سرقة الأنظمة الأمنية الحيوية على مواقع الانترنت، و تكون من تنظيم مجموعة من الإرهابيين الالكترونيين، أي جماعات تسعى للاستفادة من الثغرات الخاصة بهذه المواقع و الأنظمة.[33]

- جرائم الاحتيال و الاعتداء على الأموال التي تشمل إدخال بيانات غير صحيحة أو غير مشروع التصريح بها، الهندسة الاجتماعية، و التصيّد، بالإضافة إلى حذف أو تعديل المعلومات المحفوظة ناهيك عن إساءة استخدامها.

- المطاردة الالكترونية التي تشمل المضايقات الالكترونية أو إحراج عام أو سرقة مالية للأفراد عن طريق تعقبهم و مطاردتهم عبر وسائل التواصل الاجتماعي، و من ثم تهديدهم بمحادثات شخصية أو صور أو غيرها من المعلومات الخاصة بهم، و قد تمتد الجرائم من هذا النوع لتصل حد السب والشتم والتشهير.

– الوصول للمواقع المشفرة و المحجوبة، وسرقة المعلومات المحفوظة فيها ثم نشرها و توزيعها بأساليب غير مشروعة.

ثالثا: صفات المجرم المعلوماتي وأنماطه

الإنسان نوعان: إنسان يتفق مع الأخلاق والقانون والنظام ويحترمها، وإنسان يختلف عنها بالكلام عن النوع الثاني فقد أنجبت ثورة المعلومات نسلا جديدا من المجرمين اتفق على تسميتهم "مجرمي المعلوماتية". وجوهر الجريمة يرتبط بالإنسان، شخصيته، ودوافعه لأنه لا يمكن للعدالة أن تأخذ مجراها ما لم تأخذ بعين الاعتبار شخصية المجرم.

والمجرم المعلوماتي هو شخص يختلف عن المجرم التقليدي حيث يستخدم الكمبيوتر المتصل بشبكة الانترنت لإحداث نموذج إجرامي، وقد يكون من ذوي المناصب رفيعة المستوى وأصحاب الكفاءات، وحتى يمكن أن يكون شخصا موثوقا من قبل الناس.

1– صفات المجرم المعلوماتي

أثّر ارتباط الجرائم المعلوماتية بالحاسوب والانترنت على تمييز كل من الجريمة و المجرم المعلوماتي وتحلي هذا الأخير بسمات وصفات معينة نذكر منها:

أ– الاحترافية والذكاء

يتميز المجرم المعلوماتي بالذكاء وعدم الميول لاستعمال العنف والقوة[34]، وهذا الأمر بديهي فالمجرم الذكي يسعى لإخفاء جريمته بإحكام وذلك بعد ترك أدلة ضده فيفضل العمل بهدوء ولا يلجئ للعنف الذي يترك دليلا ماديا واضحا. ولأن الجريمة المعلوماتية توافي شروط عمله كونها تتطلب مقدرة ذهنية وعقلية عميقة، فهذا الأخير يستخدم طرقا جديدة لا يعرفها أحد سواه. فكلما قلت معرفة الآخرين بالطريقة، كلما صَعُب اكتشافها من طرف عناصر الأمن المتخصصة.

ب– الشخصية الاجتماعية

يعتبر المجرم المعلوماتي إنسانا اجتماعيا قادرا على التكيف مع هذا المجتمع. في معظم الأحيان يكون موثوقا من محيطه وبعيدا عن الشبهات وهو الأمر الذي يجعله يتمادى في جرائمه عسيرة الاكتشاف.

ج– الخوف من كشف الجريمة

على عكس المجرمين التقليديين، يخشى المجرم المعلوماتي من أن يكتشف أمره وأن يفضح أكثر من غيره من المجرمين وذلك راجع إلى مكانته الاجتماعية كونه محل ثقة العديد من المحيطين به، ناهيك عن أنه قد يكون أحد الكفاءات المرموقة أو ذا منصب رفيع المستوى.

يضمن المجرم المعلوماتي نجاح جريمته طالما لم تطرأ له أية عوامل غير متوقعة لا يمكن التنبؤ بها؛ ذلك أن الحواسيب تعمل بطريقة آلية تجعل احتمال كشف الجريمة ضئيلا جدا طالما أن جميع خطوات التنفيذ معروفة مسبقا بحيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شانها الكشف عن الجريمة[35].

د- السلطة تجاه النظام المعلوماتي

وهي مجموعة من الحقوق و المزايا التي تميز المجرم المعلوماتي وتضمن له ارتكاب جريمته. تتمثل في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات التي تتيح فتح الملفات وقراءتها ومحو المعلومات أو تعديلها؛ وأيضا استعمال الأنظمة المعلوماتية بشتى الطرق.

هـ- أنه إنسان متخصص

المجرم المعلوماتي إنسان متخصص ماهر في الحاسوبية وتقنياتها، يستغل ما له من مهارات في الاختراق ليحوز المعلومات المختلفة التي تساعده في جرائمه من نصب واعتداء وابتزاز مقابل المال؛ ثم يختفي وكل أثر لجريمته فلا تكشفه أي أنظمة أمنية بتعددها[36].

و- تكرار الجريمة نفسها

كمجرم معلوماتي فهو شخص عائد، يرجع إلى الثغرات التي أدت إلى كشفه في أحد المرات، وإن لم يفلح في سدها فإنه سيضبط مجددا بنفس الجريمة ويُقاد مرة أخرى إلى المحاكمة.

كل هذه الصفات المميزة لا تنفي أن المجرم الالكتروني لا يعد مجرما لأن حدود جريمته افتراضية رقمية، وإنما تضفي إلى أنه شخص ارتكب فعلا إجراميا لا بد أن يعاقب عليه

2- أنماط مجرمي المعلوماتية

الجرائم المعلوماتية جرائم مستحدثة بلغ منها التطور الحد الذي يجعل لمسة زر فقط كافية لإسقاط أقوى أنظمة الحماية والحواجز الأقوى تشفيرا عن المعلومات الأكثر سرية. وبسبب اختلاف الأساليب المستعملة في خرق الحواجز الأمنية، صَعُب تصنيف مجرمي المعلوماتية. رغم هذا أمكننا أن نبين أنماط المجرم المعلوماتي كما يأتي:

أ- صغار السن

وهم تلك الفئة المهووسة بالمعلومات وأنظمتها. " الصغار المتحمسين للحاسوب، شعور بالبهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب"[37]. وعادة ما يكونون دون سن الأهلية.

ب- القراصنة

هم مبرمجون ذوي خبرة في مجال المعلوماتية، هدفهم كسر الحواجز الأمنية في سبيل الولوج لأنظمة غير مسموح لهم بالدخول إليها. وهم نوعان:

-القراصنة الهواة (الهاكرز)

هم المبرمجون الذين يقومون بكسر الحواجز الأمنية فقط لهذا الهدف، من أجل الخبرة و التعمق في عمل الأنظمة المعلوماتية، وبدافع الفضول أو إثبات الذات؛ أي أن الدافع الإجرامي لديهم غير موجود عند اتصالهم، نذكر على سبيل المثال عصابة 414 من أمريكا التي نسب إليها 60 فعلا إجراميا من هذا النوع. ونجدهم أشخاصا عاديين أكفاء في مجال الحواسيب و المعلوماتية، يحتلون مكانة مرموقة في المجتمع، حيث يعرّف الأستاذ Vivant الهاكر بأنه: " كل شخص يدخل إلى النظام لإرضاء رغبته بدون تخريب للمعطيات الموجودة داخل النظام".

ويتفرع منهم القراصنة الأخلاقيون الذين يسعون إلى قرصنة المواقع لحجب ما فيها وما تعرضه من أمور غير أخلاقية. ومنهم من يسعون جاهدين إلى اكتشاف ثغرات في أنظمة المؤسسات المالية قصد سدها.

إذ يتفرعون إلى مجموعتين: أصحاب القبعة البيضاء وذوي القبعة السوداء، فالأوائل –الهاكرز– يطلب منهم القرصنة لصالح الشركات، والمنظمات. أما ذوي القبعة السوداء –الكراكرز– فهم هنا للفساد.

من أهم أهداف الهاكرز دراسة كيفية عمل الأنظمة و الشبكات على الحاسوب، و إيجاد الثغرات ثم سدها. أي بكلمات أخرى تحسين النظام بجعله أكثر أمانا و تحصينا ضد القراصنة المحترفين باسم القرصنة الأخلاقية.

من أشهر الهاكرز في الانترنت هما كين تومسن و دنيس ريتشي، و هما مطورا لغة السي تي التي تعد أم جميع لغات البرمجة لصناعة نظام اليونكس.

–القراصنة المحترفون (الكراكرز)

الهدف الرئيس من اعتداءاتهم هو التخريب، حيث تميل هته الفئة بقدرتها التقنية الواسعة وكذا خبرتها الشاملة إلى استخدام برامج تقنية للحصول على المعلومات السرية أو القيام بعمليات تخريبية معينة كالاستيلاء على البطاقات الائتمانية واستخدامها، تدمير أو تشفير الملفات المهمة، سرقة التفاصيل الشخصية والمعلومات و بيعها.. وغيرها من أشكال الجرائم الالكترونية غير المشروعة. ويطلق عليهم اسم العناكب spiders لأنهم يعملون في الخفاء، ولا يتركون آثار مادية لأفعالهم لذلك فهم خطيرون إلى درجة كبيرة[38].

إن المحفز الأساسي و الذي على أساسه تتم جرائم الكراكرز التي تطال أيا كان هو الكسب المادي. و يجدر الإشارة إلى أن جرائمهم قد تكون عشوائية، و قد تكون منظمة في حال ما إذا عينوا من قبل بعض المنافسين في عالم الأعمال لتخريب و تدمير معلومات الشركات المنافسة. و هنا فالهدف واحد و هو المال، و لكن الكيفية و الأسباب والمجرم الحقيقي يختلفون.

وهناك مجموعات من الكراكرز تقوم بجرائمها بدافع الدعاية الإعلامية وإثبات الذات و القوة في هذا العالم الافتراضي الذي بات متصلا بالعالم الواقعي أكثر من أي وقت مضى.

ولا يخفى عنا أن أخطر نوع من أنواع الكراكرز إنما هم المبتدؤون الذين يستخدمون برامج التخريب دون علم أو اطلاع جيد، فيقومون في أغلب الأحيان بأضرار و دمار كبيرين دون دراية بالأمر، و غالبا ما ينتهي بهم الأمر بين أيدي أجهزة الأمن السيبرالي كونهم سطحيين في إخفاء معالم الجريمة.

–السكامرز

لا يوجد مصطلح عربي يوافق كلمة السكامرز، و هذا إن دل على شيء إنما يدل على أن الجرائم الالكترونية و المجرمين الالكترونيين إنما تبدأ غربية ثم تنتشر. و أن سرعة انتشارها كبيرة، و أنه لا يمر يوم حتى تظهر أنواع جديدة، وأسماء جديدة.

السكامرز هم أشخاص غير محترفين و لا يمتلكون مهارات فريدة في مجال البرمجة و لا في مجال الاختراق، ويلجؤون إلى استخدام الهندسة العكسية الاجتماعية إذ يلجؤون إلى الحيل و المخططات من أجل الحصول على بعض المصالح من الأفراد و التي تشمل عادة االنقود.

-السبامرز

و هم النوع الذي يعمدون إلى إرسال رسائل غير ذي صلة و غير مرغوب فيه الأكبر عدد من مستخدمي الانترنت قصد الإشهار غير المدفوع، أو التصيد، أو نشر البرامج الضارة. و تعد نهب و سرقة الأموال أكبر هدف لهته الفئة.

ج- الموظفون العاملون في مجال الأنظمة المعلوماتية

هم الذين يرتكبون بعض الجرائم تحت تأثير طبيعة عملهم في سبيل تحقيق مآرب شخصية أهمها كسب المال. وهناك فئة منهم حاقدون تكون أهدافهم عادة الانتقام والثأر. ومن أمثلة ذلك الثأر لتصر صاحب العمل معهم، أو لتصرف منشأة ما سبق لهم التعامل معها. ولذلك فهم ينقسمون إلى مستخدمين للنظام بوصفهم موظفين أو إلى غرباء عن النظام، ولا يتصفون بالضرورة بالمعرفة التقنية الاحترافية حيث يستخدمون الفيروسات والبرامج الضارة للتخريب والإتلاف الكلي أو الجزئي، ولهذا السبب هم أكثر طائفة يسهل كشفها.

د- أصحاب الآراء المتطرفة

وهم الجماعات الإرهابية المتطرفة ذوي المعتقدات المختلفة والتي يرغبون في فرضها بأيها طريقة كانت، وغالبا ما يلجؤون إلى العنف. ساهمت مواقع التواصل الاجتماعي في توسيع نطاق هذه الفئة وضم أشخاص جدد إليهم ثم الهجوم على المواقع التي تخالفهم المعتقد والقيام بغلقها.

هـ- مجرمو المعلوماتية في إطار الجريمة المنظمة

وهم الذين يعملون مقابل الربح المادي بطريقة غير مشروعة. يكون نشاطهم منظما وكل خطوة لهم تكون قد سبق التخطيط لها. ويعد هذا النوع من الجرائم أكثر الأنواع جذبا للانتباه بحكم أنها توفر للجاني مقابلا ماديا لقاء مخاطرته وتعبه. وكذلك لارتفاع قيمة ما تدره من أرباح مادية مع صعوبة الكشف عنها وإثباتها بالمقارنة مع الجرائم التقليدية.

إن انضمام مجرم معلوماتي ما لإحدى هذه الفئات لا يعني بالضرورة أن لكل تخصصه في مجال الجريمة المعلوماتية؛ يوجد أيضا المجرم الملم بكل هذه الأنماط. فاختلاف دوافع كل نمط لا يعني تعني تفرد المجرم بدافع واحد دون غيره، وإنما قد يملك من الدوافع و الصفات وظروف العمل المختلفة ما يخوّل تصنيفه في كل ما سبق.

الخاتمة

إن التطور السريع والملحوظ الذي يشهده العالم اليوم في عالم الانترنت يتفرع عنه ليس فقط تنوع في الإيجابيات والخدمات التي تيسر الحياة، وإنما بقدر هته الإيجابيات هناك من السلبيات. لعله كان من المتوقع أن تظهر الجريمة المعلوماتية عاجلا أم آجلا، لكن وقتها لم يكن الإنسان غفل عن هذا لأنه فضّل النظر للجانب المشرق من الأمور. وعليه

فإن الجريمة المعلوماتية اليوم تشكل تحديا لجميع العاملين والمستهلكين وحتى المستثمرين في هذا القطاع، خاصة وأنها باتت جريمة يصعب تقفيها أو وقفها وهي التي عبرت حدود الدول.

وجب في مرحلة ما وضع ماهية للجريمة المعلوماتية ولهذا تمت هذه الدراسة حيث تم تناول تعريفها، خصائصها، والسمات التي تكتسي المجرم المعلوماتي.

من خلال هذا البحث تم التوصل إلى النتائج والاقتراحات الآتية:

أ- النتائج المتوصل إليها:

1- نظرا لحداثة الجريمة المعلوماتية، فإنه لا يوجد مصطلح قانوني موحد للدلالة عليها، ويفضل البعض تسميتها بهذا الاسم "الجريمة المعلوماتية".

2- كما أن هناك اختلاف فقهي في تعريفها بين موسع ومضيق بالاعتماد على معايير مختلفة منها وسيلة ارتكاب هذه الجريمة، أو موضوعها أو حتى الغاية منها و نتيجتها.

3- التجديد المستمر الحادث في مجال الجرائم المعلوماتية يستدعي مراقبة مستمرة و سريعة من أجل معرفة وفهم مجريات الجريمة، و اللحاق بركب ما يحدث، و من ثم الاستعداد لأي تطور جديد محتمل الحدوث.

4- إن المجرمين المعلوماتيين في ازدياد دائم، وهذا ما يتطلب زيادة عدد المكافحين لهم من طرف جهات مكافحة الجريمة المعلوماتية (الأمن السيبراني) .

ب- الاقتراحات: من خلال دراسة هذا الموضوع، يقترح ما يلي:

1- ضرورة إعطاء تعريف موسع للجريمة المعلوماتية، وقد يقترح التعريف الآتي لها: تعد جريمة معلوماتية كل جريمة يمكن ارتكابها بواسطة شبكة الانترنت أو داخل نظام معلوماتي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها سواء على تكنولوجيا المعلومات أو المرتكبة بواسطة المعلوماتية، وذلك بسبب التطور المستمر اللامتناهي لتكنولوجيا المعلومات والاتصالات الذي يؤدي إلى إثارة عدد من المشكلات العملية يتمثل أهمها في صعوبة تقدير حجم هذه الجريمة وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذا صعوبة تحقيق التعاون الدولي لمكافحتها.

2- يستحسن تحديد قائمة بجرائم الكومبيوتر والأنترنت، وبالتالي وضع نص مجرم لكل سلوك إجرامي في هذا المجال.

3- يستحسن بالمشرع الجزائري أن يعمل على تعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية والتي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.

قائمة المصادر والمراجع:

I النصوص القانونية

1- القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47، سنة 2009، المعدل و المتمم.

II الكتب

1- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

2- أمير فرج يوسف، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكومبيوتر و الانترنت، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2011.

3- بالطي غنية، الجريمة الالكترونية "دراسة مقارنة"، الدار الجزائرية للنشر، الجزائر، 2015.

4- بشرى حسين الحمداني، القرصنة الالكترونية و أسلحة الحرب الحديثة، الطبعة الأولى، دار أسامة للنشر و التوزيع، الأردن، 2014.

5-خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دون طبعة، دار الثقافة، الأردن، 2011.

6-عادل يوسف عبد النبي البشكري، "الجريمة المعلوماتية و أزمة الشرعية الجزائية"، العدد السابع، الكوفة.

7- عبد العالي الدربي، محمد صادق اسماعيل، الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة، 2012.

8- عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة"، دون طبعة، منشورات الحلبي الحقوقية، بيروت، 2007.

9- علي حسن الطوابلة، الجرائم الالكترونية، الطبعة الأولى، مؤسسة الفخراوي للدراسات و النشر، البحرين، 2008.

10- محمد أمين الرومي، جرائم الكومبيوتر و الانترنت، دون طبعة، دار المطبوعات الجامعية، الإسكندرية، 2004.

11-محمد إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014.

12- محمد حماد مرهج الهيتي، جرائم الحاسوب: -دراسة تحليلية-، الطبعة الأولى، دار المناهج للنشر و التوزيع، الأردن 2006.

13-محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2004.

14- محمد كمال الدستوري، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر و القانون للنشر و التوزيع، المنصورة، 2010.

15-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، 2005.

16-نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة، الأردن، 2010.

III المداخلات العلمية

1- دياب موسى البداينة، "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، ملتقى علمي بالمملكة الأردنية الهاشمية، يوم 2014/9/4.

III I المواقع الالكترونية

- رماح الدلقومي، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، الجزيرة، اطلع عليه بتاريخ 2020/12/1.

الهوامش:

[1] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص87. دياب موسى البداينة، "الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية"، ملتقى علمي بالمملكة الأردنية الهاشمية، يوم 2014/9/4، ص2.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الإسكندرية، 2005، ص97.

[3] محمد إبراهيم غازي، الحماية الجنائية للخصوصية و التجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص120.

*إن مصطلح الالكترونية يستخدم لوصف فكرة جزء من الحاسب أو عصر المعلومات،و جملة فإن عبارة الجريمة الالكترونية تعني: " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة و بقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت". انظر: دياب موسى البداينة، المرجع السابق، ص3.

[4] محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2004، ص43.

[5] دياب موسى البداينة، المرجع السابق، ص2.

[6] نائلة عادل محمد فريد قورة، المرجع نفسه، ص28.

[7] محمد إبراهيم غازي، المرجع السابق، ص118.

[8] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص84.

[9] خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دون طبعة، دار الثقافة، الأردن، 2011، ص29.

[10] محمد علي العريان، المرجع السابق، ص44.

[11] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة، الأردن، 2010، ص48.

[12] عادل يوسف عبد النبي البشكري، "الجريمة المعلوماتية و أزمة الشرعية الجزائية"، العدد السابع، الكوفة، ص113.

[13] انظر: أمير فرج يوسف، الجريمة الالكترونية و المعلوماتية و الجهود الدولية و المحلية لمكافحة جرائم الكومبيوتر و الانترنت، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2011، ص10. محمود إبراهيم غازي، المرجع السابق، ص118.

[14] نهلا عبد القادر المومني، المرجع السابق، ص49.

[15] علي حسن الطوابلة، الجرائم الالكترونية، الطبعة الأولى، مؤسسة الفخراوي للدراسات و النشر، البحرين، 2008، ص49.

[16] المرجع نفسه، ص 50.

[17] انظر: دياب موسى البداينة، المرجع السابق، ص3.

[18] المادة الثانية من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، ج ر عدد 47، الصادرة في سنة 2009، المعدل والمتمم. و تنص على أنه: " يقصد في مفهوم هذا القانون بما يأتي: أ. الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية".

[19] القانون رقم 05/18 المؤرخ في 10 مايو سنة 2018، المتعلق بالتجارة الالكترونية، ج ر، عدد 28، الصادرة في 16 ماية سنة 2018.

[20] انظر: المادة 2 من القانون رقم 04/09 السابق ذكرها أعلاه.

[21] انظر: محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، ص47.

[22] محمد كمال الدستوري، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر و القانون للنشر و التوزيع، المنصورة، 2010، ص17.

[23] عبد العالي الدربي، محمد صادق اسماعيل، الجرائم الالكترونية، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة، 2012، ص ص 55، 56.

[24] نائلة عادل محمد فريد قورة، المرجع السابق، ص49.

[25] محمد حماد مرهج الهيتي، جرائم الحاسوب: -دراسة تحليلية-، الطبعة الأولى، دار المناهج للنشر و التوزيع، الأردن 2006، ص36.

[26] عفيفي كامل، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون "دراسة مقارنة"، دون طبعة، منشورات الحلبي الحقوقية، بيروت، 2007، ص270.

[27] انظر: نهلا عبد القادر المومني، المرجع السابق، ص56.

[28]المرجع نفسه، ص57.

[29]أحمد خليفة الملط، المرجع السابق،ص 114.

[30]بالطي غنية، الجريمة الالكترونية "دراسة مقارنة"، الدار الجزائرية للنشر، الجزائر، 2015، ص ص 15،16.

[31]انظر: مجلة تكنولوجيا المعلومات، المرجع السابق، ص4.

[32]رماح الدلقومي، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، الجزيرة، اطلع عليه بتاريخ 2020/12/1.

[33]رماح الدلقومي، المرجع نفسه.

[34]انظر: محمد أمين الرومي، جرائم الكومبيوتر و الانترنت، دون طبعة، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 22.

[35]نائلة عادل محمد فريد قورة، المرجع نفسه ، ص60.

[36]انظر: بشرى حسين الحمداني، القرصنة الالكترونية و أسلحة الحرب الحديثة، الطبعة الأولى، دار أسامة للنشر و التوزيع، الأردن، 2014، ص59.

[37]علي حسن الطوابلة، المرجع السابق، ص65.

[38]بالطي غنية، المرجع السابق، ص39.