

المجرم المعلوماتي Cyber criminal

فليج غزلان

جامعة تلمسان

مخبر الحقوق والحريات الأساسية

felidjghizlene@yahoo.fr

دركاوي عبد القادر *

جامعة تلمسان

مخبر الحقوق والحريات الأساسية

abdelkaderderkaoui012@gmail.com



- تاريخ النشر: 2025/06/05

- تاريخ القبول: 2025/05/29

- تاريخ الإرسال: 2025/04/23

ملخص:

إن الظاهرة الإجرامية قديمة قدم البشرية، ومع التطور الذي شهدته الحضارة عبر العصور، كانت تظهر للوجود أنماط جديدة من الجرائم، وباختراع الحاسوب ثم شبكة الإنترنت في منتصف القرن الماضي، ظهر صنف آخر من الجرائم نتج عن إساءة استخدام مخرجات التكنولوجيا الحديثة، اصطلاح على تسميته بجرائم الكمبيوتر والإنترنت، أو الجريمة المعلوماتية ... الخ، وفي خضم ذلك نشأ وترعرع قراصنة الكمبيوتر والإنترنت كجيل جديد من المجرمين، ينتظر أن يكون لهم مستقبلاً أثراً واضحاً في مختلف دول العالم.

ولأن المكافحة الفعالة للظاهرة الإجرامية يجب أن تتأسس على فهم معمق لأحوال المجرمين، قبل وبعد سن القواعد القانونية اللازمة لمواجهة الجريمة، وحيث أن الوصول إلى المجرم وضبطه يستلزم الوقوف على كيفية ارتكابه لها، والأسباب الكامنة وراء إتيانه للبعث منها دون الآخر، فقد ارتأينا تسليط الضوء على شيء من تلك الجوانب، تطبيقاً على شخصية المجرم المعلوماتي.

الكلمات المفتاحية: المجرم المعلوماتي، القرصان المعلوماتي، مجرم تكنولوجيا المعلومات.

ABSTRACT:

The phenomenon criminal is old as feet of mankind, and with evolution witnessed by civilization through the ages, it was showing up to exist new styles of crimes. And by invention of computer, then the internet in the middle of the last

* - المؤلف المرسل:

century, another row appeared of crimes resulted of miss use of technology outputs, i twas named (computer and internet crimes), or (information crime) ... etc. And in the meantime the hackers are grew up as a new generation of criminals, waiting to have them in the future a clear trace in different countries of the world. Because effective control of the criminal phenomenon must be astablished by deep understanding of the criminal case, before and after anactement of legal rules necessary to face crime, and where to reach the criminal and adjust it requires standing on how to commit it, and the underlying causes behind his commission of some of them instead of the other, we have saw to clear on something from those aspects an application to the character of the information criminal.

key words: information criminal, Information pirate, criminal of information technology.

مقدمة:

إن أية جريمة من الجرائم الواقعة في البيئة المعلوماتية¹، سواء تلك المرتكبة من خلال شبكة الإنترنت، أو بواسطة الهواتف الذكية عبر شبكات الهاتف المختلفة، تتطلب وجود طرفان أحدهما يقوم بالفعل الإجرامي أو الجريمة، وهو الجاني أو المجرم المعلوماتي أو الفاعل، والثاني تقع عليه الأفعال، وهو المجني عليه أو الضحية. فالجريمة المعلوماتية إذن شأنها شأن غالبية الجرائم التي تتضمنها التشريعات الجزائية التي تعنى بمكافحة الجرائم في العالم المادي²، لا يمكن تصور تحققها بدون أطراف، ووجه الخلاف بينهما يتمثل، في إحدى صوره الأساسية، في شخصية المجرم المعلوماتي التي ما زالت محطة اهتمام الباحثين في ميادين علمية عدة، كعلم الاجتماع، والنفس، والقانون الجنائي، بطبيعة الحال، بغية فهم هذه الشخصية غير العادية المسلحة بالمعارف التقنية والفنية التي تسخرها في اقتحام الشبكات المعلوماتية والسطو على الأموال، وتعطيل النظم التي تقدم خدماتها للأفراد.

وغني عن البيان بأن فكرة القرصان المعلوماتي، أو المجرم الإلكتروني، فكرة جديدة على الفقه الجنائي³، إلا أن البعض من رجالات هذا الفقه قد تصدى لوضع تعريف له، فبعضهم يرى أنه "مجرم ذو مهارات تقنية وذو علم

¹ - والجريمة المعلوماتية حسب أفضل التعاريف التي وضعت لبيان المقصود بها هي "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".
الحامي محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، ط 1، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص 10-9.

² - حول معنى الجريمة بوجه عام، انظر على سبيل المثال:

- محمد علي سالم العياد الحلبي، شرح قانون العقوبات (القسم العام)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1997، ص 94.

- د. علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت، 1982، ص 134.

³ - David Johnson, electronic privacy, Stodder, Cannada, 1997, p 67.

بالآليات المستخدمة في نظم الحواسيب يستعملها في جريمته"¹، أو هو "ذاك النوع من المجرمين الذي لديه الدراية والمقدرة الفنية على فهم التكتيكات الموجودة في الحاسوب والقادر على تسخيرها في أغراضه الإجرامية، سواء باختراق الكود السري لتغيير البيانات والمعلومات، أو بتقليد البرمجيات، أو التنقل عبر الشبكات المعلوماتية.

وفي حقل مكافحة الجرائم، يؤكد المتخصصون بأن المواجهة الفاعلة للظاهرة الإجرامية "ترتبط ارتباطاً وثيقاً بمعرفة الجرم، ومدى تقديره للمخاطر المتعلقة بالجريمة، ودوافعه ومكونات سلوكه الذاتية، وتحليلها وتقديم تفسير دقيق لها"²، لكي تتمكن دوائر الشرطة من أخذ زمام المبادرة في مكافحة الجريمة"، ومن المؤكد بأن الوصول إلى مثل هذه الغاية مرهونٌ بمدى التوصل للتحليل الدقيق لما يدلي به المجرمون من خلال استجوابهم، كاستنتاج الدوافع الخاصة بارتكاب الجريمة، والسمات المتصلة بمقتربها، وأسباب انجذابهم تجاه نوع محدد من الجرائم، وما يتوجب القيام به حيالهم، كرد فعل وقائي أو علاجي من طرف المجتمع.

لذا، وإنه ونظراً لكثرة وتشعب المشاكل القانونية التي أثارها وما زالت تثيرها المعلوماتية، كإحدى الظواهر الإنسانية المستحدثة، إن على مستوى القوانين العقابية، أو في نطاق فروع القانون الأخرى، فإن البحث الذي بين أيدينا يحاول مناقشة جانب من تلك المشكلات، ألا وهو استظهار معالم شخصية مجرمي الإنترنت، اعتقاداً منا بأنها تعد من بين أهم الإشكالات المطروحة التي يتوقف على فهمها -على الوجه الصحيح- فك طلاس لغز الجريمة المعلوماتية، ولا نبالغ إذا قلنا بأن هؤلاء يمثلون الجيل الجديد من مجرمي الألفية الثالثة بلا منازع.

وعلى ذلك، وتوخياً للإلمام بجوانب الموضوع محل البحث، فقد ارتأينا تخصيص ثلاثة محاور لدراسته كما يلي: المطلب الأول: الصفات المميزة للمجرم المعلوماتي، والمطلب الثاني: تصنيفات المجرم المعلوماتي، والمطلب الثالث: دوافع المجرم المعلوماتي.

المطلب الأول: الصفات المميزة للمجرم المعلوماتي

ليس هناك اتفاقاً على صفات مرتكبي الجرائم المعلوماتية ومنفذيها، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم بها مرتكبو الجرائم المعلوماتية، إلا أن هناك صفات ذات دلالات مشتركة يجمع المتخصصون بأنها توجد في كل الأشخاص الذين تم التحقيق معهم والقبض عليهم في جرائم من هذا النوع³. وعلى العموم يمكن إجمال تلك الخصائص أو الصفات في ما يلي:

الفرع الأول: صغر السن

¹ - فتحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل درجة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2011 - 2012، ص 49.

² - قولقحان سيوفي بورجن ريم، السطو على المصارف من منظور المجرم، ترجمة: عبد القادر أحمد عبد الغفار، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1408 هـ، ص 13.

³ - منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، الملتقى العلمي للجرائم المعلوماتية، نظمته هيئة التحقيق والإدعاء العام، الرياض، المملكة العربية السعودية، 2009، ص 3.

يتضح من الدراسات والبحوث التي تناولت هذه الجريمة، سواء في الولايات المتحدة الأمريكية أو أوروبا، أن معظم مرتكبيها ينتمون إلى الجيل الحديث من الشباب¹، إذ تتراوح أعمارهم بين الرابع عشر والثلاثين، ولعل ذلك يعود لعدد من الأسباب، ومنها أن علم الحاسب الآلي من العلوم الحديثة والذي يتطلب متابعة يومية للتعرف على الشفرات الأمنية التي يمكن الولوج منها للأنظمة، وهذه المتابعة تتطلب نوعاً من التفرغ والجلوس لعدد من الساعات أمام جهاز الحاسب، وعمل تحول داخل الشبكات العالمية للحصول على هذه المعلومات، وذلك يعتبر أمراً مكلفاً للأشخاص العاملين، فهم لا يجدون الوقت الكافي للقيام بذلك، بعكس طلاب المدارس والجامعات. كما أن حسابات الريح والخسارة تختلف بين صغار السن وكبارهم، فصغار السن قد لا يخسرون شيئاً في ما لو اكتشفت جرائمهم، كما أن القوانين والأنظمة لا تعاقب مثل هؤلاء، بينما يتعرض كبار السن والموظفين لخسائر ومخاطر، قد تكلفهم وظائفهم أو حريتهم².

الفرع الثاني: حدة الذكاء

الذكاء بصفة عامة هو "المقدرة على التفكير والفهم"، ويعرفه علماء النفس بأنه "قدرة الإنسان على فهم العلاقات التي توجد بين العناصر المكونة لموقع من المواقع، وعلى التكيف معه من أجل تحقيق أهدافه"³. والمجزم في مجال التقنيات الرقمية⁴ لديه ذكاء من أنواع معينة ودراية بأحدث ما توصلت إليه التقنية. لذا فإنه يلاحظ بأن جرائم التكنولوجيا الحديثة تتطلب مقدرة عقلية وذهنية خاصة لدى الجاني، حيث أن هذه الجرائم لا تتطلب إجراءات تميل إلى العنف بقدر ما تتطلب مقدرة عقلية، فمثلاً الإتلاف المعلوماتي لا يحتاج للقيام بعمل عنف، فهو يرتكب بواسطة تقنيات التدمير الناعمة، كما يحلو للبعض أن يطلق عليها، والتي تتمثل في التلاعب بالمعلومات، أو الكيانات المنطقية، أو البيانات، ويحدث هذا التلاعب عن طريق ما يعرف بالقنابل المنطقية والفيروسات المعلوماتية⁵.

إن الوصول إلى أنظمة المعلومات، واختراق التحصينات الدفاعية والرقابية، يتطلب في الغالب إجراء عدة محاولات تستغرق مدداً طويلة، كما أن أكثر الاختراقات تحدث عن طريق تقنية المحاولة والخطأ، والتي تستلزم إجراء عدد من المحاولات، واستخدام عدد كبير من الأدوات والبرامج للقيام بذلك، كما أن اختيار التقنية المناسبة والعدة والبرامج التي تتطلبها مثل هذه الاختراقات، واختيار الوقت والمكان المناسبين لإجراء الاختبارات، إتباع الطرق المناسبة

¹ - د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، الطبعة الثانية، دون ناشر، ودون مكان نشر، 2000، ص 33.

² - محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، بحث مقدم للحصول على درجة الماجستير في التشريع الجنائي الإسلامي، قسم العدالة الجنائية، كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1423-1424 هـ، ص 53-54.

³ - د. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها ومكافحتها)، دار الكتب القانونية، المحلة الكبرى، مصر، 2005، ص 20.

⁴ - د. مصطفى محمد موسى، نفس المرجع السابق، ص 20.

⁵ - د. عفيفي كامل عفيفي، المرجع السابق، ص 33.

لتلاني عمليات التتبع وتقفي آثار المعتدي، كالانتقال من شبكة إلى أخرى حتى الوصول إلى الهدف، كل ذلك يتطلب درجة عالية من الذكاء لدى منفذ مثل هذه العمليات¹.

الفرع الثالث: المهارة الفنية

المجرم المعلوماتي شخص ذو مهارات فنية عالية، متخصص في الجرائم المعلوماتية، شخص قادر على استخدام مهاراته في الاختراقات وتغيير المعلومات، وشخص قادر على تقليد البرامج وتحويل الأموال². ومرد ذلك على الأرجح إلى أن معظم مرتكبي هذه الجرائم ينتمون³ إلى الطبقة المتعلمة تعليماً فنياً ذا علاقة بالحاسب الآلي وعلومه، مما يمكنهم من ارتكاب الجريمة وإخفاء معالمها، ما يتيح لهم التغلب على مختلف العقبات والمشكلات الفنية التي قد تواجههم أثناء ارتكابهم لها، وهذه مهمة قد تكون صعبة، إن لم نقل مستحيلة، لمن لا تتوفر في جانبهم المقدرة الفنية المتخصصة.

غير أنه وبمرور الوقت، وازدياد مقدار السهولة في استخدام تقنيات المعلومات، وشيوع البرامج الجاهزة المتوفرة في شبكة الإنترنت، أصبح ارتكاب الجرائم المتصلة باستخدام الكمبيوتر أكثر سهولة عن ذي قبل. فإذا كانت القرصنة المعلوماتية تتطلب في الماضي قدراً من المعرفة العلمية والبرمجة في جانب من يقوم بها، فإنه يمكن الحصول في الوقت الحاضر على الإرشادات اللازمة لتحقيق تلك الغاية خطوة بخطوة وبكل حرية، من خلال شبكة الإنترنت، ومن ثم استخدامها في تنفيذ هجمات عبر الشبكة.

الفرع الرابع: الاحتراف المهني

لقد أكدت معظم الدراسات والإحصاءات التي أجريت حول ظاهرة الإجرام السيبراني بأن مرتكبها⁴ شخص محترف في التعامل مع الشبكات، وذلك على اعتبار أن التخصص الدقيق، والإتقان والمهارة، والتمرس على أدوات الاختراق والبيئة المستهدفة، أمر ضروري لإجراء عمليات الاحتيال المعلوماتي وارتكاب الجريمة⁵، وهذا ما جعل من الجرم الإلكتروني جرم أصحاب اختصاص وخبرة ومهارة، غير الجرائم العادية التي هي في متناول جميع الناس⁶. ولعل ما يؤكد على احترافية المجرم المعلوماتي هو شيوع ظاهرة جرائم التكنولوجيا العالية بنسب ملحوظة بين فئات الموظفين العاملين بالمؤسسة الذين يستغلون منصب عملهم في اقتراف جرائم غالباً ما تكون مالية.

¹ - محسن بن سليمان الخليفة، المرجع السابق، ص 54.

² - منصور بن مصلح الجهني، المرجع السابق، ص 4.

³ - محسن بن سليمان الخليفة، المرجع السابق، ص 54.

⁴ - منصور بن مصلح الجهني، المرجع السابق، ص 3.

⁵ - محسن بن سليمان الخليفة، المرجع السابق، ص 55.

⁶ - د. محمد دباس الحميد ود. ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط 1، دار حامد للنشر والتوزيع، عمان، الأردن، 2007، ص 64.

ومن أمثلة ذلك حالة تتلخص وقائعها في قيام أحد المبرمجين في مركز حاسبات إحدى الشركات الألمانية الكبرى بإعداد ووضع برنامج في حاسب الشركة، يتيح له إدخال بيانات مرتبات أشخاص وهميين على ذاكرة الحاسب، وتحويل هذه المرتبات على حساب خاص به، ولأن مثل هذا التلاعب قد صار معروفا بعد أن تعرضت له شركات عدة، وإمكانية اكتشافه من خلال حوافظ المرتبات، وعمليات مراجعتها، وبيانات الحسابات والميزانيات، فقد سعى الجاني إلى تجنب اكتشاف أمره بأن يجري تعديلاً في برنامج دفع المرتبات، كي لا يطبع الحاسب ضمن مخرجاته حوافظ مرتبات للموظفين الوهميين، وبالتالي لا تظهر مدفوعات رواتبهم في قوائم المراجعة التي يعدها الحاسب للشيكات التي تم صرفها للموظفين. وعن طريق تعديل آخر أجراه على البرامج الخاصة ببيانات حسابات الشركة وميزانياتها، نجح الجاني في استقطاع المبالغ المستولى عليها من حساب إجمالي للضرائب على المرتبات الواجب سدادها لإدارة الضرائب، ومن ثم لا يظهر هذا المبلغ في حسابات الشركة وميزانياتها بوصفه عجزاً. وبهذا التلاعب المتعدد تمكن الجاني من الاستيلاء على (193.000) مارك، من بعد اكتشاف أمره عرضاً وفي عام 1978 حكم عليه بعامين للاحتيال وإساءة الائتمان¹.

الفرع الخامس: التعاون والتواطؤ

تتميز جرائم التكنولوجيا الحديثة بأن مرتكبيها قد يحدث بينهم تعاون على ارتكابها، إضراراً بالجهة المجني عليها، وغالباً ما يكون متضامناً فيها متخصص الحاسبات، يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من محيط أو خارج المؤسسة المجني عليها، لتغطية عملية التلاعب وتحويل المكاسب المادية إليه². لذلك يسعى المجرم المعلوماتي إلى تدعيم علاقاته الإنسانية حيث عمله وسط المجتمع، فهو إنسان اجتماعي بطبعه، وتطبيقاً لذلك ترتكب كثيراً من جرائم المعلومات بدافع الكبرياء، أو للرد على تعرضه للفصل من العمل، أو الاستغناء عن خدماته، أو بدافع النصب، أو الحسد، أو بدافع اللغو، أو لإظهار ما يتمتع به من مهارات تبرز تفوقه في مواجهة أنظمة أمن المعلومات، أو لمجرد الحصول على منفعة مالية³.

كما أنه من عادة من يمارسون التلصص على الحاسبات تبادل المعلومات بصفة منتظمة حول أنشطتهم⁴، وقد يصل بهم الأمر إلى حد عقد مؤتمرات لتبادل الخبرات والمعلومات حول كفاءات وأساليب ارتكاب الجريمة، ومما يشار إليه في هذا السياق أنه قد انعقد في الفترة من 28 إلى 30 مارس 2000 م بالعاصمة الإسرائيلية "تل أبيب"

¹- هامش رقم 39 مشار إليه لدى وليد العاكوم وآخرون، بحث مؤتمر القانون والكمبيوتر والإنترنت، الإمارات العربية المتحدة، 1-3 مايو 2000 م، ج2، ط2، الناشر: كلية القانون، جامعة الإمارات، العين، أبو ضي، الإمارات العربية المتحدة، 2004، ص 422.

²- د. عفيفي كامل عفيفي، المرجع السابق، ص 32.

³- د. عبد الله بن سعود محمد السراي، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، 2011، ص 32-33.

⁴- د. عفيفي كامل عفيفي، المرجع السابق، ص 32.

مؤتمر دولي لقراصنة الكمبيوتر وشبكات المعلومات أشرفت عليه منظمة إسرائيلية تسمى "الناس والكمبيوتر"¹ وذلك تحت (Y2 Hack) وذلك لتبادل المعلومات والأفكار فيما بينهم، وتم إنشاء موقع على شبكة الإنترنت كان عنوانه: (www.2600.org)

الفقرة السادسة: المعرفة الوثيقة بظروف محل الجريمة

تتطلب معظم جرائم نظم المعلومات التعرف إلى جميع ما يحيط بمحل الجريمة، كالأجهزة والبرامج والاحتياجات الأمنية ووسائل الرقابة والتحكم التي تتبعها المنظمة لحماية معلوماتها من التدخل الخارجي. وإن أكثر الأشخاص معرفة بهذه الظروف هم العاملون في هذه المنظمات وخاصة الفنيين، مما يمكنهم من ارتكاب الجريمة وإخفاء معالمها، ومعرفة هؤلاء بأنظمة المعلومات من جهة وجهل الأطراف الأخرى بتقنية المعلومات، يسهل على هؤلاء ارتكاب الجريمة وإخفاء معالمها، ويجعلهم يعتقدون أنهم بمأمن من وصول يد العدالة إليهم، ناهيك عن صعوبة اكتشافها من المنظمة وإدارتها أصلاً².

الفرع السابع: صفات أخرى للمجرم المعلوماتي: ومن هذه الصفات ما يلي:

- 1- عدم وجود سوابق إجرامية لدى معظمهم.
- 2- المتوسط لأعمارهم 29 سنة.
- 3- يتمتعون بالذكاء وعادة يكونون محل ثقة ويتسمون بالنشاط ولديهم دافع قوي للعمل ومرغوبون في سوق العمل.
- 4- لا يشكلون فئة أو وظيفة متميزة عن غيرهم.
- 5- أكثرهم من الذكور، وذلك يرجع إلى كثرة الذكور العاملين في مجال الحاسب الآلي عن النساء.
- 6- أكثرهم يخشون ضبطهم وافتضاح أمرهم بين ذويهم وأصدقائهم.
- 7- يعرف عنهم اعتدالهم في القيم والأخلاقيات بوجه عام وتسويغهم الذاتي لأفعالهم³.

المطلب الثاني: تصنيفات المجرم المعلوماتي

وضع بعض المهتمين بمكافحة ظاهرة الجريمة المعلوماتية عدداً من التصنيفات لمرتكبيها، وذلك بغرض التمييز بين طبقاتهم، لتسهيل تحديد مدى خطورتهم على مجتمع المعلومات، وفي ما يلي عرضٌ موجزٌ لأشهرها:

الفرع الأول: المجرمون المستخدمون والمجرمون المبرمجون

المجرم المستخدم هو من توافرت لديه المهارة الكافية بآلية عمل الحاسب الآلي ومكوناته الأساسية ومعرفة بعض البرامج التي يجري العمل بها. ومع الإقرار بأن تكنولوجيا الحاسب الآلي تكنولوجيا حديثة ودخولها واقع الحياة اليومية

¹ - هامش رقم 82 مشار إليه لدى وليد العاكوم وآخرون، المرجع السابق، ص 447.

² - محسن بن سليمان الخليفة، المرجع السابق، ص 54.

³ - محسن بن سليمان الخليفة، نفس المرجع السابق، ص 54.

حديثا نسبيا، عندنا تحديدا، وبالتالي فإن أعداد المستخدمين بدأت قليلة نظرا لقلّة المعرفة بهذه التكنولوجيا، لذا فإن الجرائم المتصور ارتكابها من هذه الفئة تبقى قليلة وبسيطة وغير ذات أهمية¹.

أما المجرمون المبرمجون، فإن خطورة أفراد هذه الطائفة أو الفئة تتمثل في أنهم أشخاص يعرفون معرفة تامة بخصوصيات الأنظمة المعلوماتية وعمومياتها، بالإضافة إلى أساليب المراجعة الأمنية والتدقيق وأدوات الاقتحام وكيفية استخدامها وإدخال التعديلات المناسبة عليها إذا لزم الأمر، كما في حالة إذا ما فشلت محاولاتهم الهجومية على الأهداف التي حددوها لأنفسهم، فهؤلاء باستطاعتهم إعداد برامج خاصة لتجاوز مختلف العقبات التقنية التي تواجههم، ويتميزون أيضا بأنهم لا يكتفون بمجرد القراءة النظرية عن الثغرات الأمنية التي قد تتواجد في الأنظمة المعلوماتية، وإنما يعاينونها بالفعل معاينة شخصية فيكتشفون سائر مواطن الضعف التي يمكنهم من خلالها توجيه ضرباتهم إلى تلك الأنظمة، كما أنه بوسعهم إيجاد المسارات التي تتيح لهم إمكانية الاختباء والتخفي دون أن يشعر بهم أو يلتفت إليهم أحد².

الفرع الثاني : المجرمون الهواة والمجرمون المحترفون

في معرض تعريف هواة ارتكاب جرائم الحاسب الآلي، أطلق "د. محمد سامي الشوى" عليهم لقب "صغار نوابغ المعلوماتية"، وأورد تعريفا لهذه الطائفة بقوله "ويقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية". أما "توم فوريستر" فأطلق على هذه الطائفة لقب "المتلعثمين" وهي طائفة ممن يقومون باستخدام الحاسب بصورة غير مصرح بها ولأغراض خاصة أو لمجرد التخريب الأعمى أو العبث لمجرد العبث بواسطة خطوط الهاتف بعد إيجاد كلمة السر.

ويهدف هاوي ارتكاب جرائم الحاسب الآلي (hacker) إلى الحصول على المعلومات بشتى الوسائل ويسخر قدراته في هذا المجال، ومن أمثلة الجرائم التي قامت طائفة الهواة بارتكابها، أفراد العصابة (414) الأمريكية التي نسب إليها أكثر من 60 فعل وتعدّي واختراق لذاكرات الحاسب الآلي، كذلك قيام أولاد في المدرسة الثانوية في "مانهاتن" عام 1980 باختراق شبكة بيانات شركة الاتصالات الكندية وتدمير ملفات زبائن الشركة³.

أما المجرمون المحترفون، فيطلق عليهم مصطلح (Crackers) أغلب هذه الطائفة من الشباب الذين تجاوزوا الخمسة والعشرين عاما، ويتميز أفراد هذه الطائفة بالتخصص العالي في مجال الحاسب الآلي والمعرفة التقنية والذكاء، وتدل الاعتداءات التي يرتكبها أفراد هذه الطائفة على جانب كبير من الخطورة الإجرامية بعكس طائفة الهواة، وكذلك فإن أغلب

¹ - محمد حميد مضحي المزمومي، جريمة الاعتداء على الأموال عن طريق الحاسب الآلي - دراسة قانونية بالفقه الإسلامي -، بحث مقدم لنيل درجة الماجستير في الفقه الإسلامي، جامعة الملك عبد العزيز، الرياض، المملكة العربية السعودية، 1428 هـ، ص 22-23.

² - Piter Stephenson, investigating computer trlated crime, C.R.C. press, Washington, USA, 2000, p 27.

³ - محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، المملكة الأردنية، 2009، ص 40-41.

أفراد هذه الطائفة ممن يعملون في منشآت تستخدم الحاسب وباستمرار، وهم بحكم وظيفتهم يتصلون بالحاسب الآلي اتصالاً وثيقاً، الأمر الذي يجعلهم يطلعون باستمرار على محتويات الحاسب وأسرار العمل¹.

المطلب الثالث: دوافع المجرم المعلوماتي

إذا كانت الدوافع الباعثة على اقتراف جرائم التكنولوجيا المتقدمة كثيرة ومتنوعة تختلف من مجرم معلوماتي إلى آخر، وقد تختلف من جريمة معلوماتية إلى أخرى، فإنه يكون من المتعذر حصرها، غير أنه يمكن على أية حال ضرب بعض الأمثلة التي تحدث عنها المتخصصون والخبراء المتابعون لتطور ظاهرة الإجرام الإلكتروني المستحدث، وفي الفقرات الموالية تفصيل لذلك:

الفرع الأول: الدوافع الشخصية

1- السعي إلى تحقيق المكسب المادي:

في دراسة أشار إليها الأستاذ "Parcker" فإن 43% من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال. ووفقاً للدراسات، فإن القطاع المالي يعد أكثر القطاعات استهدافاً من قبل جرائم الحاسب الآلي، ويرجع ذلك إلى أن البنوك تعتمد بشكل أساسي على أنظمة تحويل إلكتروني (EFTS- Electronic Fund Transfer Systems) الأمر الذي زاد فرص النصب، وبشكل هائل، فمجرد سقوط رموز التحويل الإلكتروني في الأيدي الخاطئة فإن ملايين الدولارات يمكن أن تنتقل، وفي ثوان معدودة، دون أن يترك دليلاً ضده. ويقدر النصب على البنوك الأمريكية بواسطة بطاقات التسليف بحوالي (2 مليون دولار)، وذلك في عام 1985 فقط². وعادة ما يكون هؤلاء المجرمين من العاملين على إدخال البيانات في ذاكرة الجهاز، أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات³، وقد يقوم الجناة ببيع تلك المعلومات⁴، أو بمقايضتها مع أشخاص آخرين.

كما أن شركات التأمين تعد من المؤسسات المستهدفة بعمليات النصب والاحتيال، كما أنها قد تقوم بدور الجاني في بعض الأحيان كشركة تأمين "أكوايتيفينغ" بمدينة "لوس أنجلوس" الأمريكية التي تمكن مستخدميها، وبمساعدة نظامها المعلوماتي، من خلق عملاء وهميين مؤمن عليهم، حيث تمكنت هذه الشركة من بيع (46 ألف) بوليصة تأمين إلى شركة مناظرة في إطار اتفاقيات تشيئة التأمين⁵.

2- الرغبة في تحدي وقهر النظام المعلوماتي:

¹ - محمود أحمد عبابنة، نفس المرجع السابق، ص 42-43.

² - محمود أحمد عبابنة، نفس المرجع السابق، ص 25.

³ - خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، جمهورية مصر العربية، 2010، ص 76.

⁴ - André Vitalis, pouvoir et libertés, édi economica, Paris, 1981, p 135.

⁵ - محمود أحمد عبابنة، المرجع السابق، ص 25.

لوحظ بأن هذه الجرائم قد ترتكب أحيانا لمجرد قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله¹، فالدافع في هذا الفرض لا ينبئ عن خطورة إجرامية كامنة في نفس مقتري هذه الأفعال، إذ أنهم عادة لا يكونون من معتادي الإجرام، بل يتمثل في رغبة هؤلاء بتحدي النظام التكنولوجي المعقد للحاسب الآلي بكل مكوناته ومعطياته ومحاولة اختراقه عن طريق الوصول إلى المعلومات. ففي الوقت الذي يزداد فيه الاهتمام بأمن الحاسب الآلي عن طريق تطوير طرق جديدة وصعبة للاختراق كبرمجيات التشفير التي تمكن مستخدميها وحده من فهمها، ومن الأمثلة على ذلك وزارة الدفاع الأمريكية (البيتاغون) التي تقوم بتغيير أنظمة الترميز للبيانات المستخدمة يوميا حتى أن بعض المعلومات الحساسة تغير كل ساعة أنظمة ترميزها، وهذا مما لا شك فيه يدل على قدر عال من التقنية والنظام المتطور، فإن الجانب الآخر الذي يقف على الضفة الأخرى -أصحاب الشغف الإلكتروني- يتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، والدليل على ذلك قيام أحد الهواة في أوروبا بحل شفرة أحد مراكز المعلومات في البيتاغون وتمكنه من العبث في بيانات هذا المركز².

الفرع الثاني: الدوافع السياسية

هنالك نوع آخر من الاختراقات يرتبط بأهداف سياسية³، فلقد سخرت شبكة الإنترنت في الصراعات السياسية الدائرة اليوم، وشهدت السنوات القليلة الماضية محاولات دولية لاختراق شبكات حكومية لمختلف دول العالم، فالتجسس عبر الإنترنت يتم يوميا من قبل أجهزة المخابرات. كذلك فإن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، وخير مثال على ذلك عندما استطاع ثلاثة إخوة من قرية "كفر قاسم" الفلسطينية من اختراق شبكة المخابرات الإسرائيلية "الموساد" وجهاز الأمن الإسرائيلي "شين بيت" واستطاعوا أن يتنصتوا على عدد من المكالمات والحصول على بعض المعلومات السرية وتقديمها إلى السلطة الفلسطينية، علما بأن الأشخاص الثلاثة من فاقد البصر.

وقد ذكر تقرير ورد بجريدة الأهرام المسائي أنه في محاولة للاحتجاج على احتلال إسبانيا لجزيرة "إليلى" المغربية قام مجموعة من قراصنة المغرب باختراق موقع إسباني على شبكة الإنترنت، وقد تمكنت المجموعة التي تحمل اسم وشعار "منظمة الهاكرز المغاربة" من الوصول إلى الموقع الإسباني وتصميم صفحة خاصة وضع عليه خاتم المجموعة الشهيرة به، وهو شكل صورة مركبة من الألوان والرموز والحروف التي ترمز للمجموعة، وقد تركت هذه المجموعة رسالة على الموقع الإسباني توضح أن الاختراق له علاقة بالأحداث التي هزت العلاقات المغربية الإسبانية. ويمضي التقرير

¹ - وليد العاكوم وآخرون، المرجع السابق، ص 445.

² - محمود أحمد عبابنة، المرجع السابق، ص 25.

³ - وليد العاكوم وآخرون، المرجع السابق، ص 446.

قائلا: "وتجدر الإشارة إلى أن هذه ليست هي المرة الأولى التي انتقلت فيها الحروب بين الشعوب إلى شبكة الإنترنت، فقد كشف تقرير صدر عن أكثر من مئة وخمسة عشر موقعا يهوديا على شبكة الإنترنت أنه قد تعرض للاختراق"¹.

الفرع الثالث: دوافع أخرى

قد ترتكب جرائم الحاسب الآلي بدوافع شخصية خاصة بمرتكبيها، وتكون هذه الدوافع بهدف الانتقام من صاحب العمل، كقيام أحد المحاسبين بالتلاعب في البرامج المحاسبية للشركة بعد أن يتم إبلاغه برغبة رب العمل بفصله، بحيث تختفي هذه البرامج وتتآكل، رغبة في الانتقام.

كما قد ترتكب هذه الجرائم بهدف الاحتفاظ بالوظيفة، ومن الأمثلة عليها قيام أحد المستخدمين الذي يعمل في إحدى شركات التأمين بتهديد المسؤول عليه بأنه في حال إلغاء بطاقة أجره من ذاكرة الحاسوب الخاص بالشركة، فإن هذه الشركة سوف تدمر بياناتها تلقائيا باستخدام تقنية القنبلة المنطقية.

كما قد ترتكب هذه الأفعال خدمة لمصالح الغير، فقد تقوم بعض الشركات والمصانع والمنشآت باستئجار محترفي التقنية بهدف التجسس على منشآت أخرى، بقصد الاطلاع على أسرار المهنة أو آخر ما توصل إليه من علوم، اختصارا للوقت في البحث، أو لأجل المنافسة التجارية².

الخاتمة:

إن الدراسات التي أجريت في مختلف أنحاء العالم أثبتت حقيقة لا تقبل الشك، وهي أن مجرمي التقنيات الحديثة ليسوا كغيرهم من الجناة، ليس فقط لكون أنشطتهم تشيع بالأساس فقدان الثقة بالتقنية بدلالاتها الواسعة، وتهدد إبداع العقل البشري، وتطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، بل لأنها هزت صورة نمطية لطالما نالت على الدوام حظاً وافراً من التبجيل والاحترام لدى العام والخاص، ألا وهي شخصية الإنسان المتعلم والمتقف الذي تبوأ مركزاً وظيفي أو اجتماعي مرموق، كان يفترض في صاحبها أن يلتزم بكل ما تقتضيه مقومات تلك الشخصية، لكنه سخرها للوصول إلى مآرب خاصة، لا تختلف في جوهرها عن مآرب المجرم التقليدي التي اعتادت البشرية منذ القدم على التعامل معها، فمثل هذا النوع من الشخصيات، المركب من مجموعة من المتناقضات التي انصهرت وامتزجت مع بعضها لتخرج للعالم نموذجاً غير معهود من المجرمين، لا شك أنها تثير العديد من علامات الاستفهام التي تتطلب التوصل إلى أيجاد تفسير لها، وهي مسألة ليست بالسهلة، كما يؤكد المختصون باستجلاء ملامح وأحوال المجرمين.

¹ - د. محمود عبد الرحيم الذيب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2005، ص 48-49.

² - محمود أحمد عبابنة، المرجع السابق، ص 28-29.

- بعد دراسة موضوع قرصنة الإنترنت، يرى الباحث تقديم بعض المقترحات، يتوخى أن تضيف ولو قدراً علمي يسير إلى الجهود الرامية لمواجهة ظاهرة الجرائم الناشئة عن استخدام التكنولوجيا، لخصناها في النقاط الآتية:
- 1- نلفت نظر الباحثين إلى ضرورة الاهتمام بظاهرة الإجرام المعلوماتي، بل وإلى أهمية تخصص فئة منهم في هذا المجال، أو على الأقل أن يجعلوا له جانب ولو يسير من دراساتهم البحثية، على يشمل كافة العلوم ذات الصلة بمكافحة الجريمة، وألا يقتصر فقط على رجالات القانون الجنائي، لأن تسليط الضوء على شخصية مرتكبي جرائم الكمبيوتر والإنترنت يقع بالدرجة الأولى على ثلة من العلوم الأخرى، كعلم النفس، وعلم الاجتماع، وعلم الإجرام، وعلم السياسة الجنائية.
 - 2- دعم مختلف هيئات البحث العلمي الوطنية، من مراكز ومعاهد وجمعيات علمية، بكافة الوسائل التي من شأنها تسهيل العمل فيها، بغرض تقديم منتج علمي ذا قيمة ومصدقية، وعلى مستوى من الجودة، بحيث يحظى بقبول واحترام من طرف الغير.
 - 3- يجب على من ولج عالم هذا النمط من الجريمة أن يركز على المواضيع التي تشغل بال الدارسين في أنحاء المعمورة، فيبدؤون حيثما انتهوا عنده، ولا يخوضوا فيما فرغوا منه منذ زمن بعيد، على أن يأخذوا في عنايتهم من الموضوعات ما يهم مجتمعنا، ويراعي طبائعه وخصوصياته، كي لا تصطدم برفض أفراده المشاركة فيها، أو عدم مبالاتهم بمضامينها.
 - 4- ضرورة التنسيق الجهود المبذولة، سواء من طرف الهيئات البحثية فيما بينها، أو الباحثين الأفراد فيما بينهم، من أجل تبادل الآراء والأفكار، ولما لا توسيع النطاق الجغرافي للدراسات، خصوصاً تلك التي تتطلب النزول إلى الميدان، والتواصل مع الأشخاص من خلال اللقاء المباشر.
 - 5- ينبغي الإكثار من القنوات التي تتيح للباحثين نشر أعمالهم، قصد تمكين البقية منهم من الاطلاع عليها للاقتباس منها، أو تقييمها بإبداء الملاحظات والردود عليها، على اعتبار أن ذلك من أفضل سبل ترقية البحث المتعارف عليها.
 - 6- يضم الباحث صوته إلى أولئك الداعين إلى وجوب إدراج مادة القانون الجنائي، ليس فقط في المعاهد والكلليات التي تدرس العلوم المتصلة بالكمبيوتر، وإنما في سائر التخصصات الجامعية الأخرى، بما يتلاءم مع طبيعة الدبلوم المرغوب الحصول عليه، لأن الواقع العملي يؤكد ازدياد معدلات أنواع محددة من الجرائم، سواء في المجال الطبي، أو الهندسة المعمارية ... الخ، فلا غرابة إذن أن يتخرج من جامعاتنا وجامعات العالم جيل من القرصنة يعتبر اقتحام أنظمة أمن المعلومات مجرد لعبة تستدعي التحدي لإثبات القدرات الشخصية، رغم إدراكهم أن أنشطتهم تنطوي على تعدٍ على حقوق ومصالح غيرهم من الناس.
 - 7- وما دامت الوقائع تطالنا عن وجود هذه الفئة من المجرمين بين جنبتنا، وطالما أن الردع والتوعية وحدهما لا يكفيان لإزالة الشغف المعلوماتي لدى الكثير من هؤلاء، نظراً لارتباطهم بوسائل تقنية المعلومات منذ نعومة أظافرهم، وأصبح من شبه المستحيل فصلهم عنها، فإنه يصبح من الأهمية بما كان البحث عن فضاءات قانونية تسمح لهم بممارسة هواياتهم بكل حرية، وذلك بإقامة نوادي خاصة تمنح لهم فرصة التباري تحت أنظار المجتمع، ولما لا

الاستفادة من عباقرتهم من طرف القطاعين الاقتصادي والحكومي فيما بعد، وعدم تركهم يلحون بيئة الجريمة من حيث لا يعلمون.

8- ومن خلال مثل هذه الفضاءات، يمكن تلقينهم أخلاقيات استخدام التكنولوجيا الحديثة، من خلال الاختلاط بهم، وعلاج المدمنين منهم على استخدامهما، وتوجيه طاقاتهم وجهات أخرى من شأنها أن تعود بالنفع عليهم في حاضرتهم ومستقبلهم.

9- توفير الحماية القانونية المناسبة لأنظمة الحماية الإلكترونية من مخاطر العبث واستخدامها لأغراض غير مشروعة، وذلك بإصدار قوانين تنظم إنتاج وتداول واستخدام برمجيات الحماية، مثل برامج مضادات الفيروسات، وبرمجيات كسر كلمات المرور، وبرامج تشفير البيانات والمعلومات.

10- ضمان التنظيم التشريعي الأمثل للبنية التحتية المعلوماتية، بما يسمح باستعمالها في حدود القانون، ويمنع استغلالها في أغراض جرمية.

11- المسارعة للانضمام للاتفاقيات الدولية، الإقليمية والعالمية، المتصلة بمكافحة الجرائم الناشئة عن سوء استخدام الكمبيوتر والإنترنت، لكي يتسنى للأجهزة المكلفة بإنفاذ القانون الحصول على المعلومات التي من شأنها أن تفضي للوصول إلى مرتكبي هذا النوع من الجرائم، بل حتى اكتساب المهارات الفنية اللازمة لاقتفاء أثر مجرمي التقنية الرقمية.

12- يتعين أن تأخذ هيئات إنفاذ القانون التحديات الأمنية للفضاء السيبراني بمحمل الجد، وأن تضع إستراتيجية علمية متكاملة لمواجهة تلك التحديات، يقوم بإعدادها أشخاص من ذوي الاختصاص.

13- سبق وأن رأينا بأن قراصنة الإنترنت يتميزون بقدرات عالية من الذكاء والمهارة الفنية والتخصص الدقيق في مجال تقنية المعلومات، لذلك فإن عملية مكافحة الجريمة المعلوماتية تقتضي ضرورة أن يتميز الأشخاص المكلفون بمتابعة هذا النوع من الإجرام أن يتمتعون بمستوى علمي رفيع، يماثل أو يفوق المستوى المهاري للمجرمين، ولا يمكن على الإطلاق الوصول لتلك الغاية بمجرد الاكتفاء بإدراج الجريمة المعلوماتية ضمن المقررات التكوينية لضباط الشرطة ورجال القضاء، أو إعطائهم بعض الدورات التدريبية دون إعادة تقييم مدى استيعابها، أو الحكم على مدى نجاعتها على أرض الواقع.

قائمة المصادر:

أولاً: المصادر العربية

أ- الكتب:

1- الكتب العامة:

د- علي حسين الخلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت، 1982.

- قولقجان سيرفي بورجن ريم، السطو على المصارف من منظور المجرم، ترجمة: عبد القادر أحمد عبد الغفار، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1408 هـ.

- محمد علي سالم العياد الحلبي، شرح قانون العقوبات (القسم العام)، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1997، ص 94.

2- الكتب المتخصصة:

- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، ج م ع، 2010.

- د. عبد الله بن سعود محمد السراي، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، 2011.

- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، الطبعة الثانية، دون ناشر ودون مكان نشر، 2000.

- الحامي محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، ط 1، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.

- د. محمد دباس الحميد ود. ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط 1، دار حامد للنشر والتوزيع، عمان، الأردن، 2007.

- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، المملكة الأردنية، 2009.

- د. محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2005.

- د. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها ومكافحتها)، دار الكتب القانونية، المحلة الكبرى، مصر، 2005.

- وليد العاكوم وآخرون، بحوث مؤتمر القانون والكمبيوتر والإنترنت، الإمارات العربية المتحدة، 1-3 مايو 2000، ج 2، ط 2، الناشر: كلية القانون، جامعة الإمارات، العين، أبو ظبي، الإمارات العربية المتحدة، 2004.

ب- الرسائل العلمية:

- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل درجة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2011 - 2012.

- محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، بحث مقدم للحصول على درجة الماجستير في التشريع الجنائي الإسلامي، قسم العدالة الجنائية، كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية، الرياض، م ع س، 1423-1424 هـ.

ج- الأوراق العلمية:

- منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، الملتقى العلمي للجرائم المعلوماتية، نظمته هيئة التحقيق والإدعاء العام، الرياض، المملكة العربية السعودية، 2009.

ثانياً: المصادر الأجنبية

- André Vitalis, pouvoir et libertés, édi economica, Paris, 1981.

- David Johnson, electronic privacy, Stodder, Cannada, 1997.

- Piter Stephenson, investigating computer trlated crime, C.R.C. press,

Washington, USA, 2000.