جامعة أحمد بن يحي الونشريسي
كلية الحقوق
قسم القانون العام

الجـــريمة الالكترونيـة في التشـريع الجزائري

مطبوعة بيداغوجية موجهة لطلبة السنة:
الثالثـــة قانـــــون عام

الدكتور/ الطاهر عليليش

السنة الجامعية: 2023-2024

الجريمة ظاهرة قديمة، عرفتها المجتمعات البشرية منذ القدم، وظهرت في هذه المجتمعات السلطة الحاكمة انطلاقا من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لاستتباب الأمن لدى الفرد والمجتمع، واعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله وسلامته الجسدية، فعل محرم يستحق العقاب عليه.

لكن بعد ظهور فكرة الدولة تولت بنفسها سلطة تحريم الأفعال والعقاب عليها، حيث أصدرت تشريعات منها ما هو موضوعي" قانون العقوبات"، الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي " قانون الإجراءات الجزائية " الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان، قد حددت كليات خمس لا تستقيم الحياة إلا بها، وهي حفظ الدين، حفظ النفس، حفظ العقل، حفظ النسل، حفظ المال، وبينت أن مسألة المحرم

تكون استنادا لمبدأ حرية الاختيار، قال تعالى : " إن الذين كذبوا بآياتنا واستكبروا عنها لا تفتح لهم أبواب السماء ولا يدخلون الجنة حتى يلج الجمل في سم الخياط وكذلك نجزي المجرمين. "[1]

غير أنه بتطور الإنسان في شتى الميادين، خصوصا في مجال التقنية، إذ ظهر الحاسب الآلي وشبكة الأنترنت، وغزت هذه الوسيلتين جميع المجالات نظرا لما تتسم به من الدقة والسرعة، وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المحرمين، وهو الإنعكاس السلبي لهذه الثورة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية، فهذه التقنية تسمح بنقل المعلومة صوتا وصورة عبر الأنترنت، وفي أي مكان من العالم، مما يسمح

[1] سورة الأعراف، الآية 40.

للـبعض اسـتغلال هـذه الشـبكة فـي ارتكـاب جـرائمهم، وهـذا يعتبـر خطـر يهـدد المجتمـع والعـالم ككـل، وهـذا مـا يعطـي أهميـة كبيـرة للموضـوع يسـتدعي دراسـة هـذه الظـاهرة المسـتجدة باعتبارهـا ثابـت غيـر معروفـة فـي القـانون الجنـائي، لـذا كـان اهتمـامي بالبحـث فـي موضـوع الجريمـة الإلكترونيـة، بغيـة شـرح وتحليـل المفـاهيم القانونية المتعلقة بها.

و هـدفي مـن دراسـة الموضـوع هـو إثـراء المكتبـة وسـد الـنقص فـي المراجـع المتخصصـة فـي هـذا المحـال، ومحاولـة دراسـة الظـاهرة وتحليلهـا وبيـان كيفيـة مكافحتهـا، غيـر أنـه قـد واجهتنـي بعـض الصـعوبات فـي إنجـاز البحـث، كـون أن الموضـوع لـه علاقـة بالجانـب التقنـي والفنـي، وهـذا مـا يسـتدعي التخصـص للإلمـام أكثر بالموضوع.

والإشـكال الـذي يطـرح فـي هـذا الصـدد هـو : هـل التـدابير والإجـراءات المتاحـة لمراقبـة الأنظمـة المعلوماتيـة وضـمان حمايـة المسـتخدمين كفيلـة لمواجهـة خطـر الجريمـة الإلكترونيـة؟ ومـا هـي الاسـتجابات الجزائيـة للمشـرع الجزائـري فـي هـذا الشـأن؟ للإجابـة عـن هـذه الإشـكالية الجوهريـة، لابـد بالبحـث فـي بعـض التسـاؤلات التـي تتفـرع عنهـا والتـي مـن بينهـا، مـا الإطـار المفـاهيمي للجريمـة الإلكترونيـة مقارنـة بالجريمـة التقليديـة؟ مـا إجـراءات البحـث والتحـري عـن الجريمـة الإلكترونيـة؟ ومـا طبيعـة الـدليل المناسـب لإثباتهـا؟ ومـاهي الصـعوبات التـي تحـول دون مكافحتها ؟

لقد شهد العالم في الآونة الأخيرة تطور ملحوظ في مجال التقنية، مما نتج عنه استعمال الحاسب الآلي وشبكة الأنترنت في جميع الميادين، لكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة، الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال، وهو ما يعرف بالجريمة الإلكترونية، ونظرا لحداثة هذه الجريمة، فقد اختلف الفقهاء في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص، وعرفت نوع جديد من المحرمين لهم عدة دوافع لارتكاب هذه الجريمة، وسأحاول التطرق في هذا الفصل إلى مفهوم الجريمة الإلكترونية في المبحث الأول، وبيان خصائص و أنواع الجريمة الإلكترونية في القانون الجزائري من خلال المبحث الثاني.

المبحث الأول : مفهوم الجريمة الإلكترونية..

من خلال هذا المبحث سأحاول التعرض إلى التعاريف المختلفة للجريمة الإلكترونية وكذا الأركان التي ترتكز عليها وبيان الدوافع المؤدية لارتكابها، نظرا لطبيعتها الخاصة باعتبارها تقع في العالم الإفتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس، وذلك من خلال المطلبين المواليين:

المطلب الأول: تعريف الجريمة الإلكترونية وأركانها.

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والإتصال، جرائم الكمبيوتر والأنترنت الجرائم المستحدثة[1]، الجريمة الناعمة، إحرام ذوي الياقات البيضاء[2]. وتجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات

[1] عادل يوسف عبد النبي الشكري، بحث بعنوان: الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة ، 2008 ، ص 112.

[2] مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية، 2012، العدد 21، ص 08.

المخزنة به، فإن جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والإتصالات) وظهور مصطلح cybercrime[1] وقد انقسم الفقهاء إلى اتجاهين، منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، ومنهم من ينظر إليها بمفهوم واسع، كما أن للجريمة الإلكترونية أركان لا تقوم الجريمة إلا بتوافرها، وهذا ما سأتناوله في الفرعين المواليين.

الفرع الأول: تعريف الجريمة الإلكترونية.

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للإختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع، وسأحاول التعرض لهذه التعاريف من خلال البندين المواليين.

البند الأول: الإتجاه المضيق من تعريف الجريمة الإلكترونية.

يعرف أنصار هذا الإتجاه الجريمة الإلكترونية بأنها، كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية الملاحقته وتحقيقه من ناحية أخرى[2]. " حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط 2 لارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها. وهذا التعريف يضيق بدرجة كبيرة من الجريمة الإلكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو

[1] مفتاح بوبكر المطرودي الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث الرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23/25/2012، ص 13.

[2] حمزة بن عقون السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة 2011/2012، ص 13، نقلا عن قورة نائلة، جرائم الحاسب الاقتصادية، القاهرة، 2004. ض 21 .

هي الفعل الإحرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية. كما يرى الأستاذ tredmann أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[1].

ويرى الاستاذ rosenblatt بأن الجريمة الإلكترونية هي نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه "[2].

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التحريم. ويرى الأستاذ باركار أن الجريمة الإلكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[3].

البند الثاني: الإتجاه الموسع من تعريف الجريمة الإلكترونية.

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب[4].

---

[1] حمزة بن عقون الرسالة السابقة الذكر، ص 14، نقلا عن أحمد هلالي عبد اللاه، ص 13.

[2] حمزة بن عقون، نفس الرسالة، ص 14، نقلا عن يونس غرب دليل أمن المعلومات والخصوصية، ص 213.

[3] محمد أمين أحمد الشوابكة جرائم الحاسوب والأنترنت مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط 1 ، ص 8-9.

[4] سميرة بنظام الجريمة الإلكترونية وتقنية الإجرام المستحدث من 01/04

culture/net.alukah.www//http/br 2016/11/30. 2030.

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات، أو بيانات أو برامج، أو محوها، أو كتابتها، أو أي تدخل آخر في مجال إنجاز البيانات، أو معالجتها وتبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر[1].

ودائما حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة[2]. أما البعض من الفقهاء يعرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسوب الآلي الرقمي و شبكة الأنترنت بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف[3].

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا تكون أمام جريمة

---

[1] مليكة عطوي المحلة السابقة الذكر، ص 09، نقلا عن الطاهر رواينية، المسائلة، مقال، العدد 01، 1991، ص 15

[2] كامل فريد السالك الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية حلب 21/23/ تشرين الأول، 2000، بدون صفحة.

[3] صغير يوسف الجريمة المرتكبة عبر الأنترنت مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال جامعة مولود معمري تيزي وزو 06/03/2013، ص 09، نقلا عن كحلوش على جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني، العدد 84، 2007، ص 51.

إلكترونية، كمن يقوم بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك.

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04[1] على أنها: "جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية".

2 من خلال هذا التعريف نستنتج أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي التحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات[2] من المادة 394 مكرر إلى 394 مكرر 07، وترك المجال واسع لإي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[3]. ومن أمثلة الجريمة الإلكترونية المرتكبة في

---

[1]القانون رقم 09-04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج و العدد 47.

[2]القانون رقم 04-15 الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66/156، الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج والعدد 71.

[3]سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة ابوبكر بلقايد، تلمسان، 201116-2010 ، ص من 14 إلى16

الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية[1]."

الفرع الثاني: أركان الجريمة الإلكترونية.

إن للجريمة الإلكترونية أركان ثلاثة وتتمثل في الركن الشرعي وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

أما الركن المادي يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي، وأخيرا الركن المعنوي وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني (المحرم الإلكتروني) وبهذا المعنى يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي ، أما المجني عليه يكون في الغالب الأعم شخص معنوي، كالبنوك والشركات وغيرها من المنظمات والهيئات التي تعتمد في إنجاز أعمالها على الحاسب الآلي، علما أن للجريمة الإلكترونية محلا يتمثل في المعلومات، الأجهزة، الأشخاص أو الجهات[2]."

المطلب الثاني: دوافع ارتكاب الجريمة الالكترونية.

من خلال ما سبق يتضح لنا، أن الجريمة التقليدية والمجرم التقليدي يختلفان تماما عن الجريمة الإلكترونية والمحرم الإلكتروني، لذا من الطبيعي أن تجد نفس الإختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير

---

[1] جازية سليماني، موقع العربي الجديد.

htt//www.alaraby.co.uk/media news.

[2] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة الماجستير في القاون العام، جامعة الشرق الأوسط، ،2014ص من 26إلى 36.

المشروع، فالدافع (الباعث)، الغرض، الغاية، مفاهيم لكل منها دلالته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الإستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز، فالدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى. أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي اصرف إليها القصد الجنائي أو الإعتداء على الحق الذي يحميه قانون العقوبات. وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الإنتقام، أو سلب مال المجني عليه في جريمة القتل.

وبالنسبة للجريمة الإلكترونية، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الإعتداء المختلفة المنطوية تحت هذا المفهوم، وأهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين.

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية.

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المحرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين.

البند الأول: الدوافع المادية.

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمحرم

الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحساب أو الحساب شركائه، أو الحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة *"securite informatique* وهي مجلة متخصصة في الأمن المعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال و 23% من أجل سرقة معلومات و 19% أفعال إتلاف و 15% الإستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المحرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباحالمادية التي يحققها المحرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس المعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الإعتداءات[1]" .

[1]سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة 2012-2013، من 60-61،

البند الثاني: الدوافع الذهنية لارتكاب الجريمة الإلكترونية.

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي و إثبات الذات. وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المحرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المحرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي و إثبات المقدرة[1]" .

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية.

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإحرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال البندين المواليين.

البند الأول: دافع الإنتقام وإلحاق الضرر برب العمل.

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[2]، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك

نقلا عن تملا عبد القادر المومني، الجرائم المعلوماتية، 02 2010، ص 90، ونقلا عن ضاح محمود الحمود ونشأت مقضى المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005، ص 31.

[1] سعيداني نعيم رسالة الماجستير السابقة الذكر، من 61-62.

[2] صغير يوسف، رسالة الماجستير السابقة الذكر، ص 42.

الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المحرم الإلكتروني الرغبة في الإنتقام من رب العمل، ومثال ذلك أن الإنتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

البند الثاني: دافع التعاون والتواطؤ.

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[1].

وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية، مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإحرامي والدوافع لارتكاب الجريمة الإلكترونية قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الإبتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة[2].

[1] سعيداني نعيم رسالة الماجستير السابقة الذكر، ص 62.

[2] سعيداني نعيم نفس الرسالة، ص 62.

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية في القانون الجزائري.

بعد التطرق لمفهوم الجريمة الإلكترونية، وبيان الدوافع المؤدية لارتكابها من طرف المحرم الإلكتروني، أحاول من خلال هذا المبحث بيان خصائص هذه الجريمة وذلك بالتطرق للسمات الخاصة بالجريمة الإلكترونية والسمات الخاصة بالمحرم الإلكتروني وتنوع هذه الجريمة في التشريع الجزائري بحسب ما إذا ارتكبت باستخدام النظام المعلوماتي، أو كانت موجهة ضده، وهذا ما يتم بيانه في المطلبين الآتيين.

المطلب الأول: خصائص الجريمة الإلكترونية.

لما كانت الجريمة الإلكترونية هي نتاج التطور العلمي والتكنولوجي، وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا تجد لها مجموعة من الخصائص، أو السمات تجعلها منفردة عن غيرها من الجرائم، سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة، وهذا ما يتم بيانه من خلال الفرعين المواليين.

الفرع الأول: السمات الخاصة بالجريمة الإلكترونية.

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظيرتها التقليدية بمجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، وتتلخص هذه السمات فيما يلي:

خفاء الجريمة وسرعة التطور في ارتكابها، حيث تتسم بأنها خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الإتصالات، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو

إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[1] . وقد تتم في ثانية أوجزء من الثانية في بعض الجرائم.

– ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات وتجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب (hardware) ومكوناته البرمجيات.(software) .

– يقوم بها محرم ذو طبيعة خاصة وإمكانات خاصة علمية معلوماتية)، يستخدم في ارتكاب جريمته الموارد المعرفية والأساليب الإحترافية.

صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على المتوفر. ولعل صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجريمة في الدليل المتوفر[2]. مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم 2 اقتراف جرائمهم دون أن يتركوا آثار تدل عليهم.[3]

الجريمة الإلكترونية تستلزم طرقا خاصة مستحدثة للإثبات قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسب الآلي، لذا فإنها تقتضي وجود رجل شرطة إلكتروني، ومحقق إلكتروني، وقاضي إلكتروني، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الإستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.

---

[1] صغير يوسف رسالة الماجستير السابقة الذكر، ص 14-15.

[2] عبد الناصر محمد محمود فرغلي محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 10.

[3] موسى مسعود ارحومة الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا، طرابلس، 28/29/10/2009، ص 03.

هذه الجريمة لا يحدها مكان، فهي عالمية، إذ يمكن عن طريق الحاسب الآلي أو حتى هاتف نقال لشخص في الصين مثلا أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ضد شخص طبيعي أو معنوي في الو.م. أ، أو العكس.

تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات ومؤسسات ، لتجنب الإساءة للسمعة و الرغبة في عدم زعزعة ثقة العملاء، ففي إحدى الوقائع تعرض أحد البنوك، وهو بنك marchant bank "city في بريطانيا لسرقة ثمانية مليون جنية إسترليني من إحدى أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته، قام البنك بدفع مليون جنية له ، بشرط التزام الفاعل بعدم الإعلام عن جريمته، و إعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئسي.

– غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه[1].

ذاتية الجريمة الإلكترونية تبرز بوضوح في أسلوب إرتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر، وتقليد المفاتيح كما هو الحال في جريمة السرقة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الأنترنت مع وجود محرم يوظف خبراته وقدراته على التعامل مع الشبكة، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغرير أو التغرير بالقاصرين، كل ذلك دون الحاجة السفك الدماء.

–الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سعيد المسماري، المرجع السابق الذكر، ص 10-11

الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها، لتغطية عملية التلاعب وتحويل المكاسب.[1]

الفرع الثاني: السمات الخاصة بالمجرم الإلكتروني.

المعرفة والمهارة والذكاء: بمعنى التعرف على كافة الظروف التي تحيط بالجريمة وتنفيذها وإمكانية تحها، واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم. كما أن المحرم الإلكتروني يستطيع أن يكون تصورا كاملا الجريمته، بالإضافة إلى أنه يتمتع بقدر لا يستهان به من المهارة في مجال تقنية الحاسوب والأنترنت فتنفيذ جريمة يتطلب قدرا من المهارة لدى الجاني التي قد يكتسبها عن طريق الخبرة في مجال تكنولوجيا المعلومات الجريمة الإلكترونية هي جريمة الأذكياء بالمقارنة بالجريمة التقليدية التي يكون فيها الميل إلى العنف، فالمجرم الإلكتروني يسعى إلى معرفة طرق جديدة ومبتكرة لا يعرفها أحد سواه، من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية، ثم نيل مبتغاه.[2]

المحرم الإلكتروني يبرر ارتكاب جريمته، إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم، خاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبوا هذه الجرائم بين الإضرار بالأشخاص الذي يعدونه غاية في اللا أخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم. ويبدو أن الإستخدام المتزايد للأنظمة المعلوماتية قد أنشأ مناخا نفسيا ملائما لتصور استبعاد فكرة الخير والشر قد ساعد على عدم وجود احتكاك مباشر بالأشخاص، هذا التباعد في العلاقة الثنائية بين الفاعل والمجني

[1] سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة 2013 – 2014، ص 18.

[2] اسمية مزغيش، رسالة الماستر السابقة الذكر، ص 20.

عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.

المحرم الإلكتروني يتصف بالخوف من كشف جريمته، وبالرغم من أن هذه الخشية تصاحب المحرم على اختلاف أنماطه، إلا أنها تميز المحرم الإلكتروني بصفة خاصة، لما يترتب على كشف أمره من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان، كما أن طبيعة الأنظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله، ذلك أن كثير ما يعرض المحرم إلى اكتشاف أمره، هو أن يطرأ أثناء تنفيذ جريمته عوامل غير متوقعة، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة الإلكترونية هي الحواسيب إنما تؤدي عملها غالبا بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي تمر بها، أي من العمليات التي يقوم بها من مرة إلى أخرى.

المحرم الإلكتروني يميل إلى التقليد، حيث يبلغ هذا الأخير أقصاه حينما يوجد الفرد وسط جماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك من خلال محاولة الفرد تقليد غيره بالمهارات الفنية، مما يؤدي به الأمر إلى ارتكاب الجريمة، وذلك لعدم الإستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة.[1]

– القيام بالتخطيط والتنظيم، ففي عالم الشبكات الإلكترونية، كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة حيث ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسب الآلي يقوم بالجانب الفني

[1] سمية مزغيش، رسالة الماستر السابقة الذكر، ص 20-21.

من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه.

التكيف الإجتماعي، فالمحرم الإلكتروني يقوم بواجباته ويمارس حقوقه الإجتماعية والسياسية دون أي عائق في حياته اليومية[1]، إذ تعتبر هذه الخاصية إمتداد لسمة التخطيط و التنظيم، حيث أن التكيف الإجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار نوابغ المعلوماتية لاشك أن يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم روابط تساعدهم على ارتكاب جرائمهم، وتتعدى تلك الروابط النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي، وإقامة المؤتمرات الدولية بين هذه المجموعات خير دليل على تلك الصلات والروابط الدولية بينها، بالإضافة إلى أن المحرم الإلكتروني هو عادة إنسان إجتماعي[2]، بطبعه حيث يحي وسط المجتمع، ويمارس عمله في المجال المعلوماتي أو غيره من المجالات، وبناء عليه فإن كثير من الجرائم ترتكب بدافع الكبرياء (موظف طرد من عمله، أو بدافع النصب أو الحسد أو اللهو وإظهار قدراته)[3].

التطور في السلوك الإجرامي، حيث يساهم وجود المجرم الإلكتروني في جماعة إجرامية إلى سرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة، إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة وبناءا على ما تقدم يمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة:

المخترقون أو المتطفلون يتحد في هذا الإطار نوعين من المجرمين.

---

[1] مليكة عطوي، المرجع السابق الذكر، ص 12.

[2] سمية مزغيش، رسالة الماستر السابقة الذكر، ص 22.

[3] محمد على العربان الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص 62.

الهاكرز وهو الشخص الذي يقوم بإنشاء أو تعديل البرمجيات و العتاد الحاسوبي، ويقصد يهم الشباب البالغ المقترن بالمعلوماتية والحاسبات الآلية، وقد يطلق على بعضهم صغار نوابغ المعلوماتية، وأغلبهم طلبة لهم معرفة في مجال التقنية المعلوماتية إن الباعث الأساسي لدى الهاكرز هو الإستمتاع باللعب والمزاح باستخدام هذه التقنية لإثبات قدراتهم، باكتشاف مواطن الضعف في الأنظمة المعلوماتية دون إلحاق ضرر بها، لديهم الرغبة في المغامرة والتحري و الإكتشاف[1]. والهاكرز أنواع، الهاكر ذو القبعة البيضاء (الهاكرز الأخلاقي)، ويطلق عليه الهاكر المصلح، ثم يوجد الهاكر ذو القبعة السوداء وهو الهاكر المفسد، وأخير هناك الهاكر ذو القبعة.

الرمادية ويسمى بالمترنح بين الإصلاح والعبث[2]، وما يهمنا هنا هو الهاكر ذو القبعة السوداء وذو القبعة الرمادية، أما الهاكر الأبيض فهو أخلاقي ولا يرتكب جرائم.

الكراكز : وهو المقتحم، وتعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين وأعمارهم تتراوح بين 25-45 عاما. ومن أبرز سمات هذه الطائفة أنهم ذوي مكانة في المجتمع، وأنهم غالبا من المتخصصين في مجال التقنية الإلكترونية، أي أنهم يتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية، تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات.[3]

مجرموا الحاسب الآلي المحترفون: هذا النوع من المجرمين يعرف كيف يصل إلى أهدافه، باستخدام ما لديه من علم يطورونه باستمرار، وهدفهم المصاريف وسحب الأموال من الأرصدة ونيتهم إحداث التخريب[4]، تتميز هذه الطائفة بسعة

---

[1] سمية مزغيش، رسالة الماستر السابقة الذكر، ص 23.

[2] مخترق، ويكيبيديا الموسوعة الحرة، التاريخ: على الرابط

https//ar.wkiped.org/wiki/

[3] سمية مزغيش، رسالة الماستر السابقة الذكر، ص 22-23

[4] مليكة عطوي المرجع السابق الذكر، ص 13

الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، لذا فإن هذه الطائفة تعد الأخطر من بين محرمي التقنية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجماعات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي. إن الأفعال الصادرة عن هذه الفئة تعكس ميولا إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب، وهم أكثر خطورة من الصنف الأول.

الحاقدون: هذه الطائفة يحرك أنشطتهم الرغبة في الإنتقام من صاحب العمل، أو التصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين بالنظام محل الجريمة، و إلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم، إن أعضاء هذه الطائفة لا تتسم بالمعرفة التقنية الإحترافية، ومع ذلك يسعى الواحد منهم إلى الإلمام بالمعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه ويستخدمون تقنيات الفيروسات والبرامج وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الأنترنت، كما أنهم من أعمار مختلفة، ولا تتوافر عناصر التفاعل بين أعضاء هذه الطائفة، وهم الطائفة الأسهل من حيث كشف أنشطتهم لتوفر ظروف وعوامل تساعد على ذلك.[1]"

صغار السن: يسمون بصغار توابع المعلوماتية، وهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، ومن بينهم فئة لم تزل دون سن الأهلية مولعين بالحوسبة والاتصال، وقد تعددت أوصافهم في الدراسات الاستطلاعية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بالمتعثلمين الدال حسب تعبير الأستاذ " طوم فورلستر" على الصغار المتحمسين للحاسوب بالشعور بالبهجة

[1] سمية مزغيش، رسالة الماستر السابقة الذكر، ص 23 - 24.

دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب ويسميهم البعض كذلك بمجانين (معدلات ومعدلات عكسية)، بالإستناد إلى كثرة استخدامهم لتقنية المعدل و المعدل العكسي المورديم"، الذي يعتمد على الإتصال الهاتفي لاختراق شبكة النظم. ويثير محرموا الحوسبة من هذه الطائفة جدلا واسعا، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، ظهرت مؤلفات ودراسات تخرج هذه الفئة من دائرة الإحرام إلى دائرة العبث و أحيانا البطولة من هذه المؤلفات على سبيل المثال، كتاب "خارج نطاق الدائرة الداخلية كيف تعملها ؟"، لمؤلفه الأمريكي لبيب لاندريد، وكتاب" الدليل الجديد للمتعثلمين"، لمؤلفه هو جوكوزن، وكتاب المتعلمين أبطال ثورة الحاسوب"، لمؤلفه ستيفن ليفي.[1]

مجرمون ذوي دوافع سياسية: وهم أشخاص لهم ميول ودوافع سياسية معينة، تدفعهم الإختراق نظم الحاسب الآلي غير المصرح بالدخول إليها، والتي تحتوي على معلومات وبيانات غاية في السرية تتعلق بالدفاع والأمن، ويمثل المساس بها مخاطر كارثية[2]" .

المحرم الإلكتروني محرم يعود للإحرام، فهو يوظف مهاراته في كيفية عمل الحاسوب، وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات من خلال الدخول غير المصرح به مرات ومرات، فهو قد لا يحقق جريمة الإختراق بهدف الإيذاء، وإنما نتيجة شعوره بقدرته ومهارته في الإختراق.

فالإحرام الإلكتروني هو إحرام الذكاء دونما الحاجة إلى استخدام القوة والعنف، وهذا الذكاء هو مفتاح المحرم الإلكتروني، لإكتشاف الثغرات واختراق البرامج المحصنة. ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي : – عادة ما تتراوح أعمارهم ما بين 18 و 45 عاما – المهارة والإلمام الكامل والقدرة الهائلة في مجال نظم المعلوماتية – الثقة الزائدة بالنفس الإلمام

[1] سمية مزغيش، نفس الرسالة، من 24-25 .

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق الذكر، ص 09.

التام بمسرح الجريمة، وبما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره[1].

المطلب الثاني: أنواع الجرائم الإلكترونية في القانون الجزائري.

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية[2] على خلاف هذه الجريمة، فإن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، وذلك بسبب الإختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الإعتداء وتعدد الحق المعتدى عليه[3]. أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات، وهذا ما سيتم بيانه في الفرعين الموالين.

الفرع الأول: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة التسهيل النتيجة الإجرامية ومضاعفا الجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار، وسأوضح كل نوع منها في البنود الآتية.

---

[1] رضاع فتيحة، رسالة الماجستير السابقة الذكر، ص 69.

[2] أحسن بوسقيعة الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، 2002، ط 01، ص 24.

[3] سوبر سفيان، رسالة الماجستير السابقة الذكر، من 33.

البند الأول: الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية.

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

1 -الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية.

يكون النظام المعلوماتي وسيلة للإعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الإختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 03-05 الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المحاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الإختراع[1].

2 -الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة.

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الإعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق

[1] سوير سفيان، رسالة الماجستير السابقة الذكر، ص 34-35.

معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

البند الثاني: الجريمة الإلكترونية الواقعة على النظم المعلوماتية الآخرى.

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية.

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الإستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة أو استخدام شاشة النظام، أو الإطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الإئتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الإئتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة إئتمانية إنتهت مدة صلاحيتها أو تم إلغاؤها، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة إئتمانية للحصول على السلع والخدمات[1].

البند الثالث: الجريمة الإلكترونية الواقعة على الأسرار.

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[2]، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والإقتصادية لهذه الأخيرة خاصة في الدول

[1] سوير سفيان، نفس الرسالة، ص 38.
[2] صغير يوسف رسالة الماجستير السابقة الذكر، ص 54.

التي يكون فيها نزاعات[1]، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الإمتناع عن القيام بعمل.

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات بالإضافة إلى المادة 394 مكرر 03 التي تنص على : " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد. [2]

الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي.

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04-15 الصادر في 10 نوفمبر 2004 المتضمن قانون العقوبات بتحريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 07، وتأخذ صور الإعتداء صورتين وهما : الدخول والبقاء في منظومة معلوماتية المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ما سأتناوله في البنود الموالية.

[1] سوبر سفيان رسالة الماجستير السابقة الذكر، من 38.
[2] الأمر رقم 04-15، القانون السابق الذكر .

البند الأول: جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية.

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[1]" .

1- فعل الدخول غير المشروع: لا نعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الألية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل فنيات الدخول الإحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول إلى المنظومة.

[1]

2- فعل البقاء غير المشروع: يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الإطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية. [1]"

البند الثاني: جريمة المساس بمنظومة معلوماتية.

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 15/04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإحرامي يتجسد في ثلاث صور هي الإدخال المحو التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، و أفعال الإدخال والإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير

[1] حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 183 - 184.

صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.

البند الثالث: أفعال إجرامية أخرى.

حرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر[1]، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعوماتية في حد ذاتها[2]، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لإي غرض[3] .

من خلال التعرض إلى ماهية الجريمة الإلكترونية، يتضح بأن لهذا النمط من الجرائم طبيعة خاصة ومتميزة، وهي حريمة ناعمة حال ارتكابها، تتجاوز حد الخشونة في نتائجها، إذ بمجرد ملامسة الجاني لزر أو أكثر من لوحة المفاتيح، قد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه، وهذا ما يؤدي إلى صعوبة في مكافحتها، ويعاب على المشرع الجزائري أنه اهتم بالجريمة الإلكترونية بالنص على بعض الجرائم الإلكترونية وليس كلها وأهمل المحرم الإلكتروني، إذ لم يتعرض له في أي نص قانوني، بالإشارة إلى تعريفه أو سماته.

كما أن التطرق لماهية الجريمة الإلكترونية والتعرف عليها بعمق يفيدنا في إيجاد الحلول لمواجهتها.

---

[1] حمزة بن عقون، نفس الرسالة، ص 184.

[2] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منشوري، قسنطينة 2012-2013، بدون صفحة.

[3] حمزة بن عقون، رسالة الماجستير السابقة الذكر، من 184 -185.

بعد التطرق إلى ماهية الجريمة الإلكترونية، من خلال تعريفها وأنواعها والدوافع المؤدية لارتكابها. أتعرض في هذا الفصل إلى بيان كيفية التصدي للجريمة الإلكترونية من طرف المشرع الجزائري، وذلك بتوفير الحماية الموضوعية والإجرائية للنظام المعلوماتي، من خلال مختلف التشريعات التقليدية أو المستحدثة التي تناولت الجريمة الإلكترونية، وهذا ما سيتم توضيحه في المبحثين الأتيين.

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي.

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى، استوجب ذلك توفير حماية جنائية خاصة بها، فالمعلومة أصبحت تقوم ماليا، وبالتالي تدخل في عناد الأموال الإقتصادية، وقد تكون المعلومة شخصية وإفشائها يهدد الحياة الخاصة من جوانب متعددة. ونظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات) شبكة الأنترنت)، 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 لاستحداث قواعد قانونية جديدة المواجهة هذه الجرائم المستحدثة" [1].

المطلب الأول: الحماية في نصوص الملكية الفكرية.

يقصد بالحقوق الذهنية أو الفكرية، بأنها حقوق ملكية معنوية ترد على أشياء غير مادية وتقسم إلى ثلاثة أنواع: – حق الملكية الصناعية، ويرد على ابتكارات جديدة تمكن صاحبها من احتكار استغلال ابتكاره قبل الكافة، وهي أنواع حقوق تتعلق بابتكار جديد من حيث الشكل والمظهر الخارجي للمنتجات (الرسوم أو التصميمات أو النماذج الصناعية)، حقوق تتعلق بابتكار جديد من حيث الموضوع كالإختراعات حقوق ترد على شارات مميزة تمكن صاحبها من احتكار استغلال علامة تستخدم لتمييز المنشآت كالإسم التجاري.

[1] رضاع فتيحة، رسالة الماجستير السابقة الذكر، ص 88.

– حقوق الملكية التجارية وهي تتضمن ما للتاجر من حق على محله التجاري، باعتباره مال منقول.

– حقوق الملكية الأدبية والفنية، وتعني ما للمؤلف من حق على إنتاجه الذهني في الأداب والفنون والعلوم" [1].

وقد اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة، تتمثل في وجود المصنف أولا ثم عدم مخالفته للنظام العام ثانيا، وأخرى خاصة وهي وجود ابتكار جديد في المصنف أولا ثم القيام بإيداعه القانوني ثانيا[2].

الفرع الأول: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية.

ترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالإختراعات، ومعنى الإختراع إيجاد شيء لم يكن موجودا من قبل، أو اكتشاف شيء كان موجودا ولكنه كان مجهولا وغير ملحوظا ثم أبرزه في المجال الصناعي، فالإختراع الذي لا يؤدي إلى تقدم ملموس في الفن الصناعي لا يستحق براءة عنه[3]. ولما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب الآلي، فهي من هذه الزاوية تصبح قابلة للبراءة[4]. وقد نص عليها الأمر رقم 03-07 الصادر في 2003، حيث نصت المادة الثالثة منه على الشروط الواجب توافرها حتى يحظى الإختراع بالحماية بقولها: "يمكن أن تحمى بواسطة براءة الإختراع، الإختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصناعي ....."[5] وعليه يمكن القول أنه حتى يحظى أي اختراع ما بالحماية

[1] محمد عبد الرحيم الناغي الحماية الجنائية للرسوم والنماذج الصناعية (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2009، 13-12

[2] بن زبطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط01، ص 37 .

[3] عفيفى كامل عفيقي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، 2000 51 ط02، ص51.

[4] بوعناد فاطمة زهرة مكافحة الجريمة الإلكترونية في التشريع الجزائري مجلة الندوة للدراسات القانونية، سيدي بلعباس 68 2013، العدد 01، ص68.

[5] الأمر رقم 03-07 ، الصادر في 19 يوليو 2003 المتعلق ببراءات الإختراع، ج والعدد 44.

ضمن نطاق براءات الإختراع، وجب توافر شرطي الإبتكار والجدة والقابلية للتطبيق الصناعي[1].

وتجدر الإشارة إلى أنه يمكن الحصول على براءة الإختراع بخصوص برامج الإعلام الآلي في حالتين: – أن يكون البرنامج جزءا من ذاكرة الحاسوب نفسه ومثاله البرنامج المبني.

أن يكون البرنامج جزءا، أي أن طلب البراءة ينصب على وسيلة صناعية جديدة، يستخدم البرنامج في تحقيق إحدى مراحلها، فالحماية تبقى رهينة توفر الشرطان المذكوران، مما يصعب توفرها، فالمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الإختراع[2] طبقا للمادة 07 من الأمر رقم 03–07 التي تنص على : لا تعد من قبيل الإختراعات في مفهوم هذا الأمر برامج الحاسوب" [3]

الفرع الثاني: خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية والفنية.

تظهر الملكية الأدبية والفنية من خلال حق المؤلف، وهو حق استثاري يمنحه القانون المؤلف أي مصنف للكشف عنه، كابتكار له أو استنساخه أو توزيعه أو نشره على الجمهور، والإذن للغير باستعماله على وجه محدد[4] . وقد انقسم الفقه إلى اتجاهين، اتجاه يرى أن برامج الحاسب الآلي مصنفة ضمن قانون حق المؤلف وأنه لا حاجة لتعديل النصوص التقليدية في قانون حق المؤلف، باعتبار برامج الحاسب الآلي ما هي إلا طرق مختلفة للتعبير عن الأفكار الإنسانية وهو مثل سائر المصنفات، أما الإتجاه الآخر أقر لبرامج الحاسب الآلي الصفة المميزة عن سائر المصنفات الأخرى المحمية بموجب قانون حماية حق المؤلف، وتبنى هذا التوجه العديد من الدول التي عدلت قوانينها بما

[1] ختير مسعود الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر طبعة 2010، ص .69

[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 66.

[3] الأمر رقم 03-07، القانون السابق الذكر.

[4] عفيفى كامل عقيقي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003، ص 75.

ينسجم والصفة المميزة لبرامج الحاسب الآلي[1]، ومنهم الجزائر حيث جاء الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة باستخلاص ما يلي: - أن المشرع وسع قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي - تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لاسيما المصنفات المعلوماتية[2]، حيث تنص المادة 05 من القانون رقم 03-05[3] على أنه : " تعتبر أيضا مصنفات محمية الأعمال الآتية .... مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواءا كانت مستنسخة على دعامة قابلة للإستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى... تكفل الحماية المؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية. والمادة رقم 04 من نفس القانون نصت على أنه: تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل ... وبرامج الحاسوب ..... كما أن مدة الحماية تحدد ب 50 سنة بعد وفاة المبدع وفقا للمادة 58 فقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي المؤلف برنامج فعلا من أفعال التقليد، حيث نص المشرع في المادة 151 من الأمر رقم 03/05، على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء فني أو في حالة المساس بسلامة مصنف أو أداء فني، أو في حالة استنساخ مصنف أو أداء فني بأي أسلوب في شكل نسخ مقلدة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول.

[1] جلال محمد الزعبي، أسامة أحمد المناعة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع عمان الأردن، 2010، ط 01، في 189.

[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 66.

[3] الأمر رقم 03-05، الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج و العدد 44.

وقد قرر المشرع جزاءات الجرائم التقليد، حيث ربط المشرع الجزائري حماية المصنف بتاريخ الإنتهاء من الإبتكار أو تاريخ النشر أو التوزيع لأول مرة، كما حول المشرع لصاحب المصنف المعتدى عليه القيام بإجراء تحفظي يتمثل في حجز التقليد، وبواسطته يتم حجز الوثائق والنسخ الناتجة عن الإستنساخ غير المشروع أو التقليد والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من 156/153 إلى 159 من نفس القانون السابق الذكر، حيث قدرت العقوبة الأصلية بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 1.000.000 دج سواء تمت عملية النشر داخل الجزائر أو خارجها، ومنح المشرع للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الإستغلال غير الشرعي المصنف أو أداء محمي، ومصادرة وإتلاف كل عتاد أنشأ خصيصا المباشرة النشاط غير المشروع، وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبية، كما للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر..[1]

المطلب الثاني: الحماية في قانون العقوبات.

إن القانون الجنائي التقليدي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الجديدة، لاسيما أن نصوصه وضعت في عصر لم يكن الأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن استخدامه[2]، لكن نجد أن المشرع الجزائري تدارك الفراغ القانوني في محال الإجرام المعلوماتي ولو نسبيا، خصوصا بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات، إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات، وقد سبق

[1] سوير سفيان، رسالة الماجستير السابقة الذكر، من 75- 78- 80.

[2] سمير سعدون مصطفى، وآخرون، الجريمة الإلكترونية عبر الأنترنت وسبل مواجهتها، بحث مقدم بتاريخ 20/09/2010 بدون سنة ، بدون صفحة.

ذكرها في المبحث الثاني من الفصل الأول، أما العقوبات سأتطرق لها من خلال الفروع الموالية.

الفرع الأول: العقوبات الأصلية.

نص المشرع الجزائري في القانون رقم 15/04 على عقوبات أصلية لجريمتي الدخول والبقاء غير المشروعان للنظام المعلوماتي، وكذا جريمة المساس بمنظومة معلوماتية وفق الآتي:

- **عقوبة الدخول أو البقاء غير المشروعان للنظام** في حالة الدخول غير المشروع من طرف المحرم الإلكتروني للنظام كله أو جزء منه أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه، ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب النظام، تكون العقوبة بالحبس من ثلاثة أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج طبقا للمادة 394 مكرر من قانون العقوبات رقم 15/04.

أما في حالة الدخول أو البقاء ونتج عنه حذف أو تغيير المعطيات المنظومة، أو البحر عن هذا الدخول أو البقاء تخريب لنظام اشتعال المنظومة، فإن العقوبة تضاعف إلى الحبس من سنة أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج، وذلك وفقا للمادة 394 مكرر من قانون العقوبات السابق الذكر.

عقوبة المساس بمنظومة معلوماتية: نص المشرع الجزائري في المادة 394 مكرر 01 من نفس القانون السابق الذكر على عقوبة الإعتداء العمدي على المعطيات الموجودة داخل النظام، وذلك بالحبس من 06 أشهر إلى 03 سنوات وغرامة من 500.000 دج إلى 2.000.000 دج، وذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة

المعلوماتية تكون العقوبة الحبس من شهرين إلى 03 سنوات وغرامة من 1.1.000.000 دج إلى 5.000.000 دج[1]

الفرع الثاني: العقوبات المقررة للشخص المعنوي.

نص المشرع الجزائري في المادة 51 مكرر من القانون رقم 04/15 على مسألة الشخص المعنوي وذلك وفق شروط : أن ترتكب إحدى الجرائم المنصوص عليها قانونا أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي أن ترتكب الجريمة الحساب الشخص المعنوي. كما نصت المادة 394 مكرر 04 من نفس القانون على العقوبات الواجبة التطبيق على الشخص المعنوي في حالة ارتكابه لأي جريمة اعتداء على نظام المعالجة الآلية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[2] "

الفرع الثالث: عقوبة الإشتراك و الشروع في الجريمة.

عقوبة الإشتراك: نصت عليها المادة 394 مكرر 05 من القانون رقم 04/15 بقولها :" كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد الجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير محسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها."

عقوبة الشروع نصت عليها المادة 394 مكرر 07 من نفس القانون بقولها :" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها."

الفرع الرابع: العقوبات التكميلية.

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية يحكم بها إلى جانب العقوبات الأصلية وهي كالتالي:

---

[1] ختير مسعود، المرجع السابق الذكر، من 99-100.

[2] ختير مسعود، المرجع السابق الذكر، من 100-101

المصادرة وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام وذلك ببيعها، أو حجزها مع مراعاة حقوق الغير حسن النية.

إغلاق المواقع إغلاق مواقع الأنترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لارتكاب هذه الجرائم أو ساهمت في ارتكابها.

إغلاق المحل) المقهى الإلكتروني: يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم. "

ومن الملاحظ أن هذه العقوبات جاءت رادعة حيث تضاعف عند الضرورة، كما اشتملت على عقوبات تكميلية، وحتى عقوبات الشخص المعنوي.

المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

صدر القانون رقم 09-04 الصادر في 05 أوت 2009، ويتضمن 19 مادة موزعة على ستة فصول، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية، كما يتضمن القانون أحكام خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب، والجرائم الماسة بأمن الدولة أو حالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية المؤسسات الدولة أو الدفاع الوطني أو النظام العام. وينص القانون على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والإتصال ومكافحته تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، كما تتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج،

علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل يعتبر القانون رقم 09-04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء تحريمه للأفعال المخالفة للقانون و التي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا.[1]

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي.

إن القاعدة الإجرائية ليست غاية في ذاتها، وإنما هي وسيلة لغاية تتمثل في حسن تطبيق القانون الجنائي الموضوعي، فبينما تجرى بالدعوى العمومية محاكمة القاضي للمتهم، فإنه بتطبيق القواعد الإجرائية التي خالفتها الدعوى تجرى محاكمة القانون للقاضي، وبالتالي فإن للإجراءات الجنائية خطورة لا تقل بحال القواعد المقررة في قانون العقوبات لأنها تمس مباشرة بحريات المواطنين واستقرارهم[2]. وعليه كان لابد من التطرق إلى الجوانب الإجرائية بخصوص الجريمة الإلكترونية، ومدى توافر الحماية الإجرائية للنظام المعلوماتي، وذلك من خلال المطالب الآتية.

المطلب الأول: التحقيق في الجريمة الإلكترونية.

يعرف التحقيق بأنه إجراء يتخذ بعد وقوع الجريمة، لما له من أهمية في التأكد من وقوع الجريمة، وإسنادها إلى مرتكبيها بأدلة الإثبات بأنواعها، وبالتالي تتحلى الحقيقة التي تهدف إلى إدانة المتهم من عدمه. وتمر الدعوى الجنائية بمرحلتين مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بدورها بمرحلتين مرحلة التحقيق الأولي (الضبطية القضائية) ومرحلة التحقيق الإبتدائي (قاضي التحقيق، وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون

[1] ختير مسعود المرجع السابق الذكر، ص 102 103.

[2] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية 2009،ص 342-343 .

الإجراءات الجزائية، فإذا كان التحقيق يعتمد على ذكاء المحقق وقوة ملاحظته، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى ذلك تطوير الأساليبه، وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطورها[1] وهذا ما سيتم بيانه في الفروع الموالية.

الفرع الأول: الأجهزة المكلفة بالبحث والتحري.

نظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني، بالنسبة لجهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى فرق متخصصة مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر توجد على مستوى مراكز الأمن الولائي، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني[2].

الفرع الثاني: خصائص التحقيق والمحقق.

للتحقيق الإلكتروني مميزات خاصة عن التحقيق الجنائي التقليدي وكذا المحقق الإلكتروني، المسايرة متطلبات الجريمة الإلكترونية بما فيها العالم الإفتراضي الذي ترتكب فيه.

[1] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص .102-103-

[2] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص .106-107.

أولا: خصائص التحقيق الإلكتروني:

1- منهج أو أسلوب التحقيق الإبتدائي: وضع خطة عمل التحقيق وذلك وفق المعلومات المتوفرة لدى المحقق، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك بوضع خطة مناسبة، ولا تبتدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة، ثم التخطيط الفني للتحقيق من أجل الوصول إلى أفضل الطرق للتعامل مع هذه الجريمة بالتفصيل والوضوح، وبعدها عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل، وهو ما يؤدي إلى ضمان مستوى جيد من الأداء، تحديد الإجراءات المسبقة التي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبراء أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة. ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية، يتم الإرتكاز عليها أثناء تنفيذ الخطة وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب إيضاحها معهم وتقدير مدى الحاجة للإستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الظروف المحيطة بالواقعة، إذ أن هذه الظروف قد تشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها: مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة – مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها – مدى الإختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش، وذلك بتحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.[1] "

– **تشكيل فريق التحقيق:** يجب أن يتشكل الفريق من فنيين وأخصائيين ذوي الخبرة في مجال الحاسوب والأنترنت ما يكفي لمكافحة هذا النشاط الإجرامي، وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين في مجال المعلوماتية والمعرفة باللغات الأجنبية[2]، ولهم مهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهم الإستعانة بخبراء ليتمكنوا من فك التعقيدات التي تفرضها ملابسات كل جريمة، ويتكون الفريق من المحقق الرئيسي، ويكون ممن لهم خبرة في التحقيق الجنائي، خبراء الحاسوب وشبكات الأنثرنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم، خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب، خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية، خبراء التصوير والبصمات والرسم التخطيطي.

2–إجراءات التحقيق – إجراءات سابقة على بدء التحقيق الإبتدائي:

– تحديد نوع نظام المعالجة الآلية للمعطيات أي هل الحاسوب معزول أم متصل بشبكة معلومات وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة، مع كشف تفصيلي عن المسؤولين بها ودور كل واحد منهم – إذا وقعت الجريمة على شبكة، فإنه يجب حصر طرفيات الإتصال بها أو منها، المعرفة الطريقة التي تمت بها عملية الإختراق من عدمه، وهل هناك حواسب آلية خارج هذه المشكلة ولها إمكانية الإتصال بها أم لا؟ – مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة الإلكترونية – مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة يجب فصل التيار الكهربائي عن

[1] سعيداني نعيم رسالة الماجستير السابقة الذكر، ص 110-111

[2] كوثر قرام الجريمة المعلوماتية على ضوء العمل القضائي المغربي بحث نهاية التدريب المعهد العالي للقضاء، 2007 - 2009، ص88.

موقع المعاينة أو جمع الإستدلال لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، لأنه من الخدع التي يستعملها الجاني عند الإختراق أن يتم ذلك بخط هاتفي مسروق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة والتخطيط) – إبعاد الموظفين عن أجهزة الحاسب الآلي بعد حصول المتهم على كلمة السر، وكذا الشفرات في حالة وجودها – تصوير الأجهزة المستهدفة – التي وقعت بها أو عليها الجريمة – من الأمام والخلف لإثبات أنها كانت تعمل.[1] "

إجراءات أثناء التحقيق الإبتدائي عمل نسخة احتياطية من الأقراص الصلبة أو الإسطوانة المرنة قبل استخدامها، والتأكد فنيا من دقة النسخ عن طريق الأمر – نزع غطاء الحاسب الآلي المستهدف، والتأكد من عدم وجود أقراص صلبة إضافية – أن يكون الهدف من نسخ محتوى الإسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات، وكذا معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في اختلاس معلوماتي – العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها – حفظ المعدات والأجهزة التي تضبط بطريقة فنية سليمة. [2]"

ثانيا: خصائص المحقق الإلكتروني: تتمثل في الخصائص الفنية للمحقق الإلكتروني، وتأهيل و تدريب المحقق الإلكتروني.

[1] سعيداني نعيم، رسالة الماجستير السابقة الذكر، من من 111 إلى 113.
[2] سعيداني نعيم، رسالة الماجستير السابقة الذكر، من 113-114.

الخصائص الفنية للمحقق الإلكتروني: معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت، لأن افتقار ضابط الشرطة القضائية إلى التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل – إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك، ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة لأي مؤثرات خارجية، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها – معرفة آلية عمل تشكيلات الحاسوب والأنترنت معرفة المحقق بالأنظمة المختلفة، لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة – معرفة معطيات الحاسوب المعرفة صيغ الملفات وما تحتويه معرفة وإدراك أساليب ارتكاب الجريمة الإلكترونية، وتقنيات الأمن المعلوماتي.

تأهيل وتدريب المحقق الإلكتروني: لابد من وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب إلى العاملين بأجهزة الضبطية القضائية. ويرى الفقه الجنائي أنه في حالة التدريب على التحقيق يتعين مراعاة شخص المتدرب، ومنهج الدورة التدريبية، وصفة وأسلوب التدريب، كما يجب أن يشمل منهج التدريب تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، والمتعلقة بالكشف عنها وكيفية اتباعها ومعاينتها وفحصها فنيا[1]. ومن العقبات التي تعيق عمل الأجهزة حتى على فرض أنه تم إعدادها الإعداد المناسب، ضخامة حجم البيانات محل الفحص ما يتعذر على المحقق الكفئ الوصول إلى الدليل المناسب[2] .

[1] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 116-117-119

[2] موسى مسعود أرحومة، المرجع السابق الذكر، من 05.

الفرع الثالث: الدليل المناسب لإثبات الجريمة الإلكترونية.

الدليل هو أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر مثلا وبالنسبة للجريمة الإلكترونية فإنها تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها، وهي تعرف بالدليل الرقمي المتواجد في أماكن افتراضية، ويعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطسية أو كهربائية، يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، أو أنه ذلك الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة، ويتميز الدليل الرقمي بجملة من الخصائص : أنه دليل علمي يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات أنه من طبيعة تقنية إذ ما تنتجه هذه الأخيرة هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب، وبالتالي لا وجود للدليل الرقمي خارج بيئته الرقمية، ويتميز الدليل الرقمي بقابليته للنسخ مطابق للأصل مع نفس القيمة العلمية، وهذا ما لا نجده في الدليل المادي أنه دليل متنوع ومتطور، حيث يشمل كافة البيانات الرقمية الممكن تداولها رقميا، وتطوره يظهر في حركة الإتصال عبر الأنترنت ومدى تطورها أنه دليل صعب التخلص منه، إذ أنه كلما حدث اتصال بتكنولوجيا المعلومات بإدخال بيانات إلى هذا العالم، فإنه من الصعب التخلص منها، إذ تتوفر برمجيات ذات طبيعة رقمية، يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب أنه ذو طبيعة رقمية ثنائية 1-0، حيث تعتمد تكنولوجيا المعلوماتية الحديثة على تقنية الترقيم، التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي، قوامه الرقمان 0 و 1" ، فالكتابة مثلا في العالم الرقمي ليس لها وجود مادي، وإنما هي مجموعة أرقام لها أصل

واحد وهو الرقم الثنائي 0 و 1 . والدليل الرقمي نوعان، الدليل الرقمي الأصلي والدليل الرقمي المكرر، وهذا الأخير هو استنساخ رقمي لجميع المستمسكات البيانية التي يحتويها الدليل الرقمي الأصلي. "[1]

المطلب الثاني: إجراءات جمع الأدلة التقليدية.

إن التطور التقني الذي لحق نظم المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل، وهو ما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية[2]، لذا سأبين مدى اعتماد هذه الإجراءات في مجال الجريمة الإلكترونية للحصول على الدليل الرقمي وفق الفرعين المواليين.

الفرع الأول: الإجراءات المادية (المعاينة، التفتيش الضبط)

أولا: المعاينة هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه وتقتضي المعاينة إثبات حالة الأشخاص والأشياء[3]، وكل ما يعتبر في كشف الحقيقة، وبهذا المعنى تستلزم المعاينة الإنتقال إلى محل الواقعة أو أي محل توجد به أشياء، أو آثار يرى المحقق أن لها صلة بالجريمة، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملابساتها وتوفير أدلة مادية، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها، لأن الجريمة التقليدية غالبا لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية، على خلاف الجريمة الإلكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة، لأن الجريمة الإلكترونية قلما تخلف آثار مادية، وأن كثير من الأشخاص يردون إلى مسرح

[1] سعيداني نعيم رسالة الماجستير السابقة الذكر، من 119-120-121-123-124-125 - 126

[2] سعيداني نعيم، نفس الرسالة، ص 221.

[3] عبد الله دغش العجمي المرجع السابق الذكر، ص 77

الجريمة خلال فترة من زمان وقوع الجريمة، وحتى اكتشافها أو التحقيق فيها وهي طويلة نسبيا، الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالأثار المادية للجريمة إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة[1]، ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي: تصوير جهاز الحاسوب وما قد يتصل به من أجهزة طرفيه ومحتوياته – عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغنطيسية في العالم الخارجي حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية – ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها، مما يتيح الجهات التحقيق قراءة بياناتها من دون تغييرها.

ثانيا: التفتيش التفتيش هو إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم الإجراءات لأنه غالبا ما يسفر عن أدلة مادية تؤدي إلى نسبة الجريمة للمتهم[2]، والمستهدف من التفتيش هو جهاز الحاسوب بمكوناته المادية (وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل)، (والمكونات المعنوية) الكيانات المنطقية، فعندما يستهدف التفتيش الكيانات المادية لا يشكل عائق، وإنما الإشكال يثور عندما ينصب على المكونات المعنوية (البرامج قواعد البيانات...)، لأنه هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات[3].

تفتيش مكونات الحاسوب المادية: لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه، فلا يجوز

[1] عبد الفتاح يومي حجازي الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2002 ص 21-20

[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 68.

[3] زبيحة زيدان الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر، 2011، ص ص 131-133.

تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وحسب المادة رقم 45 ف 3 تنص على: " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم.... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و المادة 47 ف 3 تنص على: "عندما يتعلق الأمرب ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... فإنه يجوز إجراء التفتيش... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل..."، والمادة 64 ف 2 تنص على: " وتطبق فضلا عن ذلك أحكام المواد 44، 47 من هذا القانون[1]."، بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الإلكترونية، حيث لا يشترط حضور الشخص المشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه، وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء.[2] "

مدى خضوع مكونات الحاسوب المعنوية للتفتيش: عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراءات التفتيش، وانقسم إلى اتجاهين، إتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب، وقد عملت الدول التي تبنت هذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل حيزا ماديا في فراغ معين، هذا الحيز يمكن قياسه والتحكم فيه، وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب، ويمكن قياسه بمقياس معين هو البايت" و" الكيلوبايت "و "الميغابايت"، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية، لذا فإن طبيعة البيانات والمعطيات المعالجة تتطلب قواعد خاصة تحكمها، فالنصوص

[1] المواد 45. 47 ،64 من الأمر رقم 22/06، الصادر في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية، ج ر العدد 84
[2] سعيداني نعيم رسالة الماجستير السابقة الذكر، من 145.

التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية، لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية[1].

- **مدى خضوع شبكات الحاسوب للتفتيش عن بعد:** تفرق هنا بين فرضين.

الفرض الأول: إتصال حاسوب المتهم بحاسب موجود في مكان آخر داخل الدولة: لقد أجاز المشرع في المادة 05 من القانون رقم 09-04 إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك[2]، حيث تنص المادة 05 منه على : " ... في الحالة المنصوص عليها في الفقرة" أ " من هذه المادة إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

الفرض الثاني: إتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة.

ويكون بالدخول إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها ولو عن بعد، وذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل، تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة الحماية المعطيات المعلوماتية التي تتضمنها[3]، حيث تنص المادة 05 من القانون رقم 09-04 على أنه: " ... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي

[1] سعيداني نعيم، نفس الرسالة، من 147.

[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 69.

[3] بن دعاس فيصل إجراءات التحري في الجرائم المعلوماتية محاضرة في إطار التكوين المحلي المستمر للقضاء، مجلس قضاء قسنطينة، من 33.

يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل. "[1]

ثالثا ضبط الأشياء يختلف ضبط الأشياء في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل، ففي هذه الأخيرة يكون المحل أشياء مادية، أما في الجريمة الإلكترونية تكن الأشياء ذات طبيعة معنوية كالبيانات المراسلات الإلكترونية، وتجدر الإشارة إلى أن ضبط الأشياء قد يرد على عناصر معلوماتية منفصلة مثل الإسطوانات الممغنطة، وهنا لا يثور أي إشكال عند القيام بالضبط، لكن الصعوبة تكون عندما يلزم ضبط النظام كله، أو الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها . أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية: وحدات الإدخال (لوحة المفاتيح، الفأرة، نظام القلم الضوئي)، وضبط وحدة الإخراج (الشاشة الطابعة الرسم والمصغرات الفيلمية)، وكل ما يتم ضبطه من بيانات إلكترونية يتعين تحريزها وتأمينها فنيا[2] ، تنص المادة 06 من القانون رقم 09-04 على أنه : "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم، أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية ... "[3]

[1] المادة 05 من القانون رقم 04/09، القانون السابق الذكر.
[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر، من 69
[3] المادة 06 من القانون رقم 09-04 السابق الذكر.

الفرع الثاني: الإجراءات الشخصية (الشهادة الخبرة)

أولا: الشهادة في الجريمة الإلكترونية الشاهد هو الفني صاحب الخبرة والتخصص في التقنية وعلوم الحاسب الآلي، لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق عليه إسم الشاهد الإلكتروني، تمييزا له عن الشاهد التقليدي[1] نتيجة لقصور أحكام الشهادة في الحصول على الدليل الإلكتروني، يرى بعض الفقهاء ضرورة البحث عن وسيلة قانونية جديدة، ما لم تستطيع فكرة الإلتزام بالشهادة أن تؤديه، وهذه الوسيلة هي الإلتزام بالإعلام في الجريمة الإلكترونية وذلك بضرورة وجود نص صريح في القانون يفرض تقديم أي معلومات ضرورية من أجل إعانة سلطات التحقيق والإستدلال في الحصول على الدليل، وفرض مثل هذا الإلتزام قد يلعب دور وقائي في حفظ النظام المعلوماتي[2].

ثانيا: الخبرة تكون الخبرة في مجال المعلوماتية بتحري الحقيقة، عن طريق جمع معلومات من الأدلة الرقمية، وتحصيلها من خوادم المواقع، ومن الجهاز المعتدى عليه بعد التوصل إلى تحديده، ثم يقوم الخبير بعملية تحليل رقمي لها، لمعرفة كيفية إعدادها البرمجي، ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ثم التوصل إلى معرفة بروتكول الأنترنت للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية[3]، غير أنه قد تواجه سلطات الإستدلال والتحقيق بعض المشاكل الفنية والتقنية التي تستلزم خبير إلكتروني مختص، وهنا قد لا تتوافر مثل هذه النوعية من الخبرة في من يحملون جنسية الدولة، وهنا يثور التساؤل حول مدى إمكانية الإستعانة بخبير إلكتروني أجنبي[4]؟ فالبعض يرى أن الإستعانة بخبير أجنبي يشكل تهديد وخطر على

[1] كوثر فرام المرجع السابق الذكر، ص 93.
[2] بوعناد فاطمة زهرة المجلة السابقة الذكر، من 70.
[3] سعيداني نعيم رسالة الماجستير السابقة الذكر، ص 171.
[4] بوعناد فاطمة زهرة، المجلة السابقة الذكر، من 70.

سيادة الدولة وأمنها، والبعض يرى أنه ليس هناك مانع باللجوء إلى خبير إلكتروني أجنبي، وهو أمر تسمح به مقومات العالم الإفتراضي، باعتباره بيئة إتصالية رقمية عالمية. [1]

المطلب الثاني: إجراءات جمع الأدلة الحديثة.

تتمثل هذه الإجراءات في حفظ المعطيات والتسرب واعتراض المراسلات الإلكترونية.

الفرع الأول: حفظ المعطيات.

ألزم المشرع الجزائري مقدي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين، في حين اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير) معطيات المرور)، وهي كما عرفتها المادة الثانية من قانون رقم 09-04 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة، باعتبارها جزءا في حلقة الاتصالات توضح مصدر الإتصال، الوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة. وقد حضر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من القانون رقم 09-04 وتتضمن المعطيات التي تسمح بالتعرف على مستعملي الخدمة- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها –المعطيات التي تسمح بالتعرف على المرسل إليه، الإتصال وكذا عناوين المواقع المطلع عليها وبما أن حفظ المعطيات إجراء وقتي، واحتراما للحق في الخصوصية، فإن المشرع الجزائري فرض على

[1] سعيداني نعيم رسالة الماجستير السابقة الذكر، ص 168.

مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل، إن مزودي الخدمات يعتبرون مصدرا لجهات التحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها"[1] .

الفرع الثاني: التسرب واعتراض المراسلات الإلكترونية.

أولا: التسرب استحدث المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات، وذلك بسبب عجز الأساليب التقليدية، ومن بينها إدراج المشرع لعملية التسرب بموجب القانون رقم 06-22، مؤرخ في سنة 2006، المتضمن قانون الإجراءات الجزائية، حيث خص الفصل الخامس منه تحت عنوان" في التسرب"، المواد من 65 مكرر 11 إلى المادة 65 مكرر 18، إذ تناول من خلالها مفهوم هذه العملية وشروط إجراءها، والحماية الجنائية للقائم بعملية التسرب.

تعريف التسرب قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك، وهذا ما نصت عليه المادة 65 مكرر 12 من قانون الإجراءات الجزائية، ومثاله في الجريمة الإلكترونية إشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة، ويحاول الإستفادة حول كيفية اقتحام الهاكرز الموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم[2].

[1] سعيداني نعيم، رسالة الماجستير السابقة الذكر، من من 139 إلى 141.
[2] بوعناد فاطمة زهرة المجلة السابقة الذكر، من 69-70.

شروط صحة التسرب صدور إذن من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية – أن يكون الإذن مكتوبا ومسببا يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة يحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 04 أشهر، غير أنه يمكن أن تجدد، حيث تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على :" ... يجوز لوكيل الجمهورية أو القاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن.... حسب الحالة بمباشرة عملية التسرب .[1]

ثانيا: إعتراض المراسلات الإلكترونية: يقصد بهذا الإجراء مراقبة الإتصالات الإلكترونية أثناء بنها، وليس الحصول على اتصالات إلكترونية مخزنة، وقد استحدث المشرع الجزائري هذا الإجراء من خلال القانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، حيث حدد الحالات التي يجب فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو مؤسسات الدولة أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، أو لمقتضيات التحريات والتحقيقات القضائية، وهذا طبقا للمادة 04 من القانون رقم 09-04 ، ويترتب على المراقبة السرية للإتصالات عموما، ومن ضمنها الإتصالات الإلكترونية في الغالب تسجيل محتوى تلك الإتصالات وتخزينها على وسائط مادية قابلة للنقل بغية استخدامها فيما بعد لإثبات الجريمة الواقعة، وتختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الإلكترونية المراقبة هي عبارة عن اتصال صوتي فقط، أو أنها اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون في الثاني تسجيل صوتي مرئي ، كما تجدر الإشارة إلى أن المراقبة

[1] بوعناد فاطمة زهرة، نفس المجلة، ص 70.

السرية للإتصالات الإلكترونية، ومن ضمنها المحادثات الهاتفية، لا يمكن اعتبارها نوع من أنواع التفتيش، لأن المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة (الإتصالات الإلكترونية حال إجرائها)، دون التي انتهت وخزنت، في حين التفتيش يرد فقط على البيانات الإلكترونية الساكنة أو المخزنة (الإتصالات الإلكترونية التي تمت وخزنت، وتكون عملية المراقبة في جميع الحالات بإذن مكتوب من السلطة القضائية المختصة طبقا للمادة 04 من القانون الرقم 09 04 التي تنص على: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه، إلا بإذن مكتوب من السلطة القضائية المختصة ..."[1]

المطلب الرابع: صعوبات مكافحة الجريمة الإلكترونية.

يعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية وذلك للأسباب التالية:

- يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.
- صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام إسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنثرنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.
- تنازع القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين سوف يخضع لها الجاني ؟
- صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل المستخدم للشبكة على موقع فيحد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الإتصال، أم مورد المنافذ، أم مورد المعلومات، أو غيرهم من العاملين في مجال الأنثرنت.

[1] بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 72.

– إفتراض العلم بقانون جميع الدول ففي حالة ارتكاب الجريمة في بلد ما، وتحقق النتيجة في بلد آخر يجد الجاني نفسه يخضع لقانون هذه الدولة، وقد يكون هذا الفعل المرتكب مباح في بلده.

– صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص.

– جهل الناس بثقافة الأنترنت يجعلهم يقومون بأفعال لا يعرفون بأنها تشكل جريمة يعاقب عليها القانون[1].

– عدم ظهور الدليل المادي للجريمة الإلكترونية أو آثار مادية ملموسة.

– عجز الوسائل التقليدية عن ضبط آثار الجريمة الإلكترونية.[2]

– عولمة هذه الجريمة تؤدي إلى تشتيت جهود التحري والتنسيق الدولي، لتعقب مثل هذه الجرائم، وهي بمثابة صورة صادقة من صور العولمة[3].

– صعوبة تقدير حجم الجريمة الإلكترونية، فالإحصائيات الجنائية لا تعبر عن الإجرام الحقيقي إذ منها ما يصل إلى علم السلطات المختصة بصورة دائمة، ومنها ما لا يصل إلى علمها إلا نادرا، كالجرائم الماسة بالعرض، وهنا يظهر الفارق بين الحجم الحقيقي للجريمة الإلكترونية، وبين ما هو مسجل بالإحصائيات[4].

من خلال التطرق لمكافحة الجريمة الإلكترونية في التشريع الجزائري استنتج أنه لا بد من الوقاية من هذا النوع من الجرائم قبل انتشارها، واللجوء إلى مكافحتها، وذلك بتربية النشأ على الوازع الديني والأخلاق الفاضلة، اللذان هما بمثابة واقي للفرد يحول دون ارتكاب أي نوع من الجرائم، و يجعلان الفرد يعني مدى

---

[1] جعفر حسن جاسم الطالي، جرائم تكنولوجيا المعلومات (رؤية جديدة للحريمة الحديثة، دار البلدية، عمان الأردن، 2007، 223 ط 01، ص من 220 إلى230

[2] عبد الفتاح بيومي حجازي الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007، ص 105.

[3] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ط01، ص33.

[4] نالله عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت 2005، ط01، ص68.

خطـورة التعـدي علـى حقـوق الغيـر، عـلاوة علـى ذلـك توعيـة الأفـراد بأخطـار وسـلبيات الأنترنـت مـن خـلال عقـد نـدوات ودراسـات حـول مخـاطر الأنترنـت فـي الجامعات والثانويات، وجميع الأنشطة من جمعيات وغيرها.

فـي آخـر المطـاف، فـإنني حاولـت معالجـة الموضـوع مـن خـلال فصـلين أساسـيين، حيـث تعرضـت للفصـل الأول إلـى ماهيـة الجريمـة الإلكترونيـة، وذلـك بـالتطرق إلـى مفهومهـا المتضـمن الإتجـاه المضـيق والموسـع لهـا، وكـذا الـدوافع المؤديـة لارتكابهـا، ثـم بيـان خصائصـها التـي جعلتهـا تنفـرد عـن نظيرتهـا التقليديـة، سـواء تعلقـت هـذه الخصـائص بالجريمـة ذاتهـا، أو بـالمحرم الإلكترونـي، كمـا أن هـذا الـنمط مـن الجـرائم يتنـوع بحسـب مـا هـو واقـع أو مسـتهدف النظـام المعلومـاتي، أو مـا يرتكـب باسـتخدام النظـام المعلومـاتي هـذه الطبيعـة المتميـزة للحريمـة الإلكترونيـة جعلـت المشـرع الجزائـري يـدرك مـدى خطـورة هـذه الجريمـة علـى الفـرد وعلـى المجتمـع علـى حـدا سـواء، وكـان لا بـد مـن التصـدي لهـا، خصوصـا أن الجزائـر تشـهد اسـتعمال موسـع للتقنيـة المعلوماتيـة فـي جميـع القطاعـات وهـذا مـا تعرضـت لـه بالتفصـيل مـن خـلال الفصـل الثـاني، حيـث تطرقـت للحمايـة الموضـوعية والإجرائيـة للنظـام المعلومـاتي فـي التشـريع الجزائـري، إذ أن المشـرع الجزائـري قـام بتعـديل قـانون العقوبـات رقـم 04/15، وإصـدار قـانون رقـم 09/04 ، لمـا يتناسـب والظاهرة المستجدة.

من خلال هذه الدراسة توصلت للنتائج التالية:

– إن عـدم إجمـاع الفقهـاء علـى تعريـف موحـد للجريمـة الإلكترونيـة يعـود أساسـا إلـى الإخـتلاف حـول تحديـد نطـاق هـذه الجريمـة، خصوصـا أن الـبعض وسـع كثيـرا مـن نطاقهـا واعتبـر أن كـل فعـل غيـر مشـروع يكـون للحاسـب الآلـي دورا فيـه جريمـة إلكترونيـة، وقـد تبنـى هـذا الإتجـاه المشـرع الجزائـري، حيـث نـص علـى ذلـك فـي القـانون رقـم 04/09 ، و حـدد نطـاق الجريمـة الإلكترونيـة بالجريمـة التـي تمـس بالنظـام المعلومـاتي، أو أي جريمـة ترتكـب أو يسـهل ارتكابهـا عـن طريـق منظومـة معلوماتيـة، أو نظـام للإتصـالات، وهـو توسـيع لا يتفـق وماهيـة الجريمـة الإلكترونيـة، باعتبارهـا تسـتهدف بالدرجـة الأولـى الجانـب البرمجـي للـنظم المعلوماتية.

– إن هذه الجريمة مع تعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد والمجتمع، وهي تتسم بالغموض، حيث يصعب إثباتها والتحقيق فيها، مما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء.

– قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم 15/04، حيث اعتبر الدخول غير المشروع للنظام المعلوماتي والبقاء فيه، والمساس بمنظومة معلوماتية وبعض الأفعال الأخرى أفعال إجرامية وسطر لها عقوبات، واستدرك النقص في المجال الإجرائي، بإصدار قانون رقم 04/09 ، إذ تضمن قواعد إجرائية وأخرى وقائية وهذه خطوة إيجابية إلا أنها غير كافية لمواجهة خطر الجريمة الإلكترونية.

– إن المشرع الجزائري تطرق للجريمة الواقعة على النظام المعلوماتي، وأغفل الجرائم الماسة بمنتوجات الحاسب الآلي، حيث لم ينص على جريمة التزوير المعلوماتي، وإنما أخضعها للنصوص التقليدية الخاصة بتزوير المحرر، ولم يوسع من مفهوم المحرر ليشمل المستند المعلوماتي.

– المشرع الجزائري لم يقم بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي، وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراتها.

القرآن الكريم.

النصوص القانونية

1- الأمـر رقـم 03-07 مـؤرخ فـي 19 جمـادى الأولـى عـام 1424، الموافـق ل 19 يوليو 2003، المتعلق ببراءات الإختراع، ج و العدد 44.

2- الأمـر رقـم 03-05 مـؤرخ فـي 19 جمـادى الأولـى عـام 1424، الموافـق ل 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج را العدد 44.

3- الأمـر رقـم 04-15، مـؤرخ فـي 10 نـوفمبر 2004، المعـدل والمـتمم للأمـر رقـم الصـادر فـي 08 جـوان 1966 ، المتضـمن قـانون العقوبـات، ج ر العـدد 71.

4- الأمـر رقـم 06-22 مـؤرخ فـي 20 ديسـمبر 2006، المعـدل والمـتمم لقـانون الإجراءات الجزائية، ج و العدد 84، صادر في 2006.

5- الأمـر رقـم 09-04 مـؤرخ فـي 05 أوت 2009، يتضـمن القواعـد الخاصـة للوقايـة مـن الجـرائم المتصـلة بتكنولوجيـات الإعـلام والإتصـال ومكافحتهـا، ج ر العدد 47.

الكتب:

6- أحسـن بوسـقيعة الـوحيز فـي القـانون الجزائـي العـام الـديوان الـوطني للأشـغال التربوية، 2002، ط 01، بدون بلد نشر

7- بـن زيطـة عبـد الهـادي، حمايـة بـرامج الحاسـوب فـي التشـريع الجزائـري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط 01.

8- جعفـر حسـن جاسـم الطـائي، جـرائم تكنولوجيـا المعلومـات (رؤيـة جديـدة للجريمة الحديثة)، دار البلدية، عمان الأردن، 2007، ط 01.

9- جـلال محمـد الزعبـي، أسـامة أحمـد المناعسـة، جـرائم تقنيـة نظـم المعلومـات الإلكترونية، دراسة مقارنة دار الثقافة للنشر والتوزيع، عمان، 2010، ط 01

10- ختيـر مسـعود الحمايـة الجنائيـة لبـرامج الكومبيـوتر أسـاليب وثغـرات، دار الهدى للنشر والتوزيع، الجزائر، طبعة 2010.

11- زبيحـة زيـدان الجريمـة المعلوماتيـة فـي التشـريع الجزائـري والـدولي دار الهـدى للطباعة والنشر، الجزائر، 2011، بدون طبعة.

12- طـارق إبـراهيم الدسـوقي عطيـة الأمـن المعلومـاتي، النظـام القـانوني للحمايـة المعلوماتية، دار الجامعة الجديدة الإسكندرية 2009، بدون طبعة.

13- عبـد الفتـاح بيـومي حجـازي الإثبـات الجنـائي فـي جـرائم الكمبيـوتر والأنثرنـت، دار الكتب القانونية، مصر، 2007، بدون طبعة.

14- عبـد الفتـاح بيـومي حجـازي الـدليل الجنـائي والتزويـر فـي جـرائم الكمبيـوتر والأنترنت، دار الكتب القانونية، مصر، 2002، بدون طبعة.

15- عبد الله عبد الكريم عبد الله جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ط 01.

16- عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصـــنفات الفنية ودور الشرطة والقانون، دراسة مقارنة 2000، ط 02، بدون بلد نشر.

17- عفيفي كامل عفيفي جرائم الكمبيوتر وحقوق المؤلف والمصـــنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية بيروت، 2003، بدون طبعة.

18- محمد أمين أحمد الشـــوابكة، جرائم الحاســـوب والأنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط 0

19- محمد عبد الرحيم الناغي الحماية الجنائية للرســوم والنماذج الصــناعية (دراســة مقارنة)، دار النهضة العربية، القاهرة، 2009، بدون طبعة.

20- محمد علي العربان الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، بدون طبعة.

21- نائلة عادل محمد فريد قورة جرائم الحاســب الآلي الإقتصــادية، دراســة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005، ط 01.

الرسائل العلمية:

22- حمزة بن عقون الســـلوك الإجرامي للمحرم المعلوماتي، بحث مكمل لنيل شـــهادة الماجســـتير في العلوم القانونية، تخصـــص علم الإجرام و علم العقاب، جامعة الحاج لخضر، باتنة، 2011 2012

23- رصـاع فتيحة الحماية الجنائية للمعلومات على شـبكة الأنترنت، مذكرة لنيل شـهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان، 2011-2012

24- ســـعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شـــهادة الماجســـتير في العلوم القانونية، تخصـــص علوم جنائية، جامعة الحاج لخضر، 2013-2012 باتن

25- ســـمية مزغيش جرائم المســـاس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شـهادة الماستر في الحقوق، تخصـص قانون جنائي، جامعة محمد خيضـر بسكرة، 201-2013

26- سـوير سـفيان جرائم المعلوماتية مذكرة لنيل شـهادة الماجسـتير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد تلمسان، 2010 201

27- صـغير يوسـف الجريمة المرتكبة عبر الأنترنت مذكرة لنيل شـهادة الماجسـتير في القانون، تخصـــص القانون الدولي للأعمال جامعة مولود معمري تيزي وزو، تاريخ المناقشة .0/03/2013

28- عبد الله دغش العجمي المشـكلات العملية والقانونية للجرائم الإلكترونية، (دراسـة مقارنة)، رسالة مكملة للحصـول على درجة الماجسـتير في القانون العام جامعة الشرق الأوسط، 2014.

29- در دور نســـيم، جرائم المعلوماتية على ضـــوء القانون الجزائري والمقارن، مذكرة لنيل شـــهادة الماجســـتير، شـــعبة القانون الجنائي، جامعة منتوري قســـنطينة 2012 – 2013.

المقالات والمجلات

30- عادل يوسف عبد النبي الشكري الجريمة المعلوماتية و أزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، 2008، العدد 07

31- عبد الناصر محمد محمود فرغلي محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي 12/14/11/2007، الرياض.

32- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المنعقد بأكادمية الدراسات العليا بليبيا في أكتوبر 2009

33- كامل فريد السالك الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، 21/23/ تشرين .الأول 2000، حلب

34- محمد علي قطب الجرائم المعلوماتية وطرق مواجهتها مركز الإعلام الأمني، الأكادمية الملكية للشرطة، وزارة الداخلية.

35- مفتاح بوبكر المطرودي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث الرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23/25/09/2012

36- موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكادمية الدراسات العليا، طرابلس، خلال الفترة 28/29/10/2009

37- سميرة بيطام، الجريمة الإلكترونية وتقنية الإحرام المستحدث، culture/net.alukah.www//http/br 9 مليكة عطوي الجريمة المعلوماتية حوليات جامعة الجزائر، مجلة علمية، 01/06/2012.

38- بوعناد فاطمة زهرة مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية سيدي بلعباس 2013، العدد 01

39- سمير سعدون مصطفى محمود خضر سلمان حسن كريم عبد الرحمن، الجريمة الإلكترونية عبر الأنترنت وسبل مواجهتها، بحث مقدم بتاريخ 04/05/2011

40- بن دعاس فيصـــل إجراءات التحري في الجرائم المعلوماتية، محاضـــرة في إطار التكوين المحلي المستمر للقضاة مجلس قضاء قسنطينة

41- كوثر فرام الجريمة المعلوماتية على ضـوء العمل القضـائي المغربي، بحث نهاية التدريب المعهد العالي للقضاء، فترة التدريب، 2007-2009

14 .جازية سليماني، موقع العربي الجديد،

https//www.alaraby.co.uk/media news.

https//ar.wkipedia.org/wiki. 15

قائمـــــة المراجـــــــــع / .....