الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف –المسيلة–

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية الحقوق والعلوم السياسية

قسم: الحقوق

تخصص: قانون جنائي

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر تخصص: قانون جنائي

بعنوان

الجريمة الإلكترونية وإجراءات مواجهتها

إعداد الطلبة:

شاهين خضر

رضوان سعادة

إشراف الأستاذ

فواز لجلط

السنة الجامعية: 1441–1442 هـ /2020–2021

بسم الله الرحمن الرحيم

إهداء

قال تعالى:" قل اعملوا فسيرى الله عملكم ورسوله والمؤمنون"

لكل بداية نهاية، ولكل زرع حصاد، ولكل عمل خاتمة تسر القلوب بإذن الله مختومة بالصلاة على سيد المرسلين.

سلكنا أكثر من درب، وبذلنا أكثر من جهد، وعانينا الصعوبات مناجاةً للقمم، وها نحن اليوم نطوي سهر الليالي، وخلاصة المشوار، وتعب ألف يوم ويوم....

إلى ذلك الصرح العظيم، إلى قدوتي وفخري ومعلمي، نبراس متوهج بفضل عظيم، كزرع طيب أصلك ثابت ورأسك شامخ في سماء قلبي..

أبي الغالي... يا تاجاً أحمله على رأسي ... يا شرفاً يزيد وقاري...

إلى التي رأتني بقلبها قبل عيناها، إلى التي جعل الله الجنة تحدت قدماها، كل الحروف والعبر قد انحنت تحت طيف حبك، وبكل فخر تزفكي كلماتها...

إلى إخوتي وأخواتي، يا من حبكم يجري في عروقي، يا من وجودكم يشعل أنواراً لتنير طرقاتي، يا من تشتاق لكم روحي، كالورود أنتم في بستان قلبي...

وفي الختام أحبتي الكرام....

لا يسعني في هذا المقام إلا أن أتوج هذا العمل لأولى القبلتين وثالث الحرمين،

إلى مسرى رسولنا الكريم، فلسطين...أيقونة الصمود ورمز النضال.

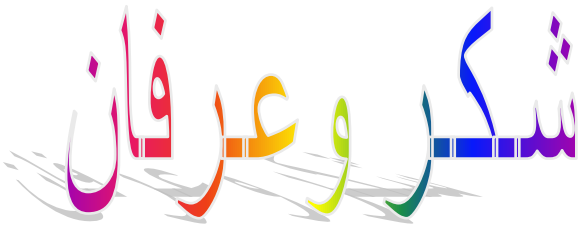
إلى شهدائنا الأبرار، وأسرانا البواسل، وجرحانا الكرام....

إلى بلد المليون ونصف مليون شهيد...

جزائرنا الحبيبة...

وذكريات السنين...

وقصة وطن نفيس، وشعب عريق قد سمي نفسه "جزائسطين".



" لا يشكر الله من لا يشكر الناس"

تتزين حروفي اليوم هنا لشكركم...وتهديكم أجمل عباراتي...

وكلماتي تسطع بحروفكم... وبأسماكم تكونت أجمل المعاني...

تلبسكم تاج الإمتنان بوقفتكم... ودعمكم بفرحتي ونجاحي...

فبدايتي قدوتي أنتم معلميني... ولا حروفاً تنصفك معلمي...

الأستاذ القدير/ لجلط فواز

كل الإحترام لك محملاً بكل شكر وعرفان، أدامك الله نبراساً ينير لنا طريق العلم والمعرفة.

وكذلك لا ننسى من زادنا بكرمه ونصائحه لنا، فوجوده كان عطراً زاد جهدنا رفعةً ووساماً.

الأستاذ الفاضل / بوبعاية كمال

والشكر أيضاً إلى من هو بمثابة أخوتي وسندي في غربتي الطلبة الفلسطينيين كل باسمه ولقبه فلا حروفاً تنصفه عمراً عشناه معاً، زاد من محبتنا وأخوتنا.

وفي الختام نشكر كل من كان له فضل في تعليمنا، أساتذتي وجامعتي...

كل التقدير لكم آبائي...

الملخص

لقد ساهمت تكنولوجيا المعلومات في تسهيل حياة البشر وتوفير الوقت والجهد، كما وأصبحت جزءً أساسياً في الحياة اليومية، وفوائدها ومكتسباتها كثيرةً جداً، وبالرغم من ذلك إلا أنه هناك أضراراً ناتجة عن إساءة استخدام التكنولوجيا المعلوماتية، فقد ظهرت الجريمة الإلكترونية مكشرةً عن أنيابها لتصبح ملاذاً آمناً للمجرمين لسهولة ارتكابها في أجواء هادئة بعيداً عن العنف، وصعوبة اكتشافها، بل وأنها غامضة و لا تعرف الحدود، الأمر الذي جعل منها خطراً كبيراً يهدد مصالح الأفراد وأمن الدول واستقرارها، لذلك تسعى العديد من الدول حول العالم إلى التصدي لهذه الجريمة ومواجهتها بوضع حد لها، فالإشكال المطروح في عدم مواكبة التشريعات القانونية لتطور الأنظمة المعلوماتية، وعجزها عن حماية مصالح الأفراد المستخدمين للنظم المعلوماتية.

الكلمات المفتاحية: الجريمة الإلكترونية، نظام المعالجة الآلية للمعطيات، الفضاء الإلكتروني، جرائم ذوي الياقات البيضاء، الجرائم السيبرانية.

Summary

Information technology has contributed to facilitating human life, saving time and effort, and has become an essential part of daily life, and its benefits and gains are many. However, there are damages resulting from the misuse of information technology. Cybercrime has emerged out of its teeth to become a safe haven for criminals because it is easy to commit in a calm atmosphere, far from violence, and the difficulty of detecting it, even as it is vague and does not know the borders, which made it a great danger threatening the interests of individuals and the security and stability of states, Therefore, many countries around the world seek to address this crime and confront it by putting an end to it. The problem arises in the failure of legal legislation to keep pace with the development of information systems, and its inability to protect the interests of individuals who use information systems.

Key words:
Cybercrime, automatic data processing system, cyberspace, white collar, crimecybercrime.

لقد شهد العالم تطوراً حضارياً في مختلف مجالات الحياة، منها مجال تكنولوجيا المعلومات الذي أصبح منافساً لجميع مناحي الحياة، وانعكست استخداماته على المجتمعات الحديثة، وأصبح سمةً من سمات العصر الراهن، وشكل أحد ميادين الحرب بين الأمم خصوصاً وأن هيئات إستراتيجية مثل الجيوش والمصارف والشركات وغيرها صارت تعتمد على المجال الإلكتروني في تخزين المعلومات وتكوين البنية التحتية المعلوماتية مما يجعلها عرضةً للهجمات الإلكترونية.

هذا وقد ربطت تكنولوجيا المعلومات العالم برباط واحد من خلال الشبكة العنكبوتية "الانترنت" إذ أصبح العالم بفضلها كقرية صغيرة وأحدثت ثورة في شتى المجالات، وقد أصبح النظام المعلوماتي في نهاية القرن الماضي من لوازم الحياة الضرورية والمتطورة على المستوى العام أو الخاص، ولا يخفى أن كل تطور تقني تكون له انعكاساته على المستوى القانوني بصفة عامة، وفي إطار القانون الجنائي بصفة خاصة، فكل المخترعات الحديثة تثير بعض المصالح والحقوق التي تحتاج إلى الحماية الجنائية لها سواء في إطار النصوص التقليدية أو باستحداث النصوص الملائمة لطبيعتها والدور الذي تؤديه في مختلف مجالات النشاط حيث تؤثر في الإنسان كياناً ونشاطاً[1].

وكما أن هذا العالم الجديد أصبح يزخر بتطورات تنير درب البشرية فإن له كذلك جانباً مظلم، حيث فتح مجالاً لإساءة استخدام تكنولوجيا المعلومات، والعمل على توظيفها سلبياً وبشكل غير قانوني لإشباع رغبات النفس الإنسانية.

ووفقاً لإحصاءات الانترنت فقد اجتازت الشبكة العنكبوتية 1.83 مليار موقع إلكتروني حول العالم لعام 2021 وتستقطب حوالي 4.803.660.196 مستخدم[2] .

[1]- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، ط2، الإسكندرية، 2006،ص8.
[2]- https://ar.vpnmentor.com/blog، 22/04/2021 بتوقيت الساعة 17:00.

وعندما حدث هذا التطور واجه المستخدمون والحكومات والمشرعون تحديات لم يتخيلوها من قبل، فقد أضفى طبيعة خاصة على جرائم كانت تقليدية قبل ظهور هذه التكنولوجيا، والتي أدت إلى ظهور أنماط مستحدثة من الأفعال الاجرامية لم تكن مألوفة لدى المجتمع والتي يمكن أن نطلق عليها جرائم تكنولوجيا المعلومات أو الجرائم الإلكترونية والتي أصبحت مصدر تهديد في الفضاء إلكتروني أو ما يسمى بالعالم الافتراضي،وبالتالي قد انتقل الناس من العالم الواقعي إلى العالم الافتراضي وكذلك انتقلت الجريمة[1].

وتكمن خطورة الجرائم الإلكترونية في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لاسيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية والمؤسسات والشركات العامة والخاصة.

ولا شك أن ازدياد الجرائم الإلكترونية والتي نشهد جزءً كبيراً منها اليوم يرتبط بازدياد هذا الاعتماد على شبكات الانترنت والحاسوب في البنى التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الجرائم الإلكترونية لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل. وقد أوجدت هذه التطورات التكنولوجية فرصاً لا تعد ولا تحصى للمجرمين لارتكاب أشكال مختلفة من الجرائم عبر الفضاء الإلكتروني، وإن كان التطور المستمر والمتجدد قد يؤدي إلى عدم استيعاب النصوص الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة، إلا أن وضع قواعد قانونية تنظم أوجه الحماية أفضل من ترك ما يستجد على الساحة الجنائية بدون حماية، وهذا ما يقع على عاتق الفقه بوضع نظرية عامة تسهم في صياغة المشرع للنصوص التشريعية، وتساعد القضاء في تفسير النصوص وتكييف الوقائع.[2]

[1]- أحمد عبدالاه المراغى، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، المركز القومي للإصدارات القانونية، ط1،القاهرة،2017، ص8.

[2]- غنية باطلي، الجريمة الإلكترونية، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص9.

فالتطور المتسارع لتكنولوجيا المعلومات والغموض الذي يحيط بالجرائم الإلكترونية حتى في البلدان التي أدخلت هذا النوع من الجرائم في تشريعاتها القانونية، وعدم دراية أصحاب الاختصاص في سن القواعد القانونية بأصول عمل هذا النظام وعدم وضوح هذا النوع من الجرائم وحداثته وقلة القضايا المعروضة أمام القضاء لهذا الشأن أدى إلى خلق فراغ قانوني في التشريعات القانونية .

وقد أسفرت محاولات تطبيق النصوص التقليدية على هذه الأنماط الجديدة من الإجرام عن كثير من المشكلات القانونية، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية، ولا يمكن أن تكتشف إلا بمحض الصدفة، فقد اختلفت آراء الفقهاء في شأن تطبيق النصوص التقليدية عليها، فصدرت أحكام تطبق النصوص التقليدية على أي سلوك ينطوي على الجرائم الإلكترونية، في حين اعتبرته أحكام أخرى بأنه فعلاً مباحاً لم يرد بشأنه نص يجرمه، فالقاعدة العامة " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون [1]"، بينما رأى آخرون أن تلك النصوص ينحصر نطاق تطبيقها عن الإحاطة بجرائم الحاسب الآلي، لأن موضوعها معلوماتي ولا يمكن اعتباره مالاً منقولاً تحميه النصوص الجنائية[2].

ويكاد يكون من المستحيل تقدير مقدار الجرائم الإلكترونية التي تحدث في معظم الدول في جميع أنحاء العالم بسبب نقص التعريفات القانونية الموحدة للجريمة الإلكترونية وغموضها. ومع ذلك تشير الأدلة إلى أن معدلات الجرائم الإلكترونية آخذة في الازدياد مع استمرارا معدلات الجرائم التقليدية.

وفي الآونة الأخيرة وخاصةً مع انتشار الأوبئة، تفاقمت هذه التحديات بسبب الخوف المؤدي إلى تصرفات متهورة وغير عقلانية، ويعتمد مجرمو الانترنت على

[1]- المادة 1 من أمر رقم 66-156، المؤرخ في 18.صفر.1386، الموافق 08.يونيو.1966، المتضمن قانون العقوبات، الجريدة الرسمية الجمهورية الجزائرية، عدد 49 صادر في 21.صفر.1386 الموافق 11.يونيو.1996، معدل ومتمم.

[2]- محمد عبدالله أبو بكر، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، 2007،ص9.

مبادئ نفسية أساسية لإغراء ضحاياهم والاستيلاء على معلوماتهم الخاصة، وشن حملاتهم الاحتيالية باستغلال الناس في مثل هذه الظروف حيث يكون الناس فيها أكثر استعداداً للتخلي عن حذرهم واندفاعهم لفتح الرسائل العشوائية، أو روابط التصيد الاحتيالي التي تبدو وثيقة الصلة بالقصص الإخبارية.

✓ **أسباب اختيار الموضوع:**

- التعلق بالحاسوب والأنظمة المعلوماتية.
- غموض الجريمة الإلكترونية وحداثتها.
- معاصرة الجرائم الإلكترونية والنظر إليها من الجانب القانوني.
- سهولة ارتكاب الجريمة الإلكترونية وتخفي المجرمين.

✓ **أهمية الموضوع:**

- دور الأنظمة المعلوماتية في شتى المجالات، والحاجة إلى مكافحة الجرائم الناتجة عنها.
- عجز التشريعات القائمة عن مواجهة هذا الخطر الداهم.
- نقص كفاءة السلطات على التعامل مع الجرائم الإلكترونية.
- ضرورة التصدي للجرائم الإلكترونية ووضع حد لها.

ولتسليط الضوء أكثر على الموضوع نطرح الإشكالية الآتية:

ما هي الجريمة الإلكترونية وآليات مواجهتها ؟

وللإجابة على الإشكالية المطروحة اعتمدنا على بعض المناهج الملائمة لطبيعة الموضوع، منها المنهج الوصفي حيث قمنا بوصف الجريمة الإلكترونية وتمييزها عن غيرها من الجرائم ودراستها، ثم المنهج التحليلي وذلك بتوضيح المفاهيم

الخاصة بالجريمة الإلكترونية وتحليلها، ثم المنهج المقارن من خلال مقارنة السبل التشريعية لبعض الدول في مكافحة الجريمة الإلكترونية.

متبعين في ذلك خطة منهجية ثنائية الفصول، خصصنا الفصل الأول منها إلى الجريمة الإلكترونية متطرقين في ذلك إلى مفهومها في المبحث الأول من خلال تعريفها وصورها وكذا خصائصها وأسبابها في المبحث الثاني.

أما الفصل الثاني فقد تناولنا فيه آليات مواجهة الجريمة الإلكترونية، والجزاءات المقررة للجريمة الإلكترونية، حيث تطرقنا إلى آليات السلطة التشريعية في مكافحة الجريمة الإلكترونية في المبحث الأول، والجزاءات المقررة للجريمة الإلكترونية في المبحث الثاني.

الفصل الأول

ما هي الجريمة الإلكترونية

تشهد البشرية منذ حوالي ربع قرن اتساعاً مطرداً لنطاق استخدام تقنية المعلومات في المجتمع وازدياداً بالغاً لدورها في تسيير كافة أموره، ونتج عن ذلك ظهور الجرائم المعلوماتية ونظرا لجسام أخطارها وفداحة خسائرها وسهولة ارتكابها وسرعة انتشارها ولاسيما في الدول الصناعية أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين و المهتمين بأمن الصرح المعلوماتي[1]، حيث إن غياب تعريف قانوني دقيق لهذا المصطلح وترك الأمر إلى الفقهاء لإعطاء مفاهيم وتصورات مختلفة جعل الأمر أكثر تعقيدا ويعتبر هذا الاختلاف مصدر التداخل أو الخلط لهذه المصطلحات سواء على مستوى مجال انعكاسه أو المصطلح المختار[2]. ونظراً لحداثة الظاهرة من ناحية، والتطور المتلاحق الذي يطرأ عليها من ناحية أخرى فقد تعددت تعريفات التي استخدمت للدلالة عليها واختلف الباحثون في تقسيم جرائم تقنية المعلومات والأفعال التي تدخل في إطار هذه الجرائم[3].

ونظراً لما قد يترتب على انتشار الحاسب الآلي في مجالات المختلفة من ظهور مشاكل وصعوبات قانونية في مجالات الإثبات والحماية المدنية والجنائية لبرامج الحاسب الآلي والتجارة الإلكترونية واستخدام التقنية فيما يسمى بالجريمة المنظمة وغيرها[4]، وبناءً على ما سبق سنقسم الدراسة في هذا الفصل إلى مبحثين نتناول في المبحث الأول مفهوم الجريمة الإلكترونية، وفي المبحث الثاني خصائص وأسباب الجريمة الإلكترونية، وذلك حسب النموذج الآتي:

[1] - احمد خليفة الملط، مرجع سابق، ص67 .
[2] - غنية باطلي، مرجع سابق، ص19.
[3] - علي جعفر،جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة ، منشورات زين الحقوقية، بيروت، ص75.
[4] - احمد عبد اللاه المراغى، مرجع سابق، ص23.

المبحث الأول: مفهوم الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الظواهر الحديثة وقد أحاط بتعريفها الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها, ولم يتفق الفقه على تعريف محدد بل ذهب البعض إلى عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني[1].

المطلب الأول: تعريف الجريمة الإلكترونية

في بداية حديثنا عن تعريف الجرائم المعلوماتية نلاحظ من خلال الأبحاث والدراسات التي أجريت بشأنها أنه لا يوجد مصطلح موحد للدلالة عليها وذلك خشية حصرها في مجال ضيق يمكن أن يضر بها،ومع ذلك لا بد من وضع تعريف لها يشمل العناصر الأساسية التي تسمح بتحديدها[2].

وينقسم هذا المطلب إلى ثلاثة فروع بدءً بالتعريف الضيق للجريمة الإلكترونية في الفرع الأول، مروراً بالتعريف الموسع في الفرع الثاني، وصولاً إلى التعريف العام في الفرع الثالث.

الفرع الأول: التعريف الضيق

اختلف الفقه في تعريف الجريمة الإلكترونية من وجهة نظر ضيقة فمنهم من اعتمد اعتماد معيار الوسيلة ومنهم من اعتمد معيار توافر معرفة تقنية الحاسب الآلي ومنهم من يرى أن الجريمة الإلكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي[3].

[1]- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية, الدار الجامعية، الإسكندرية، 2008، ص1و2.
[2]- المرجع نفسه, ص85.
[3]- غنية باطلي، مرجع سابق،ص17.

أولاً: معيار وسيلة ارتكاب الجريمة:

من التعريفات الضيقة للجريمة الإلكترونية ما جاء به الفقيه "Merwe" حيث يرى أن هذه الجريمة تتمثل في " الفعل غير المشروع الذي يشترط في ارتكابه الحاسب الآلي"[1].

يرى البعض أن الحاسب الآلي هو أساس هذه الجريمة ويميزها عن غيرها من الجرائم بوسيلة ارتكابها, حيث أصبح هذا الجهاز وسيلة ضرورية وتستعمل بشكل يومي ومتكرر نظرا للإمكانيات الهائلة التي يتمتع بها وسهولة التعامل معه ومسايرته لمختلف المجالات وتخزين كم هائل من المعلومات[2].

وعرف الفقيه Leslie D.Ball الجريمة الإلكترونية بأنها: " كل فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية[3].

وهذا تعريف موسع لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع, ولما كانت الجريمة بوجه عام سلوك ضار أو غير مشروع فكل جريمة عالجتها القوانين الجنائية التقليدية يمكن أن تدخل ضمن نطاق الجريمة المعلوماتية وهذا أمر غير مقبول, فرغم أن التعريف تحفظ واشترط في السلوك غير المشروع أن يكون مرتبط باستخدام الحاسب الآلي إلا أن ذلك لا ينبغي أن يشمل كافة الجرائم التقليدية[4].

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أيضاً أن الجريمة الإلكترونية هي "التي تقع على جهاز الحاسوب أو داخل نظامه فقط, أو هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تلك التي يتم تحويلها عن طريقه"[5].

---

[1] علي جعفر، مرجع سابق.
[2] غنية باطلي، مرجع سابق، ص15.
[3] احمد عبد الله المراغى، مرجع سابق، ص27.
[4] أيمن عبد الله فكرى،جرائم نظم المعلومات،دار الجامعة الجديدة،الإسكندرية، 2007، ص83.
[5] خالد ممدوح ابراهيم مرجع سابق، ص43.

وعرفها كلاً من Rtattory، A Hardcastleg من خلال تعريفهما للجرائم المرتبطة أو المتعلقة بالحاسب بأنها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسوب وبعبارة أخرى تلك الجرائم التي يكون دور الحاسب فيها ايجابيا أكثر من سلبيا[1].

ثانياً: معيار موضوع الجريمة

يرى آخرون أن تعريف الجريمة الإلكترونية إنما يرجع إلى موضوعها وغير متعلق بالوسيلة المستعملة أو الفاعل. حيث يرى هؤلاء أن الجريمة الإلكترونية هي التي تكون موضوعها المال المعلوماتي المعنوي, دون النظر فيما إذا كان الحاسب هو الأداة المستعملة في ارتكابه من عدمه[2].

ويرى واضعو هذه التعريفات أن الجريمة الإلكترونية ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع على النظام أو داخل نطاقه، ومن أنصار ذلك التعريف "روزن بلات" وآخرين الذين يرون أن الجرائم الإلكترونية هي: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه. ويندرج هذا النوع تحت جرائم المعالجة الآلية للبينات[3].

ثالثاً: معيار توفر المعرفة بالتقنية المعلوماتية

إن أصحاب هذا الرأي لا يستندون في تعريفهم على وجود الحاسب الآلي إنما على الشخص مستخدم الحاسوب حيث أن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم أن مرتكبيها يحيطون علماً ومعرفة بتقنية المعلومات وفي غياب هذه المعرفة لا يمكنهم ارتكاب هذه الجرائم[4].

[1] أيمن عبد الله فكرى، مرجع سابق، ص84.
[2] غنية باطلي، مرجع سابق، ص17.
[3] احمد خليفة الملط, مرجع سابق، ص87.
[4] غنية باطلي، مرجع سابق, ص16

ويعرفها آخرون بأنها "أي عمل ليس له في القانون أو العرف جزاء يضر بالأشخاص والأموال ويوجه ضد التقنية المتقدمة لنظم المعلومات"[1].

ويعرف جانب من الفقه الجريمة الإلكترونية على أساس سمات شخصية لدى مرتكب الفعل وهي تحديد السمة الدراسية والمعرفة التقنية ومن هذه التعاريف تعريف وزارة العدل الأمريكية لعام 1989 حيث عرفت الجريمة الإلكترونية بأنها "أي جريمة لفاعلها معرفة فنية بالحسابات تمكنه من ارتكابها"[2].

الفرع الثاني: التعريف الموسع

لقد وجهت للتعاريف السابقة العديد من الانتقادات أهمها أنها قاصرة على الإحاطة بأوجه ظاهرة الإجرام الإلكتروني فمثلاً الوسيلة المستعملة في ارتكاب الجريمة لا تدخل في تعريفها[3].

فعرفها أصحاب الاتجاه الموسع بأنها «كل سلوك إجرامي يتم بمساعدة الحاسوب» أو هي كل جريمة تتم في محيط أجهزة الحاسوب أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها[4].

وفي ذات الاتجاه يرى الفقيهان "Michel& Credo" أن سوء استخدام الحاسوب أو جريمة الحاسوب تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به[5].

[1] احمد خليفة الملط، مرجع سابق,ص86.
[2] علي جعفر، مرجع سابق,ص80.
[3] غنية باطلي، مرجع سابق, ص18.
[4] خالد ممدوح إبراهيم، مرجع سابق, ص42.
[5] علي جعفر، مرجع سابق, ص82.

وكذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية وتمتد أيضا لتشمل سرقة جهاز الحاسب أو مكوناته[1].

إن الأخذ بهذا التعريف الموسع منتقد كذلك لأنه لا يمكن الاعتماد على الوسيلة أو المناسبة التي حدث فيها الاعتداء وإنما وجب البحث في العمل الأساسي المكون لها وليس لمجرد استخدام الحاسب في ارتكابها ، ونعتبرها من الجرائم الإلكترونية بمعنى لتعريف أي جريمة ينبغي النظر في تلك الجريمة في حد ذاتها ونتيجة للمعايير السابقة الواردة في الاتجاه الضيق أو الاتجاه الموسع ظهر اتجاه آخر يعتمد على المصلحة المحمية أو الغاية من التجريم[2].

الفرع الثالث: التعريف العام

على الرغم من تباين التعريفات حول الجريمة الإلكترونية إلا أنني حاولت جمع بعض التعريفات الملمة بالظاهرة التي لا تعرف الخمول وفي تطور مستمر ومن أهمها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على الحاسب أو التي تحول عن طريقه كما تعرف بأنها كل فعل إجرامي متعمد أيا كان صلته بالمعلومات وسينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل[3].

وهناك تعريف أيضاً يطلق عليه اصطلاحا جرائم تكنولوجيا الحديثة ويعلق عليها باعتبارها مرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحاسبات وغيرها من أجهزة التقنية التي قد تظهر في المستقبل[4].

[1] غنية باطلي، مرجع سابق,ص19.
[2]- المرجع نفسه، ص20.
[3]- سعيدى سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، ط1، الإسكندرية، 2017،ص55.
[4]- احمد خليفة الملط, مرجع سابق, ص87.

ولقد أضاف Bloch.M و Alterman.M تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي على الجريمة الإلكترونية بأنها "كل سلوك غير مشروع أو يتعارض مع قواعد السلوك أو غير المرخص والذي يخص المعالجة الآلية للمعطيات أو انتقال المعطيات"[1].

ويعرفها الدكتور مصطفى محمد موسى بأنها " كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف[2].

وبالعودة إلى التعريفات السابقة نجد أنها تعود إلى حقب زمنية مختلفة من مراحل التطور الذي شهدته كل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات, فهذه التعريفات رافقت ظاهرة جرائم التقنية منذ بدايات ما يعرف بثورة تقنية المعلومات ومن ثم أخذت بالتوالي مواكبةً لتطور وتكنولوجيا المعلومات والاتصالات[3].

وختاماً يمكن القول أن جرائم تكنولوجيا المعلومات الحديثة هي تعبير شامل يشير إلى كل نشاط إجرامي مرتبط باستخدام تقنية المعلومات الحديثة بحيث أن غياب الارتباط بها يمنع ارتكاب مثل هذا العمل غير المشروع ولا يختلف الأمر سواء أكانت وسيلة تقنية المعلومات الحديثة أداة لإتمام النشاط الإجرامي أم كانت محلا له أو بهدف الاعتداء[4].

ويمكن إجمالها بأنها "الجريمة التي يكون محلها المعطيات المعالجة بلغة الأدلة أي المعلومات والبرامج, أو بالنظام المعلوماتي, إضافة إلى وسيلة ارتكابها الحاسوب أو أية وسيلة إلكترونية لها نفس إمكاناته لأنه لا يمكن الدخول إلى النظام بدونه[5].

[1]- غنية باطلي، مرجع سابق, ص20.
[2]- سعيدي سليمة، بلال حجازي، مرجع سابق, ص56.
[3]- علي جعفر، مرجع سابق, ص85 .
[4] المرجع نفسه.
[5]- غنية باطلي، مرجع سابق, ص24.

المطلب الثاني: صور الجريمة الإلكترونية

مع بداية انتشار شبكة الانترنت لم يكن هناك قلق تجاه الجرائم التي يمكن أن تنتهك على الشبكة، وذلك نظراً لمحدودية استخدامها، حيث كانت قاصرة على أغراض البحث العلمي فقط، علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين والعلماء وطلبة الجامعات.

لكن مع بزوغ فجر الثورة المعلوماتية وتوسع استخدام شبكة الإنترنت وبدء استخدامها في المعاملات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة وازدادت مع الوقت وتعددت صورها وأشكالها، وهذه الجرائم يطلق عليها الجرائم الإلكترونية، ومن صور الجرائم الإلكترونية نذكر[1]:

الفرع الأول: جريمة الدخول أو البقاء الغير مشروع في النظام المعلوماتي

أولاً: المقصود بفعل الدخول

يقصد به الولوج إلى المعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام، أو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له استخدامه والدخول إلى المعلومات.

ويجب النظر إلى فكرة الدخول على أنها فكرة معنوية، أي الدخول إلى العمليات الحسابية التي يقوم بها نظام المعالجة الآلية للمعطيات، وهذا ما يدل عليه المشرع الفرنسي عندما استعمل مصطلح Accéder بدلاً من مصطلح entrée، إلا أن المشرع الجزائري تحفظ في مفهوم الدخول إلى نظام المعالجة الآلية للمعطيات، ويظهر منطقياً أن النص يجرم فعل النفوذ داخل أي نظام معلوماتي[2].

[1]- أحمد عبداللاه المراغى، مرجع سابق,

[2] غنية باطلي، مرجع سابق,

ولم يحدد المشرع الوسيلة أو الطريقة التي يتم الدخول بها إلى النظام، وبالتالي يستوي أن يتم الدخول بطريقة مباشرة أو غير مباشرة، ويكون الدخول مباشراً عند استعمال الرمز السري أو كلمة المرور الصحيحة من أجل الدخول أو أثناء المعالجة باليد يتم إدخال برنامج للتجسس، أما الدخول غير المباشر يكون عن بعد أي عن طريق جهاز مرتبط بشبكة الإنترنت.

1- حالات الدخول الغير مصرح به

أ- حالة عدم وجود ترخيص مطلقاً

وهي الحالة التي لا يكون فيها للشخص أي علاقة بالنظام، كأن يكون من أحد العاملين الذين لا تخول له وظيفته الاتصال بهذا النظام أو ليس من العاملين أصلاً. ففي كلا الحالتين لا يجوز الدخول إلى النظام وقد يتوقف الدخول إلى النظام إما على تسديد مبلغ معين من المال أو أن يكون عضو هيئة أو جهة معينة أو قد يكون غير جائز مطلقاً.

ب- حالة تجاوز التصريح المصرح به للدخول:

في هذه الحالة قد يكون الدخول مصرح به ولكن في حدود معينة أو محددة ولكن الفاعل يتجاوز هذه الحدود كأن يكون له التجول في جزء من النظام فإذا به يتجول في كل النظام.

يكون الفاعل في أغلب الحالات من العاملين لذا الجهة التي يتبعها النظام، بحيث يكون مسموح له بالدخول لكنه يتجاوز حدود السلطة المخولة له بدخوله لهذا النظام في غير الحالات المصرح له فيها بذلك ومع ذلك فيعتبر من الصعب إثبات فيما إذا كانت هناك تجاوز لإختصاصه بالفعل، وهل كان هذا التجاوز عن قصد أو غير قصد.

وعليه يجب تحديد مجالات اختصاص كل واحد من العمال بدقة.

وهناك من القوانين التي تنص صراحة على وجوب أن تكون هناك تعليمات واضحة داخل المؤسسة تحدد فيها من له الحق من العمال في الدخول إلى النظام ومن ليس له الحق

في ذلك، أي تحديد اختصاصات ومجالات كل عامل، إلا أن الأمر لا يتوقف عند هذا الحد، فق يكون التجاوز يتعلق بالغرض الذي منح الترخيص من أجله.

ثانياً: البقاء الغير مشروع في النظام المعلوماتي

المقصود بفعل البقاء هو التواجد داخل نظام المعالجة الآلية ضد إرادة من له حق السيطرة على هذا النظام.

ويتحقق البقاء الغير مشروع سواء كان مستقلاً عن الدخول الغير مشروع أو كان مقترناً به أو كان مقترن بدخول مصرح به، فجريمة البقاء الغير مشروع تبدأ من الوقت الذي يبدأ فيه المتدخل بالتجول داخل النظام بعد انتهاء الوقت المحدد والمصرح له به.

ويكفي في جريمة البقاء الغير مشروع البقاء ساكناً حتى ولو لم يتم التقاط المعلومات، أي لا يشترط أي نتيجة.

الفرع الثاني: جرائم الاعتداء على البريد الإلكتروني

أولاً: جريمة انتهاك سرية رسائل البريد الإلكتروني

مجرد الدخول إلى موقع البريد الإلكتروني والإطلاع على رسائله بدون إذن من صاحبه، يعد جريمة انتهاك سرية المراسلات المكفولة بنصوص الدستور.

وإذا كان من المقرر وفق القواعد العامة أن القانون يقرر حماية المراسلات والمخابرات التليفونية ويكفل سريتها فلا يجوز مراقبتها أو انتهاك سريتها أو الإطلاع عليها إلا في الأحوال المبينة في القانون، فإن ذلك ينطبق أيضاً على وسائل الاتصال الإلكترونية ومنها البريد الإلكتروني، فنتيجة الانتشار السريع والمتفاقم لتكنولوجيا المعلومات وزيادة الاعتماد عليها في كافة نواحي الحياة وبصفة خاصة في التجارة والمعاملات الإلكترونية ازداد الاهتمام بسرية وخصوصية المعلومات الشخصية، أو ما يسمى بالخصوصية الإلكترونية e-privacy، ونتيجة تضخم حجم البيانات المتبادلة عبر البريد الإلكتروني ظهرت الحاجة الملحة لحماية البيانات والمعلومات وتأمين تداول هذه المعلومات بين

الأطراف عبر شبكة الإنترنت، ولذلك ظهر ما يسمى الأمان الإلكتروني، وهو برنامج يقوم بتقدير مواقع الإنترنت على أساس مدى كفاءتها في حمايتها للخصوصية الفردية.

ثانياً: جريمة تضخيم البريد الإلكتروني

ويعرف مصطلح تضخيم البريد الإلكتروني، بأنه تراسل نسخ مكررة بعدد كبير من نفس الرسالة عبر النظام التراسلي لبريد إلكتروني بما يترتب عليه عدم انتظام سير النظام التقني المعلوماتي.

كما عرفه البعض بأنه استقبال عدد كبير من الرسائل الإلكترونية المزعجة، وتتم جريمة تضخم البريد الإلكتروني عن طريق وصول عدد ضخم من الرسائل مجهولة المصدر إلى حساب البريد الإلكتروني للمستلم النهائي، ويستخدم في إرسالها برامج معدة خصيصا لذلك وهي برامج محظورة لكونها تهدد قواعد البيانات بتضخيم قاعدة عمل البريد الإلكتروني، حيث يجد صاحب البريد الإلكتروني نفسه أمام سيل منهمر من الرسائل عديمة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم، مما يترتب عليه إلغاء صندوق البريد على إثر تضخمه وحمله فوق طاقة الاستخدام المقررة له، مما قد يسبب خسائر اقتصادية ضخمة بالنسبة للشركات والمؤسسات العاملة في مجال التجارة الإلكترونية والتي تنتظر مئات الرسائل الإلكترونية يومياً بغرض إبرام الصفقات التجارية.

الفرع الثالث: جرائم التعدي على نظام التحويل الإلكتروني للأموال

نظام التحويل الإلكتروني للأموال Electronic Funds Transfer-EFT. هو جزء بالغ الأهمية من البنية التحتية لأعمال البنوك الإلكترونية التي تعمل عبر الإنترنت، ويتيح هذا النظام بطريقة إلكترونية آمنة نقل التحويلات المالية من حساب بنكي إلى حساب آخر، بالإضافة إلى نقل المعلومات المتعلقة بهذه التحويلات.

وقد عرفت لجنة الأمم المتحدة للقانون التجاري الدولي UNCITRAL المقصود بنظام التحويل الإلكتروني للأموال بأنه: عملية تبادل القيم المادية والتي تتم مرحلة بها أو أكثر

بواسطة وسائل إلكترونية بعد أن كانت نفس هذه المرحلة تتم قديماً بالوسائل الكتابية التقليدية.

وفي هذا النظام يتم استخدام أجهزة الحاسوب للسيطرة على عملية التحويل، ويمكن تنظيم نظام التحويل الإلكتروني للأموال بأشكال وصور مختلفة تلبي الاحتياجات المختلفة للعملاء والبنوك ومؤسسات الأعمال ويتكون نظام التحويل الإلكتروني من عدة عناصر تعمل كشبكة متكاملة وهذه العناصر هي: الحاسوب المركزي CENTERAL COMPUTER، ونقاط البيع SEGMENT RETAIL POINT-OF-SALE، والنهايات الطرفية في البنوك، وأجهزة الصراف الآلي.

ومن صور التعدي على نظام التحويل الإلكتروني للأموال ما أشار إليه التقرير الصادر عن إدارة العدالة الأمريكية عام 1982م بعنوان جرائم الحاسب الآلي، نظم التحويل الإلكتروني للأموال.

ومن هذه الوسائل :

1- التلاعب في المكونات المادية لنظم التحويل الإلكتروني للأموال، ويتضمن ذلك استعمال خطوط الاتصال لخلق أو تدمير البيانات أو الطلبات الخاصة بعمليات التحويل

2- استعمال البرامج الخاصة بنظم التحويل الإلكتروني للأموال والتلاعب بها بغرض البدء في إجراء عملية تحويل غير مشروعة أو بغرض إخفائها

3- التلاعب عن طريق إصدار بطاقات ائتمان مزدوجة.

4- استخدام بطاقة شخص آخر لسحب مبالغ نقدية من الرصيد الخاص بصاحب البطاقة.

ويستفاد من ذلك أن التلاعب في نظام التحويل الإلكتروني للأموال قد يتم بأي وسيلة من وسائل الاحتيال المعلوماتي، حيث قد يتم التلاعب عند إدخال البيانات أو في برامج الحاسوب أو في المكونات المادية له، أو أثناء عملية نقل البيانات إلكترونياً.

ولا شك أن صور التعدي على نظام التحويل الإلكتروني للأموال قد تسبب الكثير من المشاكل في نطاق سداد مصاريف الدعوى الإلكترونية سواء تم السداد عن طريق تحويل الأموال إلكترونياً من الحساب البنكي للمتقاضين إلى الحساب البنكي الخاص بالمحكمة،أو عن طريق بطاقات الائتمان، حيث قد يتمكن بعض المتسللين من اقتحام هذا النظام والعبث في البيانات والمعطيات سواء في مرحلة الإدخال أو أثناء عملية التحويل الإلكتروني للبيانات، مما قد يشكل عائقاً كبيراً في الثقة في إجراءات التقاضي الإلكتروني . إلا أن مكافحة الجريمة الإلكترونية لا تحقق هدفها إلا عبر تعاون دولي يقوم على أساس تنسيق جيد ومساعدة متبادلة في مواجهة التطور السريع لا من حيث الكم أو الكيف في مجال الجرائم المعلوماتية، ومن أجل تحقيق تعاون دولي فعال يجب عقد مؤتمرات دولية وإبرام معاهدات واتفاقيات لتدعيم هذا التعاون الدولي في مجال مكافحة الجرائم الإلكترونية[1].

الفرع الرابع: جرائم التجارة الإلكترونية

في هذا العصر الرقمي الذي انتشر فيه الإنترنت انتشارا هائلاً شاعت التجارة الإلكترونية والتي تتيح العديد من المزايا، فقد أصبح من الممكن لرجال الأعمال تجنب مشقة السفر والانتقال من بلد إلى آخر للقاء شركائهم وعملائهم وأصبح بمقدورهم توفير الوقت والمال من أجل الترويج للمنتجات والخدمات، كما أصبح في متناول المستهلك الحصول على ما يريده دون التنقل أو استخدام النقود التقليدية وكل ما يحتاجه المستهلك هو اقتناء جهاز كمبيوتر وبرنامج مستعرض للإنترنت واشتراك بشبكة الإنترنت[2].

ولا تقتصر التجارة الإلكترونية على عمليات بيع وشراء السِلَع والخدمات عبر الإنترنت، إذ إن التجارة الإلكترونية– منذ انطلاقها– كانت تتضمَّن دائما معالجة حركات البيع والشراء وإرسال التحويلات المالية عبر شبكة الإنترنت، ولكن التجارة الإلكترونية في

[1] محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ص1.
[2]- خالد ممدوح ابراهيم، مرجع سابق, ص68.

حقيقة الأمر تنطوي على ما هو أكثر من ذلك بكثير، فقد توسَّعت حتى أصبحت تشمل عمليات بيع وشراء المعلومات نفسها جنبا إلى جنب مع السِلَع والخدمات، ولا تقف التجارة الإلكترونية عند هذا الحد، إذ إن الآفاق التي تفتحها التجارة الإلكترونية أمام الشركات والمؤسسات والأفراد لا تقف عند حد معين.

فالتجارة الإلكترونية هي نظام يتيح عبر شبكة الإنترنت حركات بيع وشراء وتأجير السلع والخدمات والمعلومات، ويمكن تشبيه التجارة الإلكترونية بسوق إلكتروني يتقابل فيه البائعون والموردون والوسطاء والمستهلكون وتقدم فيه المنتجات والخدمات في صورة رقمية أو افتراضية ويتم دفع ثمنها بالنقود الإلكترونية.

ويزيد من حجم الجرائم المرتكبة ضد الجرائم الإلكترونية تخلف الآليات القانونية التقليدية عن التعامل معها تلك القوانين التي وضعت لتنظيم نوع آخر من التجارة وهو التجارة التقليدية والتي تعتمد على السلع المادية والنقود التقليدية والتعامل بالأوراق والمستندات الرقمية كدليل للإثبات، في حين أن التجارة الإلكترونية لا تعتمد على هذه الوسائط حيث تسلم الخدمات والمنتجات إلكترونياً، فعدم وجود مستندات ورقية بخط اليد يحدث مشكلة عدم القدرة على التمييز بين الرسالة الأصلية والنسخة مما يسبب في ازدياد جرائم تزوير الرسائل الإلكترونية المتبادلة عبر الإنترنت.

كما يتم الوفاء بنوع جديد من النقود تعرف باسم النقود الإلكترونية أو العملات الرقمية، أو الوفاء ببطاقات الائتمان، إذ نتيجة إدخال النظام المعلوماتي في مجالات عمليات البنوك أدى إلى ظهور وسائل وأساليب إجرامية جديدة في مجال المعالجة الآلية للمعلومات وإساءة استعمال البطاقات الائتمانية.

وأيضاً من جرائم التجارة الإلكترونية عمليات السطو والقرصنة على البيانات الشخصية عبر الإنترنت، ولكن لمواجهة ذلك تستخدم العديد من التقنيات لتذليل العقبات

التي يواجهها المتعاملون عبر الإنترنت وأهم هذه التقنيات بروتوكول الطبقات الأمنية وبروتوكولات الحركات المالية الآمنة.

ومما لاشك فيه أن جريمة انتحال الشخصية أو الصفة هي جريمة الألفية الجديدة وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية، وتتمثل هذه الجريمة في انتحال هوية شخصية أخرى بطريقة غير شرعية، بهدف الاستفادة من مكانة تلك الهوية أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى، وللتغلب على هذه المشكلة فقد بدأت الكثير من مؤسسات الأعمال التي تتعامل عبر شبكة الإنترنت في الاعتماد على التوقيع الإلكتروني كوسيلة للتأكد من الطرف الآخر، فالتعاقد الإلكتروني هو مجال تتعدد فيه وسائل الغش والخداع، ولقد أصبحت إعلانات التجارية الإلكترونية أحد أهم المعالم البارزة لعصر ثورة التكنولوجيا والمعلومات، وبحكم انتشارها وتنوع أساليبها وتطورها التقني تؤثر في سلوك المستهلك ويبني عليها قراره في الإقبال على التعاقد.

الفرع الخامس: جريمة التزوير الإلكتروني

تعد جريمة التزوير في المجال المعلوماتي من أخطر جرائم غش المعلوماتية، ويعرف التزوير الإلكتروني على انه تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بغية استعماله[1]، وينحصر نشاطها الإجرامي في أفعال الإدخال والمحو والتعديل على المحررات والوثائق الإلكترونية، ولا يشترط اجتماعهما معاً حتى يتوفر النشاط الإجرامي فيها[2].

ولقيام جريمة التزوير لابد من توافر ركنين: ركن معنوي, يتخذ صورة القصد الجنائي العام والخاص، وركن مادي يتمثل في تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون , على نحو يسبب ضرر للغير[3]، وبالتالي فإن جريمة التزوير لا تتوافر إلا إذا كان

[1] - علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، ط3، بحث مقدم لمؤتمر والكمبيوتر والانترنت، منظم من قبل كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004،ص152.

[2]- خالد ممدوح ابراهيم، مرجع سابق,

[3]- محمود نجيب حسني, شرح قانون العقوبات, القسم الخاص, الجرائم المخلة بالمصلحة العامة, 1972, ص280 .

محل تغيير الحقيقة محرراً ويقصد بالمحرر كل كتابة منسوب صدورها إلى شخص أو جهة معينة من شأنها أن تولد مركز قانوني معين أو ترتيب نتائج معينة, ويشترط في المحرر الكتابة, وأن تكون منسوب إلى شخص معين, وأن يحدث اثر قانوني معين[1].

ويكفي لقيام الركن المادي القيام بفعل واحد على حدى، لكن القاسم المشترك في هذه الأفعال جميعاً هو انطوائها على التلاعب في المعطيات التي يتضمنها معالجة البيانات بإدخال معطيات جديدة أو بالمحو أو التعديل على محرر أو وثيقة إلكترونية، والنشاط الإجرامي لجريمة التزوير يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير والمقصود هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير، أو مراكزهم القانونية الثابتة في تلك المحررات، وعليه يمكن تصور تغيير الحقيقة في نطاق المعالجة المعلوماتية بالتلاعب في المعطيات مما يؤثر على أصالتها[2].

الفرع السادس: جرائم السب والقذف عبر الإنترنت

جرائم السب والقذف عبر الإنترنت تعد من أكثر الجرائم انتشاراً أصبحت الشغل الشاغل لكثير من الناس، فهي وإن كان البعض يراها إبداء رأي، خاصة في حال التعليق على منشور معين، قد يراها الطرف الآخر ضرراً وإساءة وقذفاً أو حتى تنمراً، وهو ما فتح الباب للحديث عن جرائم السب والقذف الإلكتروني وشدة وقوعها وأثرها البالغ مادياً ومعنوياً على المتهمين فيها، خاصة أن سرعة انتشارها كبيرة جداً، وقد يراها الجميع ممن يخصهم الأمر وممن لا يخصهم، ويرى فيها البعض خراب بيوت، على الرغم من أن بعضها تعد جرائم بسيطة لا تستحق، وهو ما جعل بعض القانونيين يطالبون بتخفيف الغرامة، ويطرحون اقتراحات قانونية للتوعية ضد الوقوع في هذا النوع من الجرائم.

[1]- محمد عوض, الجرائم المضرة بالمصلحة العامة, دار المطبوعات الجامعية, الإسكندرية, 1985, ص174.
[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، جامعة بن عكنون، الجزائر، 2006،ص139.

وقد عرفت **المادة 297** من قانون العقوبات الجزائري السب على أنه: كل تعبير مشين أو عبارة تتضمن تحقيراً أو قدحاً لا ينطوي على أية واقعة.

ويعرف القذف بأنه: إسناد واقعة معينة للغير واحتقاره بشكل علني يوجب عقابه قانوناً، هذا ويتضح من هنا العلاقة بين جريمتي السب والقذف في كون كل منها تحمل اعتداء على شرف واعتبار الأشخاص غير أنهما تختلفان، حيث أن جريمة القذف يشترط فيها تحديد الواقعة وذلك على خلاف جريمة السب.

المبحث الثاني: خصائص وأسباب الجريمة الإلكترونية

المطلب الأول: خصائص الجريمة الإلكترونية

أولاً: الجريمة المعلوماتية جريمة عابرة للحدود

الجريمة المعلوماتية تتم غالبا بالطابع الدولي، ذالك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط on line ،يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارات ولذلك فهي جريمة عابرة للقارات، فهي تعتبر شكلاً جديداً من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة[1].

حيث ألغت شبكة الانترنت كل الحدود بين الدول إذ يمكن التحدث ما بين الأشخاص ليس في بلدان مختلفة فقط وإنما في قارات مختلفة ومنه فإن الجرائم التي ترتكب عن طريق الانترنت تتخطى حدود الدولة التي ارتكبتها فيها لتتعدى آثارها كافة البلدان على مستوى العالم[2].

[1]- خالد ممدوح إبراهيم، مرجع سابق, ص44.
[2]- سعيدي سليمة، بلال حجازي، مرجع سابق، ص89.

وأصبحت ترتكب في دول وتمر عبر دولة أخرى وتتحقق نتيجتها في دولة ثالثة أو عدة دول، وكل ذلك في ثوان معدودة، وصارت أكثر من دولة مسرحا لتلك الجريمة[1]، وهنا تثور مشاكل الاختصاص والإجراءات والتحري والتفتيش والضبط....الخ[2].

ثانياً: ترتكب في بيئة تكنولوجية

تعد هذه الخاصية متفردة عن باقي الجرائم التي ترتكب ،ذلك أن الحاسوب الآلي هو الأداة الوحيدة التي يمكن الشخص من الدخول على الشبكة وقيامه بتنفيذ جريمته أي كان نوعها[3].

وهو ما يميزها عن الجريمة التقليدية فأداة ارتكابها هو الحاسب الآلي وشبكة الانترنت ومحلها هي المعلومات المخزنة على الحاسوب وشبكاته كما أنها قد ترتكب أثناء إحدى تشغيل نظام المعالجة الآلية للمعلومات سواء في مرحلة الإدخال أو المعالجة أو الإخراج[4].

ثالثاً: صعوبة إثبات الجريمة الإلكترونية

تتصف الجرائم المعلوماتية بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها وهي خطيرة وصعبة الاكتشاف أو هي صعبة في تحديد مكان ونوعها، أو مكان التعامل بسبب اتساع نطاقها المكاني وضخامة البيانات[5].

فأيضاً لا يوجد جثث لقتلى أو آثار لدماء وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة والدليل على ذلك انه لم يكتشف منها إلا نسبة 1%فقط ،و الذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15%من النسبة السابقة[6].

[1]- أحمد عبد اللاه المراغى، مرجع سابق, ص73.
[2]- عبدالله عبد الكريم عبدالله ،جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، ط1، بيروت-لبنان،2007، ص 33.
[3] - سعيدي سليمة، بلال حجازي، مرجع سابق, ص89.
[4]- احمد عبدالله المراغى، مرجع سابق، ص71.
[5]- خالد ممدوح ابراهيم، مرجع سابق،ص45.
[6]- احمد خليفة الملط، مرجع سابق، ص94.

وحتى في حال اكتشاف وقوعها والإبلاغ عنها فوسائل المعاينة وطرقها التقليدية لا تفلح غالباً والإبلاغ عنها، فجريمة التقنية الحديثة تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع الملموس لتقوم أركانها في نظام معلوماتي إلكتروني، فالجريمة التقليدية التي لها مسرح تجري عليه الأحداث ،حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة عن طريق المعاينة[1].

وإضافة إلى ذلك نجد:

1. أنها جريمة يصعب فنياً الاحتفاظ بآثارها إن تركت آثر.
2. أنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الاجرامية وما تخلفه من آثار غير مرئية.
3. أنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعريف على مرتكبيها بشكل يفوق بكثير الجريمة التقليدية.
4. أنها جريمة يصعب توضيحها لهيئة المحكمة ، ويسهل زرع الشك في وجدانها فيما يتعلق بالدليل المتحصل عليه[2].

رابعاً: جريمة لا تتسم بالعنف

فهي جريمة تتسم بالهدوء ،فهي جريمة فنية لا تترك آثارا كآثار المادية المترتبة على الجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة قتل أو الاختطاف أو في صورة الخلع ،أو الكسر وتقليد مفاتيح كما هو الحال في جريمة السرقة[3].

[1]- علي جعفر، مرجع سابق.
[2]- أحمد عبد اللاه المراغي، مرجع سابق، ص75.
[3]- غنية باطلي، مرجع سابق، ص43.

خامساً: الجريمة المعلوماتية جريمة مستحدثة

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي تمكن أن تشكل أخطارا جسمية في ظل العولمة ،فلا غرابة أن تعتبر الجرائم المعلوماتية سواء التي تتعرض لها أجهزة الحاسوب أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة ،حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جهل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية بل انه أضعف قدراتها في تطبيق قوانينها ،بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها[1].

الفرع الأول: سمات المجرم الإلكتروني

مما لا شك أن المدى الزمني لنشأة وتطور العلوم الجنائية وما نتج في نطاقها من دراسات وتحديدا في ميدان علم الإجرام أمكن في ظلها بلورة سمات عامة للمجرمين عموما وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين تبعا للجرائم التي يرتكبونها, فعلى سبيل المثال أفرزت الجرائم الاقتصادية ما يعرف بإجرام ذوي الياقات البيضاء وبالتالي كان طبيعياً أن تحمل ظاهرة الإجرام عبر تكنولوجيا المعلومات الحديثة في جيناتها ولادة طائفة جديدة من المجرمين اصطلح جانب من الفقه على تسمية من ينتمي إليها بالمجرم المعلوماتي[2].

فالصحيح انه لا يوجد نموذج محدد للمجرم المعلوماتي ويرى عدد كبير من الباحثين أن المجرم وإن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب عليه[3].

[1]- محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، ط1، الأردن، 2005،ص222.
[2]- علي جعفر، مرجع سابق، ص105.
[3]- المرجع نفسه، ص106.

فكل ما في الأمر انه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء من حيث انتماء المجرم في أكثر الحالات إلى وسط اجتماعي حسن، وتميزه بدرجة من العلم والمعرفة وليس معنى ذلك أنهم اقل خطورة من الناحية الإجرامية عن المجرمين ذوى الياقات الزرقاء "المجرم بطبيعته" ويرمز بعض الباحثين بكلمة SKRAH إلى مجموعة الخصائص التي تميز المجرم في الجريمة الإلكترونية بصفة عامة عن غيره من المجرمين وهي تعني المهارة SKILLS, المعرفةKNOW ledge الوسيلة Resources, السلطة Authority, الباعث Motive, [1]، ويرى الأستاذ باركر أن المهارة هي أبرز خصائص مجرم تكنولوجيا المعلومات الحديثة, فتنفيذ جريمة تكنولوجيا المعلومات الحديثة يتطلب قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومة الحديثة أو بمجرد التفاعل الاجتماعي مع الآخرين[2].

فالمجرم المعلوماتي ذو دراية بالتكنيك المستخدم في نظام الحاسب الإلكتروني وقادر على استخدام هذه المهارات فضلاً عن كونه قد يمتلك الخبرة في اختراق الكود السري لتغيير ونقل المعلومات أو البيانات أو تقليد البرامج أو التحويل من الحسابات أو التجسس وزرع الفيروسات وغيرها من الجرائم التي تحتاج لمجرم ذو دراية بتقنية الحاسب الآلي وشبكات الانترنت[3].

فالمجرم المعلوماتي يتميز بأنه إنسان ذكي واجتماعي فهو بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة قائمة بذاتها فهو من جهة مثال منفرد للمجرم الذكي ومن جهة أخرى إنسان اجتماعي بطبعه حيث يقال عادة أن الإجرام المعلوماتي هو إجرام الأذكياء فلقد ترك عالم المجرمين البؤساء ـ المجرم التقليدي ـ ليدخل عالم مجرمي المهارات المعلوماتية فهو مجرم لا يستخدم العنف أو القوة لارتكاب الجريمة كما له قدرة كبيرة في

[1]- علي جعفر، مرجع سابق، ص107.
[2]- المرجع نفسه.
[3]- احمد عبد اللاه المراغي، مرجع سابق، ص40.

التكيف داخل المجتمع مع انه تتوفر فيه الشخصية الإجرامية وتزداد خطورته الإجرامية بازدياد ذكائه الذي يسهل عليه التكيف داخل المجتمع الأمر الذي يصعب معه رصده كمجرم عادي[1].

فالعنصر الجامع بين محترفي جرائم نظم المعلومات تمتعهم بقدرة عالية من الذكاء وإلمامهم الجيد بالتقنية العالية واكتسابهم معارف عملية وعلمية وانتمائهم إلى التخصصات المتصلة بالحاسب من الناحية الوظيفية والسمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء ففيما يتعلق بكفاءة مجرمي الحاسب فإن الدراسات القليلة المتوفرة تشير إلى تمتعهم بكفاءة عالية إلى درجة اعتبارهم مستخدمين مثاليين من قبل الجهات العاملين لديها وممن يوسمون بالنشاط الواسع والإنتاجية الفاعلة[2].

المعرفة:

أما المعرفة فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه حتى لا يواجهوا بأشياء غير متوقعة من شأنها إفشاء أفعالهم أو الكشف عنهم.

وتميز المعرفة بمفهومها السابق مجرمي تكنولوجيا المعلومات الحديثة حيث يستطيع مجرم التقنية الحديثة أن يكون تصوراً كاملاً لجريمته ويرجع ذلك إلى أن المسرح الذي يمارس فيه جريمة تكنولوجيا المعلومات الحديثة هو نظام الحاسب الشامل فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[3].

[1]- احمد عبد اللاه المراغي، مرجع سابق، ص41.
[2]- أيمن عبدالله فكرى، مرجع سابق، ص114.
[3] علي جعفر،مرجع سابق، ص108.

فالهاكرز يمتازون بقدرتهم على التعامل مع جميع الشبكات ويتقنون على الأقل أربعة لغات برمجة من اللغات المعروفة وهذا ما يجعلهم يستطيعون اكتشاف الأخطاء والثغرات في أنظمة المعلومات ولذا فمن الملاحظ أنه من خلال دراسة أجراها معهد STAND FORD RESEARCH أن اغلب مرتكبي هذه الجرائم هم ممن لهم علاقات وطيدة بعالم الحاسوب وكانت النتائج كالأتي:

- 25% من مرتكبي هذه الجرائم هو محلل البيانات داخل المؤسسة.
- 18% من مرتكبي هذه الجرائم هو مبرمج.
- 16% من مرتكبي هذه الجرائم هو الصراف.
- 12% من مرتكبي هذه الجرائم هو الشخص الأمني من المنشأ.
- 11% من مرتكبي هذه الجرائم هو المشغل[1].

الوسيلة :

أما الوسيلة فيراد بها الإمكانية التي يتزود يها الفاعل لإتمام جريمته فمجرمو تكنولوجيا المعلومات الحديثة يتميزون بالقدرة على الحصول على ما يحتاجون إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي[2].

والحقيقة انه كلما كان نظام المعالجة الآلية المستهدفة غير مألوف كانت الوسيلة المتطلبة أكثر صعوبة في الحصول عليها لاقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام[3].

السلطة:

[1] سعيدي سليمة، بلال حجازي،مرجع سابق، ص35.
[2] علي جعفر،مرجع سابق، ص108.
[3] المرجع نفسه.

أما السلطة فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم في جريمة تكنولوجيا المعلومات الحديثة والتي تمكنه من ارتكاب جريمته وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى نظام المعالجة الآلية وقد تتمثل هذه السلطة في الحق في استعمال الجهاز الذي يحتوي مرايا نظام المعلومات الإلكتروني أو إجراء بعض التعاملات أو مجرد الدخول إلى أماكن التي تحتوي على أنظمة المعلومات الإلكترونية وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر وبالنسبة لهذه السمة فإننا نرى أيضا أن غالبية صور الجرائم تكنولوجيا المعلومات الحديثة أي عندما لا يكون نظام المعلومات الإلكتروني هو هدف الجريمة لا تتطلب توافر السلطة لكي يتمكن من ارتكاب جريمته[1].

أما الباعث أو الدافع أو الغرض أو الغاية فكلها تعبيرات لها دلالتها في الإصلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص في الجريمة، فالباعث "الدافع" هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام وهو إذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة المبتغاة لتحقيق غاية معينة وهو يختلف من جريمة إلى أخرى أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي وتتمثل في تحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة فإشباع شهوة لانتقام أو سلب مال المجني عليه في جريمة القتل والأصل أن الباعث والغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين علم الجاني بعناصر الجريمة واتجاه إرادته لتحقيق هذه العناصر أو الى قبولها ولا تأثير الباعث أو الغاية على قيام الجريمة والانعقاد علها فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلاً أو رذيلاً أو كانت الغاية شريفة أو دنيئة[2].

[1]- علي جعفر، مرجع سابق، ص109.
[2]- -المرجع نفسه، ص110.

فالمجرم في جرائم تكنولوجيا المعلومات الحديثة لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة إلا أنه لا يرى غضاضة في أن يكون هذا الاعتداء عن طريق وسائل التقنية الحديثة[1].

وبناءً على ما تقدم يتضح لنا أن مجرمي التقنية الحديثة تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب وسمات خاصة تبعاً للطبيعة المميزة لبعض جرائم تكنولوجيا المعلومات الحديثة، والأغراض المراد تحقيقها لذا فإن تصنيف مجرمي التقنية الحديثة وبيان السمات الأساسية لكل فئة يشكل أنجع الوسائل لردع هذه الفئات أو الحد من نشاطها[2].

المطلب الثاني: أسباب ودوافع الجريمة الإلكترونية

الأصل أن القانون الجنائي لا يعتمد كقاعدة عامة بالدوافع والبواعث على ارتكاب الجرائم ولكن استثناء يعتد بها وبموجب نص قانوني ويعتبر إما ظرفا مشدداً للعقاب أو عذراً قانونيا مخففاً للعقاب[3].

ولا يمكن أن يكون الدافع إليها محصوراً أو محدداً بنوع معين أو محدد بحيث يختلف باختلاف الجريمة، فبالنسبة للدافع في الجريمة المعلوماتية يختلف من جريمة الى أخرى حسب الحق الذي تنال منه بالاعتداء أو المصلحة التي تتعرض لها وان كان الدافع الذي يدفع الجناة لارتكاب جرائمهم ضد المؤسسات والشركات المالية غالباً ما يكون هو الإضرار بهذه الشركات والحصول على النفع المادي[4]، وغالباً ما يكون الدافع في الجرائم المعلوماتية مادياُ إلا أن هذا لا يمنع من وجود بواعث أخرى تدفع بالجاني إلى ارتكاب جريمته كالتلاعب بالمعلومات والبيانات بهدف الانتقام.

[1]- علي جعفر، مرجع سابق، ص111.
[2]- المرجع نفسه.
[3]- محمد حماد مرهج الهيتي،مرجع سابق، ص142.
[4]- المرجع نفسه، ص143 .

الفرع الأول: الرغبة في التعلم وجمع المعلومات

هناك من يقوم بارتكاب جرائم الحاسوب بغية التعلم فيرى قراصنة الحاسوب أن الحصول على المعلومة يجب ألا يكون عليه أي قيد، فالقرصان يوطد كل جهده في تعلم كيفية اختراق المواقع الممنوعة، وغالباً ما يكون القراصنة مجموعات يكون الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والإخبار ويفضلون التخفي ليتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول فترة ممكنة[1].

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة إلى أخلاقيات هؤلاء القراصنة التي ترتكز على مبدئيين أساسين هما:

1. الدخول إلى النظام المعلوماتي يمكن أن يعلمك كيف يسير العالم.
2. أن جميع المعلومات يجب أن تكون غير خاضعة للقيود.

وبناءً على هذين المبدأين فان أجهزة الحاسوب المعنية ما هي إلا آلات للبحث والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات وأن جميع المعلومات لابد أن تكون غير خاضعة لأية قيود، أي تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص.[2]

وقد كتب احد القراصنة: اعتقد أن ما نقوم به يشبه قيام شخص باكتشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والمتعة[3].

الفرع الثاني: الرغبة في تحقيق مكاسب مالية

تعتبر الدوافع المادية من أهم البواعث على ارتكاب الجرائم المعلوماتية ولما تحققه من ثراء فاحش[1]، وذلك عن طريق إتاحة معلومات وهمية لمن يطلب والمساومة عليها أو استعمال بطاقات السحب الآلي المزورة أو منتهي الصلاحية[2].

[1]- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر والتوزيع، ط1،عمان- الأردن، 2008، ص144.
[2]- سعيدي سليمة، بلال حجازي،مرجع سابق، ص36.
[3] غنية باطلي،مرجع سابق، ص27.

ولقد أشارت مجلةSécurité informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت إلى أن:

- 43%من حالات الغش المعلن عنها من اجل اختلاس الأموال.
- 23% من اجل سرقة المعلومات.
- 19% أعمال إتلاف.
- 10% سرقة وقت الآلة أي استعمال غير المشروع للآلة لتحقيق أغراض شخصية[3].

لذلك نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن يكون سببه سداد الديون آو مشاكل مالية عائلية أو إدمان العاب القمار والمخدرات ويمكن أن نبين في هذا المجال واقعة استلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريط ممغنط يحتوي على معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها لشركات منافسة إذا لم تدفع فدية قدرها 200000 دولاراً[4].

إذن فنتيجة للأرباح الطائلة التي يمكن أن يجنبها مرتكبي الجريمة فإنها تشكل دافعا قوياً لأصحاب النوايا السيئة في ارتكاب جريمتهم في استبيان أجراه أحد الباحثين في أمريكا عام 1995 بين أن معدل أرباح مرتكب جريمة الحاسوب وصلت إلى 600000 دينار مقابل 300000 دولار لمرتكب الجريمة في النظام اليدوي[5].

الفرع الثالث: دافع الانبهار بالتقنية والإثارة والمتعة

مع ظهور التقنية المعلوماتية الحديثة وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو تعلق الأمر بالحاسبات الآلية فإن الأمر في النهاية يؤدي إلى الانبهار بالتقنية ولذلك فان هؤلاء الدخلاء ليسوا على قدر كبير من الخطورة الإجرامية وإنما هم في

[1] احمد خليفة الملط،مرجع سابق، ص89.
[2] غنية باطلي،مرجع سابق، ص27.
[3]- سعيدي سليمة، بلال حجازي،مرجع سابق، ص37-38
[4]- المرجع نفسه، ص38.
[5]- عبد الحكيم رشيد توبة، مرجع سابق، ص144

الغالب يفضلون تحقيق انتصارات تقنية دون أن تتوافر لديهم أية نوايا سيئة ونضرب مثلا لذلك نشر في مجلة exérèses الفرنسية وتدور أحداث القصة حول عامل طلاء مباني قد توجه إلى احد البنوك لإيداع شيك خاص به وتعاصر ذلك مع لحظة عطل الموزع الآلي للنقود حيث شاهد مستخدم بطاقة خاصة وقد احدث هذا الابتكار للآلة تصدعا في الحياة العادية لعامل الطلاء الذي عكف تعلم تقنية الحاسب لمدة عامين ثم قام بالسطو على الموزع الآلي للبنك وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب وقد ألقي عليه القبض قبل أن يستفيد من براعته المستحدثة وقد نسبت إليه جريمة السرقة[1].

وعادة ما يلجأ مرتكبي هذه الأفعال إلى التركيز على دقة الأسلوب أكثر من الفعل ذاته لإظهار تفوقهم ومستوى براعتهم لدرجة انه إزاء ظهور أي تقنية مستحدثة فإن لديهم شغف بالآلة ويحاولون إيجاد الوسيلة إلى تخطيها[2].

ويزداد هذا الدافع لدى فئة صغار السن من مرتكبي هذه الجرائم الذين يمضون وقتاً طويلاً أمام الحاسوب في محاولة لكسر حواجز الأمن لأنظمة الحواسب وشبكات المعلومات ولإظهار تفوقهم على وسائل التقنية ويمكن القول أن هذا الدافع هو أكثر الدوافع التي يجري استغلالها من قبل المنظمات الإجرامية "مجموعات الجريمة المنظمة" وهي استدراج محترفي الاختراق لقبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة[3].

الفرع الرابع: الأسباب والدوافع الشخصية

تتعدد المؤثرات والأسباب الشخصية التي تدفع الإنسان إلى احتراف مثل هذا السلوك الإجرامي سواء كان ذلك بدوافع الكبرياء أو الحقد أو الانتقام حيث دفع الحقد والكراهي بمحاسب شباب إلى التلاعب في برامج الحاسوب الخاصة بالشركة التي يعمل بها بأن على أن تختفي كل البيانات الخاصة بديون الشركة بعد مضي ستة أشهر من تاريخ شركة العمل

[1]- سعيدي سليمة، بلال حجازي،مرجع سابق، ص39
[2]- غنية باطلي،مرجع سابق، ص30.
[3]- المرجع نفسه.

وحدث ما أراد بالفعل بعد ستة أشهر[1]، وقد يكون الدافع الشخصي لمرتكب جرائم الحاسوب دافع مذهبي ومن أمثلة ذلك:

ما تقوم به جماعات الألوية الحمراء في ايطاليا حيث تعرضت عدة وزارات وجماعات ومؤسسات مالية في ايطاليا لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها ولقد أصدرت هذه الجماعات منشور عام 1988 شرحت فيه استراتجياتها وأغراضها وهدافها ويبدأ المنشور بتحديد أهداف هذه الجماعة وهي مهاجمة الهيئات متعددة الجنسيات التي ترمز للامبريالية وإعادة توزيع الحركة الثورية بتنظيم من الحزب الشيوعي المحارب، ويقصد بالهيئات متعددة الجنسيات تلك الموجودة بالولايات المتحدة الأمريكية ويعتبرون الحاسوب سلاح خطير ضد الإرهاب بفضل قدرته على حفظ المعلومات[2].

ومن بين الدوافع كذلك التنافس الاقتصادي والسياسي والتسابق القضائي والعسكري وقد تكون مناهضة العولمة احد الدوافع لارتكاب هذا الفعل[3].

إن الأسباب المؤدية لانتشار هذه الجريمة تختلف عن تلك المعروفة في الجريمة التقليدية، لأن الفرق بين الإجرام في العالم الحقيقي، وتلك الذي يقع في العالم الافتراضي يكمن أساساً في خصوصية الشبكات الرقمية وعلاقتها بالمستخدم[4].

[1]- عبد الحكيم رشيد توبة، مرجع سابق، ص144.
[2]- المرجع نفسه، ص145.
[3]- غنية باطلي،مرجع سابق، ص32.
[4]- المرجع نفسه.

الفصل الثاني

آليات مواجهة الجريمة الالكترونية والجزاءات المترتبة

الفصل الثاني

مواجهة الجريمة الإلكترونية

تسعى الدولة القانونية إلى الموازنة بين المحافظة على حقوق الانسان، ومعاقبة من يرتكب الجرائم الإلكترونية، فلا بد من الإحاطة بالجرائم الإلكترونية والتأهب لمواجهتها من خلال التشريعات المختلفة، لما تشكله من خطر على أمن الدول وحقوق الأفراد والمصالح الخاصة[1].

وقد خصت منظمة الأمم المتحدة الجرائم الإلكترونية ومواجهتها اهتماماً كبيراً في العديد من المؤتمرات أهمها مؤتمر الأمم المتحدة العاشر لمنع الجريمة الإلكترونية المنعقد في فيينا عام 2000، وكذلك من خلال المؤتمر الحادي عشر لمنع الجريمة الإلكترونية[2]، وبالتالي يجب التوفيق بين ضرورة النظم المعلوماتية، وتفادي أي ضرر يمكن أن يصيب الأفراد، فوسائل حماية الأفراد من أضرار النظم المعلوماتية تأخذ صورتين، الأولى حماية وقائية تتمثل بالوسائل التقنية والتنظيمية ذات الطابع الوقائي لهدف منع التعدي على حقوق الآخرين باستخدام التكنولوجيا، والثانية تتمثل بالحماية التشريعية بتوقيع العقوبات على المعتدين، فهي ذات طابع جزائي لاحق على وقوع الإعتداء[3].

ولذلك خصصنا هذا الفصل في مواجهة الجريمة الإلكترونية من خلال عرضنا الآتي:

[1] علي حسن محمد الطوالبة، مرجع سابق، ص1.
[2] آمنة زعيطي، بحث بعنوان مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري، مجلة حقوق الانسان والحريات العامة، جامعة مستغانم، العدد7، 2019.
[3] علي جعفر، مرجع سابق، ص412.

المبحث الأول: آليات السلطة التشريعية لمكافحة الجريمة الإلكترونية

يعبر المشرع بصفة عامة عن مجموع القواعد المكتوبة التي تنظم العلاقات القائمة بين الأطراف المعنية والداخلة فيه ولهذه القواعد القوى الجبرية اللازمة لتنفيذه والتقيد به والعقاب في حالة المخالفة ولكي يكون للقواعد تشريعا لابد أن تكون مكتوبة حيث يعتبر الدستور في الدولة الحديثة هو أعلى مستويات التشريع ويحاول المشروع تطوير هذه القواعد من حيث الآخر حتى تتماشى مع التطورات الحاصلة في المجتمع وبما أن الجرائم المعلوماتية هي من أهم الجرائم التي أفرزتها الثورة المعلوماتية الخالية فإن المشروعين في كافة أنحاء العالم عكفوا على إيجاد تشريعات تعتم بهذه الفئة من الجرائم نظر للخصوصية التي تكتسبها سواء من حيث طبيعة الفعل أو من حيث مرتكب الجريمة[1].

المطلب الأول: الإثبات كوسيلة مكافحة للجريمة الإلكترونية

الإثبات في اللغة مأخوذ من ثبت الشيء ثبوتا أي دام وثبت الأمر بنفسه أي عرفه حق المعرفة وأكده بالبيانات فمادة تفيد المعرفة والبيان والدوام والاستقرار والمصدر إثبات وثبوت وثبت واثبت حجته أي أقامها وعلى هذا فالإثبات في اللغة إقامة الحجة على أمر ما ويؤخذ من كلام الفقهاء أن الإثبات إقامة الدليل الشرعي أمام القاضي في مجلس قضائية على حق أو واقعة من الوقائع[2].

ويمكن تعريفه بأنه "كل ما يؤدي إلى إظهار الحقيقة وإقامة الدليل على وجود واقعة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون" أو إقامة الدليل أمام القضاء على تصرف كالقرض أو واقعة كالسرقة بوسائل إثبات يحددها المشرع [3].

[1]- سعيدى سليمة، بلال حجازي،مرجع سابق، ص142.
[2]- المرجع نفسه، ص72
[3]- محمد حماد مرهج الهيتي،مرجع سابق، ص222

الفرع الأول: وسائل الإثبات في الجريمة الإلكترونية

قبل الدخول في وسائل الإثبات وآليات التحقيق وجب التطرق إلى الخصائص الفنية للمحقق في جرائم الحاسوب والانترنت.

إن مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع احد عدم توافرها لدى المحقق وعليه فإن التركيز هنا سوف ينصب على الخصائص الفنية التي تتم بالحادثة والناتجة عن التطور الإنساني في مجال تقنية المعلومات والأنظمة الإلكترونية[1].

وليقوم المحقق بعمله على أحسن وجه يجب أن تتوافر بعض الأمور:

1. معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعلق بالجريمة المرتكبة.
2. وصول الاخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنين الذين يعملون على هذه الأجهزة.
3. تشكل فرق تحقيق تقني وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش على مسرح الجريمة.
4. إتباع الإجراءات الصحيحة والمشروعة من اجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك ومنع حذفها.
5. البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول على البرامج المخزنة وكيفية الحصول على الأرقام السرية والشيفرات الفنية التي تمكنهم من الدخول إلى الحاسوب[2].

[1]- خالد عياد الحلبي إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت, دار الثقافة للنشر والتوزيع، ط1، 2011، ص182.
[2]- المرجع نفسه، ص182.

أولاً: التفتيش

يقصد بالتفتيش في مجال الإجراءات الجنائية البحث عن شيء يتصل بجريمة وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة[1].

ويعرف جانب آخر من الفقه التفتيش بأنه: إجراء من إجراءات التحقيق التي تقوم به سلطة حددها القانون يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة ويتمثل مستودع السر في شخص أو في مكان الذي يعمل ب أو يقيم فيه[2].

وبالنسبة للحدود التي تحكم الحق في التفتيش عن المعلومات في الوسائل التقنية الحديثة من الناحية الموضوعية تتمثل في :

أ- وقوع جريمة من جرائم المعلوماتية.

ب- توافر الدلائل الكافية على نسبة الجريمة إلى المتهم

ج- الاعتقاد بوجود معلومات أو أجهزة معلوماتية تتعلق بالجريمة وتنفيذ في كشف حقيقتها عند المتهم أو غيره.

والحدود التي تحكم الحق في التفتيش عن المعلومات في وسائل التقنية الحديثة من الناحية الإجرائية تتمثل بالإضافة إلى الحدود الزمنية السابق الإشارة إليها والتي تتعلق بوقت إجراء التفتيش فأولاً: إجراء التفتيش بالكتابة وثانياً: الحضور الضروري لبعض الأشخاص أثناء التفتيش، ثالثاً: الكيفية الخاصة لإجراء التفتيش في مجال وسائل التقنية الحديثة[3].

[1]- الشحات ابراهيم محمد منصور،الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية, دار الفكر الجامعي، ط1، الإسكندرية،2011،ص196.

[2]- علي حسن محمد الطوالبة،التفتيش الجنائي على نظم الحاسوب والانترنت, عالم الكتب والحديث، ط1، الأردن، 2004، ص10.

[3]- بكرى يوسف بكرى،التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، ط1،الإسكندرية،2011، ص86.

إن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أو خاص إذا ن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في تمكين المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي تجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة ومحل التفتيش الخاص بنظم الحاسب الآلي هي كل مكونات الحاسب سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب الآلي محل التفتيش[1].

1-الإنابة في التفتيش:

الأصل في تنفيذ أمر التفتيش أن يباشره القانون بالمدعي العام ولم يعطي القانون هذا الحق لغير المدعي العام استثناء في ذلك بعض الحالات التي يخشى من عدم الإسراع بالتحقيق قوات تطبيق العدالة أو ضياع أدلة الجريمة والذي يؤدي كشفها في لحضتها إلى بيان الحقيقة[2].

الإنابة أو الإذن أو الندب للتحقيق عموما يراد به الإنابة الصادرة ممن له سلطة تحقيق إلى احد أعضاء الضبطية العدلية يفوضه بموجبه إجراء عمل أو أكثر من أعمال التحقيق ويعرفها جانب من الفقه بالآتي تصرف إجرائي يصدر ممن له سلطة التحقيق بمقتضاه يفوض أحد مأموري الضبط القضائي ليقوم به بدلا منه وفي الشروط التي يجب أن تنفذ بها بمباشرة إجراء معين أو أكثر من إجراءات التحقيق التي تدخل في سلطته ويعرفه جانب آخر من الفقه بأنه أمر إنابة أو ندب في مباشرة إجراءات التحقيق لغيرها من مأموري الضبط القضائي عندما تدعو لذلك ضرورة عملية كلزوم سرعة اتخاذ الإجراءات أو كثرة أعمال التحقيق في القضية ذاتها أو كون الإجراء يلزم للقيام به والخروج عن دائرة الاختصاص[3].

[1]- الشحات إبراهيم محمد منصور، مرجع سابق، ص196.
[2]- علي حسن محمد الطوالبة، مرجع سابق، ص102.
[3]- المرجع نفسه، ص103.

ثانياً: معاينة مسرح الجريمة:

يقصد بالمعاينة محض مكان أو شيء أو شخص له علاقة بالجريمة واثبات حالته كمعاينة جسم أو ملابس الجاني أو المجني عليه لإثبات ما بجسم من جراح وما على الثياب من دماء وما بها من مزق أو عطب.

ولذا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ومرد ذلك إلى:

1. أن الجرائم التي تقع على نظم المعلومات قليلاً ما يترتب على ارتكابها آثار مادية.
2. أن عدد كبير من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغير أو إتلاف أو عبث بالآثار المادية.

ثالثاً:الخبرة في مجال الجريمة المعلوماتية

يحتاج الأمر إلى الاستعانة بالخبير لإيضاح بعض المسائل التي تقابله وتستعصي ثقافته العامة على فهمها والخبرة لها أهمية خاصة في مجال الجريمة المعلوماتية نظرا لان شبكات الحاسبات وشبكات الاتصالات بينهما أنواع ونماذج مختلفة ولما كان الأمر في غاية الصعوبة ويحتاج إلى فحص حيث أنها أمور فنية قد رأى أن يستعان بالخبير في هذا المجال وللخصوم حق الحضور أثناء عمل الخبير وغالبا ما يحتاج المحقق إلى خبير خاصة في الأمور الأكثر تعقيدا مثل الأشرطة الممغنطة لأسطوانات البرامج, وكذلك في البحث عن المعلومات داخل جهاز الحاسب الآلي نفسه[1].

الفرع الثاني: صعوبة الإثبات في الجريمة

[1]- الشحات إبراهيم محمد منصور،مرجع سابق، ص195.

هناك الكثير من المشاكل والمعوقات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها, وانعكاسها أيضاً على المجرم نفسه بشعوره أن الجهات الأمنية لن تكتشف أمره وان خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه الأمر الذي يعطيه ثقة كبيرة في ارتكاب هذه الجرائم بحرية تامة[1].

ويتضح مما سبق أن مكافحة جرائم تكنولوجيا المعلومات لن يكون مجديا أو لن يكون له أي تأثير يذكر إلا إذا كان هناك تعاوناً دولياً بين الأفراد والمنظمات والشركات والدول , ووضع استراتيجيات أمنية شاملة لنظم المعلومات ومن ثم العمل على تنسيق تلك الجهود المبذولة بين كافة الدول[2].

إضافة إلى كل الأسباب سالفة الذكر هناك رغبة المجني عليه في استمرار حركة المعاملات ومحاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب آخر كل هذه الأساليب تدعوا المجني عليه لعدم مساعدة السلطات في إثبات الجريمة والكشف عنها[3].

أولاً: صعوبة الاحتفاظ بالدليل

إذ يستطيع المجرم المعلوماتي في اقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الحاسوب لذا فإن للمصادفة وسوء الحظ نصيباً أكبر في اكتشافها يفوق دور أساليب التدقيق والرقابة، ومعظم مرتكبيها الذين تم ضبطهم وفقاً لما لاحظه أحد الخبراء في مجال الجريمة المعلوماتية إما أنهم تصرفوا بغباء أو لم يستخدموا الأنظمة المعلوماتية بمهارة[4].

[1]- خالد عباد الحلبي،مرجع سابق، ص220.
[2]- عبد الحكيم رشيد توبة،مرجع سابق، ص219.
[3]- سعيدي سليمة، بلال حجازي،مرجع سابق، ص73.
[4] - خالد ممدوح ابراهيم،مرجع سابق، ص46.

ومن ذلك يتم إدخال فايروس إلى الجهاز عن طريق الاتصال شبكة الانترنت ويظل الفيروس كامنا حتى لحظة معنية ثم يقوم النشاط بتدمير البرامج والمعلومات فهنا المجني عليه لا يدري الوقت الذي تم فيه أصابته بالفيروس كما أن الفيروس ممكن أن يدمر نفسه في النهاية بحيث لا يعرف نوعية الفيروس أو من قام بإدخاله[1].

فالجاني يمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا علمت بها والضخامة البالغة لحجم المعلومات والبيانات المتعين فحصها وامكانية خروجها عن نطاق إقليم الدولة وعدم المعرفة بمكونات الجريمة المتعلقة بشبكة الانترنت من قبل بعض الأطراف المعنية[2].

ثانياً: صعوبة التوصل إلى الجاني

كثيراً ما يقوم الجاني بالدخول إلى الشبكة باستخدام اسم مستعار وغالبا ما يدخل إلى الانترنت عن طريق مقاهي الانترنت وبالتالي يصعب معرفة وتحديد موقع اتصاله[3]، واستخدام عناوين ومعلومات غير صحيحة وغير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه ويستخدم عنوان IP وهمي او لعدة مستخدمين بنفس العنوان وبعد مرور فترة زمنية يقوم بغلق الاتصال, وبعد فترة يعاود الاتصال مما جعل النشاط الإجرامي غالبا موزعاً على عدة عناوين لل IP والتي قد تكون غير حقيقية أو زائفة[4].

[1]- عبد الحكيم رشيد توبة، مرجع سابق، ص221.
[2]- خالد عياد الحلبي،مرجع سابق، ص223.
[3]- عبد الحكيم رشيد توبة، مرجع سابق، ص221.
[4]- خالد عياد الحلبي، مرجع سابق، ص226.

ثالثاً: عدم الاستعانة بالخبراء

إن عدم الاستعانة بالخبراء في مجال التحقيق في جرائم الحاسوب والانترنت يجعلها تفتقر إلى المعلومات الإحصائية عن تلك الجرائم التي تساعد في تحديث القوانين التي تجرم وتعاقب على هذه الجرائم[1].

لأنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها حيث تتطلب جرائم الإلكترونية إلمام خاص بتقنيات الحاسوب ونظم المعلومات سواء لارتكابها والتحقيق فيها أو لملاحقتهم قضائيا لذلك تجد مأموري الضبط القضائي أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هده النوعية من الجرائم فضلا عن صعوبة إجراء التحريات السرية وتتبع مسار العمليات الإلكترونية العابرة للحدود[2].

رابعاً: القصور في القوانين

أدى ذلك القصور إلى محاولة الفقه والقضاء إلى إخضاع جرائم الانترنت إلى نصوص قانون العقوبات وحدث هذا في فرنسا وأمريكا فجرائم الانترنت هناك تعتبر من جرائم الصحافة باعتبار الشبكة من وسائل النشر[3].

ويؤدي عدم وجود نصوص تجريمية ضد مجرمي جرائم الحاسوب والانترنت إلى ظاهرة هذه الجرائم ستتفاقم وتصل إلى مرحلة تصبح فيها عملية العلاج لهذه الظاهرة أصعب مما يتوقع، خصوصاً وأن جميع المعلومات والإجراءات ستكون إلكترونية, حيث إن القضاء لا يعتمد الأدلة والقرائن التي تعدها هيئات التحقيق عند

[1]- خالد عياد الحلبي، مرجع سابق.
[2]- خالد ممدوح إبراهيم، مرجع سابق، ص46.
[3]- سعيدي سليمة، بلال حجازي، مرجع سابق، ص76.

التفتيش والضبط والتحقيق مع مجرمي الحاسوب والانترنت وذلك ناتج عن غياب القوانين والعقوبات التي توضح السلوك الإجرامي غير المشروع.

فقانون أصول المحاكمات الجزائية يفتقر إلى كثير من النصوص القانونية اللازمة لمواجهة الطبيعة الخاصة لجرائم الحاسوب والانترنت وذلك كما يلي:

1. عدم وجود قواعد لتنظيم والتفتيش عندما يكون الحاسوب متصلا بآخر خارج الدولة.
2. ضرورة تحديث نظرية الإثبات الجنائي بما يتماشى مع قبول الدليل المعنوي في الإثبات.
3. لم يشر قانون أصول المحاكمات الجزائية إلى الإجراءات اللازم اتخاذها لمواجهة رفض مالك الحاسوب في السماح بالدخول إلى ملفاته ونظام جهازه بأن يرفض إعطاء الرقم السري أو يضع فيروسا لتعطيل عمل جهات التحقيق ولمحو الأدلة التي تثبت تورطه بارتكاب الجريمة[1].

خامساً: عدم وجود الكفاءة البشرية للتحقيق

من أهم معوقات التحقيق والإثبات تلك المتعلقة بشخصية المحقق مثل قلة المعرفة في استخدام الحاسوب وقلة الإلمام باستخدام الانترنت وعدم متابعة المستجدات في مجال جرائم الحاسوب والانترنت وقلة المعرفة بمصطلحات الحاسوب والانترنت والأساليب المتبعة في ارتكاب هذه الجرائم[2].

[1]- خالد عياد الحلبي، مرجع سابق، ص220.
[2]- المرجع نفسه، ص227.

كما أن هناك عدة معوقات وصعوبات تمنع من توقيع العقاب على مرتكبي الجرائم المعلوماتية منها:

1. قلة التشريعات التي تناسب الجرائم المعلوماتية بحيث نجد أفعال إجرامية لا ينطبق عليها أي نص قانوني في قانون العقوبات
2. جرائم المعلوماتية ذات بعد دولي فيمكن أن ترتكب الجريمة داخل قطر دولة معنية وتقع النتيجة في دولة أخرى ومنه نتجت إشكالية توقيع العقاب والى أي القوانين القضائية تخضع الجاني [1]
3. صعوبة المطالبة بالتعويض المدني: هناك صعوبة بالنسبة للمطالبة بالتعويض المدني عن ارتكاب احد جرائم الانترنت حيث يرجع ذلك لأحكام القانون الدولي الخاص ومباشرة من صعوبات واتجاهات فقهي وتشريعية معارضة
4. صعوبة إلحاق العقوبة بالجاني المقيم: هناك صعوبة في حالة ما إذا تم ارتكاب الجريمة بواسطة شخص أجنبي مقيم بالخارج ووقت الجريمة في مصر, فهنا لابد من تدخل الإنتربول الدولي للقبض على الجاني وإخضاعه للعقاب[2].
5. تنازع القوانين الجنائية من حيث المكان هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي وعينية القانون الجنائي وشخصية القانون الجنائي وعالمية القانون الجنائي وتثور المشكلة في حالة ارتكاب الفعل المؤثم في الخارج فأي من القوانين الجنائية سوف يخضع لها الجاني
6. في كثير من الأحيان لا يعرف المجني عليه انه اصيب بفيروس مثلا وذلك لوجود فيروسات تظل كامنة حتى تنشط وتبدأ في أثارها التدميرية ولو عرف

[1] سعيدي سليمة, بلال حجازي، مرجع سابق، ص75.
[2] عبد الحكيم رشيد توبة، مرجع سابق، ص221.

ذلك فمن الصعب بل من المستحيل معرفة المتسبب في هذا الفعل وبالتالي تسليط العقاب عليه

7. في كثير من الأحيان يفضل المجني عليه خاصة إذا كانت مؤسسة مالية كبيرة كالبنوك مثلا عدم التبليغ عن الإصابة وذلك كي لا تهتز ثقة المتعاملين معها.
8. أحيانا تكون الآثار الناجمة عن الجرائم المعلوماتية غير مادية وبالتالي يصعب تقديرها كإتلاف أو مسح البيانات[1].
9. صعوبة السيطرة على أدلة الإثبات : حينما يتمدد مكان ارتكاب الجريمة التي تمت بواسطة استخدام شبكة الانترنت ويتوجه أفراد الضبطية القضائية للقبض على الجاني وتحرير أدلة الجريمة منها جهاز الحاسوب المستخدم في الاتصال بالشبكة وما يحويه من برامج ومعلومات تثور مشكلة معرفة الرقم السري الذي بدونه لا يعمل جهاز الحاسوب وفي هذه الحالة لا يجوز لأجهزة التفتيش إجبار المتهم على الإفشاء عن الرقم السري حيث يعد ذلك إجراء غير قانوني كذلك قد يتمكن الجاني من تدمير البيانات المخزنة داخل الحاسوب التي تعد دليل إدانته في ثواني معدودة أثناء إجراء التفتيش كذلك قد يحتوي جهاز الحاسوب على ملفات سرية لا يجوز للغير الاطلاع عليها حيث يعد الاطلاع عليها مشكلة لجريمة انتهاك حرمة الغير ففي هذه الحالات المختلفة يكون هناك صعوبة في جمع الأدلة المادية التي تثبت ارتكاب إحدى جرائم الانترنت[2].

بالإضافة إلى هذه المعوقات التي ذكرتها والتي تمنع تسليط العقاب على مرتكب الجريمة المعلوماتية أضف إلى ذلك الأسباب التي تمنع من إسقاط الأحكام القضائية

[1] سعيدي سليمة, بلال حجازي، مرجع سابق، ص76.
[2] عبد الحكيم رشيد توبة، مرجع سابق، ص222.

التقليدية عليها والتي ترجع إلى عدم تطور قانون العقوبات بنفس السرعة المذهلة التي تتطور بها التكنولوجيا وعدم مسايرتها لتطورات التي تستخدمها الذهن البشرية لتطويع هذه التكنولوجيا لأغراضه الإجرامية[1].

إذن وربما يحسن في هذه المرحلة للنظر عند تقويم هذه القضايا من زاوية أن ما نشاهده اليوم في مسرح الجريمة التقني ما هو إلا عبء جديد يضاف إلى كاهل مؤسسات الأمن والقضاء في أن معا في ظل الاتجاه العالمي لتحويل كثير من الأنظمة المالية إلى أنظمة الدفع الإلكتروني وفي هذه المرحلة يفضل أن تبدأ الأجهزة الأمنية الدولية المختصة في مكافحة جرائم الانترنت والمعلوماتية عموما في استخدام خطة وقائية عبر التخطيط الدقيق والفعال لمواجهة السلبيات الحالية والمحتملة كذلك توظيف ايجابيات شبكة الانترنت والتعاون الدولي في مجال مكافحة الجريمة عبر مقاربة كل هذه التعديات وربطها بالبعد الإجرامي للجرائم التي تتم عبر الانترنت، ولعل هذا ينطوي على تحديات ومشكلات جمة تتمثل تجلياتها في التالي:

أ. الحاجة إلى سرعة الكشف عن الجريمة وتعقبها خشية ضياع الدليل بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم.

ب.مدى قانونية وحاجية الأدلة للجرائم التي تتم عبر الانترنت

ت.مشكلات الاختصاص القضائي والقانون الواجب التطبيق.

ث.الحاجة إلى التعاون الدولي الشامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود.

وهذه المشكلات كانت ولا تزال محل اهتمام على الصعيدين الوطني والدولي[2].

[1] سعيدي سليمة، بلال حجازي، مرجع سابق، ص76.
[2] عبدالله عبد الكريم عبدالله، مرجع سابق، ص48.

المطلب الثاني: السبل التشريعية للحد من الجريمة الإلكترونية

يشكل الاعتماد المتزايد على الأنظمة المعلوماتية في تسيير شؤون المجتمع ضغطاً كبيراً على قانون الإجراءات الجنائية يدفعه للتعامل مباشرة مع المعلومات ويسرع خطاه لدخول مجال جديد يصعب فيه تطبيق إجراءات الإثبات التقليدية المتعلقة بالماديات على الأموال المعنوية كالمعلومات ومع إدراك خطورة وسهولة ارتكاب جرائم المعلوماتية التي أفرزتها بيئة المعالجة الآلية للبيانات ونبيه لأثارها السلبية على جهود التنمية الإدارية والاجتماعية والاقتصادية وامن المواطنين بدأت مكافحتها تحظى باهتمام متزايد من الحكومة وبعض المنظمات الدولية واخذ فنيون والخبراء امن المعلومات والنظم المعلوماتية فضلا عن رجال الصناعة يركزون جهودهم البحثية وتجاربهم العلمية على سد ثغرات الأنظمة الأمنية وعلى تحسين وتطوير أساليب الحماية الفنية والجنائية للنظم المعلوماتية ومحتوياتها لكي تصل إلى أقصى درجة من الفاعلية[1].

الفرع الأول: التعاون على المستوى الدولي

التعاون لغة هو العون المتبادل أي تبادل المساعدة لتحقيق هدف معين وهذا هو المعنى العام لكلمة التعاون ويفهم منه التضافر المشترك بين شخصين أو أكثر لتحقيق نفع مشترك أو خدمة مشتركة على وجه العموم وقد ورد في في القران الكريم آية تحث على التعاون بقوله تعالى: "وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان"[2].

[1] احمد خليفة الملط، مرجع سابق، ص118.
[2] احمد اللاه المراغى، مرجع سابق, ص123.

وبالتالي لابد من خلق تعاون بين الدول لملاحقة هذا النوع من الجرائم كونها جرائم عابرة للحدود، والدولة وحدها لا تستطيع السيطرة عليها، فقد أنشئت العديد من الاتفاقيات والجهود للتعاون الدولي في مكافحة الجريمة الإلكترونية منها:

أولاً: اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية

بتاريخ 20نيسان 2000 تقدمت اللجنة الأوربية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الحاسوب وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلا الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001وتعرف باتفاقية بودابست 2001 "اتفاقية الجرائم الإلكترونية"[1]، وهذا بعد أن وصلت تلك الجرائم إلى حد خطير حيث أصبحت تهدد الأشخاص والممتلكات وبعد التوقيع على تلك الاتفاقية من مسؤولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا هو نتاج مباحثات ومفاوضات استغرقت ما يزيد عن أربعة أعوام حتى يتم توصل إلى الصيغة النهائية المناسبة لتلك الاتفاقيات حتى يتم التوقيع عليها من طرف جميع الأطراف دون اعتراض وقد كان الخلاف الوحيد هو مجال محاربة العنصرية ومن المعروف إن الجريمة يعاقب عليها القانون الدولي ولابد من النص في الاتفاقية على لزوم العمل على إزالة تلك المواقع التي على التحريض الكراهي[2]، ومن ضمن الجوانب العديدة التي تناولتها تلك الاتفاقية الإرهاب الإلكتروني وعمليات التزوير بطاقات الائتمان ودعارة الأطفال وتلك الجرائم تعتبر من أكثر الجرائم انتشارا على المستوى العالمي بصفة عامة وفي أوربا وأمريكا بصفة خاصة ولم تفلح أي جهود فردية تم بذلها من جانب أي من الدول الموقعة على الاتفاقية وعليه فقد كان

[1] عبدالله عبد الكريم عبدالله، مرجع سابق، ص124.
[2] سعيدي سليمة، بلال حجازي، مرجع سابق، ص146.

من المحتمل التنسيق بين تلك الجهود على اقل تقدير أن لم يكن التوحيد بينها لتؤتي ثمارها في الحد من ارتكاب تلك الجرائم التي تأثر على التقدم الاقتصادي المتواصل في اقتصاديات تلك الدول المتقدمة كذلك تحدد الاتفاقية أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهدت الدول الموقعة بالتعاون الوثيق من اجل محاربتها[1].

وتتلخص أهداف الاتفاقية بالتالي:

أ. السعي بتحقيق وحدة التدابير التشريعية بين الدول الأوربية والدول المنظمة للاتفاقية من غير الدول الأوروبية .

ب. التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الحاسوب والانترنت وإيجاد مرجعية ودليل إرشادي لتدابير التشريعية الوطنية في ميدان مكافحة جرائم الحاسوب والانترنت.

ت. ضرورة فاعلية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الحاسوب وشبكات الحاسوب وأنشطة اساءة استخدام الحاسوب والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الحاسوب على المستوى الوطني والدولي[2].

ثانياً: المعاهدة الأوربية لمكافحة جرائم الانترنت

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة البلدان في مكافحة الجرائم وسط انتقادات من دعاة حماية الحرية الشخصية وبعد أن تتم المصادقة عليها من

[1] عبد الحكيم رشيد توبة، مرجع سابق، ص228.
[2] عبدالله عبد الكريم عبدالله، مرجع سابق، ص126.

قبل رئاسة المجلس وتوقيعها من البلدان المعنية تستلزم اتفاقية الدول الموقعة عليها بين الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى الشبكة[1].

والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالحاسوب وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي تتضمن بنود المعاهدة التي تم تعديل مسودتها 27 مرة قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول مساعدة بعضها في جمع الأدلة وفرض قانون لكل صلاحيات دولية الجديدة ستكون على حساب حماية المواطنين من إساءة حكومات استخدام السلطات التي أعطتها لهم تلك الاتفاقية التي قد يؤون استخدامها.

هذا وقد اتجهت كافة الدول المتقدمة تكنولوجياً إلى استحداث نصوص قانونية جديدة تجرم الجرائم الإلكترونية الجديدة على قوانينها التقليدية القديمة وعليه فقد صاغت تلك الدول نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجياً[2].

ثالثاً: الجهود العربية المبذولة لمكافحة الجريمة الإلكترونية

ليس هناك في العالم العربي ما يستحق الوقوف عنده كثيراً فإنه للأسف الشديد لا توجد أي دولة عربية قد قامت بسن قوانين جديدة خاصة لها أو حتى تحديث قوانينها الخاصة لتستوعب تلك المستجدات الإجرامية فالدول العربية لازالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي بينما نجد أن الدول العربية لازالت لا تحرك ساكناً[3].

[1] سعيدي سليمة،بلال حجازي، مرجع سابق، ص147.
[2] عبد الحكيم رشيد توبة، مرجع سابق، ص228.
[3] المرجع نفسه، ص232.

ولعل من أبرز ما يمكن أن يقال عن الجهود العربية المبذولة من اجل الحماية من جرائم الحاسب اعتمد مجلس وزراء العدل العربي للقوانين العربي الموحد كقانون نموذجي بموجب القرار رقم 229 وبالرجوع إلى مذكرة الإيضاحية لهذا القانون نجد أن الباب السابع الخاص بالجرائم ضد الأشخاص الناتج عن المعالجات المعلوماتية حيث عليه وجوب حماية الحياة الخاصة على الأسرار من أخطار المعالجة الإلكترونية أما المادة 464 فقد نصت على عقاب من يقوم بفعل الدخول بطريقة الغش إلى نظام أو جزء من نظام المعالجة الآلية وتعد هذه المحاولة بالرغم من تواضعها من أبرز ما تم على صعيد تعزيز التعاون على مستوى العربي من الناحية الشرعية[1].

رابعاً: تبادل الإنابة الدولية القضائية

يقصد بالإنابة الدولية القضائية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدول الطالبة إلى الدول المطلوب إليها للفصل في مسألة معروضة على السلطة القضائية في الدول الطالبة ويتعذر عليها القيام به بنفسها. والإنابة القضائية تسهل إذناً الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، مثال ذلك إجراء التفتيش والضبط والمعاينة.

وتستلزم الإنابة القضائية إرسال الملف الخاص بالدعوى الجنائية بمرفقاته: محاضر جمع الاستدلالات والتحقيق والمستندات التي أجريت بمعرفة سلطة التحقيق في الدولة إلى السلطة المختصة في الدولة المطلوب منها اتخاذ الإجراء المطلوب.

[1] سعيدي سليمة، بلال حجازي، مرجع سابق، ص147.

وقد نصت المادة 8 من قانون تنظيم الاتفاقية على أن يكون للإجراء القضائي الذي يتم بواسطة إنابة قضائية وفقاً للأحكام المتقدمة نفس الأثر القانوني الذي يكون له فيما لو تم أمام السلطة المختصة في الدول الطالبة[1].

الفرع الثاني: السبل التشريعية على المستوى الداخلي:

أولاً: في التشريع الجزائري

وسنورد فيما يلي أهم المواد من القانون الجزائري والتي عدلت لتتماشى مع التوجهات الحديثة في معالجة المعلومات بطريقة إلكترونية، ويمكن تلخيص أهم الاعتداءات المشمولة بالمعالجة القانونية في:

أ. الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

ب. الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.

ت. الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام[2].

وقد اصدر المشرع الجزائري بعض التشريعات المتعلقة بالجرائم المعلوماتية تمثيل قانون رقم 24,96 لسنة 1996 المتعلق بالبريد والمواصلات وخاصة ما يتعلق منها بمخالفات الحسي بالأجهزة السلكية واللاسلكية.

وبالإضافة إلى النصوص والقوانين الجزائية التي تتصدى لظاهرة الإجرام المعلوماتي توجد قوانين أخرى واتفاقيات بالظواهر المستحدثة كالقانون رقم09-08 المعلق بحماية الأشخاص الذين اتجاه إلى معالجة المعطيات ذات الطابع الشخصي والقانون

[1] احمد عبد الله المراغي، مرجع سابق، ص134.
[2] سعيدي سليمة، بلال حجازي، مرجع سابق، ص 148.

رقم 02 المتعلق بحقوق المؤلف والحقوق المجازة كما وقع تغيره وتنميته بموجب القانون رقم 34,05 المؤرخ في 2006/02/14 والقانون رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية والاتفاقيات للجريمة بين الدول العربية والخاصة بمحاربة الجريمة الإلكترونية التي صادق عليها المغرب كم سبق ذكرها من قبل[1].

ثانياً: التشريعات في مصر

لم يصدر المشرع المصري قانونا خاص بالجرائم المعلوماتية بل لجأ في بعض القوانين والتشريعات الخاصة إلى إضافة بعض المواد التي تهتم بالبيانات والحاسبات كما هو الحال في قانون الأحوال المدنية الجديدة رقم 143 لسنة 1994 وقانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002[2].

بحيث ورد في نص الدستور المصري بالمواد 41,45 على حماية الحياة الخاصة من جوانب منفذة بحيث نصت المادة 41 من الدستور على أن الجريمة الشخصية حق طبيعي مصون لا يمس وفيما عدا حالة التلبس لا يجوز القبض على احد أو تفتيشه أو حبسه أو قيد حريته بأي قيد أو منعه من التنقل إلا بأمر تستلزمه ضرورة التحقيق، ويصدر هذا الأمر من القاضي المختص أو النيابة العامة وذلك وفقاً لأحكام القانون ويجدد القانون مدة الحبس الاحتياطي وفي المادة 44 للمساكن حريته فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائي وفقاً لأحكام القانون وبالمادة 45 لحياة المواطنين الخاصة حرمة تحميها القانون[3].

[1] احمد عبد اللاه المراغي، مرجع سابق، ص111 .
[2] احمد خليفة الملط، مرجع سابق، ص 155.
[3] أيمن عبد الله فكرى، مرجع سابق، ص732.

هذا واصدر المشرع المصري بعض التشريعات المتعلقة بالمعلوماتية ولكنها تشريعات خاصة مثل قانون الأحوال المدنية رقم 143 لسنة 1994 وقانون مكافحة غسل الأموال رقم 80 لسنة 2002 وقانون حماية الملكية الفكرية رقم 82 لسنة 2002 وقانون تنظيم الاتصالات رقم 10 لسنة 2003 وقانون التوقيع الإلكتروني رقم 16 لسنة 2004 إلا انه حتى الآن لم يبين المشرع المصري تشريع جنائي خاص بالجريمة الإلكترونية[1].

نص القانون الاتحادي رقم 2 لسنة2006 على تجريم الأفعال التالية:

1. اختراق المواقع والأنظمة الإلكترونية : عاقب هذا القانون على جريمة اختراق الموقع وأنظمة المعلومات ويزد لتلك الجريمة أنواعا من العقوبة تتدرج وفقاً لحالات أربع: حالة القيام بالفعل دون ترتب نتيجة، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإلغاء أو حذف أو تدمير المعلومات، حالة القيام بالفعل مع ترتب نتيجة متعلقة بانتهاك معلومات شخصية، حالة القيام بالفعل أثناء أو سبب العمل أو تسهيل للغير مهمة القيام بهذا الفعل .
2. تزوير مستندات معترف بها في النظام المعلوماتي:

يعاقب هذا القانون كل من زور مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية المعترف به قانوناً في نظام معلوماتي.

3. تعطيل الوصول إلى الوسائل أو البرامج أو المعلومات أو الشبكات المتعلقة بتقنية المعلومات.
4. العبث بالشبكة المعلوماتية أو إحدى وسائل التقنية والتي يترتب عليها ضرر موصوف.

[1] احمد عبد اللاه المراغي، مرجع سابق، ص109.

5. العبث بالفحوصات الطبية باستخدام الانترنت أو إحدى وسائل تقنية المعلومات[1].

والتوقيع الإلكتروني المحمي والتوقيع المستوفى لشروط المادة 20 من هذا القانون والتي تنص على: "يعامل التوقيع على انه توقيع إلكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق المحكمة مضمونا في هذا القانون أو معقولة تجارياً ومتفقاً عليها مابين الطرفين من أن التوقيع الإلكتروني كان في الوقت الذي تم فيه التوقيع".

المبحث الثاني: الجزاءات المقررة للجريمة الإلكترونية

إن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطارا للعلاقات التي تترتب على استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال، ويحدد الواجبات تجاهها، فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتاً مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال الاعتداءات التي يروجها.

فالقانون الجنائي التقليدي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا والجرائم المعلوماتية الجديدة، لاسيما أن نصوصه وضعت في عصر لم يكن الإنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن استخدامه، مما يستوجب إعادة النظر في التشريعات والنصوص العقابية بشكل دوري للإحاطة بالجرائم المستحدثة أهمها الجريمة الإلكترونية فلا عقوبة على جرم لم يأت عليه نص قانوني باعتبار أنه لا عقوبة إلا بنص[2].

[1] علي جعفر، مرجع سابق، ص160.

[2] محمود خضر سلمان وآخرون، الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها، بحث جامعي.

ومن أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون 04-15 الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394مكرر 1 – 394 مكرر 7.

لقد نص المشرع الجزائري على جملة من العقوبات الخاصة بالجرائم الإلكترونية منها عقوبات أصلية وأخرى تكميلية، بالإضافة إلى عقوبة خاصة بالأشخاص الطبيعية والأشخاص المعنوية، سنوضح أكثر من خلال المطلب الأول والمخصص بالعقوبات المقررة للشخص الطبيعي والمطلب الثاني والمخصص بالعقوبات المقررة للشخص المعنوي.

المطلب الأول: العقوبات المقررة للشخص الطبيعي

لقد أورد المشرع الجزائري على غرار المشرع الفرنسي جملة من العقوبات على الشخص الطبيعي، والتي تختلف بحسب الجريمة المرتكبة وجسامة خطورتها.

الفرع الأول: العقوبات الأصلية

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات ،إذ نجد سلم خطورة يتضمن ثلاث درجات ،جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية

جريمة الدخول والبقاء المشددة،أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.[1]

أولاً: العقوبات المقررة لجرائم الاعتداء على سير النظام

سنتناول العقوبات المقررة لكل من جريمتي الدخول والبقاء غير المشروع سواء في صورتها البسيطة أو المشددة أولاً، ثم جريمة الاعتداء على سير النظام ثانياً.

1-عقوبة جريمة الدخول أو البقاء غير المشروع:

تقرر الفقرة الأولى من المادة 394 مكرر من قانون العقوبات الجزائري عقوبتان أصليتان لجريمة الدخول أو البقاء غير المشروع في صورتها البسيطة أو المشددة.

أ- عقوبة الجريمة في صورتها البسيطة:

يعاقب المشرع الجزائري على هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألف50.000 دج إلى مائة ألف 100.000دج . وترك المشرع الجزائري السلطة التقديرية للقاضي بأن جعل له حداً أدنى وحداً أقصى في تقدير العقوبة بحسب الوقائع والظروف الواقعة أمامه، حيث يختلف الباعث من شخص لآخر فليس باعث الفضول والاكتشاف كباعث الجوسسة والربح، وعلى هذا وجب إختلاف التقدير[2].

ب- عقوبة الجريمة في صورتها المشددة

تضاعف العقوبة حسب الفقرة الثانية والثالثة من المادة 394من قانون العقوبات الجزائري لجريمة الدخول أو البقاء غير المشروع إذا ترتب على هذا الأخير

[1] سعيدى سليمة، بلال حجازي، مرجع سابق، ص152.

[2] حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث العلمي،كلية الحقوق، جامعة اكلي محند اولحاج، العدد الثاني، 2016، ص73.

إما حذف أو تغيير للمعطيات سواء في حدها الأدنى الذي أصبح ستة6 أشهر بعدما كان ثلاثة 3 أشهر ، أو في حدها الأقصى إلى سنتين بعدما كان سنة واحدة.

وبالنسبة للغرامة فتصبح 100.000 دج إلى 200.000دج بعدما كانت 50.000دج إلى 100.000دج .

أما إذا حدث تخريب لنظام اشتغال المنظومة فالعقوبة تكون كالتالي:

الحبس من ستة أشهر إلى سنتين أما الغرامة من50.000 دج إلى 150.000 دج حيث ثبت الحد الأدنى للغرامة وارتفع حدها الأقصى وفقاً للفقرة 3 من المادة 394 مكرر[1] .

ثانياً: العقوبات المقررة لجرائم الإعتداء على المعطيات

1- عقوبة جريمة التلاعب بالمعطيات

نصت عليها المادة 394 مكرر 1، ق.ع.ج. بالحبس من 06أشهر إلى 03 سنوات وبغرامة تتراوح بين 500.000دج إلى 200.000دج.

والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول أو البقاء غير المشروع سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي حذف المعطيات أو تغييرها ، فإن العقوبة المقررة لجريمة التلاعب

[1] غنية باطلي، مرجع سابق،ص208 .

تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي، بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء غير المشروع[1].

فالموقف النفسي اتجاه التلاعب بالمعطيات موجود في جريمة الاعتداء العمدي على المعطيات بينما لا يوجد في جريمة الدخول أو البقاء المشددة، بينما قبل التعديل لسنة 2004 كان هناك تقارب في العقوبة بين جريمة عمدية "الاعتداء العمدي على المعطيات" وجريمة غير عمدية "جريمة الدخول أو البقاء غير المشروع المشددة ".

2- عقوبة جريمة التعامل غير المشروع بالمعطيات

تعاقب المادة 394مكرر 2من ق. ع. ج. على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبغرامة مالية من 1.000.000دج إلى 5.000.000دج، **كل من يقوم عمداً أو عن طريق الغش بما يلي:**

أ- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ب- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

[1] د/ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية ، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية 2005، ص 288.

وبهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المشروع بهما سواء كانت في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات "غير أن حدها الأدنى يقل عن كلتا الجريمتين".

وأن الحد الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء غير المشروع في صورتيها "سنة أو سنتين".

وتتساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات "03"سنوات.

غير أن حدها الأدنى يقل عن الجريمتين معاً، لأنه في جريمة الدخول أو البقاء البسيطة 3 أشهر وفي هذه الجريمة في صورتها المشددة وفي جريمة التلاعب هو 6 أشهر[1].

3-عقوبة جريمة التزوير الإلكتروني

نجد أن القوانين الجنائية لم تفرض عقوبة الإعدام على مرتكبي هذا النوع من الجرائم، ولكنها شملت في قوانينها عقوبات أخرى كالسجن والحبس والغرامة وغيرها من العقوبات كما جاء في المواد 214 ،215 ،216 ،217 ،218 ق.ع.ج. الخاصة بالتزوير التقليدي وكذلك في المادة 394 مكرر1 إلى مكرر 7 الخاصة بالجرائم المعلوماتية وتعتبر الغرامة في جرائم التزوير المعلوماتي عقوبة مالية توقع على المجرم المعلوماتي قد تكون أصلية وقد تكون تكميلية لوجود عقوبة أخرى معها، فالقضاء هو الذي يحدد اما أن يحكم بها مع العقوبة الأصلية أو لا يحكم.

الفرع الثاني: العقوبات التكميلية

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص 219.

إلى جانب العقوبات الأصلية المطبقة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أقر المشرع عقوبات تكميلية تطبق على كافة صور المساس بأنظمة المعالجة الآلية للمعطيات وهي العقوبات المنصوص عليها بالمادة 394مكرر 6 على النحو التالي:

مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

ومن نص هذه المادة يمكن حصر العقوبات التكميلية في:

أولاً: المصادرة

عرفتها المادة 15 من قانون العقوبات الجزائري على أنها: الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء.

حيث يتم مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة، والمصادرة هنا عينية رغم اتفاقها مع الغرامة، مع مراعاة الاحتفاظ بحقوق الغير حسن النية.

وهناك عدة شروط لتطبيق عقوبة المصادرة، وهي أن يحكم على المتهم بعقوبة الأصلية بإحدى الجرائم المنصوص عليها في القسم الخاص بالاعتداء على أنظمة المعالجة الآلية للمعطيات، وأن تكون الأشياء التي تمت مصادرتها قد استخدمت في ارتكاب الجريمة.

وتعتبر الأجهزة والبرامج واردة على سبيل المثال لا على سبيل الحصر، حيث أن المشرع استعمل مصطلح "والوسائل المستخدمة" اي أنه فتح المجال لاستيعاب جميع الوسائل التي يمكن استخدامها في ارتكاب هذه الجرائم.

ويجب أن تكون الاشياء المستخدمة مضبوطة حتى يمكن مصادرتها، سواء قدمها الجاني من تلقاء نفسه أو ضبطتها الشرطة، فلا يمكن مصادرة شيء غير مضبوط والحكم على الجاني بدفع قيمته.

ويجب أن لا تخل المصادرة بحقوق الغير حسن النية، بمعنى أنه إذا كانت الوسائل المستخدمة في ارتكاب الجريمة مملوكة للغير، والغير هنا شخص لا علاقة له بالجريمة تماماً أي أنه ليس بفاعل أو شريك، وتثبت ملكيته للشيء المضبوط، وأن يكون حسن النية تجاه الوسائل واستخدامها لارتكاب الجرائم[1].

ثانياً: الإغلاق

ويتعلق الأمر بإغلاق المواقع التي تكون محلاً لجريمة من الجرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، ويشمل إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها على سبيل المثال إذا كان الجاني مستأجراً للمحل والمالك مؤجراً له، ويعلم خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الانترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالافعال الخطيرة التي يقوم بها زبونه،ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم.

والمقصود بالمواقع التي تكون محلا للجريمة تلك المواقع التي تقدم خدمات تسمح بالدخول غير المشروع لمختلف الأنظمة أو تسمح بالتلاعب بالمعطيات.

[1] غنية باطلي، مرجع سابق، ص 216.

وهناك مواقع تقوم بتعليم كيفية تصميم المعطيات غير المشروعة ونشرها والاتجار بها لتحقيق عائد مالي أو مصالح شخصية.

أما المواقع التي تم الاعتداء عليها "الضحية" فإنه لا يتصور غلقها. وكان من الأفضل استعمال المشرع لعبارة "المواقع التي تستعمل في ارتكاب الجريمة " بدلاً من " المواقع محل الجريمة" كونها تعني المواقع التي وقعت عليها الجريمة.

وبالنسبة لمدة الإغلاق فإن المشرع لم يحدد مدة معينة لغلق المحل أو مكان الاستغلال.

وعليه فقد تكون مؤبدة أو مؤقتة، مثلما هو منصوص عليه في الأحكام العامة لقانون العقوبات المادة 16 مكرر 1 مضافة بالقانون 23/06 يجوز أن يؤمر بإغلاق المؤسسة نهائياً أو مؤقتاً في الحالات وبالشروط المنصوص عليها في القانون.

المطلب الثاني: العقوبات المقررة للشخص المعنوي

لقد نص المشرع الجزائري على إقرار المسؤولية الجنائية للأشخاص المعنوية وتوقيع عقوبات خاصة بهم في المادة 18 مكرر من ق.ع.ج بعد تعديله سنة 2004 ومن بين الجرائم التي يعاقب عنها الشخص المعنوي جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وقد شدد في عقوبة هذه الجرائم إذا ارتكبها شخص معنوي، أو كانت موجهة ضد الجهات العامة أي إذا كانت هذه المعطيات تابعة للدولة، والتي تعادل طبقاً للمادة 394 مكرر 4 من ق.ع.ج 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

وتنعقد المسؤولية الجنائية للشخص المعنوي عند قيامه بجرائم لها علاقة بالمجال الإلكتروني وفي إطار الاقتصاد الحالي تقوم الشركات بالبحث عن المعلومات بأية وسيلة، وهذا البحث يمكن أن يكون عن طريق الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة أخرى منافسة والإطلاع على ملفاتها وخططها، وبعد وجود المنتج المنافس تقوم بمنافستها على ذلك الأساس وبالتالي قيام المنافسة غير المشروعة عن طريق ارتكاب جرائم إلكترونية.

ولقد شدد المشرع العقوبة على الشخص المعنوي لأن الكثير من الأشخاص المعنوية تنشأ بغرض تحقيق الربح فتقوم بالمنافسة غير المشروعة لمنافسيها عن طريق ارتكاب هذا النوع من الجرائم.

وتجدر الإشارة إلى أن المشرع الجزائري قد نص على نوعين من العقوبات المقررة للشخص المعنوي في المادة 18 مكرر من ق.ع.ج. وهي الغرامة كعقوبة أصلية، وعقوبات تكميلية كالآتي:

أ. حل الشخص المعنوي.

ب. غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس "5" سنوات.

ت. الإقصاء من الصفقات العمومية لمدة لا تتجاوز "5" سنوات.

ث. المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائياً أو لمدة لا تتجاوز "5" سنوات.

ج. مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

ح. الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس "5" سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

الفرع الأول: تشديد عقوبة الغرامة في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات

تتثمل عقوبة الغرامة في دفع مبلغ من المال من قبل المحكوم عليه بها إلى خزينة الدولة، ولا حرج في الحكم بالغرامة على الشخص المعنوي بالرغم ما تسببه من ضرر للمساهمين في الشخص المعنوي.

وفقاً للمادة 18 مكرر من ق.ع.ج.، فإن الغرامة تتراوح بين واحدة وخمس أضعاف تلك الغرامة المقررة للشخص الطبيعي.

أما المادة 394 مكرر4 من نفس القانون والتي تتعلق بعقوبة الغرامة على الشخص المعنوي في جرائم المعطيات فقد قيدت القاضي وألزمته بالحكم بالحد الأقصى لهذه الغرامة وهو خمسة أضعاف الغرامة المقررة على الشخص الطبيعي.

أما إذا كانت الجريمة موجهة ضد الأشخاص المعنوية فقد قرر المشرع تشديد العقوبة في حالة ما إذا كان الضحية من الجهات العامة وهذا حفاظاً على المصلحة العامة.

الفرع الثاني: العقوبات المقررة للشخص المعنوي في حالة الاعتداء على الجهات العامة

قد يشترط القانون بالنسبة لبعض الجرائم أن يكون موضوع النتيجة الإجرامية شيئاً أو شخصاً معيناً تتوافر فيه صفات معينة حتى يتم تشديد العقوبة.

ففي هذا النوع من الجرائم الإلكترونية أو الاعتداء على المعطيات نجد أن هذه المعطيات أو المعلومات قد تخص الأفراد أو شركات أو جهات معينة. ويأخذ المشرع في الاعتبار الجهة التي تتبعها هذه المعطيات، ويولي اهتمام أكبر للمعطيات التي تتبع للدولة والجهات العامة.

ونظراً لأن الاعتداء على المصلحة العامة أشد وأخطر من الاعتداء على المصالح الخاصة نجد أن المشرعين يقدرون ذلك لاسيما إذا كانت هذه الجهة المعتدى عليها حساسة كالدفاع والأمن الوطنيين.

وقد خطى المشرع الجزائري نفس المسلك حيث بسط حمايته على المعطيات بمختلف أنواعها والجهات لتابعة لها. إلا أنه شدد العقوبة في حالة ما إذا كان الاعتداء على المعطيات تتعلق بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام. فإن الغرامة تضاعف خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف إلى خمس "5" مرات عما هو مقرر للشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي، وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشر "10" أضعاف عما هو مقرر على الشخص العادي.

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة[1].

[1] سعيدى سليمة، بلال حجازي، مرجع سابق، ص154

خـاتـمـة

في ختام دراستنا لموضوع الجريمة الإلكترونية تبين لنا ان اختلاف تعريفات الجريمة الإلكترونية حول العالم أدت بالطبع إلى صعوبة الإلمام بالجريمة الإلكترونية ومواجهتها وأنها جريمة مستحدثة تختلف في طبيعتها عن الجرائم التقليدية ناتجة عن التطور التكنولوجي وبالتالي فان القواعد التقليدية غير ملائمة لمواجهة هذا النوع من الجرائم تاركة للمشرع الجنائي حملاً كبيراً في مواجهتها مما يتوجب استحداث قانون خاص بها.

وإن أهم ما يميز الجريمة الإلكترونية سهولة ارتكابها وأنها لا تعرف الحدود للجريمة الإلكترونية صور عديدة أوردنا منها على سبيل المثال لا الحصر فلو أردنا حصرها فإننا نحتاج إلى موسوعة علمية لمحاولة حصرها.

ورغم الجهود المبذولة والتي مازالت تبذل لمواجهة الجرائم الإلكترونية لم تحقق نجاعتها في ذلك فهناك فراغ قانوني في مواجهة هذه الجرائم.

وبناءً على ما سبق توصلنا إلى النتائج الآتية:

1. الحاسوب هو أساس ارتكاب الجريمة الإلكترونية.
2. أهم دوافع ارتكاب الجريمة الإلكترونية هو تحقيق عائد مادي.
3. الجريمة الإلكترونية لا تتسم بالعنف في ارتكابها.
4. الجريمة الإلكترونية ظاهرة حديثة وبالتالي يمكن ظهور أنواع أخرى من الجرائم المعلوماتية.
5. عجز التشريعات عن مكافحة الجريمة الإلكترونية بما فيها التشريع الجزائري يؤدي إلى إفلات مرتكب الجريمة من العقاب.
6. أبرز التحديات التي تثيرها الجريمة الإلكترونية من الناحية القانونية هو تنازع الاختصاص والقانون الواجب التطبيق.

ونخلص إلى بعض التوصيات الآتية:

1. العمل على إيجاد تعريف شامل وجامع للجريمة الإلكترونية.
2. إنشاء محاكم إلكترونية دولية للفصل في الجرائم الإلكترونية.
3. تعزيز دور التحكيم الدولي لتسهيل إجراءات مواجهة الجريمة الإلكترونية.

4. توعية المجتمع باستخدام كلمات مرور قوية للمواقع الإلكترونية والتأكد من المواقع الرسمية وتجنب المشبوهة منها، وتوعيتهم أيضاً بعدم مسايرة الرسائل العشوائية أو التي تتطلب معلومات سرية.
5. تدريب وتأهيل أفراد الضبطية القضائية على كيفية التعامل مع الأنظمة المعلوماتية بدقة.
6. توعية المجتمع عن مخاطر الجريمة الإلكترونية وأنها تعرض للجزاء.
7. خلق ثقافة الشكوى عن الضرر الناجم عن الجريمة الإلكترونية لدى المجتمع وتوعيته بإجراءات رفع الشكوى خصوصاً إذا كان المجرم من دولة أخرى.
8. استخدام "المجموع الاختباري" للتحقق من تكامل الملفات وسلامتها وذلك باتباع خوارزميات فحص سلاسل الأحرف مثل "SHA- MD5".
9. تفعيل دور الإنتربول الدولي في مواجهة الجريمة الإلكترونية وإلزام الدول بالمصادقة عليه.
10. التطوير المستمر لتشريعات الدول لسد أي فراغ قانوني حول الجرائم الإلكترونية.
11. تخصيص خبراء وفنيين في الأنظمة المعلوماتية للكشف عن الجرائم الإلكترونية.

وفي النهاية الحمدلله الذي وفقنا لكتابة بحثنا المتواضع، ونلتمس العذر منكم إن أخطأنا فما نحن إلا بشر نصيب ونخطئ، فإن أصبنا فمن الله وإن أخفقنا فمن أنفسنا ويكفينا شرف المحاولة.

قائمة المصادر والمراجع.

أولاً: القرآن الكريم.

ثانياً: النصوص القانونية:

المادة"1" الأمر رقم 156-66المؤرخ في 18 صفر 1396هـ الموافق ل 08 يونيو1966 المتضمن قانون العقوبات الجريدة الرسمية الجمهورية الجزائرية.

العدد49 صادر في 21 صفر 1386هـ الموافق ل11يونيو1996، معدل ومتمم.

ثالثاً: الكتب

1. أحمد خليفة الملط، الجرائم المعلوماتية، دار الجامعي، ط2،الاسكندرية،2006.

2. أحمد عبد اللاه المراغي، الجريمة الالكترونية ودور القانون الجنائي في الحد منها،المصدر القومي للإصدارات القانونية ،ط1، القاهرة ،2017.

3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري جامعة بن عكنون الجزائر،2006.

4. أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة الإسكندرية،2007.

5. بكرى يوسف بكرى، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامع، ط1،الإسكندرية،2011.

6. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترانت دار الثقافة للنشر والتوزيع، ط2011،1.

7. خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية الإسكندرية،2008.

8. سعدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي ،ط1، الإسكندرية ،2017.

9. الشحات إبراهيم محمد منصو، الجرائم الالكترونية في الشريعة الإسلامية والقوانين الوضعية ،دار الفكر الجامعي ،ط1،الإسكندرية،2011.

10. عبد الحكيم رشيد توبة ،جرائم تكنولوجيا المعلومات دار المستقبل للنشر والتوزيع، ط1،عمان، الأردن،2008.

11. عبد الله عبد الكريم،جرائم المعلوماتية والانترانت منشورات الحلبي الحقوقية،ط1 بيروت– لبنان.

12. على حسن محمد الطوالبة ،التفتيش عن المعلومات في وسائل التقنية،دار الفكر الجامعي ،ط1، الاسكندرية2011.

13. علي جعفر جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت.

14. غنية باطلي،الجريمة الالكترونية ،الدار الجزائرية للنشر والتوزيع،الجزائر،2015.

15. محمد ابوالعلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية.

16. محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، ط1، الأردن،2005.

17. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية 2007.

18. محمد عبدالله أبو بكر، جرائم الكمبيوتر والانترنت، المكتب العربي الحديث،الإسكندرية،2007.

19. محمد عوض، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية،1985.

20. محمود خضر سليمان وآخرون الجريمة الالكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامع،ط1،الإسكندرية ،2011.

21. محمود نجيب حسني ،شرح قانون العقوبات ، القسم الخاص الجرائم المخلة بالمصلحة العامة، 1972.

22. نائلة عادل محمد فريد قورة جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، 2005.

ثانياً: المجلات والبحوث العلمية

1. آمنة زعيطي ،بحث بعنوان مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري، مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، العدد7، 2017.

2. حمودي ناصر ،الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكادمية للبحث العلمي كلية الحقوق،جامعة آكلي محند اولحاج، العدد الثاني، 2016.

3. علي عبد القادر القهوجي، الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، بحث مقدم لمؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي الإمارات العربية المتحدة، 2003.

رابعاً: المواقع الإلكترونية

https://ar.vpnmentor.com/blog، 22/04/2021 بتوقيت الساعة 17:00.

فهرس المحتويات

فهرس المحتويات

الصفحة


تم بحمد الله