جامعة الشهيد حمه لخضر – الوادي
معهد العلوم الإسلامية
قسم الشريعة

أحكام مكافحة الجريمة الإلكترونية بين الشريعة والقانون

مشروع مقترح لإنجاز مذكرة تدخل ضمن متطلبات الحصول على شهادة الليسانس في العلوم الإسلامية – تخصص: شريعة وقانون

الطلبة:
- سمير حساني
- عبد الكامل ليحيو
- حمزة جاب الله

المشرف:
أ. الطيب بن شهرة

السنة الجامعية: 1436-1437هـ/2015-2016م

جامعة الشهيد حمه لخضر – الوادي
معهد العلوم الإسلامية
قسم الشريعة

أحكام مكافحة الجريمة الإلكترونية بين الشريعة والقانون

مشروع مقترح لإنجاز مذكرة تدخل ضمن متطلبات الحصول على شهادة الليسانس في العلوم الإسلامية – تخصص: شريعة وقانون

الطلبة:
- سمير حساني
- عبد الكامل ليحيو
- حمزة جاب الله

المشرف:
أ. الطيب بن شهرة

السنة الجامعية: 1436-1437هـ/2015-2016م


بسم الله الرحمن الرحيم

إهداء

نهدي ثمرة جهدنا

إلى الوالدين الكريمين

إلى سر النجاح أسرنا الغالية

إلى كل أساتذتنا في معهد العلوم

الإسلامية

إلى كل الأصدقاء والزملاء

شكر وعرفان

يسرنا أن نتقدم بجزيل الشكر والعرفان

إلى الذي شجعنا ووقف وراء هذا العمل

المتواضع بمجهوداته ونصائحه القيمة التي أنارت

طريقنا

أستاذنا المشرف رعاه الله

"الطيب بن شهرة"

الملخص باللغتين: العربية والإنجليزية

يناقش هذا البحث واحدة من أهم القضايا التي تقلق رجال الفكر القانوني في الوقت الحاضر ألا وهي الجريمة الالكترونية، فاتساع استخدام الحاسوب وما تبعه من استخدام الشبكة الدولية (الانترنت) وما نجم عنه من أنماط جديدة للسلوك الإجرامي لم يكن يتوقعه المشرع في معظم بلدان العالم، الأمر الذي دفع بالدول إلى الوقوف وقفة جادة لمعالجة هذه المشكلة .

وللوقوف على أهمية هذه المشكلة وأبعادها القانونية والدينية والاجتماعية فقد جاء هذا البحث في فصلين، وفي كل فصل مبحثين، حيث حاولنا في الفصل الأول أن نبين الطبيعة الخاصة للجريمة الإلكترونية تمييزا لها عن غيرها من الجرائم، وذلك من خلال التطرق لماهيتها والأحكام العامة لها .

وخصصنا الفصل الثاني للجانب العملي لهذه الدراسة من خلال معرفة الإجراءات المتبعة لمكافحة الجريمة الإلكترونية، من خلال التطرق لأساليب وطرق مكافحتها ومعرفة الجهود الوطنية والإقليمية والدولية المبذولة للتصدي لهذه الجريمة، وفي الأخير تلتها خاتمة بجملة من النتائج والتوصيات

****

This research discuss on of the Most important matter which worrys the Specialists of legal thought at present time, It is electronic Crime, The expansion of using computers and Internet results new styles of criminal behavior, this push the world countries to treet this problem .

To determine the importance of this problem and its dimensions legal, religious and social came this research in two chapters, and each chapter two sections, where we have tried in the first quarter to show the special nature of e-crime distinguish it from other crimes, through to pin down general provisions have touched.

And we have dedicated the second chapter for the practical aspect of this study through knowledge of procedures to combat cyber crime, through the methods and ways to combat it touched and knowledge of national, regional and international efforts to tackle this crime, and in the latter, followed by a conclusion a set of findings and recommendations.

قائمة المختصرات:

الرمز	المعنى
ص	الصفحة
ج	الجزء
ط	الطبعة
لا.ط	لا يوجد طبعة
لا.م	لا يوجد مكان
لا.ن	لا يوجد ناشر
د.ت	دون تاريخ
هـ	هجري
م	ميلادي

مقدمة

الحمد لله ربِّ العالمين، وبه نستعين، والصلاة والسلام على البعوث رحمةً للعالمين، وعلى آله وصحبه أجمعين، أمّا بعد:

إن الله عزّ وجل خلق الخلق، وأبدع في صنع الكون، وأعد الأرض، واستخلف الإنسان فيها لحكمة وغاية جليلة، وهي عبادته سبحانه ﴿ وَمَا خَلَقْتُ ٱلْجِنَّ وَٱلْإِنسَ إِلَّا لِيَعْبُدُونِ ﴾ [الذاريات:56] فإن الشريعة الإسلامية جاءت كاملة شاملة، صالحة لكل زمان ومكان محققة لسعادة البشرية في الآجل والعاجل، فهي من عند الله "سبحانه وتعالى" للناس كافة، بما يصلح حال دنياهم وأخراهم، قال الله تعالى : ﴿ مَّا فَرَّطْنَا فِي ٱلْكِتَٰبِ مِن شَيْءٍ ﴾ [الأنعام:38]، ومنحهم من الحريات في شتى ميادين الحياة وتعلم كافة العلوم وممارسة ماشاءوا من الأنشطة وجعل ذلك مرهونا بعدم الضرر أو الأضرار، لقول النبي صل الله عليه وسلم: «لاَ ضَرَرَ ولاَ ضِرَار» [1].

من هذا المنطلق لم يكن الإسلام ليقف في وجه التطور بجميع أشكاله، وفي كل الميادين بشتى مجالاتها، شريطة أن يحاط بسياج الشرع، وإلا سيعود بالضرر على الفرد والمجتمع، وخير مثال على ذلك التطور الحاصل في تكنولوجيا الإعلام والاتصال وظهور المواقع والشبكات تتحكم بمشاعر وأهواء وعواطف الكثير من مستخدميها وروادها ومدمنيها، وباتت تساهم أيضاً في تشكيل وعي وآراء ومواقف الكثير من الناس، وحتى في اتخاذ قراراتهم في كثير من المجالات، هذا وما حملته هذه التكنولوجيا من تقدم وخدمات، إلا أنّه لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول بأسرها، وهكذا ظهر إلى الوجود ما يعرف بالجرائم الإلكترونية.

حيث تطورت هذه الجريمة بشكل رهيب في المدة الأخيرة، وذلك بالنظر إلى التطور المستمر والمتسارع لشبكة الإنترنت، مما جعل هذه الشبكة وسيلة مثالية لتنفيذ العديد من هذه الجرائم بعيدا عن أعين الجهات الأمنية، وهو ما دفع العديد من الدول والهيئات والمنظمات إلى التحذير من خطورة هذه الظاهرة الحديثة في مجال الإجرام والتي تهدد الفرد والجماعات على حد سواء.

[1] – أخرجه ابن ماجه في سننه،كتاب الأحكام، باب من بنى في حقهما يضر جاره، رقم الحديث 2340، 784/2

وسعت المجتمعات جاهدةً إلى الحد من الجريمة الإلكترونية وذلك لما تشكله هذه الظاهرة من إشكالات قانونية واقتصادية واجتماعية معقدة، فكما واكبت المجتمعات تطور الجريمة التقليدية بالتصدي لها وردعها عن طريق سن القوانين والتشريعات، دَأبت كذلك على فعل نفس الشيء مع الجريمة الإلكترونية، وذلك بالتطرق إليها بالدراسة والتحليل من أجل وضعها في إطار قانوني يمكن من خلاله وضع الطرق السليمة لمكافحتها .

أهمية الموضوع :

أن التطوّر وتسارع إيقاع التقدم التكنولوجي والتقني الهائل وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالإنترنت وصور التواصل الإلكتروني عبر الأقمار الصناعية، فبالرغم من إيجابياته المتعددة إلا أنه يتستر في داخله على مخاطر تفوق كافة التصورات في تهديده للأمن النفسي والأخلاقي والاقتصادي، ويكفى أن نعرف أنه بلمسة واحدة يمكن لشخص أو مجموعة أشخاص "مرتكبو الجرائم الإلكترونية" أن يكبّدوا بعض المؤسسات أو الشركات الكبرى خسائر مالية كبيره أو يهددوا أمن واستقرار المجتمع، كما أن عمليات التعارف على شبكة المعلومات الدولية أدت إلى حدوث جرائم مثل جرائم خطف الأشخاص والطلاق والسرقة والاغتصاب والتهديد والقذف وتشويه السمعة وغيرها من الجرائم التي وقعت في مختلف بلدان العالم ومن بينها الجزائر، وهنا تكمن أهمية الدراسة لهذا الموضوع من أجل الوصول إلى حلول ناجعة لمواجهتها.

إشكالية الموضوع :

وفي مشروعنا سنحاول التعرف على أحكام مكافحة الجريمة الالكترونية في ظل التشريع الإسلامي والقانون بالإجابة على الإشكالية الآتية: ما هي طبيعة الجريمة الإلكترونية؟ وما هو التكييف الشرعي والقانوني لها؟ و ما هي الإجراءات المتبعة في مكافحتها؟ وما مدى نجاعة هذه الإجراءات في حماية مصالح الدول والأفراد؟

أسباب اختيار الموضوع :

السبب الذاتي في اختيار هذا الموضوع، هو الرغبة في الوقوف على حقيقة الجرائم الإلكترونية ومعرفة الجانب الإجرائي في التعامل مع هذا النوع من الجرائم، وأيضا للوقاية من هذه الجرائم.

أما الأسباب الموضوعية فتتمثل في:

– حداثة الموضوع، ومدى مساسه بالواقع وامتداد خطره؛ مما يستدعي ضرورة المعالجة الشرعية السريعة والفورية.

– التفشي غير السوي لوسائل الاتصال والتي تعد خطرا على المجتمع في ظل عدم وجود آليات واضحة لمراقبة مثل هذه الجرائم.

– الانتشار المخيف للجريمة الالكترونية وقصر مسايرة القوانين للتطور التكنولوجي.

أهداف اختيار الموضوع :

– محاولة الكشف عن الأحكام المتعلقة بالجريمة الالكترونية من خلال التشريع الإسلامي والقانوني في ظل تطور الجريمة.

– معرفة ما مدى تحقيق الإجراءات المتبعة لأهدافها المسطرة في مكافحة الجريمة الالكترونية.

– معرفة مدى مسايرة الأحكام للتطورات المسارعة للجريمة الالكترونية.

– التعرف عل طرق الوقاية من هذه الجرائم من خلال الكشف على أصنافها وأساليب ارتكابها.

الدراسات السابقة:

– الجريمة المرتكبة عبر الانترنت"صغير يوسف": مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية، جامعة مولود معمري –تيزي وزو، 2013.

– جرائم الحاسب الآلي في الفقه الإسلامي "عبير علي محمد النجار": مذكرة لنيل شهادة الماجستير في الفقه المقارن، كلية الشريعة والقانون، الجامعة الإسلامية – غزة، 2009.

- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت. (رسالة ماجستير في تخصص القانون العام)، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011.

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير في العلوم القانونية تخصص علوم جنائية)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2013/2012.

منهجية البحث :

اعتمدنا في هذا البحث على الأسلوب الاستقرائي التحليلي في جمع وتحليل الحقائق المتعلقة بموضوع البحث، والمنهج المقارن في الموازنة بين أحكام التشريع الإسلامي والقانوني،كما استخدمنا الأسلوب الإحصائي لتحديد حجم الجريمة الالكترونية في ضوء ما هو متاح بين أيدينا من إحصائيات في الجزائر وأخرى عالمية من منظمات ودوريات علمية نشرت تقاريرها ومن مباحث مختلفة في ذلك .

خطة البحث :

للإجابة على الإشكالية السابقة والوقوف على أهمية هذه المشكلة وأبعادها الدينية والقانونية والاجتماعية، فقد جاء البحث في فصلين، وكل فصل يحتوي على مبحثين، وفي كل مبحث ثلاثة مطالب، ومحتوى الخطة كالتالي:

الفصل الأول: الطبيعة الخاصة للجريمة الإلكترونية

المبحث الأول: ماهية الجريمة الإلكترونية

المطلب الأول: مفهوم الجريمة الإلكترونية

المطلب الثاني: تصنيف الجريمة الإلكترونية

المطلب الثالث: خصائص الجريمة الإلكترونية والقطاعات التي تستهدفها

المبحث الثاني: الأحكام العامة الجريمة الإلكترونية

المطلب الأول: أركان الجريمة الإلكترونية

المطلب الثاني: أساليب ودوافع ارتكاب الجريمة الإلكترونية

المطلب الثالث: موقف الشريعة الإسلامية والمشرع الجزائري من الجريمة الإلكترونية

الفصل الثاني: الإجراءات المتبعة لمكافحة الجريمة الإلكترونية

المبحث الأول: أساليب و طرق مكافحة الجريمة الإلكترونية

المطلب الأول: عقوبات الجريمة الإلكترونية بمنظور الشريعة الإسلامية والقانون

المطلب الثاني: إثبات الجرائم الإلكترونية

المطلب الثالث: موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجزائي

المبحث الثاني: مواجهة الجريمة الإلكترونية والحماية الموفرة لها

المطلب الأول: وسائل الحماية لتفادي الجريمة الإلكترونية

المطلب الثاني: المواجهة التشريعية للجريمة الإلكترونية

المطلب الثالث: التحدّيات التي تواجه الجريمة الإلكترونية

الفصل الأول

الطبيعة الخاصة للجريمة الالكترونية

إنّ الجريمة الالكترونية باعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية بخصوص تحديد ماهيتها والأفعال الإجرامية التي تدخل في نطاقها، ولذلك ارتأينا التعرض لماهية الجريمة الإلكترونية وتصنيفها ومعرفة خصائصها والقطاعات التي تستهدفها في المبحث الأول، و دراسة هذا الفعل الإجرامي من ناحية أساليب ودوافع ارتكابه، وموقف الشريعة الإسلامية والمشرِّع الجزائري منه في المبحث الثاني .

المبحث الأول

ماهية الجريمة الالكترونية

تعتبر الجريمة الإلكترونية من الآثار السلبية التي خلّفتها التقنية العالية حيث أخذت هذه الظاهرة حيزا كبيرا من الدراسة من أجل تحديد مفهومها، مما انجر عنه وضع عدّة مصطلحات للدلالة عليها، من بينها جرائم الحاسب، جرائم التقنية العالية، الجرائم المعلوماتية[1] وهناك من يطلق عليها الجرائم المستحدثة[2] .

ومن الصعوبة الواردة على مصطلحها، استوجب وضع مفهوم موحد لها في المطلب الأول ومعرفة أصناف هذه الجرائم في المطلب الثاني، وخصائصها و القطاعات التي تستهدفها في المطلب الثالث .

المطلب الأول

مفهوم الجريمة الالكترونية

تعرَّف الجرائم الإلكترونية بصفة عامة بأنها: جميع الأفعال الإجرامية المرتكبة بواسطة الحاسب الآلي من خلال شبكة الانترنت[3]، وسنحدد مفهومها من خلال تعريف الجريمة في الشريعة والقانون في الفرع الأول وتعريف الجريمة الإلكترونية في الفرع الثاني .

[1] صغير يوسف، الجريمة المرتكبة عبر الإنترنت. (رسالة ماجستير في تخصص القانون الدولي للأعمال) كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص7.

[2] عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية". الكوفة–العراق، العدد:7، 2008، ص112.

[3] علي جبار الحسيناوي، جرائم الحاسوب والإنترنت. (ط:1؛ الأردن: دار اليازوري العلمية، 2009)، ص46.

الفرع الأول

تعريف الجريمة في الشريعة والقانون

أولا: تعريف الجريمة لغة وشرعا

1- تعريف الجريمة لغة :

الجريمة في اللغة بمعنى الجُرْم: أي الذنب، ونقول منه: جَرَمَ وأَجْرمَ واجْتَرَمَ كلها بمعنى واحد[1] .

2- تعريف الجريمة في الشرع :

لفظ الجريمة من الألفاظ التي استعملها الفقهاء كوصف لبعض الحدود كأن يقولوا: جريمة الزنا؛ جريمة الحرابة، وكثيرا ما يعبر الفقهاء عن الجريمة بلفظ الجناية [2] ، ونشير إلى أن الفقهاء المسلمين قد درسوا الجريمة قديما و قدموا لها تعريفا مغايرا لما هي عليه التعريفات الحديثة لها، وسنتناول تعريفها كالتالي :

أ/ تعريف الجريمة عند القدماء :

لم يكن هناك اختلاف كبير في تعريف الجريمة بين المذاهب الأربعة، وقد عرفها الماوردي بأنها "محظورات شرعية زجر الله عنها بحد أو تعزير"[3]

شرح التعريف

المحظورات : لفظ عام يشمل جميع أنواع الممنوعات، سواء كانت شرعية أم عرفية

الشرعية : خرج بها كل نهي من غير المشرع .

زجر الله عنها : الزواجر تشمل المحرمات والمكرهات .

---

[1] إسماعيل بن حماد الجوهري، الصحاح. تحقيق: أحمد عبد الغفور عطار، ج5(ط:4؛ بيروت: دار العلم للملايين، 1990) ص1885.

[2] عبد القادر عوده، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي.ج1(لا.ط؛ بيروت: دار الكاتب العربي، د.ت) ص67

[3] علي بن محمد الماوردي، الأحكام السلطانية.(ط:1؛ الكويت: مكتبة دار ابن قتيبة، 1989)، ص285.

الحد : العقوبة المقدرة في الشرع لأجل حق لله تعالى[1] .

التعزير : هو العقوبات التي لم يرد نص من الشارع ببيان مقدارها، وترك تقديرها لولي الأمر[2] .

ب/ تعريف الجريمة عند المحدثين :

" إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم الترك معاقب على تركه أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه"[3] .

شرح التعريف

إتيان فعل محرم والحرام : هو ما طلب الشارع الكف عنه على وجه الحتم والإلزام، فيكون تاركا مأجورا مطيعا، وفاعله آثما عاصيا .

أو ترك فعل محرم الترك : كترك الواجبات، كالصلاة والصيام .

نصت الشريعة على تحريمه : بالكتاب أو بالسنة، وما يلحق بهما، بما فيها من أدلة تصرح بالتحريم، أو تنذر بالتهديد والوعيد[4] .

ثانيا: تعريف الجريمة في القانون :

المفهوم القانوني للجريمة هو "**الفعل الذي يجرمه القانون ويقرر له جزاءا جنائيا**" أو هي "**فعل أو امتناع يخالف قاعدة جنائية تحظر السلوك المكون لها وترتب لمن يقع منه جزاءا جنائيا**" ويترتب على هذا المفهوم أن وصف الجريمة محصور في نصوص قانون العقوبات، فكل سلوك يخالف ما ورد فيه فهو جريمة وكل فعل خارج عن إطاره فلا يعد كذلك حتى ولو خالف المبادئ الأخلاقية

[1] بكر بن عبد الله أبو زيد، الحدود والتعزيرات عند ابن القيم.(ط:2؛ المملكة العربية السعودية: دار العاصمة، 1994) ص347.

[2] محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي. (لا.ط؛ القاهرة: دار الفكر العربي، د.ت) ، ص29.

[3] عبد القادر عودة، التشريع الجنائي الإسلامي، مرجع سابق، ص66.

[4] عبير علي محمد النجار، جرائم الحاسب الآلي في الفقه الإسلامي. (رسالة ماجستير في تخصص الفقه المقارن)، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2009، ص5.

والقيم الاجتماعية[1]، ويفضي هذا التعريف إلى القاعدة الشهيرة (لا جريمة ولا عقوبة أو تدابير أمن بغير قانون)[2]

الفرع الثاني

تعريف الجريمة الإلكترونية

قبل الخوض في تعريف الجريمة الإلكترونية لا بد من الوقوف على بيان معنى المصطلح الثاني في هذه الدراسة ألا وهي "الإلكترونية" أو "المعلوماتية" ، فيقصد بها المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي Informatique، وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر[3] ، ونأتي على تعريف الجريمة الإلكترونية كالآتي:

أولا: تعريف الجريمة الإلكترونية في الفقه القانوني

أدت الحداثة التي تتميز بها الجريمة الالكترونية، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق، ولذلك قد انقسم الفقه إلى أربعة اتجاهات تقوم على أسس مختلفة في تعريف الجريمة الإلكترونية وهي كالآتي :

1- على أساس وسيلة ارتكاب الجريمة

عرفها الفقيه الألماني تاديمان بأنها :

"هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي"[4] .

---

[1] منصور رحماني، الوجيز في القانون الجنائي العام. (لا.ط؛ عنابة: دار العلوم للنشر والتوزيع، 2006)، ص83.

[2] المادة (01) من القانون رقم 66-156 المؤرخ في 18 صفر 1386هـ الموافق 8 جويلية 1966، والمتضمن: قانون العقوبات، المعدل والمتمم . ج1(المبادئ العامة، أحكام تمهيدية).

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية. (ط:1؛ الإسكندرية: دار الفكر الجامعي، 2009)، ص76.

[4] عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مرجع سابق، ص113.

2- على أساس توافر المعرفة بتقنية المعلومات

عرفتها وزارة العدل في الولايات المتحدة الأمريكية بأنها :

"أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكنه من ارتكابها"

وعرفها أيضا الأستاذ (David Thomson) بأنها :

"أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[1] .

3- على أساس موضوع الجريمة

يرى واضعوا هذا التعريف أن الجريمة الإلكترونية ليست هي التي يكون النظام المعلومات أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه، ومن أشهر فقهاء هذا الاتجاه الفقيه (Rosenblatt) الذي عرفها كالتالي :

"نشاط غير مشروع موجه لنسخ، أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسوب، أو التي تحول عن طريقه"[2]

4- اتجاه يأخذ بدمج عدة تعاريف

عمد أصحاب هذا الاتجاه إلى تعريف الجريمة الإلكترونية عن طريق دمج أكثر من تعريف وعرفوها كالتالي :

"الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها" .

[1] جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية. (ط:1؛ عمان – الأردن: دار الثقافة، 2010)، ص68.

[2] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص12- 13.

ثانيا: تعريف الجريمة الإلكترونية من الناحية الشرعية

عرّفها الباحث في جرائم الإنترنت "محمد عبد الله منشاوي" بأنها : جميع الأفعال المخالفة للشريعة الإسلامية، المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسية والممارسات الغير أخلاقية، جرائم الاختراقات، الجرائم المالية، جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة [1] .

وعَرَّف نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم 17 وتاريخ: 1428/3/8هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 1428/3/7هـ الجريمة المعلوماتية بأنها: " أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام "[2] .

مما سبق لا بد من الإشارة إلى وجود ندرة في تعريف الجرائم الإلكترونية من الناحية الشرعية؛ ويرجع السبب في ذلك لكون هذه الجرائم لم تظهر إلا عقب التطورات التكنولوجية في الحاسب الآلي، والتي وصلت مؤخرا للدول الإسلامية، بعد أن بُحثت في دول انتشارها الأولى .

وعليه وبعد العرض لمجموعة كبيرة ومختلفة من التعريفات للجرائم الإلكترونية، يتبين لنا أن موضوع الجريمة الإلكترونية هو "المال المعلوماتي" تمييزا لماليته المغايرة المال التقليدي والمقصود بالمال المعلوماتي الحاسب بكل مكوناته، والحاسب اصطلاحا لا يخرج عن كونه آلة الكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة [3].

[1] محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني. (**mohammed@minshawi.com**).

[2] إدارة الدراسات والبحوث بالمملكة العربية السعودية، "دراسة بعنوان دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"، 2012، ص5.

[3] أمال قارة، الجريمة المعلوماتية. (رسالة ماجستير في تخصص القانون الجنائي والعلوم الجنائية)، كلية الحقوق، جامعة الجزائر، بن عكنون، 2002/2001، ص21.

المطلب الثاني

تصنيف الجرائم الإلكترونية

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الإلكترونية، وذلك راجع إلى تشعب هذه الجرائم وسرعة تطورها، فمنهم من يصنفها عل أساس وسيلة ارتاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، وسنصنفها في هذا المطلب بالاعتماد على المعايير السابقة إلى: جرائم واقعة على الأشخاص في الفرع الأول، وجرائم واقعة على الأموال في الفرع الثاني، وجرائم واقعة على أمن الدول في الفرع الثالث.

الفرع الأول

جرائم واقعة على الأشخاص

تعد سلامة الأشخاص الهدف الأسمى لوضع القوانين وسن التشريعات، وذلك لحمايتهم من مختلف الانتهاكات التي قد يتعرضون لها، وفي وقتنا الراهن أصبحت الإنترنت تستعمل لهذا الغرض وذلك بالتعدي على الحياة الخاصة للأفراد، ومن أهم صور هذه الاعتداءات: صناعة ونشر الإباحة جرائم القذف والسب، إنتحال الشخصية والتغرير والاستدراج، وسنأتي على ذكرها بالتفصيل كالتالي:

أولا: صناعة ونشر الإباحة

لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحة الجنسية، فقد جعلت شبكة الإنترنت الإباحة بشتى وسائل عرضها من صور وفيديو ومواقع دردشة في متناول الجميع ويعتبر ذلك من أكبر سلبيات الإنترنت[1] حيث عرفت سنوات التسعينيات انفجارا في إنشاء المواقع الإلكترونية المخلة بالحياء وكانت البداية لهذا النوع من الإجرام، فقد قامت بعض الشركات بدراسة عدد الزوار لصفحات الدعارة والإباحية على شبكة الإنترنت، ووجدت أن بعض هذه الصفحات الإباحية يزورها قرابة (380034) زائر في اليوم الواحد، وهناك أكثر من مائة صفحة مشابهة تستقبل أكثر من (20000) زائر يوميا، وإن صفحة واحدة تزعم أن لديها أكثر من

[1] منير محمد الجنيبهي، جرائم الإنترنت والحاسب الآلي. (لا.ط؛ الإسكندرية: دار الفكر الجامعي، 2005)، ص29.

(300000) صورة خليعة تم توزيعها أكثر من مليار مرة، كما بلغ مجموع الأموال المنفقة على الصفحات الإباحية ثلاثة مليار دولار في عام 2003[1] .

ثانيا: جرائم القذف والسب

تعد جرائم القذف والسب من الجرائم الأكثر شيوعا وانتشارا والتي لها الأثر البالغ سلبا على شخص الإنسان، وتكون بالنيل من شرف الغير وكرامته أو اعتباره، أو تعرضه إلى بعض الناس واحتقارهم بما يتم إرساله للمجني عليه على شكل "رسالة بيانات" عبر شبكة الإنترنت[2] .

ومن جهة أخرى قد يكون بعض الفئات العادية من المجتمع عرضة لهذه الجرائم، ومثال ذلك ما حدث في مصر، بأن قام شاب يعمل في شركة بالجيزة بتصميم موقع إباحي على الإنترنت وبريد إلكتروني باسم زميلته في الشركة، وبدأ بإرسال صور وكلام مخل لجميع زملاءهم في العمل، وعلمت زميلته بالحادث فتقدمت بشكوى للجهات الأمنية، وتم كشف مصدر الرسائل التي تبين أنها من ألمانيا في حين وجود الجهاز المرسل لهذا البريد المزعج في المبنى المقابل من خلال استغلال "سيرفر" الشركة الألمانية[3] .

ثالثا: انتحال الشخصية والتغرير والاستدراج

تبدأ عملية انتحال الشخصية عبر الإنترنت عندما يستغل اللصوص بيانات شخص ما على الشبكة الإلكترونية أسوأ استغلال، وذلك بغرض استخراج بطاقات ائتمانية، أو الاستيلاء على بعض ممتلكاته أو كلها إن أمكن، وكذلك الاستفادة من سمعته إذا كان مسئول أو صاحب وجاهة[4] .

---

[1] محمد سعيد عبد المجيد، المعلوماتية والجريمة. (ط:1؛ مصر: دار ومكتبة الإسراء، 2006)، ص21.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية. (ط:1؛ مصر: دار الفكر الجامعي، 2010)، ص319.

[3] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات. (لا.ط؛ الجماهرية الليبية: دار البداية، 2006)، ص197.

[4] منير محمد الجنيبهي، جرائم الإنترنت والحاسب الآلي، مرجع سابق، ص43.

أما فيما يخص التغرير والاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة عل الإنترنت والتي تتطور فيما بعد إلى التقاء مادي بين الطرفين[1] .

الفرع الثاني

جرائم واقعة على الأموال

واكب ظهور شبكة الإنترنت تطورات كبيرة في المعاملات التجارية التي تتم خلا هذه الشبكة؛ وفي خضم هذا التطور في التداول المالي عبر الإنترنت، انتهز بعض المجرمين الفرصة للسطو على هذا المجال، ومن أبرز جرائمهم: جرائم السطو على أرقام بطاقات الائتمان، التحويل الإلكتروني غير المشروع للأموال، القمار وغسيل الأموال عبر الإنترنت، وسنأتي على ذكرها بالتفصيل كالآتي:

أولا: جرائم السطو على أرقام بطاقات الائتمان

البطاقات الائتمانية تعد نقودا إلكترونية والاستيلاء عليها يعد استيلاء على مال الغير، ونظرا لسهولة الاستيلاء على تلك الأرقام فقد تزايدت حوادث الاستيلاء عليها وأيضا تزايدت عمليات الابتزاز المصاحبة لارتكاب مثل تلك الجرائم[2] .

وأصبحت هذه الجرائم تشكل خطرا كبيرا على التجارة الإلكترونية، ويتم التلاعب فيها عن طريق الإنترنت، ويأخذ هذا التلاعب صورا عديدة منها :

1- لحصول على بطاقة ائتمانية صحيحة بناء على مستندات مزورة .

2- قيام حامل البطاقة باستعمالها بعد انتهاء مدة صلاحيتها أو بعد تنبيه البنك عليه بعدم استخدام البطاقة .

[1] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص51

[2] منير محمد الجنيبهي، جرائم الإنترنت والحاسب الآلي، مرجع سابق، ص85

3- وقد يتلاعب موظف البنك ذاته ببيانات البطاقة بالاتفاق مع العميل حامل هذه البطاقة، أو مع العصابات الإجرامية التي تتعامل في سرقة الأموال من البنوك عبر الإنترنت[1] .

ثانيا: التحويل الإلكتروني غير المشروع للأموال

اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية المخزنة في ذاكرة الحاسب الآلي، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان في العالم، وتكمن خطورة الأمر في إمكانية تلاعب الجاني في هذه البيانات المختزنة في ذاكرة الحاسب الآلي أو في برامجه وإجراء تحويلات في كل أو بعض أرصدة الغير و فوائدها وإدخالها في حسابه[2] .

تتم عملية التحويل الإلكتروني غير المشروع للأموال من خلال طريقتين :

1- الاحتيال بإيهام المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني .

2- الاحتيال باستخدام بطاقات الدفع الإلكتروني عن طريق عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة، إلى رصيد التاجر أو الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية "الفيزا كارد" و "الماستر كارد"[3] .

ثالثا: القمار وغسيل الأموال عبر الإنترنت

غسيل الأموال يعني من ابسط صوره "تحويل المصدر غير المشروع للأموال إلى مصدر مشروع" فمثلا تحويل الأموال الناتجة عن عمليات غير مشروعة كتجارة المخدرات إلى أموال مصدرها مشروع كتجارة السيارات مثلا، ولهذا كانت جرائم غسيل الأموال قريبة من اسمها، إذ يتوسل الجاني بسلوكيات معينة إلى تحويل صفة المال الموجود بين يديه من مال غير مشروع، وهو إذا يسعى إلى ذلك فإنه يعمد إلى إيجاد سبب قانوني كافٍ ومنطقي لما بين يديه من أموال[4]

[1] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، مرجع سابق، ص193

[2] أمين الشوابكة، جرائم الحاسوب والإنترنت، (ط:1؛ عمان – الأردن: دار الثقافة، 2007)، ص178

[3] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص45

[4] جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، مرجع سابق، ص168

وتعد هذه الجريمة من الجرائم المعاصرة، وهي صورة من صور الجريمة المنظمة، ولقد استخدمت تكنولوجيا المعلومات الحديثة بوصفها واحدة من الأساليب الجديدة في غسيل الأموال، وتتمثل هذه الصورة السلبية لاستخدام الإنترنت عن طريق تحويل الأموال أو توظيفها والتعامل مع البنوك عبر الإنترنت أو إجراء عمليات معقدة من التحويلات النقدية من حساب لآخر لإخفاء الصفة غير المشروعة لمصدر الأموال[1] .

الفرع الثالث

جرائم واقعة على أمن الدول

أتاحت الإنترنت لكثير من الجماعات المتطرفة مجالاً لزرع معتقداتها وأفكارها الفاسدة، وذلك من خلال ارتكاب مجموعة من الجرائم والممارسات غاية في الفتك في حق المجتمعات والدول، وتبرز أهم هذه الجرائم: في جرائم الإرهاب والتجسس وكذا الجرائم الماسة بالأمن الفكري، وبيانها كالآتي:

أولا: الإرهاب الإلكتروني

أصدر مجمع الفقه الإسلامي الدولي قرارًا في دورته الرابعة عشرة المعقودة في الدوحة في شهر ذي القعدة من عام 1423هـ ذكر فيه تعريف مصطلح الإرهاب بأنه : العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض[2] .

تبرز أهم صور الإرهاب الإلكتروني في اقتحام المواقع وتدميرها وتغيير محتوياتها أو الاستيلاء عليها، أو الدخول على شبكات الطاقة أو شبكات الاتصال بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا، أو عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية، حيث تجنِّد

[1] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، مرجع سابق، ص205.

[2] عبد الرحمان بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها. (لا.ط؛ لا.م، لا.ن، د.ت)، ص5.

عناصر إرهابية من خلالها، وتعبر من خلالها عن مسؤوليتها عن إحدى الهجمات التي ارتكبت أو تنفيها، وكذلك تستغل هذه الجماعات المواقع الإلكترونية للدعاية والترويج لنفسها، وكذلك شن حرب نفسية ضد أعدائها من خلال نشر معلومات مظلّلة أو مغلوطة، ونشر تهديدات وصور ولقطات فيديو مرعبة[1] .

ثانيا: جرائم التجسس

يتم التجسس من خلال الإطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر، وسهلت شبكة الإنترنت الأعمال التجسسية بشكل كبير، حيث يتمكن العديد من الجواسيس اختراق العديد من أجهزة الحاسب والشبكات المؤمنة الخاصة بالدول والشركات والأفراد دون أن يغادروا أماكن وجودهم .

وقد يكون التجسس عسكريا، وذلك بمحاولة فهم الأسرار العسكرية، أو صناعيا، أو تجاريا، والغاية من ذلك كله الإضرار بمصالح المؤسسات والحكومات والمجتمعات، وهو إضرار بمصالح الدول[2] .

ثالثا: الجرائم الماسة بالأمن الفكري

بناءً على خصائص الشبكة العالمية للإنترنت، التي منحت المستخدم الكثير من الخيارات، من خلال عدم خضوعها لأي رقابة، وعبورها للحدود الجغرافية بين الدول، أصبحنا نرى توالي الهجمات الثقافية والحضارية التي تمس فكر وعقيدة الشعوب العربية والإسلامية المغلوب على أمرها، وتنشر عبرها القوى الغالبة فكرها ولغتها وقيمها .

وقد ظهر في أدبيات بعض الباحثين منذ بداية الانتشار للغزو الإلكتروني، إشارات تحذير من الغزو الفكري المركز الذي تستقبله الأجيال العربية المسلمة مما قد يجعله عرضة للهزيمة الفكرية[3] .

---

[1] أنظر: منير محمد الجنيبهي، جرائم الإنترنت والحاسب الآلي، مرجع سابق، ص111، صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص55.

[2] محمد عبد الرحمان، جرائم الإنترنت والاحتساب عليها. بحوث مؤتمر القانون والكمبيوتر والإنترنت (من 1 – 3 ماي 2000)، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد: 3، 2004، ص880.

[3] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص57-58-59.

المطلب الثالث

خصائص الجريمة الإلكترونية والقطاعات التي تستهدفها

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة، التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي، ولذلك فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل، وسنبين هذه الخصائص في الفرع الأول ونبين كذلك القطاعات التي تستهدفها هذه الجرائم في الفرع الثاني .

الفرع الأول

خصائص الجريمة الإلكترونية

تتسم الجرائم بالعديد من السمات والصفات المختلفة التي تؤدي إلى الكشف عن مرتكبيها، إلا أن الجرائم المرتكبة عبر شبكة الإنترنت تتصف بخصائص وسمات قد لا توجد في الجرائم العادية، وأهم تلك الخصائص: أنها عابرة للحدود، وصعبة الإثبات، قلة الإبلاغ عن وقوع هذه الجرائم، وغيرها من الخصائص التي سنأتي على ذكرها بالتفصيل كالتالي:

أولا: الجريمة الإلكترونية جريمة عابرة للحدود

الجريمة المعلوماتية تتسم غالبا بالطابع الدولي، ذلك لأن الطابع العالمي لشبكة الإنترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط (On laine) يسهل ارتكاب الجريمة من دولة إلى أخرى[1] .

وفي مجتمع الإنترنت تذوب الحدود الجغرافية بين الدول لارتباط العالم بشبكة واحدة، ومن الملاحظ أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت يكون الجاني في دولة، والمجني عليه في دولة أخرى، ومن ذلك على سبيل المثال اختراق أنظمة الحواسب الآلية من خارج إقليم دولة المجني عليه[2].

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية. (ط:1؛ الإسكندرية: دار الفكر الجامعي، 2009)، ص77.

[2] محمد عبد الرحمان، جرائم الإنترنت والاحتساب عليها، مرجع سابق، ص876.

ثانيا: صعوبة إثبات الجريمة الإلكترونية

تكون البيانات والمعلومات المتداولة عبر شبكة الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تُقرأ إلاّ بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه للجاني يبدو أمرا صعبا لا سِيّما وأن الجاني يتعمد إلى عدم ترك أثر لجريمته، ضِف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة [1].

ثالثا: قلة الإبلاغ عن وقوع الجريمة الإلكترونية

لا يتم في الغالب العام الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أن معظم جرائم الإنترنت تم اكتشافها بالمصادفة[2] .

رابعا: وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات

من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية .

والجريمة المعلوماتية قد تقع أثناء عملية المعالة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات .

خامسا: عدم كفاية التعاون الدولي في مجال الجرائم الإلكترونية

ويتمثل ذلك في عدم وجود معاهدات دولية كافية للتسليم أو للمعاينة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة لجرائم

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت. (رسالة ماجستير في تخصص القانون العام)، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011، ص45.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص86.

الكمبيوتر وديناميكية التحريات فيها وكفالة السرعة بها، وهذا راجع إلى وجود عدة عقبات تقف في سبيل هذا التعاون ولعلّ أبرزها:

– عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات الواجب تجريمها.

– اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.

– عدم التناسق بين قوانين الإجراءات الجزائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية [1] .

سادسا: خصوصية مجرمي المعلوماتية

يتمتع نشطاء الجريمة على الإنترنت بصفات وخصائص تميزهم عن غيرهم، ولهذا التميز انعكاس حتمي على الجريمة الإلكترونية . وهؤلاء المجرمون يمكن تصنيفهم إلى الفئات التالية :

1– القراصنة Les pirates، هناك صنفان من القراصنة :

الصنف الأول – الهواة Hackers : هم أشخاص لهم قدرة فائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج وتدابير الحماية المتخذة، إلا أنهم لايقومون بأي أعمال تخريبية، هدفهم التسلية فقط .

الصنف الثاني – المحترفون Crackers : وهم أكثر خطورة من الصنف الأول ويطلق عليهم المخربين، لهم قدرة فائقة على الاختراق، وهدفهم العبث بالبيانات والمعلومات المخزنة في الحواسيب والشبكات[2].

[1] هشام محمد فريد رستم، "الجرائم المعلوماتية، أصول التحقيق الجنائي الفني" بحوث مؤتمر القانون والكمبيوتر والإنترنت من 1-3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد:2، 2004، ص440

[2] ممدوح محمد الجنيبهي، أمن المعلومات الإليكترونية. (لا.ط؛ الإسكندرية: دار الفكر الجامعي، 2005)، ص28

2- المخادعون Fraudeurs

وهؤلاء يتمتعون بقدرات فنية عالية باعتبارهم من الأخصائيين في المعلوماتية ومن أصحاب الكفاءات، وتنصب معظم جرائمهم على شبكات تحويل الأموال ويمكنهم التلاعب بحسابات المصارف أو فواتير الكهرباء والهاتف أو تزوير بطاقات الاعتماد أو ما شابه ذلك ...الخ .

3- الجواسيس Espions

يهدف هؤلاء إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها[1]

الفرع الثاني

القطاعات التي تستهدفها الجريمة الإلكترونية

دخلت مختلف القطاعات إلى عالم المعلوماتية خاصة بعد ظهور الإنترنت، نظرا للخدمات الكبيرة التي تقدمها، وخاصة باعتبارها تضمن السرعة وتقليص الوقت والتكاليف، إلا أنه بالمقابل أصبحت عرضة لكي تكون ضحية من ضحايا الجريمة الإلكترونية، ونذكر من بين هذه القطاعات، القطاع المالي والمؤسسات العسكرية إلى جانب الأشخاص الطبيعيين والوسطاء .

أولا: المؤسسات المالية والجهات الحكومية

ينجذب مرتكبو الجرائم المعلوماتية إلى القطاعات المالية مثل البنوك والمؤسسات المالية لتنفيذ أفعالهم الإجرامية، فهي من أكثر الأماكن استهدافا نظرا لما لها من أموال، ومن أهم هذه المؤسسات المالية البورصة وذلك أن أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بين الأشخاص العاديين بل قد يصل الأمر إلى التعاملات المالية بين الدول .

وقد تعدت حدود الجرائم المعلوماتية القطاعات المدنية إلى المساس بصورة أكبر إلى القطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات وهو ما يبرزه

[1] علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، مرجع سابق، ص49

الاهتمام المنصب على الجاسوسية العسكرية وما ستتبعه من ظهور حرب من نوع جديدة وهي الحرب المعلوماتية، تعتمد آلياتها على شبكات الحاسب الآلي في نقل المعلومات فتعاظم دور النظم المعلوماتية في هذا المجال نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أمام القادة لاتخاذ القرار المناسب على أساس أهمية تلك المعلومات، مما جعل الدول تبادر إلى القيام بالتجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها[1].

ثانيا: الأشخاص الطبيعيون

لا يقتصر تصنيف ضحايا جرائم المعلوماتية على القطاعات المالية والهيئات الحكومية والمؤسسات العسكرية فقط، بل يتعدى كذلك إلى الأشخاص الطبيعيين ، وقد بدأ الوعي لخطورة الكمبيوتر على حرمة الحياة الخاصة بالأفراد في الدول الغربية منذ ما يزيد عن الثلاثين سنة، فتعالت صيحات حمات الحياة الخاصة، ومن هذه الجرائم جريمة المعالجة الإسمية للبيانات دون الحصول على ترخيص بذلك من المرجع المختص، ومن هذه الجرائم أيضا جرائم التسجيل والحفظ غير المشروع للبيانات الإسمية لفترة أطول من المدة المقررة في الترخيص[2] ، وخير مثال على ذلك وقوع الكثير من الشعب الأمريكي ضحية لجريمة النصب من قبل أشخاص، مستغلين الحادث الإرهابي الذي حدث في الولايات المتحدة في الحادي عشر من سبتمبر سنة 2001، حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الإنترنت بغرض جمع التبرعات للضحايا، على هذا الأساس قامت الحكومة بتحذير رعاياها من الوقوع ضحايا لتلك العمليات الإجرامية [3].

ثالثا: مقدمي الخدمات الوسيطة في نطاق شبكة الإنترنت

وهم الأشخاص الذين يساعدون على الوصول إلى شبكة الإنترنت فقد يمكن أن يكون الأشخاص الوسطاء ما بين الزبون (العميل)، وما بين شبكة الانترنت ضحايا للجريمة الإلكترونية .

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير في العلوم القانونية تخصص علوم جنائية)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012، ص65-66

[2] وليد العاكوم، "مفهوم وظاهرة الإجرام المعلوماتي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون، المجلد:1، 2004، ص16-17.

[3] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص22-23

وهؤلاء الأشخاص هم :

1- متعهد الوصول : وهو أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل الجمهور المستخدم إلى شبكة الإنترنت وذلك عن طريق عقود اشتراك توصيل الزبون بالمواقع التي يريدها، وهو بذلك يقوم بدور فني بحت ولا علاقة له بالمادة المعلوماتية التي تصل إلى الزبون.

2- متعهد الإيواء l'hébergeur : وهو أي شخص طبيعي أو معنوي يعرض إيواء صفحات الواب على حساباته الخادمة العملاقة وذلك مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للزبون الذي ينشر ما يريد من نصوص أو صور أو تنظيم مؤتمرات أو ينشئ روابط معلوماتية مع المواقع الأخرى .

3- متعهد الخدمات : وهو ناشر الموقع والمسئول عن المعلومات التي تعبر على موقعه إلى الشبكة وهو بذلك صاحب السلطة الحقيقية في مراقبة المعلومات التي يتم بثها، ويقوم متعهد الخدمات بأدوار عديدة فهو ممول للخدمات ومالك للحاسب الخادم فضلا عن دوره في بث المعلومات .

4- ناقل المعلومات : وهو العامل الفني الذي يتولى الربط بين الشبكات بناء على عقد من عقود نقل المعلومات في هيئة حزم من جهاز المستخدم إلى جهاز الحاسب الآلي الرئيسي لمتعهد الوصول ثم نقلها من الحاسب الأخير إلى الحاسبات المرتبطة لمواقع الإنترنت أو بمستخدمي الشبكة[1].

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص66-67.

المبحث الثاني

الأحكام العامة للجريمة الإلكترونية

بعد التطرق لمفهوم الجريمة الإلكترونية نأتي على بيان بعض الأحكام و الجوانب القانونية لهذه الجريمة وذلك من خلال: تحديد أركان الجريمة الإلكترونية في المطلب الأول، ثم معرفة الأساليب والدوافع لارتكاب هذا الجرم في المطلب الثاني، و تحديد موقف الشريعة الإسلامية والمشرع الجزائري من هذه الجرائم في المطلب الثالث .

المطلب الأول

أركان الجريمة الإلكترونية

ركن الجريمة يعني جزء من ماهيتها وبانعدامه تنعدم الجريمة ولا يبقى مبرر للعقاب وهذه الأركان ثلاثة :

– أن يكون هناك نص يحظر الجريمة يعاقب عليها، وهو ما نسميه اليوم في اصطلاحنا القانوني بالركن الشرعي للجريمة، وبيان ذلك في الفرع الأول

– إتيان الفعل المكون للجريمة سواء كان فعلا أو امتناعا، وهذا ما نسميه في اصطلاحنا القانوني بالركن المادي للجريمة، وبيان ذلك في الفرع الثاني .

– أن يكون الجاني مكلفا أي مسئولا عن الجريمة، وهذا ما نسميه اليوم بالركن الأدبي أو المعنوي[1] وبيان ذلك في الفرع الثالث .

[1] عبد القادر عودة، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، مرجع سابق، ص111.

الفرع الأول

الركن الشرعي للجريمة الإلكترونية

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لمواجهة الجريمة المعلوماتية خاصة مع ظهور شبكة "الانترنيت" التي ساهمت بشكل خطير في تفشي الجريمة، وعيا بخطورة الوضع أصدر المجلس الأوروبي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص عقابية خاصة بالجريمة المعلوماتية وقد ترددت العديد من الدول في اختيار التقنية التشريعية المناسبة، فمنها من قام بإدماج نصوص خاصة بالإجرام المعلوماتي في قانون العقوبات التقليدي، ومنها من وضع قانون جنائي مستقل للمعلوماتية يدخل في إطار القانون الجنائي التقني[1] .

تثور في حالة إدماج النصوص الجديدة في قانون العقوبات التقليدي تساؤل مَفادُه : تحت أي طائفة من الجرائم يتم إدماجها ؟

هناك عدة فرضيات وآراء :

– هناك من يقول بإمكانية إدماجها في إطار إحدى الأجزاء التقليدية لقانون العقوبات.

– البعض يفضل إدماجها في إطار جرائم الأموال باعتبار أنه يمكن إسباغ صفة المال على الكيانات المادية والمعنوية للحاسوب.

– البعض الآخر يفضل إدماجها في إطار الجزء الخاص بالجرائم ضد الملكية باعتبار الكيان المادي للحاسوب (عناصر مادية) قابلة للتملك كما أن الكيان المعنوي يدخل في إطار الملكية الفكرية.

– هناك من يرى إضافة جزء آخر خاص بالجرائم المعلوماتية مستقل عن الأجزاء التقليدية باعتبار أن هذه الجرائم تتعلق بقيمة اقتصادية جديدة لها طابع خاص.

[1] أمال قارة، الجريمة المعلوماتية، مرجع سابق، ص37.

الفرع الثاني

الركن المادي للجريمة الإلكترونية

تتمثل القواعد العامة في الركن المادي للجريمة في :

1- السلوك الإجرامي : وهو فعل الجاني الذي يحدث آثارا في العالم الخارجي وهو نوعان؛ سلوك ايجابي يكون في صورة فعل أو قول يجرمه القانون يصدر عن الجاني ويؤدي إلى إحداث نتيجة، وسلوك سلبي يتمثل في امتناع الجاني عن قول أو فعل أوجبه عليه القانون .

2- النتيجة : ويقصد بها الأثر المترتب عن السلوك الإجرامي سواء كان ماديا أو نفسيا.

3- الرابطة السببية بين السلوك الإجرامي والنتيجة الضارة : وتمثل في الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة [1].

ويتمثل النشاط المادي في الجريمة الإلكترونية في الدخول غير المشروع في نظم وقواعد معالجة البيانات، سواء ترتب عن هذا الدخول غير المشروع تلاعب بهذه البيانات أم لا، وقد يتخذ هذا النشاط الإجرامي عدة صور، كانتهاك سرية الخصوصية للبيانات الشخصية والإضرار بصاحبها والإطلاع على المراسلات الإلكترونية، والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية يعد كذلك من أهم صور الركن المادي للجريمة الإلكترونية[2] .

[1] منصور رحماني، الوجيز في القانون الجنائي العام، مرجع سابق، ص93-97-99.

[2] صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مرجع سابق، ص67.

الفرع الثالث

الركن المعنوي للجريمة الإلكترونية

يعتبر الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني، ويتمثل الركن المعنوي في ظل الجرائم التقليدية في :

1- عناصر القصد الجنائي : وهي العلم والإرادة .

2- صور القصد الجنائي : وهي القصد الجنائي العام والقصد الجنائي الخاص .

ويتوفر القصد الجنائي في حق الجاني في حالات ثلاثة:

أ/ إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر والذي يعلق عليه القانون وجود جريمة.

ب/ إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل.

ج/ في حالة افتراض القانون توافر القصد الجنائي لدى الجاني، وهو مستمد من أنه طالما أن النتيجة الجسمية التي تحققه نشأت عن فعل الجاني[1] .

يقوم الركن المعنوي للجريمة الإلكترونية على أساس مجسد في توافر الإرادة الآثمة لدى الفاعل؛ فمثلا جريمة التزوير الإلكتروني في ما يخص القصد الجنائي: هو توافر لدى المجرم إرادة تغيير الحقيقة مع علمه بأن التغيير قد تم في محرر معلوماتي، والذي له نفس الأثر الذي يرتبه المحرر الكتابي، والقصد الجنائي العام لا يكفي وحده لقيام جريمة التزوير وبالتالي يجب توافر القصد الجنائي الخاص: وهو اتجاه نية المجرم إلى تحقيق غاية معينة من عملية التزوير[2] .

---

[1] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية. (رسالة ماجستير في تخصص القانون العام)، جامعة الشرق الأوسط، الكويت، 2014، ص29-30.

[2] دردور نسيم، الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن. (رسالة ماجستير في تخصص القانون الجنائي)، كلية الحقوق، جامعة منتوري، قسنطينة، 2013/2012، ص54.

المطلب الثاني

أساليب ودوافع ارتكاب الجريمة الإلكترونية

إنه وعلى خلاف الجرائم التقليدية التي تتطلب بطبيعتها نوعا من المجهود العضلي الذي قد يتخذ شكل العنف والإيذاء كما هو الحال في جريمة القتل مثلا، فإن الجرائم المعلوماتية تعد بطبيعتها جرائم هادئة لا تتطلب سوى عدد من اللمسات الخاطفة على أجهزة الحاسوب حتى تؤدي إلى اختراق أكبر نظم المعالجة الآلية وهتك سريتها أو محو ما تحتويه من معلومات أو تعطيل برامجها[1] .

وهذا ما يدعو للبحث في أساليب ارتكاب هذا الجرم في الفرع الأول، وكذا التعرف على الدوافع من ارتكاب هذه الجرائم في الفرع الثاني .

الفرع الأول

أساليب ارتكاب الجريمة الإلكترونية

تتشابه جرائم الإلكترونية مع الجرائم التقليدية من حيث استخدام المجرم لوسائل وأساليب غير مشروعة في سبيل ارتكابه لجريمته، ومع ذلك فإن جرائم المعلوماتية تتميز بارتكابها من طرف مجرمين يستعملون كل ما من شأنه خداع الحاسب الآلي والتحايل على أنظمته المعلوماتية ومن أهم هذه التقنيات هي الاختراق واستعمال البرامج الخبيثة (Vérus) وسنتطرق لها كما يلي :

أولا: الاختراق

الاختراق الإلكتروني بشكل عام هو القدرة على الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة، حيث يعتبر الهجوم على المواقع واختراقها على شبكة الإنترنت من الجرائم الشائعة في العالم، وطبقا لمؤشر سام للاختراق فإن لمستويات الاختراق أو الهجوم المعلوماتي ستة مستويات بحسب درجة الخطورة[2].

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مرجع سابق، ص46.

[2] ممدوح محمد الجنيبهي، أمن المعلومات الإلكترونية، مرجع سابق، ص26.

ويستخدم في عملية الاختراق عدة طرق تتمثل في :

1- استعمال نظم التشغيل : لكونها مليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الإنترنت، فيقوم المخترق بالبحث عن ضحية من خلال معرفة رقم (IP)(*) الخاص به، ويتم البحث عن هذا الرقم بمجموعة من الخطوات يقوم بها المخترق على جهازه الذي يشترط أن يكون متصلا بجهاز الضحية عبر شبكة الإنترنت وفي نفس اللحظة، لأن هذا الرقم يتغير مع كل اتصال جديد .

2- الاختراق باستخدام البرامج : ويشترط في هذه الطريقة وجود برنامجين أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم لأنه يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، وأخطر هذه البرامج برنامج **حصان طروادة**(*) وتتجلى خطورته لتميزه بالقدرة على الاختراق دون إمكانية كشفه وتتبعه والقضاء عليه، ويمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريق استخدام برامج الدردشة[1].

3- **انتحال شخصية الموقع** : ويعتبر هذا الأسلوب حديثا نسبيا في مجال الجرائم المعلوماتية، ويقوم هذا الأسلوب على قيام المخترق بوضع نفسه في موقع بيني بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الأنترنت وبين الموقع (WEB) ومن هذا الموقع البيني يستطيع المجرم المعلوماتي من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما له أن يقوم بسرقة هذه المعلومات أو تغييرها[2] .

---

* Address IP : يتطلب تشغيل نظم الاتصالات الكومبيوترية أن تكون هناك آلية من أجل عنونة الأجهزة سواء المرسلة أو المستقبلة، كما تتطلب أيضا أن تكون هناك آلية لضمان وصول أو التحقق من وصول الإتصال أو الرسالة للجهة المقصودة والتحقق من جهة الإرسال، ويستخدم في تحقيق هذه الغاية بروتوكول الأنترنات Internet protocol (IP)

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص57.

* حصان طروادة: صمم برنامج حصان طروادة في البداية لغرض حسن ومفيد وهو معرفة ما يقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين أو معرفة ما يقوم به الموظفون على جهاز الكمبيوتر في غياب المدراء إلا أنه تطور هذا البرنامج بحيث أصبح يمكن المخترق من الحصول على كلمة السر الخاصة بالدخول إلى الجهاز والتي يستخدمها صاحب الجهاز نفسه فلا يمكن لصاحب الجهاز ملاحظة وجود دخيل .

[2] حسن طاهر داود، جرائم نظم المعلومات. (ط:1؛ الرياض، المملكة العربية السعودية: لا.ن، 2000)، ص89.

ثانيا : البرامج الخبيثة (Les vérus)

الفيروس هو أحد أنواع برامج الحاسب الآلي، إلا أن الأوامر المكتوبة في هذا البرنامج تقتصر على أوامر تخريبية ضاره بالجهاز ومحتوياته، يمكن عند كتابة كلمه أو أمر ما أو حتى مجرد فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به[1].

ويستخدم الفيروس بشكل عام لتحقيق أحد الغرضين :

1- الغرض الحمائي : ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه ويعد ذلك بمثابة عقوبة تلحق بالناسخ .

2- الغرض التخريبي: ويتم إعداد هذه الفيروسات من طرف خبراء البرامج بهدف التخريب بحد ذاته أو إلى التخريب بهدف الحصول على منافع شخصية .

ومن الآثار التي يخلفها الفيروس والتي تختلف بحسب نوعه :

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا.
- عدم القدرة على تشغيل معظم التطبيقات وظهور رسالة خطأ كلما تمت محاولة تشغيلها.
- مسح الملفات التنفيذية وكذا حذف جميع المعطيات الموجودة داخل القرص الصلب.

أما عن أنواع الفيروسات فهي كثيرة جدا ولا يمكن حصرها، إذ أنها آخذة في التزايد بشكل متسارع وأهمها : الفيروسات المقيمة، الفيروسات النائمة، الفيروسات الاستعراضية، فيروسات الثغرات...الخ[2].

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مرجع سابق، ص75.

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص59.

الفرع الثاني

دوافع ارتكاب الجريمة الإلكترونية

الدافع هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغض والانتقام، وللجريمة الإلكترونية عدة دوافع على ارتكابها فبعضها يرجع إلى دافع شخصي ومنها ما يرجع إلى دافع خارجي ومنها ما يكون خاضا بالمنشأة، وكل هذه الدوافع تكون مصدرها هو الرغبة الإجرامية وسنتعرض لكل دافع كالآتي :

أولا: الدوافع الشخصية

1- الدوافع المادية: الرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم، ويكون ذلك إما عن طريق المساومة على البرامج والمعلومات المتحصّلة بطريق الاختلاس من جهاز الكمبيوتر أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية، ولقد أشارت مجلة (Securite inform atiqne) وهي مجلة متخصصة في الأمن المعلوماتي أن 43 % من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، 23 % من أجل سرقة المعلومات، 19 % أفعال أتلاف 15 % سرقة وقت الآلة أي الاستعمال غير المشروع لأجل تحقيق منافع شخصية[1] .

2- الدوافع الذهنية: قد تكون الدوافع لارتكاب الجريمة الإلكترونية مجرد الشغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية لها قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه .

الصورة الذهنية لمرتكبي هذه الجرائم، غالبا هي صورة البطل والذكي، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقائهم ببراعتهم، لدرجة أنه إزاء ظهور لأي تقنية مستحدثة فإن مرتكبي هذه الجرائم يحاولون إيجاد وسيلة إلى تحطيمها أو التفوق عليها[2].

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية. (ط:1؛ عمان-الأردن: دار الثقافة، 2008)، ص90.

[2] سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية. (مذكرة ماستر في تخصص قانون جنائي)، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014/2013، ص10

ثانيا : الدوافع الخارجية

الإنسان بطبيعته مخلوق هش من الناحية السيكولوجية، يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية، ولعل من أبرزها الحاجة إلى اختصار عنصر الزمن وتوفير سنوات عدة من البحث وتحاشي استثمار الملايين من الدولارات في مجال البحث العلمي، فقد يكون دافع جنون العظمة أو الطبيعة التنافسية هي التي تدفع بعض العاملين في المنشآت لإظهار قدراتهم الفنية الخارقة لإدارة المنشأة، فيفضي به ذلك إلى ارتكاب مثل هذه الجرائم حتى ينافس زملائه للوصول إلى أعلى المراكز المرموقة، وقد يكون دافع الانتقام من رب العمل أو أحد الزملاء أو الأصدقاء من بين البواعث الدافعة إلى ارتكاب هذه الجريمة[1].

ويمكن اعتبار التنافس السياسي والاقتصادي دافعا لارتكاب هذا السلوك الإجرامي، فمثلا قد يعد التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة[2].

فعلى صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم الإلكترونية هو الرغبة في قهر الأنظمة الالكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة، ويمكن لنا أن نوضح هذا الأمر من خلال ما ذكره أحد قراصنة الحاسوب : (كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى للبيت بعد يوم آخر في الدراسة وأدير تشغيل جهاز الحاسوب وأصبحت عضوا في لجنة قراصنة الأنظمة ... لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني كنت على حافة التكنولوجيا واكتشاف ما وراءها واكتشاف الكهوف الالكترونية التي لم يكن من المفترض وجودي بها)[3].

[1] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مرجع سابق، ص114-115.

[2] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي. (رسالة ماجستير في تخصص علم الإجرام وعلم العقاب)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2011، ص50.

[3] نهلا عبد القار المومني، الجرائم المعلوماتية، مرجع سابق، ص91-92.

المطلب الثالث

موقف الشريعة الإسلامية والمشرع الجزائري من الجريمة الإلكترونية

فرض الإجرام الإلكتروني نفسه كظاهرة سلبية على المجتمعات بعد التطور المعلوماتي الذي وصل إليه هذه الأخيرة، فبدأ التأثير السلبي لهذا الإجرام واضحا مهددًا للأفراد والجماعات والأموال والحكومات على حد سواء، واتخذ المجتمع الدولي موقفا بشأنه، من ذلك حاولت الشريعة الإسلامية مناقشة بعض هذه الجرائم وتحديد حكمها الشرعي وما يناسبها من عقوبة في الفرع الأول وكذلك بيان موقف المشرع الجزائري من هذه الجرائم في الفرع الثاني .

الفرع الأول

موقف الشريعة الإسلامية من الجريمة الإلكترونية

إن ديننا الإسلامي قد اهتم بالفرد كاهتمامه بالمجتمع، كما أنه شرع من الأحكام ما يحفظ عليه دينه ونفسه وعقله وماله، كما أنه أوجب عقوبات رادعة لكل من تسول له نفسه المساس بأحد الضروريات الخمس، وبسبب ما قرره الشرع نجد أن المعتدين قلة، ولكن لما شاع استخدام الحاسب الآلي والإنترنت وجدنا أن المتعاملين معهما قد استسهلوا الاعتداء على الأفراد والمجتمعات، وتختلف صور هذه الاعتداءات كما مرّ معنا سابقا، وسنبين التأصيل الشرعي لهذه الجرائم من خلال التعرض لبعض هذه الجرائم، وهي جريمتي المساس بالحياة الخاصة للأشخاص من خلال التشهير بالقذف كصورة أولى، وجريمة التعدي على الأموال الإلكترونية من خلال السرقة المعلوماتية كصورة ثانية .

الصورة الأولى: التشهير بالقذف

أولا: تعريف القذف

1- لغة : هو الرمي ومنه قذف الحجارة[1]، ومنه قوله تعالى:﴿ فَٱقْذِفِيهِ فِي ٱلْيَمِّ ﴾ [طه: 39]

2- اصطلاحا

عرفه المالكية : رمي مكلف حر مسلم بنفي نسب عن أب أو جد أو بزنا[2] .

وعرفه الحنفية والحنابلة : الرمي بالزنى[3].

وعرفه الشافعية : الرمي بالزنا في معرض التعيير، واستثنوا منه ما كان في خلوة لعدم لحوق العار[4].

ثانيا: الحكم الشرعي للقذف عبر الإنترنت

القذف هو من الأحكام التي شرع الله فيه الحد، وهو ثمانون جلدة، والتشهير بالقذف عبر الإنترنت يأخذ نفس حكم التلفظ به، بجامع أنهما يؤذيان صاحبهما ويوقعانه في الضرر بغض النظر عن الطريقة، وعليه فإن حكم القذف عبر الإنترنت حرام وهو موجب للحد للأدلة التالية[5] :

1- القرآن الكريم :

قوله تعالى: ﴿ وَٱلَّذِينَ يَرْمُونَ ٱلْمُحْصَنَٰتِ ثُمَّ لَمْ يَأْتُواْ بِأَرْبَعَةِ شُهَدَآءَ فَٱجْلِدُوهُمْ ثَمَٰنِينَ جَلْدَةً وَلَا تَقْبَلُواْ لَهُمْ شَهَٰدَةً أَبَدًاۚ وَأُوْلَٰٓئِكَ هُمُ ٱلْفَٰسِقُونَ ﴾ [النور: 04]

---

[1] إسماعيل بن حماد الجوهري، الصحاح، ج4، مرجع سابق، ص1414.

[2] أبي محمد عبد الوهاب البغدادي المالكي، التلقين في الفقه المالكي. تحقيق: محمد ثالث سعيد الغاني، ج2(ط:1؛ مكة المكرمة: جامعة أم القرى، 1986/1985)، ص199.

[3] الموسوعة الفقهية، إصدار وزارة الأوقاف والشئون الإسلامية. ج33(ط:2؛ الكويت: دار الصفوة للطباعة، 1995)، ص5.

[4] خسرو الحنفي، الدرر الحكام في شرح غرر الأحكام. ج2(لا.ط؛ لا.م: لا.ن، د.ت)، ص80.

[5] عبير علي، جرائم الحاسب الآلي في الفقه الإسلامي، مرجع سابق، ص83.

2- السنة النبوية :

عن أبي هريرة "رضي الله عنه" قال : قال "رسول الله صلى الله عليه وسلم" : « اِجْتَنِبوُا السَّبعَ الموبِقَات، قالُوا يا رسوُل الله، وما هنَّ ؟ قال النبَّيُّ صلَّى الله عليْهِ وسلَّمَ: الشّركُ بالله والسِّحر، وقَتلُ النَّفسِ الّتي حرَّمَ الله إلاَّ بالحق، وأكلُ الرِّبا، وأكلُ مالَ اليَتيمِ، والتولّي يَوم الزّحفِ وقَذفُ المحصَنَاتِ المؤْمناتِ الغَافِلاَت »[1] .

3- الإجماع :

أجمعت الأمة على أن القذف حرام وفيه الحد[2]، وما دام القذف عبر الإنترنت له نفس النتائج المترتبة على القذف اللفظي، فيتناوله الحكم بالإجماع .

وجه الدلالة :

في الدليل الأول قوله تعالى ﴿ وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ﴾ تدل بمنطوقها على عموم القذف؛ بغض النظر عن الطريقة، فيكون القذف عبر الإنترنت داخلا فيه .

وفي الدليل الثاني من السنة عد النبي صلى الله عليه وسلم قذف المحصنات المؤمنات الغافلات واحدة من السبع الموبقات، والقذف عبر الإنترنت عادة ما يكون لإنسان غافل، ونلحظ كذلك اقتران القذف بالشرك والسحر وغيره من عظائم الأمور، فوجب القول بحرمته، ولو كان عبر الإنترنت .

وبالإجماع القذف محرم وموجب للحد، ثمانون جلدة بلا مزيد رجلا كان، أو امرأة، مسلما، أو غير مسلم، هذا بخصوص القذف التقليدي، بينما القذف عبر الإنترنت أنكى خطرا، لأن شؤم هذا الأذى يتعدى الآفاق، ليصل إلى كل الأصقاع فيكون الحكم بالحد واجبا من باب أولى[3] .

---

[1] أخرجه البخاري في صحيحه، كتاب الوصايا، باب قول الله تعالى (إن الذين يأكلون أموال اليتامى ظلما إنما يأكلون في بطونهم نارا)، حديث رقم 2615، 1017/3.

[2] سعدي ابو حبيب، موسوعة الإجماع في الفقه الإسلامي. ج2(ط:3؛ دمشق:لا.ن، 1996)، ص360.

[3] انظر، المرجع نفسه، ص 360، عبير علي، جرائم الحاسب الآلي في الفقه الإسلامي، مرجع سابق، ص83-84 .

الصورة الثانية : السرقة المعلوماتية

إنَّ الصورة الغالبة لسرقة المال المعلوماتي إن أمكن الوصف تأخذ صورة الإختلاس للبيانات والمعلومات والإفادة منها باستخدام السارق للمعلومات الشخصية للمجني عليه[1] .

أولا: تعريف السرقة وبيان حكمها

السرقة هي: " أخذ مال الغير على سبيل الخفية نصابا محرزا للتمول غير متسارع إليه الفساد من غير تأويل ولا شبهة "[2] .

وحد السرقة هو قطع اليد لقوله تعالى : ﴿ وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ ﴾ [المائدة : 38]، لأن السارق يأخذ المال على وجه لا يمكن الإحتراز منه، ولو لم يجب القطع عليه لأدى ذلك إلى هلاك الناس بسرقة أموالهم[3] .

وحتى يثبت حد القطع لابد من توفر الشروط الستة التالية المعتبرة في جريمة السرقة :

1- أن يكون الآخذ مكلفا

2- أن يكون المأخوذ مالا للغير

3- أن يبلغ النصاب

4- أن يأخذ من حرز مثله

5- أن يأخذه على سبيل الخفية

6- أن تنتفي عنه الشبهة

ثانيا: مدى تحقق الشروط المعتبرة للسرقة في السرقة المعلوماتية

1- كون المسروق هو المعلومات، فيعتبر الجاني مكلفا .

2- الشرط الثاني محقق كون المأخوذ هو البيانات والمعلومات في جهاز الضحية .

3- بلوغ النصاب محقق، وهو عشرة دراهم عند الحنفية .

---

[1] أمين الشوابكة، جرائم الحاسوب والإنترنت، مرجع سابق، ص138.

[2] بكر بن عبد الله أبو زيد، الحدود والتعزيرات عند ابن القيم، مرجع سابق، ص347.

[3] أبي إسحاق إبراهيم بن علي بن يوسف الفيروزابادي الشيرازي، المهذب في فقه الإمام الشافعي. ج3(ط:1؛ بيروت: دار الكتب العلمية، 1995)، ص353.

4- بالنظر إلى الحاسب وطبيعة مالية معلوماته، وللحفاظ عليه وجب الأخذ بجميع الاحتياطات الأمنية، فيعد حرزا .

5- عرفنا سابقا أن الجرائم الإليكترونية ترتكب على سبيل الاختلاس والاختطاف والخيانة وتكون علنية، وهذا يتنافى مع اشتراط الخفية في جريمة السرقة .

6- الشبهة في المال المسروق منها ما يتعلق بالركن كفقد شرط الشهود، ومنها ما يتعلق بشبهة الدليل كسرقة الأصول والفروع والمحارم، والمعتدي على المعلومات في الحاسب الآلي قد يكون أحد هؤلاء، فتقوم الشبهة في دليل السرقة، ولا ينطبق عليها الوصف ولا العقوبة .

مما سبق نخلص إلى سقوط الحد في جريمة السرقة المعلوماتية، وهذا لاختلال الشرطين الأخيرين "الخفية وانتفاء الشبهة"، وترك تحديد العقوبة لولي الأمر بحسب دواعي المصلحة[1] .

[1] أنظر: إسماعيل عبد النبي شاهين، "أمن المعلومات في الإنترنت بين الشريعة والقانون"، بحوث مؤتمر القانون والكمبيوتر والإنترنت(من 1-3 2000)، جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون، المجلد: 3، 2004، ص988-989. عبير علي، جرائم الحاسب الآلي في الفقه الإسلامي، مرجع سابق، ص48-49-50-51.

الفرع الثاني

موقف المشرع الجزائري من الجريمة الإلكترونية

تشير الإحصائيات إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر[1].

إن تفاقم هذه الاعتداءات على الأنظمة المعلوماتية دعت المشرع الجزائري إلى ضرورة تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04المؤرخ في 10 /11/ 2004 المتمم والمعدل للأمر 66 /156 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان : **"المساس بأنظمة المعالجة الآلية للمعطيات"** ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الإتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني[2].

أولا : نظام المعالجة الآلية للمعطيات

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة؛ فضلا عن أنه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية .

ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرِّف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه إلى كل من الفقه و القضاء[3].

---

[1] فشار عطاء الله، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، 2009، ص21.

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص41.

[3] فشار عطاء الله، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، مرجع سابق، ص22.

وعُرِّف هذا النظام على أنه عبارة عن تلك العمليات المتعددة التي تتم بصفة آلية على معلومات لكي تتحول إلى معطيات عن طريق معالجتها داخل نظام آلي[1]

والمشرع حسنا فعل حينما تجنب التقيد بتعريف محدد لنظام المعالجة الآلية للمعطيات ذلك أن العناصر التي يتكون منها هذا النظام في حالة تطور تكنولوجي مستمر يخضع للتطورات السريعة والمتلاحقة التي تطرأ على البيئة التقنية التي يمثلها والتي تتسع لإمكانية شمول وسائل تقنية جديدة، لاسيما وأن العالم الافتراضي لا يزال في بدايته ولن يكون من السهولة احتواؤه، ومن جهة أخرى فإن نظام المعالجة الآلية للمعطيات يعد تعبيرا فنياً يصعب على المشتغل بالقانون إدراك طبيعته .

ثانيا : الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

بصدور القانون رقم 04/09 المؤرخ في 2009/08/05[2] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، اعتبر المشرع الجزائري أن الجرائم المعلوماتية تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07، أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء، بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها[3] .

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مرجع سابق، ص32.

[2] المادة (01) من القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق 05 أوت 2009م، والمتضمن: القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، (الجريدة الرسمية، العدد 47).

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص43-47.

الفصل الثاني

الإجراءات المتبعة لمكافحة الجريمة الإلكترونية

سنتطرق في هذا الفصل إلى مبحثين، المبحث الأول أساليب وطرق مكافحة الجريمة الإلكترونية، والمبحث الثاني مواجهة الجريمة الإلكترونية والحماية الموفرة لها.

المبحث الأول

أساليب وطرق مكافحة الجريمة الإلكترونية

بعد ما تناولنا في ما سبق من البحث التعريف بالجريمة الإلكترونية وخصائصها وأنواعها، نسعى من خلال هذا المبحث الثاني الحديث عن الأساليب وطرق مكافحتها من خلا ل ما ترتب عن هذه الجريمة من عقوبات، وكيفية الكشف عنها من خلال طرق إثباتها وأين وصل المشرّع الجزائري في قبول الأدلة الإلكترونية كمرشد ودليل للإثبات.

سنتناول الحديث عن العقوبات من الجانب الشريعة الإسلامية والقانون في المطلب الأول، و طرق الإثبات وجمع الأدلة وما الصعوبات في ذلك في المطلب الثاني، و موقف المشرّع الجزائر من الأدلة الإلكترونية في الأثبات الجزائي.

المطلب الأول

عقوبات الجريمة الإلكترونية بمنظور الشريعة الإسلامية والقانون

نتحدث في هذا المطلب عن الجريمة الإلكترونية المستحدثة وما يقابلها من العقوبة في نظر التشريع الإسلامية والقانوني، نخصص الحديث عنها في الشريعة الإسلامية في الفرع الأول، وعن الجانب القانوني في الفرع الثاني.

الفرع الأول

عقوبات الجريمة الإلكترونية بمنظور الشريعة الإسلامية

قضية التجريم والعقاب في الشريعة تتسم بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل الذي يغطي كل جوانب الحياة ويصلح لكل زمان ومكان[1]، كونه صادر من خالق و عليم بما يصلُح له ويُصلحُه.

وتركت الشريعة الإسلامية الباب مفتوحا لتجريم الأفعال المستحدثة تحت قواعد فقهية واضحة وذلك بدفع الوسائل التي تؤدي الى المفاسد، والأخذ بالوسائل التي تؤدي الى المصالح"[2]،القاعدة الكلية الكبرى "لا ضرر ولا ضرار"، والقاعدة المتفرعة منها "درء المفاسد أولى من جلب المصالح"[3].

وتقسم الجريمة أساسا على مقدار العقوبة من حيث وجوب الحكم بها[4]، إلى عقوبات مقدرة، وتضم جرائم الحدود والقصاص والدية، وعقوبات غير مقدرة، يترك للقاضي اختيار نوعها بحسب ما يراه من ظروف الجريمة وحال المجرم وتضم جرائم التعزير.

---

[1] صالح بن محمد المسند، د. عبد الرحمن بن الراشد المهيني، "جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات"، المجلة العربية للدراسات الأمنية والتدريب مجلد15، العدد29، ص184.

[2] محمد ابو زهرة، الجريمة والعقوبة في الإسلام، مرجع سابق، ص228.

[3] محمد صدقي بن أحمد بن محمد آل بورنو ابو الحارث الغزي، الوجيز في إيضاح قواعد الفقهية الكلية. (ط:4، بيروت: مؤسسة الرسالة، 1416هـ)، ص265.

[4] عبد القادر عودة، التشريع الجنائي الإسلامي، مرجع سابق، ص 633.

وتحديد الجريمة يعتبر فرعا من العقوبة في حين أن التشريع الإسلاميّ يجعل الأساس في العقوبة هو جسامة الجريمة وخطرها من حيث المساس بالضرورات الخمس[1]. وللوقوف على أنواع العقوبات لمرتكبي جرائم الإلكترونية نستعرض منها[2]:

1- الحبس

وهو عقوبة تعزيرية يوضع الشخص في مكان محدد ليقيد حريته ومنع تصرفه بنفسه، وهذا من شأنه أن يتوقف عن الاعتداء أجهزة غيره من الناس، ويخرجه الحاكم متى رأى فيه استقامته وصلاحا، ودليل مشروعيته « اشْتَرَى نَافِعُ بْنُ عَبْدِ الحَارِثِ دَارًا لِلسِّجْنِ بِمَكَّةَ مِنْ صَفْوَانَ بْنِ أُمَيَّةَ عَلَى أَنَّ عُمَرَ إِنْ رَضِيَ فَالْبَيْعُ بَيْعُهُ وَإِنْ لَمْ يَرْضَ عُمَرُ فَلِصَفْوَانَ أَرْبَعُ مِائَةِ دِينَارٍ »[3] .

2- الجلد

ودليل مشروعيته ما روي عن أبي بردة بن نيار أنه سمع النبي صلى الله عليه وسلم يقول «لاَ يُجْلَدُ فَوْقَ عَشْرِ جَلَدَاتٍ إِلَّا فِي حَدٍّ مِنْ حُدُودِ اللَّهِ »[4]، إن التعزير إذا وجب بجناية ليس من جنسها فإن الامام بالخيار، إن شاء عزر بالصرب أو بالحبس أو بالتوبيخ.

3- التوبيخ

لما روى عن النبي صلى الله عليه وسلم أنه سمع أبا ذر يعير رجلا بأمه، وقول له ا ابن السوداء، فعاتبه النبي صلى الله عليه وسلم بقوله « إِنَّكَ امْرُؤٌ فِيكَ جَاهِلِيَّةٌ »[5].

4- إيقاف عن أداء نشاطه

وذلك بفصله عن وظيفته لمدة محددة، خاصة من أساء في عمله بالاطلاع على بيانات خاصة ومعلومات سرية من خلال جهاز الحاسب الآلي في أوقات عمله لأغراض شخصية.

---

[1] عبد القادر عودة، التشريع الجنائي الإسلامي، مرجع سابق، ص 633.

[2] عبير علي النجار، جرائم الحاسب الآلي في الفقه الإسلامي، مرجع سابق، ص102.

[3] أخرجه البخاري في صحيحه، كتاب الخصومات، باب الربط والحبس في الحرم، (123/3).

[4] أخرجه البخاري في صحيحه ، كتاب الحدود، باب كم التعزير والأدب، رقم(6848)، (174/8).

[5] أخرجه البخاري في صحيحه، كتاب الأدب، باب ما ينهى من السباب واللعن، رقم(6050)،(16/8).

5- القتل

نعم! لا سيما إذا كان هذا المجرم يتجسس على معلومات أمنية، وأنشطة عسكرية تضر بالدولة، لخطره على المسلمين فعَنْ عَرْفَجَةَ الأشجعي قَالَ سَمِعْتُ رَسُولَ اللَّهِ صلى الله عليه وسلم يَقُولُ « مَنْ أَتَاكُمْ وَأَمْرُكُمْ جَمِيعٌ عَلَى رَجُلٍ وَاحِدٍ يُرِيدُ أَنْ يَشُقَّ عَصَاكُمْ أَوْ يُفَرِّقَ جَمَاعَتَكُمْ فَاقْتُلُوهُ »[1].

6- الغرامة المالية

عند تحقق التعدي والتفريط في أموال الناس، وأكل أموالهم بالباطل ، كما هو الحال في غالبية الجرائم الإلكترونية، حينها يلزم الجاني ليس فقط الغرامة، وإنما بالتعويض عن قيمتها، وهذا من تمام عدل الشرع، فالغرامة للردع والزجر، والتعويض كونه حق الغير[2].

ومن الأسئلة والقضايا التي تعد جريمة ويستحق مرتكبيها العقاب هي:

هل يجوز في الشريعة نسخ البرامج أم أن هناك حماية لحقوق المنتج؟ ما مدى شرعية نسخ حزم البرامج الجاهزة، هل هو جائز أم لا؟ وهل يختلف الحكم باختلاف الغرض من النسخ؟، فيجوز مثلا إذا كان الغرض الاستفادة الشخصية ويكون محرما إذا كان الغرض منه التجارة؟، ولقد ناقش علماء الشريعة هذه القضية وصدرت فيها فتاوى شرعية و قرارات رسمية تدعم هذا الحق وتحميه(حماية منتجي برامج الحاسوب من قراصنة النسخ) [3] [4].

---

[1] أخرجه مسلم في صحيحه، كتاب الإمارة، باب حكم من فرق أمر المسلمين وهو مجتمع، رقم(4904)، (23/6).

[2] عبير علي النجار، جرائم الحاسب الآلي في الفقه الإسلامي، مرجع سابق، ص105.

[3] صالح بن محمد المسند، د. عبد الرحمن بن الراشد المهيني، "جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات"، مرجع سابق، ص185

[4] اختلف الفقهاء في المسألة الواحد لعدة رأى، أنظر(لجنة الفتوى بالشبكة الإسلامية، فتاوى الشبكة الإسلامية، أرشيف لجميع الفتاوى العربية http://www.islamweb.net ، طب وإعلام وقضايا معاصرة3436، وسائل إعلام واتصال1128، 2009/11/18.

الفرع الثاني

عقوبات الجريمة الإلكترونية بمنظورها القانوني

إن للطبيعة الخاصة للجرائم المعلوماتية أثر على التشريعات العقابية القائمة، فالقصور الذي يعتري هذه الأخيرة في مواجهتها للجرائم المعلوماتية قد يترتب عليه آثار خطيرة تتمثل في إمكانية إفلات الجناة من العقاب بسبب عدم تقنينها في صورة جرائم ينص عليها المشرّع، وما قد ينجر عليه من توسع القضاء في تفسير النصوص العقابية التقليدية فيتم العصف بمبدأ الشرعية، وقد تباينت اتجاهات الدول المختلفة في التعامل مع ظاهرة الجريمة الإلكترونية ويرجع ذلك بصفة أساسية إلى اختلاف الأنظمة القانونية لهذه الدول من ناحية، وإلى اختلاف تجربة كل منها مع الجريمة الإلكترونية من ناحية أخرى[1]، (لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لم يعتبر جرما)[2].

ويمكن التمييز في هذا الصدد بين ثلاث مواقف تشريعية يتأثر مضمون الحماية الجنائية لنظم المعلوماتية بحسب المصلحة المحمية فما حماه البعض لم يحمه البعض الآخر.

الاتجاه الأول:

الهدف من الجريمة المعلوماتية هو حماية الملكية الفكرية، و يرى هذا الاتجاه أن المعلومات المخزنة بالحاسب الآلي والبرامج الخاصة به لا تختلف عن الأشياء التي تكون محلا لحق الملكية، لذلك تقوم التشريعات التي تأخذ بهذا الاتجاه ببسط حمايتها على النظم المعلوماتية في إطار حماية الملكية الفكرية.

الاتجاه الثاني:

يرتكز هذا الاتجاه على حماية مصلحة سلامة المعلومات مهما كانت طبيعة النشاط الإجرام الذي تتعرض له[3].

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص77.

[2] محمد ابو زهرة، الجريمة والعقوبة في الاسلام، مرجع سابق، ص31.

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق،ص78.

الاتجاه الثالث:

يهتم هذا الاتجاه بالمعلومات في حد ذاتها، فالهدف في هذا الاتجاه هو حماية سرية المعلومات فيمنع الاطلاع عليها سواء كانت هذه المعلومات متعلقة بالأشخاص أو كانت متعلقة بالأموال.

ولم يقف الاختلاف بين التشريعات في التعامل مع الجريمة المعلوماتية عند هذا الحد بل أوجد نصوص قانونية جديدة يضاف إليها البعد الخاص بالنظم المعلوماتية أو تعديل بعض النصوص القانونية القائمة بحيث تتلاءم مع هذا الشكل الجديد من الجرائم[1].

وبما ان الجرائم عابرة للحدود، ويساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة[*] فتظهر مشكلة التعارض والاختلاف بين التشريعات الإجرائية في دول العالم، ومكافحة جرائم المعلومات تقتضي إذًا توحيد التشريعات الإجرائية من ناحية، وأن يكون نظام الإثبات بالدليل الإلكتروني واحدًا بين الدول التي تقع فيها هذه الجرائم ،وهذا أمر مستحيل تحقيقه[2].

[1] سيعداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق،ص78

[*] جانب من الفقه يطلق عليه بالجرائم العالمية وهي تختلف عن الجرائم الدولية لان الأخيرة مصدرها القانون الدولي والاولى القانون الجنائي الوطني او (قوانين جنائية وطنية مجتمعة).

[2] علي حسن طوالبة، التعاون القضائي الدولي في مجال مكافحة الجريمة الالكترونية، مركز الاعلام الامني البحرين، ص01

المطلب الثاني

إثبات الجرائم الإلكترونية

الإثبات عند الفقهاء: إقامة الدليل الشّرعي أمام القاضي في مجلس قضائه على حق أو واقعة من الوقائع الإثبات، وفي القانون لا يخرج في تعريفه عما ورد في الشريعة الإسلامية، وهو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتبت عليها آثارها[1]، وسنتطرق طرق الإثبات في الفرع الأول، وجمع الأدلة في الفرع الثاني، وصعوبات الإثبات في الفرع الثالث.

الفرع الأول

طرق الإثبـــات

أولا: الإثبات في الشريعة الإسلامية

طرق الإثبات في المواد الجنائية في الشريعة الإسلامية، البيّنة، الإقرار، القرائن، الخبرة، معلومات القاضي، الكتابة، اليمين، وانفردت الشريعة الإسلامية بالقسامة(*) واللعان[2] .

وذهب جمهور الفقهاء[3] إلى أنّ وسائل الإثبات محصورة فيما ورد به النص الشّرعي صراحة، أو استنباطًا كالشهادة والإقرار واليمين، وقد اختلف أصحاب هذا القول في حصرها، فمنهم مَن حصرها في سبع، ومنهم من حصرها في ست، ومنهم من حصرها في ثلاث. واستدلّ أصحاب هذا القول بالأدلة التي فيها تحديد لطرق الإثبات، كقوله تعالى: ﴿ وَٱسۡتَشۡهِدُواْ شَهِيدَيۡنِ مِن رِّجَالِكُمۡۖ فَإِن لَّمۡ يَكُونَا رَجُلَيۡنِ فَرَجُلٞ وَٱمۡرَأَتَانِ مِمَّن تَرۡضَوۡنَ مِنَ ٱلشُّهَدَآءِ ﴾ [البقرة: 282].

---

[1] أيسر محمد عطية، دور الآليات الحديثة من الجرائم المستحدثة الارهاب الالكتروني وطرق مواجهته، (ملتقى علمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية الدولية، 2-2013/9/4م) ص18

* القسامة: طريق لإثبات الدم يقوم على حلف اليمين. (عوض عبد الله أبو بكر، نظام الإثبات في الفقه الإسلامي، لا: ط، المدينة المنورة، مجلة الجامعة الإسلامية، د.ت، 77/60).

[2] إدارة الدراسات والبحوث، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص14.

[3] المرجع نفسه.

وقوله تعالى: ﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُونُواْ قَوَّٰمِينَ بِٱلۡقِسۡطِ شُهَدَآءَ لِلَّهِ وَلَوۡ عَلَىٰٓ أَنفُسِكُمۡ ﴾ [النساء: 135] والشهادة على النفس إقرار.

وفي حديث: « اليَمِينُ عَلَى المدَّعَى عَلَيْهِ »[1] وفي زيادةٍ ليست في الصّحيحين وحسَّن إسنادَها الحافظ ابن حجر: و« الْيَمِينَ عَلَى مَنْ أَنْكَرَ »[2] والمنكِر هو المدَّعَى عليه، وهو المطلوب كما أنَّ المدعي هو الطالب[3].

وذهب جمعٌ مِن المحقّقين منهم شيخ الإسلام ابن تيمية وتلميذه ابن القيّم رحمهما الله، إلى أنَّ وسائل الإثبات غير محصورة بعددٍ مُعَيَّن من وسائل الإثبات، بل تشمل كل ما يبيّن الحق ويُظهره. ومن أدلة هذا القول حديث ابن عباس: « الْبَيِّنَةُ عَلَى الْمُدَّعِي »[4]، وبناءً على ذلك تكون وسائل الإثبات غير محصورة في عدد معيّن وطرق خاصّة، بل تكون غير محدّدة، وكل وسيلة تُظهر الحق، وتكشف عن الواقع يصح الاعتماد عليها في الحكم والقضاء بموجبها[5].

ثانيا: الإثبات في التشريعات القانونية

الإثبات الجنائي نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقا لمعيار الحقيقة الواقعية، وذلك بشأن الاتّهام أو تأكيد أو نفي آخر، يتوقف عليه إجراء قضائي، أي إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين.

---

[1] محمد بن إسماعيل البخاري ت 256هـ، الجامع الصحيح المختصر. تحقيق: د. مصطفى البغا، ج6(ط:3؛بيروت:دار بن كثير، ودار اليمامة، 1407هـ/1987م) كتاب التفسير، باب: سورة آل عمران، ص1656.

[2] أخرجه: أحمد بن حسين البيهقي ت 458، السنن الكبرى. تحقيق: محمد عبد القادر عطا،ج10(لا:ط؛ مكة المكرمة: مكتبة دار الباز،1414هـ/1994م) كتاب الدعوى والبيانات، باب البينة على المدعى واليمين على المدعى، ص252.

[3] إدارة الدراسات والبحوث، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص51.

[4] أخرجه: أحمد بن حسين البيهقي، السنن الكبرى، مرجع سابق، ص252

[5] إدارة الدراسات والبحوث، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص17.

والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة، فإنه في سبيل ذلك يستخدم وسائل معينة وهي كل ما يستخدم في إثبات الحقيقة (اكتشاف حالة أو مسألة أو شخص أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة) أي :الأدلة ونقلها إلى المجال الواقعي الملموس[1].

والقاعدة في مختلف التشريعات الجزائية ان الجريمة يجوز إثباتها بكافة طرق الإثبات، فلا قيد أو شرط على الإثبات في المواد الجنائية إلا أن تكون وسيلة الإثبات أو أن يكون الدليل قد تحصل عليه بطريقة مشروعة، إعمالا لمبدأ الشرعية الإجرائية، وتحظى قواعد الإجراءات الجنائية بشأن جرائم الكمبيوتر المتصلة بإجراءات الاستدلال والتحقيق والإثبات وإجراءات المحاكمة المتفقة مع طبيعة الاعتداءات في الدعاوى التي تتعلق بجرائم الكمبيوتر أو الاعتداء على الخصوصية[2].

اقتضت الضرورة تقييد الوسائل بعدد من الطُرق، والقيد على هذه القاعدة؛ أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإلكترونية، لأنّها ليست ماديات لتقبل بيّنة في الإثبات، من هنا كان البحث القانوني في العديد من الدول يتجه إلى الاعتراف بالحجية القانونية لملفات الكمبيوتر ومستخرجاته والرسائل الإلكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي، ولكن بطبيعتها الإلكترونية المحضة، وهي غالبا ما تكون جريمة هادئة لا عنف فيها ولا تترك أشياء مادية تدرك بالحواس ،لكونها عبارة عن أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات.[3]

الفرع الثاني

جمع الأدلـــة

قد تعارف الفقه والقضاء على الأدلة التي يمكن للقاضي الاستناد إليها ، وهذه الأدلة هي الاعتراف والمعاينة والمحررات وشهادة الشهود والخبرة والقرائن، غير أن هذه الأدلة تبدو في الأعم

[1] أيسر محمد عطية، دور الآليات الحديثة من الجرائم المستحدثة الارهاب الالكتروني وطرق مواجهته ،مرجع سابق، ص19

[2] المرجع نفسه، ص21

[3] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، مرجع سابق، ص30.

قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية الذي يتواصل بنبضات إلكترونية غير مرئية العبث بالدليل أو محوه بالكامل في وقت قصير جدا يتعذر معه كشفها.

1- الخبرة:

يعتبر تقرير الخبير من الأدلة ،وأما إجراء ندب الخبير فهو من إجراءات جمع الأدلة باعتباره إجراء من إجراءات التحقيق ،والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره ،ولذلك فإن الخبير يأخذ حكم الشاهد ويجوز استدعاؤه لسماع شهادته ومناقشته في التقرير الذي أعده وتقدم به ،غير أن الخبير يختلف عن الشهود من حيث الوقائع التي يشهد بها ،فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها أما الخبير فشهادته فنية أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة ويترتب على ذلك أنه لا يجوز سماع الخبير كشاهد إذا كان إجراء الخبرة قد وقع باطلا[1].

2- المحررات أو الدليل الكتابي:

الكتابة لا تعدو كونها رموزاً تعبر عن الفكر و القول، وأنه لا في اللغة و لا في القانون ما يتطلب أن تكون الكتابة علي الورق فقط، وهي " مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الأفكار والمعاني"، والمحررات رسمية كانت أو عرفية التي تثبت وقوع الجريمة سواء أكانت هذه المحررات موضوع السلوك الإجرامي ذاته كما في جريمة التزوير أو التهديد كتابة ، أم كانت تتضمن دليلا على ارتكاب الجريمة.

وهناك ما يسمي بالدليل الإلكتروني(الرقمي) (*) في شكل مجالات و نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجية خاصة، في أشكال متنوعة مثل الرموز و النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم يعبر عن فكر وقول يطلق عليه الكتابة الرقمية بالمعني الواسع[2] .

---

[1] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، مرجع سابق، ص32.

* هو الشيء الذي يتم الحصول عليه بواسطة التقنية الالكترونية من معطيات الحاسوب وشبكة الانترنت والاجهزة الالكترونية الملحقة والمتصلة به وشبكات الاتصال،من خلال اجراءات قانونية، لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة.

[2] المرجع نفسه، ص32-33.

وللدليل الإلكتروني ثلاث خصائص: الأولى أنه دليلا غير ملموس، والثانية أنه دليل من الأدلة الفنية أو العلمية، والخصية الثالثة أن فهم مضمون الدليل الإلكتروني يعتمد على استخدام أجهزة تجميع وتحليل فحواه ليكون دليل إثباتها، كما ان له ثلاثة أنواع كدليل إثبات، النوع الأول مخرجات ذات طبيعة ورقية والنوع الثاني مخرجات ذات طبيعة إلكترونية والنوع الثالث مخرجات مرئية[1].

ومن الوسائل و الإجراءات التي تهدف إلى جمع وفحص الأدلة المثبتة لوقوع الجريمة ونسبتها إلى فاعلها كالمعاينة والخبرة و التفتيش وضبط الأشياء المتعلقة بالجريمة وسماع الشهود والاستجواب[2].

1- المعاينة:

وهى إجراء يتم بمقتضاه الانتقال إلى مكان وقوع الجريمة لجمع الأشياء المتعلقة بالجريمة ومعاينة آثار وقوعها، وهي من مراحل الأولى للاستدلال حول ملابسات الجريمة[3].

2- التفتيش:

التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة عن التفتيش التقليدي للأشخاص والمنازل، إلا أنه يخضع في إجراءاته للضوابط التي حددها قانون الإجراءات الجنائية وما ستلزمه من وقوع الجريمة واتهام شخص أو أشخاص معينين بارتكاب جريمة، وتتمثل في:

أ- البحث في المكونات المادية للنظام المعلوماتي.

ب- البحث في المكونات المنطقية للحاسب او أي مادة معالجة بواسطة الحاسب.

ج- البحث في شبكات الحاسب الآلي، والنظم المعلوماتية[4].

---

[1] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، مرجع سابق، ص34، 36 .

[2] المرجع نفسه، ص41.

[3] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مرجع سابق، ص82.

[4] المرجع نفسه، ص76.

ونجد المشرّع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، انه يجوز للجهات القضائية وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[2].

3- ضبط الأشياء:

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشفها وسائله متعددة منها التفتيش والمعاينة وتكليف الحائز للشيء بتقديمه للمحقق، وتتمثل في:

أ- ضبط المكونات المادية للحاسب الآلي.

ب- ضبط المكونات المعنوية للحاسب الآلي.

ج- الأمر بتقديم الأشياء المراد ضبطها أو الاطلاع عليها[3].

4- ندب الخبراء:

أجاز المشرع لجهات التحقيق ندب الخبراء إذا كانت طبيعة الجريمة محل التحقيق تقتضي الاستعانة بذوي الخبرة لحسم مسألة فنية معينة، أو للبحث عن أدلة الجريمة وضبطها وللمحكمة أن تتخذ ما تراه من وسائل البحث وفهم أية واقعة فنية اعترضتها[4].

---

[1] قانون رقم 04/09مؤرخ في 14شعبان عام 1430هـ الموافق5غشت سنة 2009م، يتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته(الجمهورية الجزائرية، الجريدة الرسمية،العدد47، سنة 16غشت2009م).

[2] فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مرجع سابق، ص43.

[3] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، مرجع سابق، ص47.

[4] المرجع نفسه، ص48.

الفرع الثالث

صعوبـات الإثبـــات

الجريمة الإلكترونية هي (الجرائم النظيفة) وذلك لصعوبة اكتشاف دليل ثبوتها فلا أثر فيها لأية عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي، ومن هنا نقف على حقيقة الصعوبات التي تواجه كافة أطراف المنظومة الأمنية والقضائية في هذا الصدد[1].

وأبرز الصعوبات التي تعترض إثبات الجريمة الإلكترونية:

1- البعد الدولي: يجري النفاذ والتلاعب بالبيانات في بلد آخر وتسجل النتائج في بلد ثالث، ناهيك أنه يمكن تخزين أدلة الجريمة الإلكترونية في جهاز حاسوب موجود في بلد غير الذي ارتكب فيه المجرم الفعل، بالتالي يستطيع المجرم الإلكتروني إخفاء هويته، ونقل المواد من خلال قنوات موجودة في بلدان مختلفة، قبل الوصول إلى المرسل إليهم، نتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات، بحيث تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك.

2- مهارة التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجردة.

3 - تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال.

4- سهولة محو الأدلة في زمن قصير[2].

5- هذه البيانات توجد في شبكات لدولة أجنبية، فيستدعي تعاونها مع جهات التحقيق الوطنية.

6- صعوبة إثبات وقوع الجريمة[3].

---

[1] أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة، مرجع سابق، ص21

[2] المرجع نفسه، ص23.

[3] عبد الصبور عبد القوي علي، الجريمة الالكترونية والجهود الدولية للحد منها، (http://www.mohamoon-montada.com) ، ص6

7- صعوبة تحديد المسؤول جنائيًا عن الفعل الإجرامي.

8- صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.

9- تنازع القوانين الجنائية من حيث المكان.

10- صعوبة التوصل إلى الجاني.

11- القصور في القوانين الجنائية القائمة.

لأجل هذه الصعوبة فإن إعداد رجال الضبط الجنائي وقضاة الحكم، للبحث عن أدلة الإثبات في ميدان الجرائم المعلوماتية، يكتسب أهمية بالغة، إذ لا بد لهم من الدراية الكافية لطبيعة هذا النوع من الجرائم[1].

[1] أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة، مرجع سابق، ص23.

المطلب الثالث

موقف المشرع الجزائري من الدليل الإلكتروني في الإثبات الجزائي

إنّ النّظم القانونية التي تتبنى نظام الأدلة القانونية لا يمكن في ظلّها الاعتراف للدليل الإلكتروني بأية قيمة إثباتيه ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته في الإثبات، مهما توافرت فيه شروط اليقين، وذهب الفقه الإجرائي إلى وضع نظامين في مجال الإثبات الجزائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منهما وهذه الأنظمة هي[1]:

نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلة التي يجوز الأخذ والاستناد عليها وكذا نظام الإثبات الحر أو المطلق وفيه لا يقيد القانون القاضي بأدلة معينة في إثبات الواقعة وله أن يقتنع بأي دليل يعرض عليه، فأي من هذين النّظامين أخذ المشرّع الجزائري وما أثر ذلك على مسألة الإثبات؟، تطرقنا لأنظمة الإثبات في الفرع الأول، و موقف المشرّع الجزائري من أدلة الإثبات وأثره على الجريمة في الفرع الثاني.

الفرع الأول

أنظمة الإثبات الجزائي

أولا: نظام الإثبات المقيد أو نظام الأدلة القانونية

هذا النظام هو أن يتقيد القاضي في حكمه سواء بالإدانة أو البراءة بأنواع معينة من الأدلة طبقا لما يرسمه التشريع، فالفكرة الأساسية لهذا النظام تقوم على أنّ المشرع هو الذي يكون له الدور الأساسي في الإثبات، وذلك من خلال التحديد المسبق للأدلة المقدمة في الدعوى والتي يستند إليها القاضي الجزائي في حكمه ولا سبيل له إلى الاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات[2].

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص223.

[2] المرجع نفسه.

ثانيا: نظام الإثبات الحر أو نظام الاقتناع الشخصي للقاضي الجزائي

وفقا لهذا النظام لا يرسم القانون طرقا محددة للإثبات، إذ يتمتع القاضي الجزائي في هذا النظام بحرية مطلقة في تكوين اعتقاده من أي دليل يطرح أمامه، ومن ثمة فإن هذا النظام يقوم على خاصيتين أساسيتين[1]:

1- تتمثل في إطلاق حرية الإثبات للقاضي الجزائي انطلاقا من موضوع الإثبات في المسائل الجزائية يتعلق بوقائع مادية ونفسية لا يصلح لإثباتها مسبقا، بل إن الإثبات في هذه المسائل يكون بكافة طرق الإثبات .

2- تتمثل في حرية القاضي الجزائي في الاقتناع بالدليل المطروح عليه في جلسة المحاكمة دون أن يكون عليه أي رقيب سوى ضميره ودون أن يكون مطالبا ببيان سبب اقتناعه بدليل دون آخر.

الفرع الثاني

موقف المشرع الجزائري من أنظمة الإثبات وأثرها على الجريمة الالكترونية

نصت المادة 212 من قانون الإجراءات الجزائية[2] على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص.... "كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي قد وصلوا إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم...."[3].

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص224.

[2] المادة(112) من قانون رقم 15-02 مؤرخ في 7 شوّال عام 1436 الموافق 23 يوليو سنة 2015 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386الموافق 8 يونيو سنة 1966والمتضمن قانون الإجراءات الجزائية (الجريدة الرّسميّة للجمهوريّة الجزائرية، العدد 40 ،السنة 23يوليو2015).

[3] المادة (307) من قانون الإجراءات الجزائية، القسم الرابع، في إقفال باب المرافعة، الفصل السادس في المرافعات، ص88.

ومن خلال هذين النّصين القانونيين يتضح جليا أنّ المشرّع الجزائري قد تّبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائي، واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محدد مسبقا[1].

كما أن الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات او الجنح او المخالفات، له السلطة التقديرية المطلقة في مواجهة الأدلة المعروضة أمامه.

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع، وهذا المعنى تؤكده المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه: "لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ..."[2].

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص225.

[2] المادة(215)من قانون الإجراءات الجزائية،" لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك"، (الكتاب الثاني في جهات الحكم، الباب الأول أحكام مشتركة الفصل الأول في طرق الإثبات)، ص72.

المبحث الثاني

مواجهة الجريمة الإلكترونية والحماية الموفرة لها

التطور الحاصل في التقنيات المعلوماتية أدى إلى تطور و سائل الإجرام وهذا ما دفع بالشارع إلى التدخل وتصنيف هذه الجرائم وتقسيمها حسب الوسائل المستخدمة فيها وسن تشريعات تجرمها وتأمين الحماية لأصحاب هذه المعلومات ومستخدميها وهذا ما سوف نراه في وسائل الحماية بالمطلب الأول، والمواجهة التشريعية للجريمة الإلكترونية في المطلب الثاني، و التحديات التي تواجه الجريمة الإلكترونية في المطلب الثالث.

المطلب الأول

وسائل الحماية لتفادي الجريمة الإلكترونية

إنّ المنع الجنائي وتحديد عقوبات لجرائم المعلوماتية بصفة مسبقة بما يتماشى مع مبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار الناجمة عن هذه الجرائم من إتلاف وتدمير باهظ التكلفة في حالة الوصول إلى معلومات سرية، إلا أنه غير كاف لوحده، فحتى تكون هناك الفعالية في الحركة والأداء لابد أن تعززها حماية فنّية[1]، نتطرق إليها في الفرع الأول والحماية النظامية في الفرع الثاني، والحماية الجنائية في الفرع الثالث.

الفرع الأول

الحمايـة الفنّيـة

إنّ المحافظة على المعلومات من أهم ما تحرص عليه الهيئات والمنظمات والدول، وحتى الأفراد، لأن تعويض فقدان البيانات والمعلومات أو التلاعب بها يعد من الأمور الصعبة والمكلفة، فالمعلومات تعد من أهم ممتلكات أيِّ منظمة لذا يتم السعي للمحافظة على البيانات قدر الإمكان، ويتم إتباع مجموعة من الوسائل التي تضمن سلامة هذه المعلومات منها ما يلي:

1- الوسائل المتعلقة بالتعريف بشخص المستخدم[2]: التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام تضم كلمات السر بأنواعه البطاقات الذكية المستعملة للتعريف، كما تظم أيضا ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

2- الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة: وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة مشروعة، ومن أهم الوسائل الفنية المعتمد عليها ما يعرف بالجدران النارية وهي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت.

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص71.

[2] خالد ممدوح ابراهيم، الجرائم المعلوماتية، مرجع سابق، ص67.

3- الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين أو المصرح لهم بذلك: تهدف إلى تشفير البيانات المهمة المنقولة عبر وسائل الاتصالات كالأقمار الصناعية أو عبر الألياف البصرية بحيث يتم تشفير البيانات ،ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل.

4- وسائل مراقبة الاستخدام وتتبع سجلات النفاذ والأداء: وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

5- الوسائل التي تهدف إلى حماية التكاملية وسلامة المحتوى[1]: ومن أهمها برامج تحري الفيروسات والمقاومة لها.

6- استخدام الوسائل الحديثة التي تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي كاستخدام أجهزة التعرف على بصمة العين أو اليد أو الصوت.

7- عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة[2].

الفرع الثاني

الحمايــة النّظاميــة

هو نظام المراقبة الإلكترونية إذ يعدّ هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية ويقصد بمراقبة الاتصالات الإلكترونية، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني[3].

[1] خالد ابراهيم ممدوح، الجرائم المعلوماتية، مرجع سابق، ص68.

[2] عبد الرحمن بن عبد الله السند، وسائل الارهاب الالكتروني حكمها في الاسلام وطرق مكافحتها، مرجع سابق ص24.

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص73.

ولم يتطرق المشرّع الجزائري شأنه شأن التشريعات المقارنة إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية، مكتف فقط بتحديد مفهوم الاتصالات الإلكترونية[1] رغم أخذه بهذا النظام بموجب المادة 03من القانون 04/09[2] المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي تنص على إمكانية وضع الترتيبات التّقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها إذا تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات،

ونجد أن المشرّع الجزائري قد ميّز بين نوعين من المعطيات المعلوماتية محل المراقبة الإلكترونية، وهما المعطيات المتعلقة بحركة السيّر والمعطيات المتعلقة بمحتوى الاتصال، فبالنسبة للنوع الأول فقد عرفها المشرّع بموجب المادة 02من القانون 04/09 واعتبرها أن هذا النوع الأخير من المعطيات هو ما يكون محلا للمراقبة الإلكترونية[3]، عندما أدرجها في المادة 04[4] تحت مسمى مراقبة الاتصالات الإلكترونية، أما النوع الأول فقد خصها بإجراء آخر تحت مسمّى حفظ المعطيات المتعلقة بحركة السير في المادة 11 .

الفرع الثالث

الحمايـة الجنائيـة

أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها عبر الشبكات، وباتت الحاجة ضرورية

[1] المادة(2)، فقرة (و)من قانون 04/09، عرفت الاتصالات الإلكترونية أنها" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، ص5.

[2] قانون رقم 04/09مؤرخ في 14شعبان عام 1430هـ الموافق5غشت سنة 2009م، يتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته(الجمهورية الجزائرية، الجريدة الرسمية،العدد47، سنة 16غشت2009م).

[3] المادة(2)من قانون 04/09، المصطلحات، فقرة (هـ)(المعطيات المتعلقة بحركة السير) ص5، وخصها في المادة(11)في الفصل الثالث، القواعد الإجرائية تفتيش المنظومات المعلوماتية، ص7.

[4] المادة(2)من قانون 04/49، المصطلحات، فقرة (و)(الاتصالات الإلكترونية)ص5، وخصها في المادة(4)في الفصل الثاني، مراقبة الاتصال الإلكتروني، يتضمن 4فقرات، ص6.

لاستحداث قواعد قانونية جديرة لمواجهة هذه الجرائم، فالحماية الجنائية للمعلومات يستلزم عند تقريرها مراعاة التحول الجديد الذي أحدثته ثورة المعلومات في خصائصها لاسيما في مسألة التأثير المتطور لها، وهو أمر لا يمكن استدراكه كاملا إلا عند التعامل بالمعلومة في إطار المعالجة الآلية لها[1].

ومع ما وفرته التكنولوجيا في مجال الاتصالات الإلكترونية عن غيرها من الوسائل التقليدية للاتصال والإعلام، يتجلى لنا أمرين: الأول هو تعدد أوجه استعمالات هذه الوسائل واتساعها، والثاني هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الاستعمالات، غير أن هذه التكنولوجيا قد يساء استعمالها و يهدد استخدامها السلامة العامة والمصلحة الوطنية، فإن استعمال هذه الوسائل لا يخلو من المخاطر، فقد يستغل بعض المجرمين هذه الوسائل في ارتكاب جرائمهم بطريق الاحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم، وهو ما يعني أنّ التقدم التّقني قد أمد المجرمين بوسائل بالغة القوة والفاعلية في ارتكاب جرائمهم[2]. واختلفت التشريعات في ذلك اتّجاهين :

الاتجاه الأول:

يرى إصدار قانون يعاقب فيه على جرائم الكمبيوتر بصورها المختلفة، وتقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة مثلا "السجلات والتوقيع الإلكتروني" ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية.

الاتجاه الثاني:

من التشريعات يذهب إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى استيعاب الصور المستحدثة من الجرائم الإلكترونية، ثم تفرد هذه الخطة التشريعية قوانين خاصة ببعض الموضوعات مثل الاتصالات والتوقيع الإلكتروني والتي تتضمن نصوصا تتصل بتجريم الاعتداء على المستند الإلكتروني، ومن أمثلة التشريعات التي تبنت هذه الخطة الأخيرة القانون الألماني والفرنسي[3].

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الإنترنت، مرجع سابق، ص88-89.

[2] المرجع نفسه، ص89.

[3] المرجع نفسه، ص91.

المطلب الثاني

المواجهة التشريعية للجريمة الإلكترونية

الملاحظ في هذا الصدد أنه كلما كان الاعتماد أكبر على التقنية المعلوماتية كلما كانت الحاجة أكثر إلحاحا لوضع نصوص قانونية لحماية هذه المعلوماتية، إذ تعتبر مواجهة التشريع للاستخدام غير السوي لهذه التقنية، نتطرق فيها إلى التشريع على مستوى الداخلي للدولة(الوطني) في الفرع الاول، وعلى مستوى الاقليمي والدولي في الفرع الثاني.

الفرع الأول

على مستوى الداخلي(الوطني)

أولا: مواجهة التشريع الجزائري للجريمة الإلكترونية

لم يجد المشرّع الجزائري بدّا من تعديل قانون العقوبات[1]، بوضع نصوص جديدة تسعى إلى توفير الحماية الجزائية للأنظمة المعلوماتية المتمثل في "المساس بأنظمة المعالجة الآلية للمعطيات"[2]، والذي أفرد القسم السابع مكرر والذي تضمن ثمانية مواد (394 حتى المادة 394 مكرر 07) ونص على عدة جرائم:

1- "يعاقب بالحبس من(3) أشهر إلى سنة(1) وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات أو يحاول ذلك [3].

---

[1] قانون رقم 14-01مؤرخ في4 ربيع الثاني عام 1435 الموافق سنة2014، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم(الجريدة الرّسمية للجمهورية الجزائرية' العدد 07، سنة16فبراير2014).

[2] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في قانون الجزائري والمقارن. (ط:1، الإسكندرية: دار الجامعة الجديدة، 2008)، ص62.

[3] المادة(394)مكرر، من قانون العقوبات، ص157.

2-"يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج"، كل من يقوم عمدا وعن طرق الغش بما يأتي:

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

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[1].

3- المادة(394)مكرر5 كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

4- المادة(394)مكرر6 مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

5- المادة(394)مكرر7 يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها. وشددت العقوبة إلى الضعف إذا استهدفت الجريمة الدفاع الوطني أو المؤسسات العمومية وكذا الغرامة على الشخص المعنوي الى خمس مرات للحد الاقصى المقرر للشخص الطبيعي وذلك بعد اقرار المواد (18) مكرر ،(18) مكرر 01 ،و(51) مكرر من التعديل نفسه لمسؤولية الشخص المعنوي بوجه عام[2]، ولم يميز المشرّع الجزائري في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطالها الجريمة فيما إذا كانت معلومات تتصل بمصالح اقتصادية أو مالية أو مسائل أمنية، وذلك سعياً منه إلى تعميم الحماية للمعلومات بكافة أنواعها[3].

[1] المادة(394)مكرر2، من قانون العقوبات، ص158.

[2] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في قانون الجزائري والمقارن، مرجع سابق، ص63.

[3] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية، مرجع سابق، ص79.

ثانيا: التشريع المغربي والمصري

لم يختلف التشريع المغربي على ما نص عليه المشرع الجزائري وذلك في الباب العاشر من القانون الجنائي الفصول من3 – 607إلى11-607تحت عنوان «المس بنظام المعالجة الآلية للمعطيات» وذلك بموجب القانون رقم 07.003الصادر بتاريخ 16/6/ 1424الموافق 11/11/ 2003[1]. وأما التشريع المصري لم يعمل على سن قوانين جديدة أو تعديل إنما حاول تطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية، بتطويع نصوص قانون حماية الحياة الخاصة وقانون تجريم إفشاء الأسرار وأوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية[2].

ثالثا: التشريع في الولايات المتحدة الأمريكية

والمشرّع الأمريكي ممثلا للنّظام الإنجلوسكسوني[*]، وإذ يعد قانون فلوريدا لجرائم الحاسوب الصادر عام 1978 أول قانون في الولايات المتحدة الأمريكية يخاطب الجريمة المعلوماتية، حيث يعتبر هذا القانون أن كل دخول إلى الحاسوب غير مصرح به هو بمثابة جريمة، حتى ولو لم تكن هناك نيّة عدائية من هذا الدخول، أما على الصعيد الفدرالي فقد صدر عام 1984قانون الاحتيال وسوء استخدام الكمبيوتر وقد تم تعديله مؤخرا عام 2001 بمقتضى القانون الوطني المؤرخ في 2001/10/26وتم إدراجه في القسم 1030من الباب 18من القانون الفدرالي للولايات المتحدة الأمريكية، وتعتبر أولى الدول التي أصدرت قانون لمكافحة الإرهاب الإلكتروني، وقانون تعزيز أمن المعلومات 2002 وتأمين الفضاء الإلكتروني2003، ودعوةالبتاعون2005 على إنشاء لجنة تضم مجموعة من عباقرة الاختراق لتأمين وتحصين الفضاء الإلكتروني والشبكات الحساسة لديها[3].

---

[1] عبد الرزاق سندالي، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19-20أفريل/جوان2007، ص69.

2جعفر حسن جاسم، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، مرجع سابق، ص232.

* النظام الإنجلوسكسوني: ويسمى القانون العام أستمد من قبائل الانجليزية قديما البدائية(الانجل و السكسون)محمد سالم، تاريخ النظم المعاصرة، مؤسسة اليمامة لصحفية(الرياض)، الأحد7يونيو2013م الموافق1434/5/28هـ، العدد16449.

[3] محمد سيد سلطان، "قضايا قانونية في أمان المعلومات وحماية البيئة الالكترونية". دار ناشري للنشر الإلكتروني، الكويت، ربيع الأول1433/يناير2016، ص42.

الفرع الثاني

التشريع على مستوى الإقليمي والدولي

أولا: على المستوى الإقليمي

ما نلاحظه فيما يخص التشريع العربي هو الطابع الموحد والمشترك لنصوصه، تكاد تكون مصاغة وبنفس الكيفية ونفس النمط، ويتضح ذلك في تشريعات الأنترنيت في جميع الدول العربية تقريبا دون أدنى تمييز بينها، ويمكن أن نجمل الجرائم التي وردت في هذه التشريعات: كالآتي[1]:

1. جرائم نظم ووسائط شبكات المعلومات.
2. الجرائم الواقعة على الأموال والبيانات والاتصالات بالتهديد والابتزاز.
3. جرائم النظام العام .
4. جرائم الإرهاب والملكية الفكرية.
5. جرائم الاتجار في الجنس البشري.
6. الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجي.

إصدار "قانون نموذجي" من مجلس وزراء الداخلية العرب على صورة مشروع 2004، حول جرائم الأنترنت.

واعتمدت الجامعة العربية القانون العربي الاسترشادي[2] لمكافحة جرائم تقنية المعلومات وما في حكمها، عبر الأمانة العامة لمجلس وزراء العدل العرب، في دروته التاسعة عشر بالقرار رقم (495د-19_2003/10/08)[3]، والقانون العربي الاسترشادي للإثبات بالتقنيات الحديثة بقرار رقم (771/د24 – 2008/11/27)[4].

---

[1] أيسر محمد عطية، الإرهاب الإلكتروني وطرق مواجهته، مرجع سابق، ص41.

[2] تضمن هذا القانون 27 مادة موزعة على أربعة أبواب يعالج الباب الأول الجرائم المعلوماتية، تم النص عليها من 3إلى 22 مادة. (سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص86.)

[3] إدارة الدراسات والبحوث، دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، مرجع سابق، ص13.

[4] المرجع نفسه.

ونجد في المقابل دور المجلس الأوروبي من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات الخاصة من سوء الاستخدام والتدفق المعلومات، في1980/01/28 تم توقيع اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجات الإلكترونية للبيانات ذات الصبغة الشخصية.

وفي عام1989نشر دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب، ثم توالت الدراسات، عام 1995حول الإجراءات الجنائية في الجرائم المعلوماتية، وعلى أساس التوصيات قام المجلس الأوربي بتشكيل لجنة الخبراء الجريمة عبر العالم قصد إعداد اتفاقيات في هذا الإطار، وقد ناقش وزراء خارجية دول الاتحاد الأوربي مشروع يسمح بحماية أسس البيانات، هذا بالإضافة إلى قرارات مؤتمر قمة الدول الصناعية السبعة في فبراير من عام 1995م[1].

ولعلّ اتفاقية بودابست أصل أوروبي ذات طابع عالمي، هذا يُظهر حقيقة الاهتمام بهذا النوع من الجرائم.

ثانيا: على مستوى الدولي

– معاهدة بودابست: اتفاقية تم التوقيع عليها في2001/11/23 المتعلقة بالإجرام المعلوماتي[2] إيمانا من الدول الأعضاء في المجلس الأوربي والدول الموقعة عليها بالتغييرات الجذرية التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية، وتضمن48مادة شملت ثلاثة أقسام:

أ- مجموعة الجرائم التي يمكن أن تتعرض لها النظم المعلوماتية.

ب- مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذا النوع من الجرائم خصوصا تفتيش وضبط البيانات المخزنة في الحاسوب.

ج- التعاون الدولي بين الدول الأعضاء الموقعة على الاتفاقية.

[1] يوسف بن احمد الرميح، الارهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية، أبحاث، جامعة القصيم، ص234.

[2] مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، مرجع سابق،ص28

2- الإنتربول[1]: وقد تبلور التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجنائية Interpol (يسهل تبادل المعلومات لمساعدة وكالات لتنفيذ القانون في الولايات المتحدة وجميع أنحاء العالم في اكتشاف ومنع الجريمة والإرهاب الدولية من خلال شبكة من 187 عضوا)، التي تتولى إقامة العلاقات بين دول المنظمة، وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بجرائم المعلوماتية.

3- **الأمم المتحدة:** في عام 2000 من قبل الجمعية العامة قررت سبل مكافحة إساءة استعمال تكنولوجيا المعلومات[2].

في عام1996اعتمدت لجنة الأمم المتحدة قانون الأنسيترال الخاص بشأن التجارة الإلكترونية، الذي يعتبر من الجهود الدولية الأساسية في مكافحة الجريمة و الإرهاب الإلكتروني.

في ديسمبر 1999عقد مؤتمر دولي في الولايات المتحدة الأمريكية حول التعاون الدولي في مكافحة الجرية الإلكترونية والإرهاب.

4- الدول الثمانية: اجتماع دول الثمانية في واشنطن 1997اعتمدت عشر مبادئ لمكافحة جرائم الحاسب الآلي في أي مكان في العالم، و في ماي 2002إجتمع وزراء الدول الثمانية بكندا لإصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدود، من أجل مكافحة الأعمال الإرهابية، وفي11/مايو/2004تحسين القوانين التي تجرم إساءة استخدام الشبكات الإلكترونية.

5- دول الأوبيك: في17/نوفمبر/2004انعقد الاجتماع الوزاري لمنظمة الأوبيك في الشيلي، صدر بيان لتعزيز اقتصاديات الدول الأعضاء للقدرة على مكافحة الجريمة الإلكترونية من خلال تشريعات محلية تتفق مع أحكام الصكوك القانونية الدولية، بما فيها الجريمة الإلكترونية[3].

---

[1] THE UNITED STATES NATIONAL, CENTRAL BUREAU OF INTERPOL; U.S. Department of Justice Office of the Inspector General Audit Division Audit- Report 09-35 September 2009, P2

[2] محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، مرجع سابق، ص46.

[3] المرجع نفسه، ص47.

المطلب الثالث

التحديات التي تواجه الجريمة الإلكترونية

سنتطرق في هذا المطلب إلى مخاطر الجريمة الإلكترونية محليا وعالميا في الفرع الاول والصعوبات التي تواجه التعاون الدلي لمكافحة هذه الجريمة في الفرع الثاني.

الفرع الأول

مخاطر الجريمة الإلكترونية

أولا: على المستوى العالم

اخترنا بعض الإحصائيات فقط، وإلا فالقضية كبيرة وأكبر مما نتصور، ففي بريطانيا عام 2007 هناك جريمة إلكترونية تقع كل 10 ثواني (3 مليون جريمة في السنة، أو8 ألاف جريمة باليوم) تمثلت بين التحرش الجنسي وهي النسبة الأكبر، وسرقة الهوية لمستخدمي الأنترنت، واختراق للحواسيب بهدف السرقة والتخريب والسطو على أرقام بطاقات الائتمان، وتقول شركات التأمين أنّ 70%من هذه الجرائم تستهدف الأفراد[1].

وقد تتجاوز نتائج هذه الجرائم إلى وقوع جرائم أخرى تهدد الحق في الحياة والسلامة البدنية، إذا ما أدى العبث في المعلومات إلى تغيير طريق العلاج أو تركيبة الدواء.

في أحدث تقارير مركز شكاوى احتيال الإنترنت (IFFC) الأمريكي، أظهر التحليل الشامل للشكاوى التي قدمت للمركز، أنّ عدد الشكاوى التي تلقاها المركز خلا ستة أشهر من عملها قد بلغت 6087 شكوى، من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الإنترنت و814 تتعلق بوسائل الدخول، مع الإشارة إلى أنّ هذه الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل

[1] سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها،(http://iasj.net/iasj?func=fulltext&aId=28384) تاريخ استلام البحث 2010/9/20، تاريخ النشر: 2011/5/4، ص4.

الأرقام الحقيقية لعدد حالات الاحتيال الفعلي[1].

وكشفت تقارير دولية حديثة لحماية الشبكة الإلكترونية، أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم، يبلغ 114 مليار دولار، مؤكدة في الوقت ذاته وقوع نحو 500 مليون بالغ ضحية التهديدات الإلكترونية، أي ما يعادل مليون ضحية يوميا، كما أكدت التقارير ذاتها وجود 14 ضحية في الثانية، وكلفة الجرائم تجاوزت 288 مليار دولار[2].

جدول يلخص جريمة نشر المواقع الاباحية التي تهدم القيم والمبادئ لدى الافراد والمجتمعات [3]

المواقع	الصفحات	البحث عن المواقع	الرسائل الالكترونية اليومية	المشاهدة	استقبال غير مرغوب	متوسط ما يتلقاه كل مستعمل	التحميل	عرض الشذوذ للأطفال	عدد الزوار عالميا	المبيعات على النت
4.2مليون 12%	420مليون صفحة	68مليون 25%	2.5 مليون 8%	42.7 %	%34	4.5 رسالة الكترونية	1.5بليون 35%	100 ألف موقع	72مليون شهريا	$4.9 مليار دولار

الجدول الثاني[4]:

الفئة العمرية المتداولة	مشاهدة البالغون في العمل	مشاهدة البالغات في العمل	نسبة الاستدراج	المصابون بفقد المناعة	مشاهدة بالغو امريكا باستمرار	رسال الاغواء مسلمة للشباب
12-17سنة	%20	%13	%89	13مليون	40مليون	%20

كانت هذه الاحصائيات 2004، علما إن الإقبال على الشبكة الأنترنت يتضاعف كل مائة يوم، إذ بلغ عدد هذه المواقع 43 مليون موقع إباحي، أي بنسبة13% من مجمل المواقع العالمية

[1] يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل الى مؤتمر الامن العربي2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10، 2002/2/12، ص01.(تمهيد)

[2] المرجع نفسه.

[3] بن يحي الطاهر ناعوس، مكافحة الارهاب الالكتروني ضرورة بشرية وفريضة شرعية، ص8 .

[4] ميلود بن عبد العزيز، "الجرائم الاخلاقية والاباحية عبر الانترنت وأثرها على المجتمع من منظور شرعي وقانوني"، مجلة الواحات للبحوث والدراسات،، جامعة غرداية، العدد17،ت.ن 2012، ص167.(http://elwahat.univ-ghardaia.dz)

للإنترنت، عدد زوارها سنويا 73مليون زائر، وبلغت مشتريات هذه المادة في الإنترنت 8%من التجارة الإلكترونية والبالغ دخلها 18مليار دولار، كما بلغت مجموع الأموال المنفقة على دخول للصفحات 3مليار دولار عام2003م[1].

ثانيا: على المستوى المحلي(الجزائر)

كشفت تقارير دولية حديثة لحماية الشبكة الإلكترونية، أن المعدل السنوي لتكلفة الجرائم الإلكترونية حول العالم، يبلغ 114 مليار دولار، مؤكدة في الوقت ذاته وقوع نحو 500 مليون بالغ ضحية التهديدات الإلكترونية، أي ما يعادل مليون ضحية يوميا، كما أكدت التقارير ذاتها وجود 14 ضحية في الثانية، وأن كلفة الجرائم الإلكترونية تبلغ 288 مليار دولار، وأن ثلثي البالغين حول العالم أي 69 % كانوا ضحايا للجرائم الإلكترونية، هذه التهديدات قد وجدت ضالتها في الجزائر، حيث تحتل هذه الأخيرة مراتب أولى إفريقيا وعربيا من حيث الجريمة الإلكترونية، بنسبة 85 % في القرصنة والجريمة الإلكترونية، ما جعلها من بين أبرز عينات واهتمامات تقارير المنظمات والهيئات الدولية المختصة.

حيث تؤكد الإحصائيات وجود أكثر من 300 قضية سنوية، وما يزيد عن 100 قضية خلال 8 أشهر المنصرمة من العام 2014، ومع دخول الجزائر عالم التقنية والبدء في استخدام تقنية الجيل الثالث للهاتف النقال والجيل الرابع بالنسبة للشبكة العنكبوتية سيجد القراصنة والمجرمون الالكترونيون مساحة واسعة وسانحة تسهل من مهامهم ولصوصيتهم على الأنترنت، فمنهم من تكون جريمته الالكترونية فضولا أو تحد وأحيانا تصنف ضمن قضايا الانتقام[2].

كما أن 90 بالمائة من بين أكثر من 4 ملايين مشتركا جزائريا في الانترنت لا تتجاوز أعمارهم 35 سنة، وهذا ما يجعل العمل على هذه المواقع سريعا وأكثر تأثيرا، وعلى الجزائر أن تتدارك الوضع، فإن الأمور تخرج من بين يديها لتصير فردوسا لمجرمي الأنترنت، خاصة أن فيها شريحة كبيرة من

[1] ميلود بن عبد العزيز، "الجرائم الاخلاقية والاباحية عبر الانترنت وأثرها على المجتمع من منظور شرعي وقانوني"، مرجع سابق، ص167-166.

[2] يونس قرار، "لصوص تغلبوا على المراسيم وأهملت سُبل تجسيد القانون"، صحيفة الشروق اون لاين، 27-10-2014 20:30. (www.echoroukonline.com)

الشباب الباحث عن المال وعن الوثائق الرسمية طلبا للهجرة، وهو الأمر الذي يوجه هؤلاء نحو ارتكاب جرائم تزوير الوثائق الرسمية والحصول على المال عن طريق استخدام الكمبيوتر واختراق حسابات المصارف والأشخاص[1].

الفرع الثاني

الصعوبات التي تواجه التعاون الدولي في مكافحة الجريمة الإلكترونية

رغم الجهود المبذولة للحد من الجرائم الإلكترونية المرتكبة سواء كانت من المشرّعين أو من طرف سلطات التحقيق والضبطية القضائية، دوليا كانت أو داخلية، إلا أن هذه الجهود تصطدم بعدة عراقيل وصعوبات، تجعل هذا التعاون ليس بالأمر السهل وذلك من عدة جوانب نذكر منها:

1- عدم وجود نموذج موحد للنشاط الإجرامي، إذ لم تتفق الأنظمة القانونية في بلدان العالم على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة المعلوماتية، يغري قراصنة الحاسب الآلي على ارتكاب جرائمهم دون قيد بالحدود الجغرافية.

2- اختلاف النظم القانونية الإجرائية، إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها.

3- صعوبة اكتشاف وإثبات الجريمة الإلكترونية كون محلها معلومات أو برامج عبر الحواسيب، وعابرة للحدود، مما يقودنا لصعوبة اكتشافها ومن ثم إثباتها.

4- مقارنة بتطور الجريمة واختراقها الحدود الإقليمية، فالتعاون بين الدول قاصر ولم يتطور بتطور التقنية، مما يولد الفارق، وبطء الإجراءات المتبعة، ويرجع هذا القصور إلى:

- عدم وجود قنوات اتصال بين الدول.

- مسألة الاختصاص في الجرائم المتعلقة بالمعلومات على المستوى المحلي والدولي[2].

---

[1] طهاري عبد الكريم، "الجريمة الإلكترونية في رسالة ماجستير"، صحيفة الخبر، نشر في يوم 01/21 / 2015.

[2] صغير يوسف، الجريمة المرتكبة عير الانترنت، مرجع سابق، ص136-137

خـاتمــة

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على من ختمت ببعثته الرسالات نبينا محمد وعلى آله وصحبه وسلم تسليما كثيرًا.

يتجلى لنا من خلال دراستنا للجريمة الإلكترونية أنها من أكثر الجرائم التي عرفها العالم الحديث خطورة، وذلك لما تتسم به هذه الجريمة من اختلاف عن الجرائم المعروفة في العالم التقليدي، حيث غيرت هذه الأخيرة النظرة التقليدية التي كان ينظر بها إلى الجريمة على العموم، فهذا النوع من الإجرام ظهر معه مفهوم جديد لهذه الظاهرة لم يكن يعرفه القانون من قبل، وهذه مجموعة من أبرز النتائج المتوصل إليها بعد الخوض في غمار هذا البحث:

– تميزت الجريمة الإلكترونية بصعوبة وضع تعريف موحد لها، فقد تعددت التعريفات واختلفت في وصف هذه الظاهرة، والجرائم الإلكترونية بمختلف وسائلها هي الأفعال المخالفة للشريعة الواقعة على معطياته أو بواسطته .

– تميزت الجريمة الإلكترونية بمجموعة من الخصائص تتعلق بجميع جوانب الجريمة، من أبرزها، طابعها العابر للحدود وارتكابها في العالم الافتراضي وانعدام الآثار التقليدية لها، بالإضافة إلى ضعف مستوى القائمين على مكافحتها بالنظر إلى التطور المتسارع في ارتكابها.

– الجرائم الإلكترونية جديدة ولم يتناولها القانون الجنائي التقليدي، وبالتالي لا يوجد نصوص في قانون العقوبات تتعلق بالجريمة الإلكترونية وبالتالي من الصعوبة بمكان إصدار أحكام بحق مرتكبيها.

– أن من مقاصد الشريعة الحفاظ على الضروريات الخمس، حيث أوجد من الأحكام ما يحفظ على الناس أنفسهم وأعراضه وأموالهم وعقولهم، ومنع الاعتداء عليها، كان تجسسا على الأخبار أو سبا أو قذفا عبر البريد الإلكتروني، وأن التحايل والغش الوارد على المعلومات من سبل التحايل على الله ورسوله، فهي معصية و خيانة تلزم صاحبها العقوبة.

– مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها وتتعدد العقوبات في بعض الدول بدءا من الحبس، والغرامة، والفصل من الوظيفة، والحكم مخول للقاضي في وضع العقوبة المناسبة.

في ظل التقدم العلمي والتقني الذي فتح آفاقا جديدة وجلب معه مشكلات ومخاطر جديدة، أصبح لزاما على الجهات الأمنية والتشريعية والقضاء أن تطور أساليبها ووسائلها كي تتمكن من التعامل والتعايش مع عصر الثورة المعلوماتية، وقد تمخّضت هذه الدراسة عن عدد من التوصيات اللازمة للتصدي لهذه الجرائم والمخالفات، وهي:

– ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية.

– ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت.

– يلزم تعديل قوانين ونظم الإجراءات الجزائية، بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها.

– بشيء من المراقبة، وبشيء من التوجيه والإرشاد و التوضيح، يمكن أن نستفيد من هذه المعلوماتية ونحفظ مجتمعاتنا و أبناءنا، ونعزز الحوار الودي بين الآباء و الأبناء، ورفع مستوى الوعي والإدراك لدى الأطفال تجاه ما يمكن أن يصلهم من محتوى غير لائق.

– من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية؛ وخصوصا الإنتربول، وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

والحمد لله من قبل ومن بعد، ونستغفر الله من الزلل والخطأ، فجل من لا عيب فيه وعلا؛ وصلى الله وسلم على نبينا محمد وعلى آله وصحبه أجمعين.

فهرس الآيات القرآنية

الآية	رقم الآية	الصفحة
سورة البقرة		
﴿ وَٱسۡتَشۡهِدُواْ شَهِيدَيۡنِ مِن رِّجَالِكُمۡۖ ..... ﴾	282	43
سورة النساء		
﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُونُواْ قَوَّٰمِينَ بِٱلۡقِسۡطِ.....﴾	135	44
سورة المائدة		
﴿ وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقۡطَعُوٓاْ أَيۡدِيَهُمَا .....﴾	38	32
سورة الأنعام		
﴿ مَّا فَرَّطۡنَا فِي ٱلۡكِتَٰبِ مِن شَيۡءٖۚ ﴾	38	أ
سورة طه		
﴿ فَٱقۡذِفِيهِ فِي ٱلۡيَمِّ ﴾	39	30
سورة النور		
﴿ وَٱلَّذِينَ يَرۡمُونَ ٱلۡمُحۡصَنَٰتِ .....﴾	04	30
سورة الذاريات		
﴿ وَمَا خَلَقۡتُ ٱلۡجِنَّ وَٱلۡإِنسَ إِلَّا لِيَعۡبُدُونِ ﴾	56	أ

فهرس الأحاديث

فهرس النصوص القانونية

فهرس المصادر والمراجع

أولا: القرآن الكريم على رواية حفص

ثانيا: كتب الحديث

02	محمد بن إسماعيل أبو عبد الله الجعفري البخاري ت 256هـ	صحيح البخاري، كتاب الوصايا، باب قول الله تعالى (إن الذين يأكلون أموال اليتامى ظلما إنما يأكلون في بطونهم نارا)
		كتاب الخصومات، باب الربط والحبس في الحرم
		كتاب الحدود، باب كم التعزير والأدب، رقم(6848)
		كتاب الأدب، باب ما ينهى من السباب واللعن، رقم(6050)
		الجامع الصحيح المختصر. تحقيق: د. مصطفى البغا، ج6(ط:3؛بيروت:دار بن كثير، ودار اليمامة، 1407هـ/1987م) كتاب التفسير، باب: سورة آل عمران
03	مسلم بن حجاج النيسابوري، ت261هـ	صحيح مسلم، كتاب الإمارة، باب حكم من فرق أمر المسلمين وهو مجتمع، رقم(4904)
04	ابن ماجة أبو عبد الله محمد بن يزيد القزويني، ت273هـ	سنن ابن ماجة، كتاب الأحكام، باب من بنى في حقهما يضر جاره، رقم الحديث 2340
05	أحمد بن حسين البيهقي ت 458هـ	السنن الكبرى. تحقيق: محمد عبد القادر عطا، ج10(لا:ط؛ مكة المكرمة: مكتبة دار الباز،1414هـ/1994م) كتاب الدعوى والبيانات، باب البينة على المدعى واليمين على المدعى

ثالثا: الكتب الشرعية

06	علي بن محمد الماوردي	الأحكام السلطانية.(ط:1؛ الكويت: مكتبة دار ابن قتيبة، 1989)
07	بكر بن عبد الله أبو زيد	الحدود والتعزيرات عند ابن القيم.(ط:2؛ المملكة العربية السعودية: دار العاصمة، 1994)
08	أبي محمد عبد الوهاب البغدادي المالكي	التلقين في الفقه المالكي. تحقيق: محمد ثالث سعيد الغاني، ج2(ط:1؛ مكة المكرمة: جامعة أم القرى، 1986/1985)
09	عبد القادر عوده	التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي.ج1(لا.ط؛ بيروت: دار الكاتب العربي، د.ت)
10	محمد أبو زهرة	الجريمة والعقوبة في الفقه الإسلامي. (لا.ط؛ القاهرة: دار الفكر العربي، د.ت)
11	سعدي ابو حبيب	موسوعة الإجماع في الفقه الإسلامي. ج2(ط:3؛ دمشق:لا.ن، 1996)
12	أبي إسحاق إبراهيم بن علي بن يوسف الفيروزابادي الشيرازي	المهذب في فقه الإمام الشافعي. ج3(ط:1؛ بيروت: دار الكتب العلمية، 1995)
13	جمع من العلماء	الموسوعة الفقهية، إصدار وزارة الأوقاف والشئون الإسلامية. ج33(ط:2؛ الكويت: دار الصفوة للطباعة، 1995)
14	محمد صدقي بن أحمد بن محمد آل بورنو ابو الحارث الغزي	الوجيز في إيضاح قواعد الفقهية الكلية. (ط:4، بيروت: مؤسسة الرسالة، 1416هـ)
15	خسرو الحنفي	الدرر الحكام في شرح غرر الأحكام. ج2(لا.ط؛ لا.م: لا.ن، د.ت)

رابعا: المعاجم

16	إسماعيل بن حماد الجوهري	الصحاح. تحقيق: أحمد عبد الغفور عطار، ج5(ط:4؛ بيروت: دار العلم للملايين، 1990)

خامسا: الكتب القانونية والعلمية

17	الجريدة الرسمية للجمهورية الجزائرية	قانون العقوبات، قانون رقم 14-01 المؤرخ في4 ربيع الثاني عام 1435 الموافق سنة2014، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18صفر عام 1386 الموافق 8 يونيو سنة 1966 العدد 07، سنة16فبراير2014
		قانون الإجراءات الجزائية، قانون رقم 15-02 المؤرخ في 7 شوّال عام 1436 الموافق 23 يوليو سنة 2015 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386الموافق 8 يونيو سنة 1966، العدد 40 ،سنة 23يوليو2015
		القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها قانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق 05 أوت 2009م، العدد 47، سنة 16 أوت 2009
18	رئاسة الجمهورية، الأمانة العامة للحكومة	قانون العقوبات لسنة 2015
		قانون الإجراءات الجزائية لسنة 2014
19	علي جبار الحسيناوي	جرائم الحاسوب والإنترنت. (ط:1؛ الأردن: دار اليازوري العلمية، 2009)
20	منصور رحماني	الوجيز في القانون الجنائي العام. (لا.ط؛ عنابة: دار العلوم للنشر والتوزيع، 2006)
21	خالد ممدوح إبراهيم	الجرائم المعلوماتية. (ط:1؛ الإسكندرية: دار الفكر الجامعي، 2009)
22	جلال محمد الزعبي	جرائم تقنية نظم المعلومات الإلكترونية. (ط:1؛ عمان – الأردن: دار الثقافة، 2010)
23	منير محمد الجنيبهي وممدوح محمد الجنيبهي	جرائم الإنترنت والحاسب الآلي. (لا.ط؛ الإسكندرية: دار الفكر الجامعي، 2005)
24	محمد سعيد عبد المجيد	المعلوماتية والجريمة. (ط:1؛ مصر: دار ومكتبة الإسراء، 2006)
25	خالد ممدوح إبراهيم	فن التحقيق الجنائي في الجرائم الإلكترونية. (ط:1؛ مصر: دار الفكر الجامعي، 2010)
26	جعفر حسن جاسم	جرائم تكنولوجيا المعلومات. (لا.ط؛ الجماهرية الليبية: دار البداينة، 2006)
27	أمين الشوابكة	جرائم الحاسوب والإنترنت، (ط:1؛ عمان – الأردن: دار الثقافة، 2007)
28	عبد الرحمان بن عبد الله السند	وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها. (لا.ط؛ لا.م، لا.ن، د.ت)

29	خالد ممدوح إبراهيم	الجرائم المعلوماتية. (ط:1؛ الإسكندرية: دار الفكر الجامعي، 2009)
30	ممدوح محمد الجنيبهي ومنير محمد الجنيبهي	أمن المعلومات الإليكترونية. (لا.ط؛ الإسكندرية: دار الفكر الجامعي، 2005)
31	حسن طاهر داود	جرائم نظم المعلومات. (ط:1؛ الرياض، المملكة العربية السعودية: لا.ن، 2000)
32	نهلا عبد القادر المومني	الجرائم المعلوماتية. (ط:1؛ عمان-الأردن: دار الثقافة، 2008)
33	محمد خليفة	الحماية الجنائية لمعطيات الحاسب الآلي في قانون الجزائري والمقارن. (ط:1، الإسكندرية: دار الجامعة الجديدة، 2008)
34	محمد سيد سلطان	"قضايا قانونية في أمان المعلومات وحماية البيئة الالكترونية". دار ناشري للنشر الإلكتروني، الكويت، ربيع الأول1433/يناير2016
35	بن يحي الطاهر ناعوس	مكافحة الارهاب الالكتروني ضرورة بشرية وفريضة شرعية. (لاط؛ لا.م، لا.ن، د.ت)
36	عوض عبد الله أبو بكر	نظام الإثبات في الفقه الإسلامي، (لا: ط، المدينة المنورة، مجلة الجامعة الإسلامية، د.ت)

سادسا: المذكرات الجامعية

37	صغير يوسف	الجريمة المرتكبة عبر الإنترنت. (رسالة ماجستير في تخصص القانون الدولي للأعمال) كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013
38	عبير علي محمد النجار	جرائم الحاسب الآلي في الفقه الإسلامي. (رسالة ماجستير في تخصص الفقه المقارن)، كلية الشريعة والقانون، الجامعة الإسلامية، غزة،2009
39	أمال قارة	الجريمة المعلوماتية. (رسالة ماجستير في تخصص القانون الجنائي والعلوم الجنائية)، كلية الحقوق، جامعة الجزائر، بن عكنون، 2002/2001
40	رصاع فتيحة	الحماية الجنائية للمعلومات على شبكة الإنترنت. (رسالة ماجستير في تخصص القانون العام)، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2012/2011

41	سعيداني نعيم	آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير في العلوم القانونية تخصص علوم جنائية)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013/2012
42	عبد الله دغش العجمي	المشكلات العملية والقانونية للجرائم الإلكترونية. (رسالة ماجستير في تخصص القانون العام)، جامعة الشرق الأوسط، الكويت، 2014
43	دردور نسيم	الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن. (رسالة ماجستير في تخصص القانون الجنائي)، كلية الحقوق، جامعة منتوري، قسنطينة، 2013/2012
44	سمية مزغيش	جرائم المساس بالأنظمة المعلوماتية. (مذكرة ماستر في تخصص قانون جنائي)، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014/2013
45	حمزة بن عقون	السلوك الإجرامي للمجرم المعلوماتي. (رسالة ماجستير في تخصص علم الإجرام وعلم العقاب)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2011

سابعا: المقالات والبحوث العلمية

46	عادل يوسف عبد النبي الشكري	"الجريمة المعلوماتية وأزمة الشرعية الجزائية". الكوفة–العراق، العدد:7، 2008
47	فشار عطاء الله	"مواجهة الجريمة المعلوماتية في التشريع الجزائري" الملتقى المغاربي حول القانون والمعلوماتية،أكاديمية الدراسات العليا، ليبيا، 2009
48	وليد العاكوم	"مفهوم وظاهرة الإجرام المعلوماتي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون، المجلد:1، 2004
49	إدارة الدراسات والبحوث بالمملكة العربية السعودية	"دراسة بعنوان دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"، 2012
50	محمد عبد الرحمان	"جرائم الإنترنت والاحتساب عليها". بحوث مؤتمر القانون والكمبيوتر والإنترنت من 1 – 3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد: 3، 2004

51	هشام محمد فريد رستم	"الجرائم المعلوماتية، أصول التحقيق الجنائي الفني" بحوث مؤتمر القانون والكمبيوتر والإنترنت من 1-3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد:2، 2004
52	صالح بن محمد المسند، د. عبد الرحمن بن الراشد المهيني	"جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات"، المجلة العربية للدراسات الأمنية والتدريب مجلد15، العدد29
53	إسماعيل عبد النبي شاهين	"أمن المعلومات في الإنترنت بين الشريعة والقانون"، بحوث مؤتمر القانون والكمبيوتر والإنترنت(من 1-3 2000)، جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون، المجلد: 3، 2004
54	لجنة الفتوى بالشبكة الإسلامية	فتاوى الشبكة الإسلامية، أرشيف لجميع الفتاوى العربية ، طب وإعلام وقضايا معاصرة3436، وسائل إعلام واتصال1128، 2009/11/18.
55	علي حسن طوالبة	التعاون القضائي الدولي في مجال مكافحة الجريمة الالكترونية، مركز الإعلام الأمني البحرين
56	أيسر محمد عطية	دور الآليات الحديثة من الجرائم المستحدثة الإرهاب الالكتروني وطرق مواجهته، (ملتقى علمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية الدولية، 2-2013/9/4م)
57	مفتاح بوبكر المطردي	الجريمة الالكترونية والتغلب على تحدياتها، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23-2012/09/25
58	عبد الرزاق سندالي	أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19-20أفريل/جوان2007
59	يوسف بن احمد الرميح	الإرهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية، أبحاث، جامعة القصيم
60	يونس عرب	جرائم الكمبيوتر والانترنت، ورقة عمل إلى مؤتمر الأمن العربي2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10، 2002/2/12
61	ميلود بن عبد العزيز	"الجرائم الأخلاقية والإباحية عبر الانترنت وأثرها على المجتمع من منظور شرعي وقانوني"، مجلة الواحات للبحوث والدراسات، جامعة غرداية العدد17، 2012.

62	يونس قرار	"لصوص تغلبوا على المراسيم وأهملت سُبل تجسيد القانون"، صحيفة الشروق اون لاين، 27-10-2014
63	طهاري عبد الكريم	"الجريمة الإلكترونية في رسالة ماجستير"، صحيفة الخبر، نشر في يوم 01/21 / 2015
64	محمد سالم	تاريخ النظم المعاصرة، مؤسسة اليمامة لصحفية(الرياض)، الأحد7يونيو2013م الموافق1434/5/28هـ، العدد16449

ثامنا: المراجع الأجنبية

65	THE UNITED STATES NATIONAL, CENTRAL BUREAU OF INTERPOL; U.S. Department of Justice Office of the Inspector General Audit Division Audit- Report 09-35 September 2009, P2

تاسعا: مواقع الإنترنت

66	محمد عبد الله منشاوي	جرائم الإنترنت من منظور شرعي وقانوني. (**mohammed@minshawi.com**)
67	عبد الصبور عبد القوي علي	الجريمة الالكترونية والجهود الدولية للحد منها، (http://www.mohamoon-montada.com)
68	سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن	الجريمة الإلكترونية عبر الإنترنت أثرها وسبل مواجهتها،(http://iasj.net/iasj?func=fulltext&aId=28384) تاريخ استلام البحث 2010/9/20، تاريخ النشر: 2011/5/4

فهرس الموضوعات