مجلة المستقبل للدراسات القانونيّة و السياسيّة

السمات الخاصة للجريمة المعلوماتية

الأستاذ الدكتور :بن شهرة شول/ الأستاذ :مراد مشوش - كلية الحقوق و العلوم السياسية –جامعة غرداية

السمات الخاصة للجريمة المعلوماتية

الأستاذ الدكتور: بن شهرة شول / الأستاذ : مراد مشوش – جامعة غرداية

تاريخ استلام المقال:2020/05/03	تاريخ المراجعة: 2020/05/12	تاريخ القبول: 2020/06/01

ملخص :

الجريمة المعلوماتية هي إفراز ونتاج لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما أكسبها لونًا وطابعًا قانونيًا خاصًا يميّزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الصفات قد يتطابق بعضها مع صفات طوائف أخرى من الجرائم هذا من ناحية ومن ناحية أخرى، فإنّ اختلاف الجريمة المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية،مما جعلها تتميز بمجموعة من الخصائص أو السمات الخاصة المحيطة بالجريمة نفسها من مادياتها وحجم أضرارها وطرق البحث والتحقيق فيها، ناهيك عن الفاعل الأصلي فيها والمسمى بالمجرم المعلوماتي الذي غيّر من نوعية سلوكه المجرم وطرق ارتكابه وكذا أعطى وصف آخر لمسرح الجريمة،لذا فإنّ التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها.

الكلمات المفتاحية: المعلومة، الجريمة المعلوماتية، الحاسب الآلي، الإنترنت،المجرم المعلوماتي.

السمات الخاصة للجريمة المعلوماتية

الأستاذ الدكتور :بن شهرة شول / الأستاذ :مراد مشوش - كلية الحقوق و العلوم السياسية –جامعة غرداية

Abstract:

Information crime is a secretion and a product of information technology, as it is related to and based on it, and this has earned it a Special characterand legal nature that distinguishes it from other traditional or novel crimes with a set of attributes, some of which may be identical with the characteristics of other sects of this crime on the one hand and on the other hand, the different crime Informatics about traditional crimes in terms of criminal acts earned them extraordinary privacy, which made them distinguished by a set of special characteristics or features surrounding the crime itself from its materialities and the extent of its damages and methods of research and investigation, not to mention the original actor in it and called an information criminal who changed the quality of his criminal behavior and methods of committing He also gave another description of the crime scene, so getting to know more about the characteristics of this crime helps to find solutions to combat it.

مقدمة:

إنّ بحث أي فرع من فروع المعرفة لا بد من بيان مفهومه من خلال تعريفه وتبيان سماته الأساسية أي خصائه لكي يتم رسم الصورة العامة لهذا البناء المعرفي[1]، ومنه خلال موضوع الجرائم المعلوماتية وحول خصوصية هذا النوع من الجرائم عن غيرها من الجرائم الأخرى وبالرغم من حداثة هذا النوع من الجرائم إلاّ أنّه يصعب إيجاد تعريف موحد لهذا النوع من الجرائم فلقد وجدت العديد من المناهج والمدارس الفكرية التي خاضت في وضع تعاريف علميّة دقيقة لجرائم المعلوماتية وعلى الرغم من اختلاف هذه التعاريف والعقائد الفكرية[2] ، حولها إلاّ أنّها تصب في قالب واحد، ومن جهة أخرى ولاكتمال هذا البناء المعرفي حول تعدد هذه المناهج العلمية حول وضع تعريف شامل للجريمة المعلوماتية إلاّ أنّها تتفق حول سماتها الخاصة بها التي تميزها عن غيرها من الجرائم.

[1]-منذر الشاوي، فلسفة القانون، مطبوعات المجمع العلمي بالعراق، بغداد 1994، ص7

[2]- محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة ،1994، ص173

Email: mostakbalaflou@gmail.com————**ISSN : 2543-3865**

السمات الخاصة للجريمة المعلوماتية

الأستاذ الدكتور :بن شهرة شول / الأستاذ :مراد مشوش - كلية الحقوق و العلوم السياسية -جامعة غرداية

تتميز الجريمة المعلوماتية بخصائص وسمات تميزها عن غيرها من الجرائم الأخرى، فأول ما يلفت النظر في هذا النوع من الجرائم هو نعومتها وبعدها عن العنف فلا تتطلب لارتكابها الشدة ولا استعمال الأدوات الخطرة كالأسلحة ولا تحتاج إلى مداهمات وكسراً للأبواب أو تسلق الجدران، فنقل بيانات ممنوعة أو التلاعب بالأرصدة البنكية مثلاً لا تحتاج إلاّ إلى لمسات أزرار، ثم إنّ الجريمة المعلوماتية تمتاز أيضاً بإمكانية تنفيذها بسرعة فائقة أي ترتكب في وقت قياسي كما تتميز أيضاً بإمكانية ارتكابها عن بعد فلا تتطلب لوجود الفاعل في مكان الجريمة بل يمكنه تنفيذها في مكان بعيد عن مسرح الجريمة، فالقائم على الحاسوب في أحد المصارف في طوكيو مثلاً يستطيع تحويل مبلغاً من المال إلى أحد فروع المصارف في برلين في ألمانيا، وإنّ نسبة مُعتبرة من الجرائم المعلوماتية ترتكب عبر شبكات الإنترنت Internet حيث يكون الجاني في دولة والمجني عليه في دولة أخرى مما جعل التعاون الدولي[3] أمراً حتمياً لمكافحة هذه الظاهرة الإجرامية الجديدة، كما أنّ الجريمة المعلوماتية صعبة الإثبات لعدم وجود تلك الآثار المادية عند الجرائم التقليدية (بقع الدم، تكسير، خلع ...).

دون أن نغفل في سرد الخصائص والسمات التي تتميز بها الجريمة المعلوماتية عن غيرها من الجرائم عن الفاعل أو مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي[4]، لتميزه أيضاً عن المجرم التقليدي في أسلوبه المنفرد في تنفيذه للجريمة و سرعته و مهارته، وهذا ما يدعونا للتساؤل:

ما مظاهر السمات الخاصة للجريمة المعلوماتية ؟.

سنحاول فيما يلي التطرق إلى بعض السمات الخاصة المحيطة بالجريمة نفسها من خلال المحور الأول، أما المحور الثاني سنخصصه بدراسة أهم السمات التي يتميز بها المجرم المعلوماتي.

[3]- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع، عمان، 2006، ص361

[4]- نائلة عادل محمد قورة، جرائم الحاسب الاقتصادية دراسة نظرية و تطبيقية، ط1، دار النهضة العربية، القاهرة، 2003، ص49.

السمات الخاصة للجريمة المعلوماتية

الأستاذ الدكتور :بن شهرة شول / الأستاذ :مراد مشوش - كلية الحقوق و العلوم السياسية -جامعة غرداية

المبحث الأول: السمات الخاصة المحيطة بالجريمة

تُعد الجرائم المعلوماتية إفرازًا ونتاجًا لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما أكسبها لونًا وطابعًا خاصًا يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من السمات، قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإنّ اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية.

إنّ متابعة جرائم الحاسب الآلي والإنترنت والكشف عنها من الصعوبة بمكان حيث أن هذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة وإنّما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنّ الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستر عنها، كما تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة[5].

المطلب الأول: خصوصية الجريمة غير التقليدية

تتسم الجريمة المعلوماتية عن غيرها من الجرائم التقليدية بسمات تستأثر بها و تميزها عنها ويرجع ذلك إلى عدة أسباب أهمها:

– ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية:فقد أكدت "انتل سكيوريتي"، الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات، أن قطاعات الأعمال

[5]- أحمد سعد، الجريمة الالكترونية وطابعها الدولي، www.wata.cc، 2020/02/21، 15:30

العالمية تتكبد خسائر سنوية تصل إلى 400 مليار دولار أمريكي، وأوضحت الشركة أن الهجمات الإلكترونية أصبحت اقتصادا متناميا قائما بذاته تبلغ قيمته ما بين 2 إلى 3 ترليون دولار سنويا، أو ما يشكل 15 إلى 20% من القيمة الاقتصادية الناتجة عبر الإنترنت، وقد تكبدت شركة بريطانية خسائر بلغت 1.3 مليار دولار بسبب هجوم إلكتروني واحد، وخسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة، بين العامين 2015 و2017[6].

– صعوبة اكتشافها:فقد تقع جرائم معلوماتية معينة ولا يشعر أحد بأنّ هناك جريمة وقت إلاّ بعد مرور وقت طويل، وربما لا تكتشف نهائيا، والسبب في ذلك يعود إلى أنّ جرائم المعلوماتية عادة تقع في بيئة افتراضية غير ملموسة غالب الأحيان، ولا يمكن استشعارها بشكل عادي محسوس.

فالجرائم المعلوماتية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمرا ليس عسيرًا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها، كما أنّ المجني علية يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهو الثقة في كفاءتها[7].

[6]- عيد كامل، تحقيق حول الخسائر التي تسببها جرائم الحاسوب، www.elaph.com، 2017/12/23، 21:32

[7]- نهلا عبد القادر المومني، الجريمة المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2016، ص58

– **صعوبة إثباتها:** وتعني الصعوبة في إثبات وقوع الجريمة بعد اكتشافها، أو بعبارة أخرى الصعوبة في إثبات التنفيذ، فبعد اكتشاف الجريمة والعلم بوقوعها، هناك صعوبة في إثبات أحداثها، والسبب من ذلك هو أنّ هذا النوع من الجرائم غالبا ما يتم تنفيذه بطرق المركزية صعبة ومهارات تخصصية عالية، ويتم الوقت نفسه إخفاء أو مسح أي آثار قد يتركها الجاني.

حيث أنّ في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإنّ إثباتها أمر يحيط به الكثير من الصعاب، فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى الجهات المختصة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة[8].

تجدر الإشارة إلى أنّ وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثارا مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائية الكشف عن الجريمة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره والإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين[9]:

الأول: إنّ الجريمة المعلوماتية لا تخلف آثار مادية.

[8]- ذيب بن عايض القحطاني، أمن المعلومات، مكتبة مدينة الملك فهد للعلوم والتقنية، الرياض، 2015، ص333

[9]- نهلا عبد القادر المومني، مرجع سابق، ص60

الثاني: إنّ كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبية، الأمر الذي يعطي مجالا للجاني أو للآخرين أن يُغيّروا أو يُتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستسقاة من المعاينة في الجريمة المعلوماتية.

-يتطلب لارتكابها وجود جهاز إلكتروني: تتميز الجريمة الإلكترونية عن غيرها أنّ الجهاز الإلكتروني هو أداة الجريمة ووسيلة تنفيذها، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات والمعلومات، كما تتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والإنترنت في بعض الجرائم، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنّها لا تمتاز بالعنف، وأغلب الجرائم الإلكترونية تركب عبر الإنترنت[10].

ولذلك فإنّ ما يميّز الجريمة الإلكترونية عن غيرها من الجرائم، أنّها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والإنترنت، وتُعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع[11].

كما أثبت الواقع العملي أنّ الجرائم الإلكترونية قد ترتكب من خلال الهواتف المحمولة، خاصة بعد ظهور أجهزة الهاتف الذكية والتي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت، ويسهل تخزين ونقل المعلومات من خلالها[12]، وليس كما ذكر

[10]- رامي متولي القاضي، مكافحة الجريمة المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2011، ص14
[11]- محمد أحمد عبابنة، جرائم الحاسب وأبعادها الدولية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2017، ص22
[12]- رامي متولي القاضي، مرجع سابق، ص16

بعض الباحثين بأنّ الحاسب إلى هو الأداة الوحيدة في ارتكاب الجريمة الإلكترونية، ففي أيامنا هذه ترى أنّه يمكن تصنيف هواتف المحمول الذكية ضمن أجهزة الكمبيوتر، وذلك لأنّه لا يختلف عن الحاسوب سوى في الحجم – بل إنّ الهواتف الذكية يمكن من خلالها الاتصال المباشر بخلاف الحاسب الآلي– أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسب الآلي من خلال الهاتف الذكي.

المطلب الثاني: الطبيعة الدولية للجريمة المعلوماتية

يمكن القول أنّ من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنّها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية و حجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[13].

ومن القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية، قضية عرفت باسم مرض نقص المناعة (الأيدز)، وتتلخص وقائعها عام 1989 عند قيام أحد الأشخاص بتوزيع عدد كبير من

[13]- Clément ENDRELIN,Lesmoyensjuridiques de luttecontre la cybercriminalité Diplômeuniversitairesécuritéintérieur/extérieurdansl'UnionEuropéen , 2011, p15

Email: mostakbalaflou@gmail.com——————**ISSN : 2543-3865**

النسخ الخاصة بأحد البرامج التي يهدف في ظاهرها إلى إعطاء بعض النصائح الخاصة بهذا المرض، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)[14]، وكان يترتب تعطيل الجهاز بمجرد تشغيله، ثم تظهر عبارة على الشاشة يقوم فيها الفاعل بطلب مبلغ مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد لهذا الفيروس، وفي الثالث من فبراير 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة، وتقدمت المملكة المتحدة بطلب تسليمه لمحاكمته لديها باعتبار أن النشاط الإجرامي المتمثل في إرسال البرنامج تم في أراضيها، وأياً ما كان الأمر فإنّ لهذه القضية الأثر البالغ من ناحيتين:

الأولى: أنّها المرة الأولى التي تتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: أن يتقدّم شخص للمحاكمة بتهمة إعداد برنامج مخرب.

لقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي توجد بها المعلومات محل الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب " **إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبي وتستهدف الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، المادة 15 من القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال**

[14]- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، مرجع سابق، ص45

ومكافحتها"[15]، كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع و قبول الأدلة، ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية"[16].

وتُعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية وتجنب خلق ما يسمى "بجنة جرائم المعلوماتية "Computer Crime Havens"،إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.

ونجد أنّ هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم وإن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات[17]، والذي استحدث نصوصًا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من

[15] -القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، الجريدة الرسمية عدد 47، الصادر في 16 أوت 2009

[16]- نائلة عادل محمد قورة، مرجع سابق، ص54

[17]-قانون 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر 66-155 المؤرخ في 08 يونيو1966 المتضمن قانون العقوبات، ج.ر العدد71، الصادر 10 نوفمبر 2004،

القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات بالإضافة إلى قانون 04/09 المتضمن القواعد الخاصة للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته[18] وسنّ أحكام خاصة بالتعاون والمساعدة القضائية الدولية[19]، ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين :

الأول : داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

الثاني : دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرمو المعلوماتية عن عجز التشريعات الداخلية من ناحية ،و غياب الاتفاقيات الدولية التي تعالج سُبل مواجهة هذه الجرائم من ناحية أخرى.

[18]- قانون سبق الإشارة إليه .

[19] قد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على شرط احترام الاتفاقيات الدولية والاتفاقيات الثنائية والمعاملة بالمثل، أنظر، سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير في علم الإجرام والعقاب، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان ،الجزائر ، 2010،ص 22

المبحث الثاني: السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنّما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، ولقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker[20] واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة، وبالمجرم المعلوماتي بصفة خاصة لأنّه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر أنّه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء[21].

المطلب الأول: تميزه عن المجرم التقليدي

المجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي مُتميّز كما أنّه على درجة من العلم والمعرفة وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء[22] كما يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في أنّ الفاعل في الحالتين يبرر جريمته، بل إنّه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز إليها الأستاذ Parker بكلمة S.K.R.A.M وهي تعني: [23]

المهارة Skills،

[20]- نائلة عادل محمد قورة، مرجع سابق، ص54

[21] -Rose Philipe, La criminalitéinformatique à l'horizonanalyse prospective, Thémis, Paris, 2005, p61

[22]-EduinSuthreland ,White collar criminality ,Gers (Gilbert) in white collar criminal, The offender in business the professions,1998, p125.

[23]-Rose Philipe, Op cit, p75

المعرفة Knowledge،

الوسيلة Resources،

السلطة Anthority،

الباعث Motives.

– المهارة: المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلاّ أنّ ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إنّ الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

– أما المعرفة: فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أنّ المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو النظام المعلوماتي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

– أما الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها، كما يستطيع نظراً لمهارته ابتكارها، إذ وأنه كلما كان النظام المعلوماتي غير

مألوف ويتميز بالخصوصية كانت تشكل تحدياً للمجرم المعلوماتي وكانت الوسائل المتطلبة أكثر صعوبة[24].

– أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها، وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات.

الباعث: فمن وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الأضرار بالأشخاص الأمر الذي يعدونه غاية اللاأخلاقية، وبين الأضرار بمؤسسة أو جهة في

[24]- نائلة عادل محمد قورة، المرجع السابق، ص55

استطاعتها اقتصاديًا تحمل نتائج تلاعبهم، وهو ما يطلق عليه أعراض روبن هو[25] The Roben Hood Syndrome.

المطلب الثاني: أصناف المجرم المعلوماتي

بناء على ما تقدّم يمكن أن نقسم مجرمي المعلوماتية Cyber Criminals إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هده الطوائف فيما يأتي:[26]

– **الطائفة الأولى Pranksters**: الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم،ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

– **الطائفة الثانية Hackers**: فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

– **الطائفةالثالثة MaliciousHackers**: هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.

[25]- سفيان سوير، مرجع سابق، ص85

[26] - نائلة عادل محمد قورة، المرجع السابق، ص58

– **الطائفة الرابعة PersonnelProblemSolvers**:فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

– **الطائفة الخامسة Career Criminals**: مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على فعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ؛و يقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي[27].

– **الطائفة السادسة Extrem Advocates**: فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه؛ وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفًا جذابًا لهذه الجماعات، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم " TheRed Brigades" بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها و معتقداته.

– **الطائفة السابعة The CriminallyNegligent**: والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي

[27]- هشام محمد فريد رستم ، قانون العقوبات ومخاطرتقنيةالمعلومات، مكتبة الآلات الحديثة، أسيوط، 1995، ص69

أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح؛ ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات و لم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ[28].

[28]- محمد أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية ، المرجع السابق ، ص45

خاتمة:

اتسمت الجريمة الالكترونية بطبيعة خاصة وجدت صعوبة في وضع تعريف عام جامع وموحد لها، فقد اختلفت المفاهيم حولها باختلاف الزاوية التي ينظر إليها فمنهم من عرّفها على أنّها أساس وسيلة لارتكاب الجريمة، ومنهم من عرفها على أساس محل أو موضوع الجريمة، والبعض الآخر على أساس شخصية الجاني، والآخر جمع بين هذه التعاريف.

كما أنّ طبيعتها الخاصة تجلت في خصائصها المتميزة، والمتمثلة في أنّها جريمة عابرة للحدود باعتبارها ترتكب بواسطة الحاسوب أو في مجال الحاسب الآلي، كما تميزت بسرعة تنفيذها والتطور المتسارع في ارتكابها، ومما أعطاها خصوصية أكثر الخصائص التي تميز بها المجرم المعلوماتي وأشكاله، حيث لا يلجأ إلى العنف كما هو الحال في المجرم التقليدي، بل يتميز بالذكاء والمهارة والسلطة والمعرفة.

لذا فإنّ جرائم المعلوماتية هي جرائم غير تقليدية، وعندما ترتكب فإنّ الضرر الناجم عنها يكون غير تقليدي أيضا، وقد يكون الضرر الناجم عن جريمة المعلوماتية كبيرا جدا، ويمتد إلى عدد كبير من الضحايا، وذلك بناء على أهداف الجريمة نفسها، وقد يكون الضرر ماديا أو معنويا، وقد يشملهما معا.

النتائج:

- صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل ذات تقنية عالية.
- صعوبة قياس توقع الضّرر المترتب عليها، كونه ضرراً يمسّ الكيانات المعنوية ذات القيم المعنوية أو القيم الماديّة أو كلاهما سوياً.
- سهولة إخفاء وطمس معالم الجريمة وآثارها والدّلائل التي تُدل على مرتكبها، وهي أقل جهداً وعنفاً جسديّاً من الجرائم التّقليدية باعتبارها جريمة لا تتقيّد بمكان أو زمان مُحدّدين.

– تعتمد هذه الجرائم على قمة الذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم . إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض، وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية .

التوصيات:

– تفعيل أحدث التقنيات والوسائل للكشفِ عن هويّة مُرتكبي الجرائم.

– الاعتماد على مبدأ العالمية بالنظر لطبيعة الجرائم المعلوماتية العابرة.

– تكوين متخصص لجميع الأفراد المساهمين في مكافحة هذا النوع من الجرائم.

– أهمية تفعيل دور الأسرة في متابعة الأبناء ووقايتهم من إخطار شبكة الانترنت بالإضافة إلى توعية المجتمع المدني والجمعيات وكذا وسائل الإعلام في الحد من هذه الجرائم.

قائمة المراجع

أولا: الكتب

- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط مصر،1998.

- منذرالشاوي، فلسفة القانون، مطبوعات المجمع العلمي بالعراق، بغداد، 1994.

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

- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2006.

- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط2، دار الثقافة للنشر والتوزيع، عمان2017.

-رامي متولي القاضي، مكافحة الجريمة المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2011.

- ذيب بن عايض القحطاني، أمن المعلومات، مكتبة مدينة الملك فهد للعلوم والتقنية،الرياض 2015.

- نائلة عادل محمدقورة، جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية، ط1، دار النهضة العربية، القاهرة، 2003.

- نهلا عبد القادر المومني، الجريمة المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، 2016.

ثانيا: المذكرات

- سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير في العلوم القانونية تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان الجزائر، 2006.

ثالثا: المواقع الالكترونية

– عبد الاله مجيد، القراصنة يستهدفون الدول الغنية،wwwwww.elaph.com، 2016/02/21 15:30

– محمد عبد اللهالمنشاوي، جرائم الانترنت من منظور شرعي وقانوني، الجمعية الدولية للمترجمينwww.wata.cc، 2017/12/23، 21:32

رابعا: القوانين

– القانون 04- 15 مؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة في 10 نوفمبر 2004.

– القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

Ouvrages :

-EduinSuthreland ,White collarcriminality ,Gers (Gilbert) in white collarcriminal, The offender in business the professions,1998.

- Rose Philipe, La criminalité informatique à l'horizon analyse prospective, Thémis, Paris, 2005

Théses :

-Clément ENDRELIN, Les moyens juridiques de lutte contre la cybercriminalité, Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011.