الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التّعليم العالي والبحث العلميّ

جامعة محمد البشير الابراهيمي برج بوعريريج

كلية الحقوق و العلوم السياسية

مستخرج من محضر اجتماع المجلس العلمي للكلية

المنعقد بتاريخ 05 نوفمبر 2020

بناءا على محضر اجتماع المجلس العلمي للكلية المنعقد بتاريخ : **05 نوفمبر 2020** وفي محور جدول الاعمال الخاص بالمصادقة على تحكيم المطبوعات فإنه تمت الموافقة و المصادقة على تقارير الخبرة الخاصة **بمطبوعة الدكتور(ة): لعوارم وهيبة الموسومة بـ:**محاضرات في مقياس" المدخل للجرائم الإلكترونية موجهة لطلبة السنة الاولى ماستر تخصص قانون و اعلام آلي.

وعليه تم اعتمادها مطبوعة بيداغوجية محكمة للتدريس بكلية الحقوق و العلوم السياسية.

سلمت هذه الشهادة بطلب من المعني لاستعمالها في حدود ما يسمح به القانون.

برج بوعريريج في:10 نوفمبر 2020

رئيس المجلس العلمي للكلية

رئيس المجلس العلمي

أ. د. هدفي بشير

جامعة محمد البشير الابراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

المجلس العلمي للكلية

وزارة التعليم العالي والبحث العلمي

جامعة محمد البشير الإبراهيمي
كلية الحقوق والعلوم السياسية

مقياس

المدخل للجرائم الإلكترونية

لطلاب السنة الأولى ماستر
تخصص قانون و إعلام آلي

من إعداد الدكتورة : لعوارم وهيبة
أستاذة محاضرة قسم " أ "

السنة الجامعية 2019-2020

مقدمة

لا مناص من الاعتراف بأن ظاهرة الجرائم الإلكترونية التي باتت تتخذ أنماطا جديدة وضربا من ضروب الذكاء الإجرامي ، تمثل بلا شك تحديا جديا وجديدا في الوقت الحاضر ، تجاوزه يتطلب التعرف على هذه التحديات وإبراز جوانبها ، بما يعني التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب من ناحية ، وعلى صعيد الملاحقة الإجرائية من ناحية أخرى ، وهذا أمر يستلزم : أولا - الانطلاق من الاقتناع بخطورة هذه الظاهرة ، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية ، والنزول ولو بقدر أمام ضرورات ومقتضيات التعاون القضائي الدولي الذي بقدر نجاحه تتحقق فعالية كل الجهود والإمكانيات المسخرة للتصدي لظاهرة الجرائم الإلكترونية ومكافحتها ، وثانيا – تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل ودؤوب يسد ثغرات الأنظمة الجنائية على نحو يجعلها قادرة على إخضاع هذه الجرائم لأوصافها ونصوصها ، ومواكبة التطورات التي يتوسل بها مرتكبو هذه الجرائم ، على أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وأن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية .

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية ، فإننا نعتقد إن كان لهذا الرأي شيئا من الواقعية ، وهي أن بعض النصوص القائمة تواجه بعض الأنشطة المجرمة التي ترتكب بطريق الإنترنت ، فإنه ينبغي ألا ننكر أن هناك نصوصا أخر صادف تطبيقها بعض الصعوبات ، منها ما يتعلق بطبيعة الجريمة الإلكترونية غير المادية ، ومنها ما يتعلق بهاجس التعارض مع مبادئ هامة ومستقرة في القانون الجنائي ، كمبدأ شرعية الجرائم والعقوبات والتفسير الضيق ، دعا مشرعو بعض الدول إلى التدخل بتعديل بعض النصوص القائمة أو وضع نصوص جديدة تتلاءم وتلك الجرائم ، ودعا أيضا القضاء إلى التوسع في تفسير النصوص الجنائية السارية لكن أصبحت هناك أولوية ملحة ينبغي إنجازها على الصعيد التشريعي ،

و عليه سنتطرق لهذا الموضوع بموجب فصلين :

الفصل الأول نخصصه للأحكام الموضوعية للجريمة الإلكترونية ،

الفصل الثاني نعالج فيه الأحكام الإجرائية للجريمة الإلكترونية .

الفصل الأول

الأحكام الموضوعية للجريمة الإلكترونية

تعتبر الجريمة الإلكترونية أكبر تحدي يواجه رجال القانون نظرًا لكونها مرتبطة بالتطور التكنولوجي الهائل الذي تشهده علوم الكمبيوتر في الآونة الأخيرة ، ونظرا لخصوصة هذه الجريمة عن الجريمة التقليدية فلقد التشريع الوطني وكذا مختلف المواتيق الدولية والتشريع المقارن بأحكام تتجاوب و خصوصيتها ،

فمن خصوصية الجريمة الإلكترونية أن بعض حالات ارتكابها يتعمد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة منها مجال المعالجة الإلكترونية للبيانات ، ومجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية، في المجال الأول : يتدخل الجاني من خلال ارتكاب الجريمة الإلكترونية في مجال المعالجة الإلكترونية (الآلية) للبيانات ، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسب الآلي ، وذلك بغرض الحصول على المعلومات ، وفي المجال الثاني : يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات ، وهي طريقة أوتوماتيكية تمكن مستخدم الحاسب الآلي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات الموجودة تحت يده ، وبفضل إمكانيات الحاسب الآلي تتاح إمكانية التصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة ، وهي بذلك علاقة وثيقة بارتكاب الجريمة[1].

كما أنه غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه، مقارنة بالجرائم التقليدية ،فقد أكدت " أنتل سكيورتي " الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات ، أن قطاعات الأعمال العالمية تتكبد خسائر سنوية تصل إلى 400 مليار دولار أمريكي ، وأوضحت الشركة أن الهجمات الإلكترونية أصبحت اقتصادا متناميا قائما بذاته تبلغ قيمته مابين 2إلى 3 ترليون دولار

[1] محمد على العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر، الإسكندرية ، 2004 ، ص37 .

سنويا ،أي ما يشكل 15إلى20 ٪ من القيمة الاقتصادية الناتجة عبر الانترنت ، وقد تكبدت شركة بريطانية خسائر بلغت 1.3 مليار دولار بسبب هجوم إلكتروني واحد .

لذا أضحى التطرق إلى ماهيتها و الأحكام الخاصة بها أمرا لابد منه من خلال المباحث التالية

المبحث الأول

ماهية الجريمة الالكترونية

ترتب على ظاهرة الجريمة الإلكترونية تحديات عدة : منها ظهور وتنامي الأنشطة الإجرامية الالكترونية وتَوَسُّل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشطة داخل حدود الدولة وخارجها ، الأمر الذي أدى إلى انشغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها ، من حيث تستعصي بعض الأنشطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ؛ ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية .

المطلب الأول

مفهوم الجريمة الإلكترونية

تعددت تعريفات الجريمة المعلوماتية و تباينت فيما بينها ما ترتب عنه تعذر إيجاد فهم مشترك لها، نتطرق في هذا المطلب لتعريف الجريمة الإلكترونية تعريفا فقهيا وقانونيا،وخصائص الجريمة المعلوماتية إضافة لتصنيف الجرائم المعلوماتية ، بحيث قسمنا هذا المطلب إلى ثلاث فروع ندرس في الفرع الأول تعريف الجريمة المعلوماتية وفي الفرع الثاني خصائصها وفي الفرع الثالث تصنيف الجرائم المعلوماتية.

الفرع الأول

تعريف الجريمة الإلكترونية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، إذ يطلق عليها البعض الجريمة الإلكترونية وهناك من يسميها الجريمة المعلوماتية، ويذهب أخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال ويطلق عليها آخرون مسمى جرائم الكمبيوتر والإنترنت،ويرجع السبب لهذا الإختلاف إلى كون الإطار أو البيئة الخاصة لهذه الظاهرة الجرمية لا تزال في طور التطور.[2]

أولا : التعريف الفقهي

هناك من يعرفها " تلك الجرائم التي لا تعرف الحدود الجغرافية ،و التي يتم إرتكابها بأداة هي الحاسب الآلي عن طريق شبكة الأنترنت وبواسطة شخص على دراية فائقة بها" [3]، كما تعرف " كل فعل أو إمتناع يتم إعداده أو التخطيط له ، ويتم بموجبه إستخدام أي نوع من الحواسيب الآلية سواء حاسب شخصي أو شبكات الحاسب الآلي أو الأنترنت أو وسائل التواصل الإجتماعي لتسهيل إرتكاب جريمة أو عمل مخالف للقانون ، أو تلك التي تقع على الشبكات نفسها عن طريق إختراقها بقصد تخريبها أو تعطيلها أو تحريف أو محو البيانات أو البرامج

التي تحويها ."[4]

يمكننا إستخلاص تعريف أقره المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته " جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوب

---

[2]علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية والأدبية، ط1،2013 ، ص 76 .

[3]رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، ص 40 .

[4]عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014،ص 14 .

وتشمل من الناحية المبدئية ، جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية "[5]، وهذا التعريف قد تبناه لفقه الجزائري [6] ،

ثانيا : التعريف القانوني

إن المشرع الجزائري خطا خطوات هامة وسريعة في هذا المجال وذلك بالتكفل بتجريم صور الإعتداء على شبكة الأنترنت والمساس بالبيانات المعالجة آليا :

1- **قانون العقوبات (المعدل بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004)**[7] :

تم بموجب التعديل الحاصل لقانون العقوبات إحداث قسم جديد تحت عنون " المساس بأنظمة المعالجة الآلية للمعطيات " إحتوى أهم الجرائم التي تستهدف الأنظمة المعلوماتية بمقتضى القانون 15/04 المؤرخ في 10 نوفمبر 2004 من المواد 394 مكرر إلى 394 مكرر 7 ، بل لم يكتف عند ذلك الحد بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد حين بادر بتعديل جديد لقانون العقوبات بموجب القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 وإقرار المادة 303 مكرر إلى 303 مكرر 3 وهو بذلك وضع سياجا لحماية خصوصية الأفراد تحسبا للاستخدام السيء للوسائل التكنولوجية الحديثة . [8]

ومن الجرائم ، جريمة الدخول غير المشروع في المنظومة المعلوماتية [9]، جريمة البقاء غير المشروع في نظام المنظومة المعلوماتية[10]، جريمة إدخال معطيات في نظام المعالجة الآلية للمعطيات أو إزالتها بطرق تدليسية[11] ،جرائم نشر المعطيات المخزنة أو معالجة أو مرسلة بواسطة منظومة معلوماتية و

---

[5] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 42 .

[6] زبيحة زيدان، المرجع نفسه، ص 43 -44 .

[7] القانون15/04 المؤرخ في 10/ 2004/11 المعدل والمتمم للأمر156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج ر، عدد 71، في 10/11 /2004 .

[8] زبيحة زيدان، المرجع السابق، ص 48 .

[9] نص عليها المشرع في المادة 394 قانون العقوبات .

[10] نصت عليه المادة 394 مكرر قانون العقوبات كما نصت المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي .

[11] نصت عليها المادة 394 مكرر1 من قانون العقوبات

حيازتها والإتجار فيها [12]، جريمة تجميع أو توفير بيانات مخزنة أو معالجة آليا [13]،جريمة نشر المعطيات وإفشائها [14]،جريمة إعاقة سير المعلومات المرسلة عن طريق منظومة معلوماتية [15]، جريمة حيازة البيانات أو المعطيات[16]، الجريمة المنصوص عليها في المادة 394 مكرر 3 بارتكاب الجرائم السالفة الذكر إضرارا بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام . [17]

ب-القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (القانون 09-04 المؤرخ في 5 أوت 2009)

عرف الجريمة الإلكترونية من خلال نص المادة 2 فقرة-أ- " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية . " [18]

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" معتبرا أن النظام المعلوماتي في حد ذاته محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة و إلا فلا محل للجريمة .

ونظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب إدراك حقيقته، فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات تاركا مهمة ذلك للفقه و القضاء، فعرفه الفقه الفرنسي على أنه " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج و المعطيات وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن

---

[12] طبقا للمادة 394 مكرر2 من قانون العقوبات

[13] نص عليها المشرع في المادة 394 مكرر2 من قانون العقوبات

[14] نص عليها المشرع في المادة 394 مكرر2/ 1 من ق ع

[15] بموجب المادة 394 مكرر2 ق ع

[16] في المادة 394 مكرر2 من ذات القانون .

[17]- مختار الأخضري، محاربة الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، الجزائر، 2010 ص 56 .

[18]القانون رقم 09-04، المؤرخ في 25 شعبان 1430 هـ الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج رع 47، الصادرة بتاريخ 16-08-2009، ص 5 .

طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية. "[19]

ج-القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة :

نص القانون 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة،[20] على تجريم انتهاك حقوق المؤلف والحقوق المجاورة عن طريق التقليد بأي وسيلة كانت فيها منظومة معالجة معلوماتية.[21]

د- القانون 03-2000 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية [22]

وضع هذا القانون القواعد التي تنظم مختلف شبكات المواصلات السلكية واللاسلكية مهما كانت الوسيلة المستعملة سواء أسلاك بصريات أو لاسلكي كهربائي أو أجهزة أخرى كهربائية مغناطيسية.

الفرع الثاني

خصائص الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من بين الجرائم المستحدثة ، التي أتى بها التطور في مجال الإتصالات ، وتتميز بـ :

---

[19] سومية عكور، الجرائم المعلوماتية وطرق مواجهتها : قراءة في المشهد القانوني والأمني، الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الفترة من 2-4 / 2014/09، كلية العلوم الإستراتجية، عمان، الأردن، 2014، ص 5 .

[20] القانون 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، ج . رعدد 44، المؤرخة في 23 جويلية 2003، ص 21 .

[21] المادة 152 .

[22] القانون 03-2000 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية ،ج رعدد 48، المؤرخة في 6 أوت 2000، ص 7.

1 - شخص مرتكب الجريمة

*- مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي، في حين أن مرتكب الجريمة التقليدية في الغالب شخص بسيط ، متوسط التعليم ، فتتطلب الجريمة الإلكترونية مقدرة عقلية وذهنية فيكون لدى الجاني كفاءة عالية في مجال التقنية بل أن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال التقنية فالخبرة الكبيرة والدراية الفائقة بكل ما يتعلق بالحاسب الآلي وشبكة الانترنيت، والمهارة والذكاء في المجال التقني و المعلوماتي هي ما تميز مرتكب هذه الجريمة المعلوماتية.

نظرا للصفات التي تتمتع بها هذه الجريمة و الصعوبات التي تثور عند محاولة اكتشافها، فإن ذلك يشكل إغراء كبير للمجرمين خصوصا أنه يمكن تحقيق مكاسب طائلة من ورائها لذا فهي تستهوي الكثيرين [23].

*- تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها ، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه والاشتراك في إخراج الجريمة الإلكترونية إلى حيز الوجود ، قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها ،وقد يكون اشتراكا إيجابيا يتمثل في مساعدة فنية أو مادية.[24]

*- مرتكب الجريمة الإلكترونية يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي ، في حين أن مرتكب الجريمة التقليدية غالبا ما يكون غير متكيف اجتماعيا وباعثه هو النفع المادي السريع، كما أنها تعتبر أقل عنفا من الجرائم التقليدية، فلا تحتاج إلى أدنى مجهود عضلي بل تعتمد على الدراية الذهنية والتفكير

---

[23] ثنيان ناصر آل ثنيان، الجريمة الإلكترونية، رسالة ماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2012، ص 24 .

[24] ثنيان ناصر آل ثنيان، المرجع السابق، ص 28 .

العلمي المدروس ، فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه هذا النوع من المجرمين اعتبارا أن هؤلاء ليسوا من محترفي الإجرام بالصيغة المتعارف عليها.

2- محل الجريمة

*- تستهدف الجريمة الإلكترونية المعنويات لا الماديات، و ذلك يشكل صعوبة جمة في مجال الإثبات لأن الجاني لا يترك وراءه أي أثر مادي خارجي يمكن فحصه ، ما يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها ، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا أو شهادة شهود كما أن موضوع التفتيش والضبط قد يتطلب أحيانا امتداده إلى أشخاص آخرين غير المشتبه نظرا لارتكابها في الخفاء ،أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات و المؤسسات المجني عليها ، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة ، بحيث تكون البيانات والمعلومات المتداولة عبر شبكة الانترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لاسيما وأن الجاني عمد إلى عدم ترك أثر لجريمته ، إضافة لما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني ، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات المخزنة بحيث تكون هذه المعلومات عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة ، ومثال ذلك قيام الجاني بمسح البرامج أو وضع كلمات سرية ورموز وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه .[25]

*- الحاسب الآلي ومن في حكمه كالهاتف النقال أداة الجريمة الإلكترونية لأنه يمكن الشخص من الدخول إلى شبكة الانترنت وقيامه بتنفيذ جريمته أيا كان نوعها ، ومن بين الجرائم الإلكترونية، التزوير المعلوماتي وسرقة الإلكترونية للمعلومات المخزنة .[26]

---

[25] المرجع نفسه، ص 20.

[26] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار الكتب القانونية، مصر ط1، 2009، ص 27.

ويرى جانب من الفقه أن جريمة الحاسب الآلي هي أفعال جديدة ينجم عنها أضرار جسيمة وخسائر اقتصادية ومالية فادحة ، بعضها يرتكب بمناسبة المعلوماتية مثل جرائم الإعلانات أو الدعاية الكاذبة أو الجرائم الجمركية وهناك جرائم ترتبط بالمعلوماتية ذاتها يطلق عليها ،غش المعلوماتية وهذه الجرائم حسب هذا الرأي يمكن تصورها حسب دور الحاسب الآلي فيها وعما إذا كانت الجريمة قد وقعت عن طريقه أو وقعت عليه. [27]

3- البعد الدولي للجريمة

*- الجريمة الإلكترونية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية، وهو ما يعني أن مساحة مسرح الجريمة الإلكترونية لم تعد محلية بل أصبحت عالمية ، الأمر الذي خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة ، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية ، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام . [28]

*- تتسم الجرائم الإلكترونية بسرعة التنفيذ ، بحيث يمكن تنفيذها خلال جزء من الثانية وبصورة خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة ،فالجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة والإمعان في حجب السلوك المكون لها وإخفاءه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها ، فعند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة وإتلافها غالبا ما تكون خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها وذلك بحكم المعرفة والخبرة لدى الجاني .[29] فهي تتم في بيئة

---

[27] علي محمد سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة بابل للعلوم الإنسانية، كلية القانون، جامعة بابل، المجلد 14، العدد 6، 2007، ص 92 .

[28] عبد الله دغش العجمي، المرجع السابق، ص 22 .

[29] خبير عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض،2007 ، ص 11 .

خاصة رقمية تتميز بخطورتها المتناهية على الأفراد والحكومات والشركاء، ما يهدد الأمن السياسي و الاقتصادي للدول.[30]

الفرع الثالث

الطبيعة القانونية للجريمة الإلكترونية

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات ، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت ، لذلك انقسم الفقه اتجاهين : الأول يرى أنه وفقا للقواعد العامة أن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ ، وأن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة ، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ ، إلا في ضوء حقوق الملكية الفكرية ، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة ، ما لم تكن مسجلة على اسطوانة أو شريط ، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية ، فلا تثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية ، وإنما المشكلة تثور عندما نكون أمام سرقة مال معلوماتي غير مادي ؛ والاتجاه الثاني يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية ، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة ، وأنها ترتبط كما يقول الأستاذان Catala وVivant بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه ، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي ، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال [(31)].

وعلى الصعيد نفسه ثمة من يقول إنه يجب أن نفرق بأن هناك مالاً معلوماتيا ماديّا فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال

---

[30] محمد علي سالم، حسون عبيد هجيج، المرجع السابق، ص 92 .

[31] محمد على العريان ، المرجع السابق ، ص43 وما بعدها .

، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي الشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات من على بعد ، كما هو الحال في جرائم التجسس عن بعد ، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمته المادية وهي ثمن الشريط أو ثمن الاسطوانة ، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج ، ويرى أصحاب هذا الرأي أن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات ، وأنها لا يمكن أن تكون شيئا ملموسا محسوسا ، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي ، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته ، وبالتالي لها كيان مادي ، يمكن الاستحواذ عليه (البرامج والمعلومات) ، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة (أي المعلومات) غير مادي ، فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية) ، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[32] .

وردا على قول الرافضين لملكية الغير للشيء المعلوماتي بأن البرنامج والمعلومة من ذات نوع الخلق الفكري الذي ليس ملكا لأحد ، قال أصحاب هذا الرأي أن البرنامج من الناحية القانونية تعتبر ملكا لمن ابتكرها ، وأن التحليل المنطقي لا يمكنه إنكار ملكية شخص ما للبرنامج والمعلومة ، ومن ثم فهي ليست ملكا للسارق ، بل هو يقوم بالاستحواذ على شيء ليس مملوكا له .

يحسب للمشرع الفرنسي محاولته - التي لم يكتب لها النجاح - تعديل قانون العقوبات الجديد بالنص على تجريم سرقة المال المعلوماتي المعنوي المتمثل في البرامج والمعلومات ، وذلك في نص المادة 1/307 الذي استعمل فيه كلمة التقاط (Capter) لتعبر عن الاختلاس ، حيث نص على أن " كل من التقط بطريق الاختلاس والتحايل برنامج أو معلومات أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات يعاقب ....."

---

[32] هدى حامد قشقوش ، مرجع سابق ، ص51-52

ونعتقد أيضا بأن التسليم بأن المال المعلوماتي المعنوي غير قابل للاستحواذ وليس مالا ، وبالتالي غير قابل للسرقة سيؤدي إلى تجريده من الحماية القانونية الجنائية ويفتح المجال واسعا أمام مجرمي وقراصنة البرامج والمعلومات .

باعتبار أن المال ينقسم إلى نوعين منفصلين وفقا لطبيعته ، فهو إما مال معلوماتي ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أيا كان نوعها ، وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في أدوات والآت الحاسب الآلي الملموسة ، إذ قد يترتب على اختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلافا في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي ، ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية ، فالاعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة قانية ذات طبيعة خاصة يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط الممغنط أو الاسطوانة الممغنطة ، وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات ، وهي جريمة مستحدثة تناولها المشرع الفرنسي بموجب القانون رقم 19لسنة 1988 بشأن بعض جرائم المعلوماتية في مادته 2/462 .

ومن خلال تحديد الطبيعة القانونية للمال المعلوماتي المعتدى عليه ، يمكن تحديد الطبيعة القانونية للجريمة الالكترونية والوضع القانوني للبرامج والمعلومات ، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت ، وقد سبق التعرض لهذا الموضوع في المطلب الأول من هذا المبحث .

الفرع الرابع

تصنيف الجريمة الإلكترونية

اختلف فقهاء القانون الجنائي في تصنيف الجرائم الإلكترونية، ويرجع سبب ذلك إلى مدى اختلاف الاعتماد على وسائل التقنية الحديثة والنظم المتعلقة و تغير أنماط تلك الجرائم تبعا للتطور التقني وأساليب الحماية الأمنية لكن هناك من يعتمد في تصنيفها إلى معيارين رئيسيين هما مواطن الاختراق

ومدى مساسها بالأشخاص أو الأموال

1- تصنيف الجرائم حسب مواطن الاختراق

- **اختراق الأمن العادي:** كالاحتيال بملفات التقنية والاحتيال والالتقاط السلكي والاحتيال باسترقاق الأمواج وإنكار أو إلغاء الخدمة .
- **اختراق الأمن الشخصي للأفراد** : كالاحتيال بانتحال صلاحيات شخص مفوض والهندسة الاجتماعية والإزعاج والتحرش وقرصنة البرمجيات .[33]
- **اختراق الحماية الخاصة بالاتصالات وأمن البيانات** : كالاعتداء على البيانات والاعتداء على البرمجيات .
- **الاعتداء على عمليات الحماية:** كغش البيانات والاحتيال على بروتوكولات الانترنت والتقاط كلمات السر والاعتداء باستغلال المزايا الإضافية .

2- تصنيف الجرائم حسب مساسها بالأشخاص والأموال

أ- الجرائم التي تستهدف الأشخاص : ومن أبرزها :

*- **الجرائم غير الجنسية التي تستهدف الأشخاص** وتشمل:القتل بالكمبيوتر والتسبب بالوفاة ، جرائم الإهمال المرتبط بالكمبيوتر التحريض على الانتحار، التحريض القصدي للقتل عبر الانترنت ، والتحرش والمضايقة عبر وسائل الاتصال المؤتمنة أو التسبب بضرر عاطفي عبر وسائل التقنية والملاحقة عبر الوسائل التقنية الإطلاع على البيانات الشخصية وقنابل البريد الإلكتروني وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به وبث المعلومات المضللة أو الزائفة والانتهاك الشخصي لحرمة الكمبيوتر أي الدخول غير المصرح [34].

*- **الجرائم الجنسية :** وتشمل نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام و للقاصرين بوجه خاص، نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، إغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، حض وتحريض

---

[33] أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، ط1، 2011، ص 140.

[34] أمير فرج يوسف، المرجع السابق، ص 138 .

القاصرين على أنشطة جنسية غير مشروعة، التحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية، واستخدام الانترنت لترويج الدعارة بصورة قصرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال لدى المستخدم، للحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية .

وبإمعان النظر في هذه الأوصاف نجد أنها تجتمع جميعا تحت صورة واحدة وهي استغلال وسائل تقنية المعلومات لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة .

ب- الجرائم التي تستهدف الأموال باستثناء السرقة

وتشمل أنشطة الاقتحام أو الدخول أو الاتصال غير المرخص به مع نظام الكمبيوتر أو الشبكة إما مجردا أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر وإيذاء الكمبيوتر واغتصاب الملكية وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص وإدخال معطيات خاطئة أو مزورة إلى نظام الكمبيوتر ،والتعديل غير المصرح به لأجهزة ومعدات الكمبيوتر ،والإتلاف غير المصرح به لنظم الكمبيوتر وأنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات ، وأنشطة الاعتداء على الخصوصية (وهذه تخرج عن مفهوم الجرائم التي تستهدف الأموال لكنها تتصلب جرائم الاختراق) وإفشاء كلمة سر الغير والحيازة غير المشروعة للمعلومات ، وإساءة استخدام المعلومات ونقل معلومات خاطئة مثل: القرصنة ، التشويه ، الفيروسات وغيرها.[35]

ج- جرائم الاحتيال والسرقة

ذلك أن المعلومات والبرامج والبيانات المعالجة إلكترونيا وفي الوقت الحاضر ترتب حقوقا لصاحبها وتخوله إبرام عقود متعلقة بها مثل عقد الإيجار والحفظ والبيع وأي صورة أخرى من صور الاستغلال

[35] علي عبود جعفر، المرجع السابق، 93

لأن من خصائص المعلومات القابلية للانتقال ، وكل هذه الأمور ترتب حقيقة هامة وهي أن المعلومات مال ليس لوجود علاقة بين المال - المذكر – وصاحبه ، وإنما بسبب أن لهذه المعلومات قيمة اقتصادية فهي تطرح في السوق للتداول ، مثلها مثل أي سلعة ، ولها سوق تجاري يخضع لقوانين السوق الاقتصادية وتشمل جرائم الاحتيال التلاعب بالبيانات والنظم أو استخدام الكمبيوتر للحصول على أو البطاقات المالية للغير بدون ترخيص أو تدميرها ، والاختلاس عبر الكمبيوتر أو بواسطته وسرقة معلومات الكمبيوتر وقرصنة البرامج وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر [36].

د- جرائم التزوير

يمكن أن يتم التزوير على المعلومات المعالجة آليا داخل الكمبيوتر والمسجلة على قرص صلب أو مرن ومن هنا يمكن القول بتطبيق ذلك على برنامج الكمبيوتر ،عندما يكون هذا البرنامج قد دون على أسطوانة ،أو شريط ممغنط بحيث يعتبر محرر،ومن ذلك فإن تغيير الحقيقة فيه يعد تزوير لانتقال المعطيات والمعلومات المخزنة إلى جسم مادي ،يأخذ صفات المحرر المكتوب ،الذي يمكن قراءته بالعين عن طريق الكمبيوتر والكشف عن مضمونه من قبل ،وتشمل جرائم التزوير (تزوير البريد الإلكتروني وتزوير الوثائق والسجلات وتزوير والهوية.)[37]

هـ جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب

وتشمل تملك وإدارة وتسهيل مشروعات المقامرة على الانترنت وتشجيع مشروع المقامرة عبر الانترنت واستخدام الانترنت لترويج الكحول ومواد الإدمان للقصر .[38]

و- جرائم الكمبيوتر ضد أمن الدولة

---

[36] عبد الفتاح بيومى حجازى، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ،دار الفكر الجامعي، الإسكندرية ، مصر، ط1، 2006، ص 25 .

[37] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، طبعة 2010، ص 136 .

[38] أمير فرج يوسف ، المرجع السابق ، ص 142.

إن الدخول على حاسبات الدولة التي تتضمن أسرارها والمعلومات المتعلقة بأمنها وجيشها ،هو من الجرائم التي تقع على أمن الدولة ، وإن إثارة الفتن الطائفية عبر البريد الإلكتروني من الجرائم التي تمس أمن الدولة ، وإن اختراق الأسرار السياسية والعسكرية للدولة من الجرائم الخطيرة التي تقع على أمنها ، وكذلك إثارة الفتن فجميعها من الجرائم الواقعة على أمن الدولة وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون

والإخفاق في الإبلاغ عن جرائم الكمبيوتر والحصول على معلومات سرية والإرهاب الالكتروني وغيرها[39].

ومن الملاحظ أن بعض هذه التقسيمات ،لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم ، حيث أن جرائم الحاسوب تنصب على معطيات الحاسوب**(بيانات ومعلومات وبرامج)** ،وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب، وإلى أن الجرائم التي تنصب على الكيانات المادية مما يدخل في نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستجدة لجرائم الحاسوب.

وهناك **من يصنف الجرائم المعلوماتية إلى :**

1-تصنيف الجرائم المعلوماتية تبعا لنوع المعطيات ومحل الجريمة

استنادا إلى هذا المعيار يمكن تقسيمها الجرائم المعلوماتية إلى الطوائف التالية :

الطائفة الأولى : الجرائم الماسة بقيمة معطيات الحاسوب:وتشمل هذه الطائفة فئتين :

***- الجرائم الواقعة على ذات المعطيات :** ويقصد بها الجرائم التي تستهدف معطيات الحاسب الآلي من برامج وتطبيقات وبيانات ، وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به ،كجرائم الإتلاف حيث نجد أن الإتلاف المعلوماتي قد يتخذ عدة صور منها منها:

* شطب المعلومات والبيانات المخزنة على الحاسوب ومحوها كليا

[39] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن ط1، 2011، ص 62.

* تخريب البيانات والمعلومات وتعديلها بحيث يتم تشويهها وجعلها غير صالحة للاستعمال بما في ذلك استخدام وسيلة (الفيروسات التقنية)[40].

*** الجرائم الواقعة على ما تمثله المعطيات آليا:** من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال، حيث يعتبر الغش المعلوماتي من أبسط جرائم الحاسب الآلي وأكثرها انتشارا إلا أنه من الصعب اكتشافها وضبط الجناة فيها ويتم تنفيذ هذا النوع من جرائم الحاسب الآلي بتعديل المعلومات قبل أو أثناء الإدخال في الحاسب الآلي ويمكن أن يتم هذا التعديل من قبل أي شخص له صلاحية الوصول إلى إجراءات الإعداد ، التسجيل ، النقل ، الفحص ، المراجعة أو تحويل المعلومات ومن أمثلة ذلك التزوير والتزييف وتبادل شرائط الحاسب الآلي وبطاقاته وأقراصه مع تحضير البدائل ومخالفة ضوابط الدخول على المصادر وإحداث تغذية إضافية وتفادي المراجعة اليدوية [41]، إضافة لجرائم الاتجار بالمعطيات، وجرائم التحويل والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها لتزوير المستندات المعالجة آليا وذلك بهدف الحصول على الأموال وتكاد تنحصر الطرق الاحتيالية المستخدمة في الحصول على الفوائد والمكاسب المادية والأموال المعلوماتية في :

* استغلال المواقع الانترنت للمشاركة في مشاريع وهمية تجارية أو صناعية .

* التدخل في النظام المعلوماتي بطريقة غير مشروعة .

* إدخال معلومات أو برامج وتعديلها وإنشاء تأمينات بنكية مزيفة مع إيهام الغير بأنها تدار من قبل بنوك معروفة .[42]

الطائفة الثانية : الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة

معظم الجرائم التي ترتكب على شبكة الانترنت تستهدف إما أشخاص وإما جهات بعينها ، وغالبا ما تكون الجرائم هي جرائم مباشرة ترتكب في صورة ابتزاز أو تهديد ، أو تشهير ، أو هي جرائم غير مباشرة ترتكب في صورة الحصول على البيانات أو المعلومات الخاصة بتلك الجهات والأشخاص وذلك

---

[40] خالد عياد الحلبي، المرجع نفسه، ص 69 .

[41] محمد الأمين البشرى، المرجع السابق، ص 92 .

[42] خالد عياد الحلبي، المرجع السابق، ص 102 .

لاستخدام تلك المعلومات والبيانات بعد ذلك في ارتكاب جرائم مباشرة [43]وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة[44].

الطائفة الثالثة : الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) والتي تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع[45].وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر و المحرك للاعتداء انصب على قيمتها أو ما تمثله.والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.هذا من جهة،

ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة و حماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال) كل في ميدان وموقع مستقل. وهو في الحقيقة تمييز - ليس مطلقا - بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية. ولا بد لنا من الإشارة إلى أن حماية أمن المعطيات انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر إلى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق

---

[43] أمير فرج يوسف، المرجع السابق، ص 20 .

[44] على عبود جعفر، المرجع السابق، ص 88 .

[45] المرجع نفسه، ص 89 .

الجرائم الماسة بقيمة المعطيات، والتي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم .[46]

2- تصنيف الجرائم تبعا لدور الوسيط الإلكتروني في الجريمة

فقد تضمن هذا التصنيف ربع طوائف رئيسية لجرائم الكمبيوتر والانترنت :

الطائفة الأولى : الجرائم التي تستهدف عنصر (السرية والسلامة) المعطيات والنظم وتظم

- الدخول غير القانوني (غير المصرح به) إلى نظام معلوماتي وعبور الحدود غير المسموح به أو التسبب بأضرار نتيجة هذا الدخول غير القانوني وهو ما يطلق عليه الانتهاك السبيراني ، - الاعتراض غير القانوني ، -تدمير المعطيات ، - اعتراض النظم ، - إساءة استخدام الأجهزة .[47]

الطائفة الثانية : الجرائم المرتبطة بالكمبيوتر وتضم

- التزوير المرتبط بالكمبيوتر ،- الاحتيال بالكمبيوتر وتشمل أفعال الاختلاس عبر وسائل المعلومات واستخدام وسائل تقنية المعلومات للحصول على أو استخدام البطاقات المالية دون ترخيص .

الطائفة الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وهي الجرائم المتعلقة بالأفعال الإباحية وغير الأخلاقية وتشمل الأنشطة التي تخرق القوانين المتعلقة بالفحش.[48]

الطائفة الرابعة : الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات.[49]

ويتبين من خلال كل هذه التقسيمات مدى لزومية الحاسب الآلي في الجرائم المعلوماتية ، فلا جريمة معلوماتية بدون جهاز حاسب ، بمكوناته المادية و البرامجية ، فالحاسب الآلي إما أن يكون هدفا للجريمة أو أداة لها ، أو بيئة لها، وأخيرا أداة للكشف عنها ومكافحتها، ويمكن توضيح ذلك على النحو التالي :

---

[46] أمير فرج يوسف ، المرجع السابق ، ص 148 .

[47] أمير فرج يوسف ، نفس المرجع ،ص 149 .

[48] علي عبود جعفر، المرجع السابق ، ص 91 .

[49] سمير شعبان، المرجع السابق، ص 120 .

1-الحاسب الآلي هدفا للجريمة : وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها ، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم .

2-الحاسب الآلي أداة الجريمة لارتكاب جرائم تقليدية .

3-يكون الحاسب الآلي بيئة الجريمة : وذلك كما في تخزين البرامج المقرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه كأداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها .

4- دورالحاسب الآلي في اكتشاف الجريمة : يستخدم الحاسب لآلي على نطاق واسع في جميع مراحل الإثبات بدءا من مرحلة جمع الاستدلالات وحتى تنفيذ الحكم مرورا بالإثبات العلمي الجنائي المتمثل في أعمال الخبرة القضائية ، حيث يلعب الحاسب لآلي ذاته دورا رئيسيا في كشف جرائم الحاسب لآلي وتتبع فاعليها بل وإبطال أثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات .[50]

المطلب الثاني

أركان الجريمة الإلكترونية

تتخذ الجريمة المعلوماتية من الفضاء الإفتراضي مسرحا لها ، وهذا مايجعلها تنفرد بخصائص تميزها عن الجريمة التقليدية ، غير أن ذلك لا يعني أنها لا تتشابه مع الجريمة التقليدية ، فهي تتشابه معها في وجود الفعل غير المشروع والمجرم الذي يقوم بالفعل المجرم ، سنحاول من خلال هذا المطلب التطرق إلى الأركان التي تقوم عليها الجريمة ، وذلك من خلال تقسيم هذا المطلب إلى ثلاث فروع ، في الفرع الأول نبين مدى انطباق مبدأ الشرعية على الجريمة المعلوماتية ،وفي الفرع الثاني نتطرق للركن المادي ، لننتهي إلى تحديد الركن المعنوي في فرع ثالث .

الفرع الأول

[50] عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، المرجع السابق، ص 7-8 .

الركن الشرعي

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

ويقصد بالركن الشرعي اعتراف المشرع والنص على تجريم الفعل المرتكب " لا جريمة ولا عقوبة إلا بنص." بالنسبة للتشريع الجزائري فقد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان" **المساس بأنظمة المعالجة الآلية للمعطيات "**[51]

ويعرف كذلك" الصفة غير المشروعة للفعل ، وتتمثل قاعدة التجريم والعقاب للجرائم الإلكترونية في ما ورد النص عليه في قانون جرائم أنظمة المعلومات ".[52]، ويترتب على إعمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة ، تتمثل في عدم رجعية القاعدة الجنائية ، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري و لا مجال لإعمالها بأثر رجعي ،إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم .

والركن الشرعي للجريمة يقوم على ركيزتين أساسيتين : مطابقة الفعل لنص التجريم، و ألا -يخضع الفعل المرتكب لسبب من أسباب الإباحة ،ويقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة ، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة .

---

[51] عاقلي فضيلة ،الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الرابع عشر الجرائم الإلكترونية، من 24-25 مارس 2017، طرابلس لبنان، ص 119 .

[52] عبد الله دغش العجمي، المرجع السابق، ص 26 .

الفرع الثاني

الركن المادي

يعرف الركن المادي للجريمة " سلوك إجرامي معين تطلبه القانون كمناط للعقاب على هذه الجريمة ، على أن تتحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه العقاب على الجريمة ، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سببية وهو ما يطلق عليه الإسناد المادي ."[53] ويقصد كذلك بالركن المادي للجريمة "كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا ، يؤدي إلى نتيجة تمس حقا من الحقوق ، التي يكفلها الدستور والقانون ." ويتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب مثلا:(جريمة الغش المعلوماتي، الركن المادي فيها وتغير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية.)[54]

ويمكن تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر :

1-السلوك الإجرامي

ويعرف السلوك الإجرامي في الجريمة المعلوماتية بأنه " فعل أو امتناع عن فعل يؤدي إلى الإضرار بمعلومات مخزنة على إحدى الحواسيب الآلية ، والتي تؤدي إلى إهدار، أو إنقاص قيمة المعلومات وتسبب ضرر الآخرين" ، فالسلوك الإجرامي في الجرائم المعلوماتية لابد أن يتم من خلال أجهزة الحاسب الآلي ، أو شبكة الانترنت، [55] ذلك أن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية و اتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته ، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة ، فيقوم بتحميل الحاسب ببرامج إختراق ،أو أن يقوم بإعداد هذه البرامج بنفسه ،وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف ،كما يمكن أن

---

[53] عبد الله بن محمد كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، أطروحة ماجستير، كلية الدراسات العليا، تخصص التشريع الجنائي الإسلامي، جامعة نايف للعلوم الأمنية، الرياض، 2013، ص 40 .

[54] عاقلي فضيلة، المرجع السابق، ص 120 .

[55] عبد الله بن محمد كريري، المرجع السابق، ص 41 .

يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.[56]

2-النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث ،فالسلوك قد أحدث تغييرا ملموسا ، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج ، بغض النظر عما يمكن ، أن يحدثه السلوك الإجرامي من نتائج أخرى ،علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقق نتيجتها مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل .[57]

وللنتيجة الإجرامية مدلولان أحدهما المدلول المادي والآخر المدلول القانوني ، فالمدلول المادي يعني الآثار المادية التي تحدثها الجريمة في العالم الخارجي، ويرتب القانون على حصولها عقوبة ،وبالنسبة للمدلول القانوني وهو المصلحة المحمية بنص القانون ، وما إذا كانت قد أضرت أم لا فإن تحقق المساس بهذه المصلحة وقعت النتيجة الإجرامية في صورتها القانونية.

3-العلاقة السببية بين الفعل والنتيجة

لكي يتوافر الركن المادي في الجريمة ، فلابد من وجود علاقة سببية ما بين السلوك الإجرامي والنتيجة التي تحققت بناءا على هذا السلوك ، وعلاقة السببية هي العنصر الثالث في الركن المادي للجريمة التامة ، فلا يكفي لقيام الجريمة وقوع السلوك هو الذي أدى بذاته إلى تحقيق النتيجة وإلا ما أمكن القول بتوافر الركن المادي لها .[58]

ويراد بعلاقة السببية الصلة التي تربط مابين السلوك الإجرامي والنتيجة الإجرامية الضارة كرابطة العلة بالمعلول ، بحيث تثبت أن السلوك الإجرامي الواقع هو الذي أدى إلى حدوث النتيجة الضارة ، وبالنسبة للجريمة المعلوماتية فإنه يجب أن يكون السلوك الإجرامي من شأنه أن يحدث النتيجة ، وبالتالي فالشخص الذي يدخل على حاسب آلي بهدف ثم يقوم بمحو معلومات موجودة عليه يكون مرتكبا لجريمة تخريب معلومات ، أما إذا دخل بهدف الإطلاع بشكل غير قانوني ثم حدثت المشكلة في

---

[56] محمد علي قطب، الجريمة المعلوماتية وطرق مواجهتها، ج2، الأكاديمية الملكية للشرطة، مملكة البحرين، مارس 2010، ص 70 .

[57] عاقلي فضيلة، المرجع السابق، ص 119 .

[58] خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، (د/ط)، 2012، طرابلس، ص 126 .

التوصيلات الكهربائية لسبب لا يرجع إليه أدى ذلك إلى محو البيانات ، فإنه يكون مرتكبا لجريمة الولوج الغير مصرح به أما محو البيانات فقد حدث بسبب خارجي لايد له فيه ، وفي بعض الأحيان تتداخل بعض الأسباب لإحداث النتيجة الإجرامية .

وبالرجوع إلى التشريع الجزائري فان الدخول غير المصرح إلى نظام المعالجة الآلية للمعطيات يعد جريمة شكلية لأنها لا تشترط تحقق النتيجة، فبمجرد الوصول إلى المعلومات المخزنة تقوم الجريمة، وقد نصت المادة 394 مكرر من قانون العقوبات الجزائري على أنه "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6اشهر إلى سنتين والغرامة من50.000 إلى 150.000 دج".

والملاحظ أن المشرع الجزائري يعاقب على الشروع في الجريمة حتى ولو لم تحقق هذه الجريمة نتيجة وذلك من خلال استعمال عبارة " **أو يحاول** " في نص المادة 394 مكرر.

الفرع الثاني

الركن المعنوي

الركن المعنوي "الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني"[59]، و يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطا أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة

[59] محمد علي قطب، المرجع السابق، ص 71 .

فور علمه بدخوله غير الشرعي ولاشك أن بقاءه داخل نظام الحاسب الآلي بعد دخوله عن طريق الخطأ وتبينه ذلك لا يختلف من حيث التجريم عن الدخول غير المشروع إلى نظام الحاسب الآلي .[60]

و يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما، العلم والإرادة، فالعلم هو إدراك الفاعل للأمور أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة .

الأصل أن الفاعل في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام ،إذن فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لا يمنع أن بعض الجرائم الالكترونية يتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الانترنيت و جرائم نشر الفيروسات عبر الشبكة) .وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[61]

و الشروع في الجريمة كالجريمة نفسها إذ أن العقوبة المطبقة على الشروع في الجريمة هي نفسها عقوبة الجريمة التامة ، ويراد بالشروع في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة ، كانت لتقع بالفعل لولا تدخل عامل خارج عن إرادة الفاعل حال في اللحظة الأخيرة دون وقوعها[62] وهو ما نص عليه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات حيث اعتبر العقوبة المطبقة على الشروع في الجريمة هي نفسها المطبقة على الجريمة التامة .[63]

المبحث الثاني

الجرائم الإلكترونية في القانون الجزائري

- جرائم الاعتداء على نظام المعالجة الآلية للمعطيات -

---

[60] عبد الله بن محمد كريري، المرجع السابق، ص 46 .

[61] عاقلي فضيلة، المرجع السابق، ص 120 .

[62] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، (د/ ط)، 2009، ص 184 .

[63] مختارية بوزيدي، ماهية الجريمة الإلكترونية، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري 09-3-2017، ص 7.

يتم تناقل المعلومات و المعطيات خلال أنظمة المعالجة الآلية ، هاته العمليات تم إخضاعها لحماية قانونية ، ضد كل فعل غير مشروع قد يقع عليها التي أصبحت تتمتع بحماية جزائية منصوص عليها قانونا .

هاته الحماية هي كل إعتداء يمكن أن يمس بنظام المعالجة الآلية للمعطيات ، و يمكن أن تكون هذه الإعتداءات إما دخول أو بقاء غير مصرح به ، أو تلاعب بمعطيات الحاسب الآلي أو يمكن أن يكون تعامل في معطيات غير مشروعة ، و عليه سنتناول في هذا المبحث جميع صور الإعتداء في أنظمة المعالجة الآلية للمعطيات ، و المنصوص عليها في القسم السابع مكرر من قانون العقوبات و تقسيم هذا المبحث سيكون كالأتي : " جريمة الدخول أو البقاء غير المصرح به " كمطلب أول ، " جريمة التلاعب بمعطيات الحاسب الآلي " كمطلب ثاني و " جريمة التعامل في معطيات غير مشروعة " كمطلب ثالث .

المطلب الأول

جريمة الدخول أو البقاء غير المصرح به

يعد الإعتداء على نظام المعالجة الآلية للمعطيات عن طريق الدخول أو البقاء غير المصرح به ، أول صورة من صور المساس بأنظمة المعالجة قد نص عليها المشرع في قانون العقوبات من خلال نص المادة 394 مكرر في الفقرة الأولى منها ، و سيتم تناول هذه الجريمة في أربعة فروع ، الأول بعنوان " الركن الشرعي " ، الثاني بعنوان " الركن المادي " الثالث بعنوان " الركن المعنوي " و الرابع بعنوان " عقوبة الدخول أو البقاء غير المصرح به".

الفرع الأول

الركن الشرعي

عرف الفقه نظام المعالجة الآلية للمعطيات " مجموعة من العناصر المتداخلة و المتفاعلة مع بعضها البعض و التي تعمل على جمع البيانات و المعلومات و معالجتها و تخزينها و بثها و توزيعها بفرض

دعم صناعات القرارات و التنسيق و التامين و السيطرة على المنضومة إضافة لتحليل المشكلات للمواضيع المعقدة "[64] ،

إن فعل الدخول و البقاء غير المصرح به في هذا النظام فإنها جريمة يعاقب عليها المشرع الجزائري ، بموجب نص المادة 394 مكرر من قانون العقوبات " يعاقب بالحبس ... كل من يدخل أو يبقى عن طريق الغش في كل جزء من منضومة للمعالجة الآلية للمعطيات أو يحاول ذلك "

فتعد هذه الجريمة أبسط صور جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات ، فبمجرد القيام بفعل دخول أو بقاء في نظام معلوماتي ، بطريقة إحتيالية ، أي عن طريق الغش تقوم جريمة الدخول أو البقاء غير المصرح به .

لكن بالرغم من ذلك ، هناك جدل فقهي حول مدى تجريم فعلي الدخول و البقاء غير المصرح بهما في نظام معلوماتي، فالإتجاه الأول يرى أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما على النظام المعلوماتي ، و خاصة إذا لم يكن لدى الفاعل نية لإرتكاب جريمة لاحقة على هذا الدخول أو البقاء ،

أما الإتجاه الثاني فيذهب إلى ضرورة تجريم الدخول و البقاء غير المصرح بهما إلى النظام المعلوماتي ، حتى و لو لم يكن ذلك بقصد إرتكاب جريمة لاحقة على هذا الدخول أو البقاء .فالإتجاه الثاني يرى أن فعلي الدخول و البقاء غير المصرح بهما ، لهما تبعات مادية تتمثل في خسائر متعددة ، حيث تشير القدرات على أن هناك الآن ما يزيد عن مائة (100) خبير معلوماتي يعملون في أكثر من 20 ألف شركة في العالم و بلغ مجموع ما أنفقته الشركات على خدمات الإستشارة المعلوماتية 4.5 مليون دولار ، و كل ذالك من أجل أمن المبادلات الإلكترونية[65] .

الفرع الثاني

الركن المادي

[64] خالد ممدوح إبراهيم ، " التقاضي الإلكتروني " ، (د-ط) ، دار الفكر الجامعي ، الإسكندرية ، 2009 ، ص 298 .

[65] محمود أحمد عبابنة ، " جرائم الحاسوب و أبعادها الدولية "، دار الثقافة للنشر و التوزيع ،عمان ، 2005 ، ص 81 .

يقوم الركن المادي لهذه الجريمة في حال الدخول بكل الطرق و الأفعال التي تسمح بالولوج إلى نظام معلوماتي معين و الفعل المادي هنا ليس فعل الدخول التقليدي إلى مسرح الجريمة و إنما كل فعل دخول إلى قاعدة بيانات معلوماتية عن طريق الغش أو التحايل بطريقة فنية و تقنية على النظام المعلوماتي.

أولا : الدخول غير المصرح به

تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي ، و مدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي و الإحاطة أو السيطرة على المعطيات و المعلومات التي يتكون منها ، و فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب و نظامه ، بل يقصد به الدخول بإستخدام الوسائل الفنية و التقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني و يساوي في هذا المجال تم هذا الدخول بطريق مباشر إلى المعلومات أو تمر عن طريق الإعتراض غير المشروع لعملية الإتصال من أجل الدخول إلى النظام المعلوماتي[66].

و فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع ، و إنما يتخذ هذا الفعل وصفه الجرمي إنطلاقا من كونه قد تم دون وجه حق ، أو بمعنى أخر دون تصريح و من الحالات التي يكون فيها الدخول غير مصرح به إلى النظام المعلوماتي[67].

دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسؤول عن النظام أو مالكه ، و قد يكون الفاعل مصرح له بالدخول إلى جزء من النظام ، إلا أنه يتجاوز التصريح الممنوح له و يدخل إلى كامل النظام أو إلى أجزاء أخرى يحظرعليه الدخول إليها ، و لهذا الغرض يتم في الغالب من

---

[66] نهلا عبد القادر المومني ، المرجع السابق ، ص 158 .

[67] يشترط النظام المعلوماتي توفر مكونات مادية " "hardware" (ما هو ملموس في الجهاز وله دور مهم لتشغيل النظام محل حماية جنائية) ، و مكونات معنوية " software" (أي البرامج و المعطيات المعلوماتية الموجودة في النظام محل الحماية الجنائية) أنظر:
Hollande Alain – de belle fondsliantsXavier , pratique du droit de l'informatique , Edition , Delmas (5 EmmeEdition) , avril , 2002 , France , p 250 .

قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي كما أن التصريح بالدخول ينصرف إلى الحالات التي يكون فيها هذا الدخول مشروطا بدفع ثمن محدد ، و بالرغم من ذلك يدخل الفاعل إلى النظام من دون تسديد هذا الثمن ، أما إذا كان الولوج إلى النظام المعلوماتي بالمجان و كان متاحا للجمهور ، ففي هذه الحالة يكون الدخول إليها حق من الحقوق[68] ،

أو يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام ، و لذلك تقع الجريمة بأي وسيلة أو طريقة ، فقد يلجأ الجاني إلى التلاعب بعناصر النظام المادية لكي يصل إلى هدفه و هو الدخول ، أو يربطه بجهاز تنصت يستطيع من خلاله اختراق النظام أو استقبال المعلومات ، كما قد يكون عن طريق برنامج فيروسي ، مثل فيروس حصان طروادة " Trajan horse " أو عن طريق إستخدام الرقم الكودي لشخص أخر أو الدخول من خلال شخص أخر مسموح له بالدخول أو عن طريق الوصول إلى الرقم الكودي للدخول ، أو عن طريق تجاوز نظام الحماية الخاصة إذا كان ضعيفا في حالة وجود مثل هذا النظام ، و يستوي أن يكون الدخول مباشرة أو بطريق غير مباشر ، كما هو الحال في الدخول عن بعد عن طريق شبكات الإتصال التلفزيونية[69] ،

باختصار يمكن أن يحصل الدخول دون إذن باختراق النظام المعلوماتي عن طريق الحصول على شيفرات خاصة ، أو إستخدام فيروس يتم دمجه في إحدى البرامج الأصلية للحاسب الآلي كي يعمل كجزء منه ، ثم يقوم بتسجيل الشيفرات التي يستعملها المستخدمون الشرعيون للدخول إلى الكمبيوتر[70]، إذن فيما يخص الركن المادي للجريمة فهو الدخول سواء كان مادي أو معنوي أو بأية طريقة كانت إلى النظام المعلوماتي في جزء منه أو كله و دون أي حق أو ترخيص[71] ،

---

[68] نهلا عبد القادر المومني ، المرجع السابق ، ص 159 .

[69] علي عبد القادر القهوجي ، " الحماية الجنائية لبرامج الحاسب الآلي " ، (د-ط) ، الدار الجامعية ، بيروت ، 1999 ص 131 .

[70] نعيم مغبغب ، " حماية برامج الكمبيوتر (الأساليب و الثغرات) " ، (د-ط) ، منشورات الحلبي الحقوقية ، لبنان ، 2006 ، ص 235 .

[71] جميل عبد الباقي الصغير ، " القانون و التكنلوجيا الحديثة (الكتاب الأول ، الجرائم الناشئة عن إستخدام الحاسب الآلي) " ، ط 01 ، دار النهظة العربية ، مصر ، 1992 ، ص 150 .

و كما قلنا سابقا يعين كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي و يتحقق بالوصول إلى المعلومات و البيانات المخزنة داخل نظام معين دون رضا المسؤول عنه من شخص غير مرخص له بإستخدامه[72].

ثانيا : البقاء غير المصرح به

هو الفعل الثاني المنصوص عليه في المادة 394 مكرر من قانون العقوبات و يقصد به التواجد في نظام المعالجة الآلية للمعطيات ، عند إرادة صاحب ذلك النظام أو من له سيطرة عليه ، فقد يجد شخص نفسه داخل نظام الحاسب الآلي عن طريق الخطأ ، كما لو كان في طريق الدخول إلى نظام له الحق في الدخول إليه ثم وجد نفسه بسبب خطأ ما كإستخدام شيفرة خاطاة على سبيل المثال داخل نظام أخر ، و في هذه الحالة يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه الخطأ الذي وقع فيه ، و قد يستمر البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مصرح له بالدخول إليه[73].

يتضح الهدف من تجريم البقاء بالنسبة للجاني الذي لم يقصد الدخول عن طريق الغش للنظام و مع ذلك يبقى داخل النظام و تنصرف إرادته إلى ذلك و الذي كان يمكن أن يغادر النظام[74] .

قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام ، و قد يجتمعا و يكون البقاء معاقبا عليه إستقلالا حين يكون الدخول إلى النظام مشروعا و من أمثلة ذلك ، إذا تحقق الدخول إى النظام بالصدفة أو عن طريق الخطأ أو السهو إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورا ، فإذا بقي رغم ذالك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي ، و يكون البقاء أيضا جريمة في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء بداخله ، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية أو الإطلاع فقط ، و يتحقق ذالك أيضا بالنسبة للخدمات المفتوحة

---

[72] خالد ممدوح إبراهيم ، " أمن المستندات الإلكترونية " ، (د-ط) ، الدار الجامعية ، الإسكندرية ، 2008 ، ص 48 .

[73] محمد عبيد الكعيبي ، " الحماية الجنائية للتجارة الإلكترونية " ، (د-ط) ، دار النهضة العربية ، القاهرة ، 2010 ، ص 459 .

[74] عبد الفتاح بيومي حجازي ، " الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتي) " ، (د-ط) ، دار الفكر الجامعي ، الإسكندرية ، 2008 ، ص 83 .

للجمهور مثل الخدمات التلفزيونية و التي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق إستخدام وسائل أو عمليات غير مشروعة[75].

قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا ، و ذلك في الغرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام و يدخل إليه فعلا ، في إرادة من له حق السيطرة عليه ، ثم يبقى داخل النظام بعد ذلك ، و يتحقق في هذا الغرض الإجتماع المادي للجرائم بين الجريمتين ، و لكن في هذا الغرض تثور مشكلة و هي " متى تنتهي جريمة الدخول ، و متى تبدأ جريمة البقاء ؟

فذهب رأي في الفقه إلى أن جريمة الدخول تتحقق في اللحظة التي يتم فيها الدخول فعلا إلى البرنامج ، و إن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي بإنتهاء حالة البقاء و يؤكد على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء داخل النظام بطريقة حاسمة ، و لهذا ذهب رأي أخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقائه داخل النظام غير المشروع و أخذ على هذا الرأي أيضا صعوبة إثبات علم المتدخل[76] .

و ذهب رأي ثالث إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع أو أصبح غير مشروع ، فإذا لم ينسحب فإنه يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام ، و هذا الرأي و إن كان له وجاهته إلا أنه يفترض وجود جهاز إنذار يقوم بهذه المهمة ، و هو إن أمكن توفيره فنيا فإنه لن يكون متاحا إلا للشركات أو المؤسسات الكبيرة فقط[77] .

الفرع الثالث

الركن المعنوي

---

[75] على عبد القادر القهوجي ، المرجع السابق ، ص 130 .

[76] المرجع نفسه ، ص 131 .

[77] جباري عبد المجيد ، " دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة " ، (د – ط) ، دار هومة للنشر و التوزيع ، الجزائر ، 2006 ، ص 106 .

إن الركن المعنوي لجريمتي الدخول و البقاء غير المصرح بهما يتخذ صورة القصد الجنائي من علم و إرادة بإعتبارها من الجرائم العمدية ، و لقد عبر نص المادة 394 مكرر من قانون العقوبات الجزائري ، عن القصد العام الذي يتطلب أن يكون الدخول أو البقاء عن طريق الغش فإستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقائه في نظام المعالجة الآلية للمعطيات غير مشروع و هو نفس ما عبر عنه المشرع الفرنسي في نص المادة 01/323 من قانون العقوبات بعبارة Frauduleusement: أي أن القصد الجنائي لا يكفي إنما يجب توافر قصد جنائي و هو " الغش " ليس المقصود به نية الإضرار و إلا يكون ، هناك تناقض بين الركن المادي الذي لا يتطلب النتيجة و الركن المعنوي .

عادة يبدو طابع الغش الذي يتم به الدخول من خلال الجهاز الرقابي الذي يحمي النظام أما بالنسبة للبقاء فيستنتج من العمليات التي تتم داخل النظام .

أما القصد فيتطلب علم الجاني بكل واقعة ذات أهمية قانونية في تكييف الجريمة و بناء أركانها و إستكمال عناصرها و خاصة الركن المادي منها و أول هذه العناصر هو موضوع الحق المعتدى عليه ، فيتعين توفر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات و برامج بإعتباره محل الحق الذي يحميه المشرع فإذا إعتقد الفاعل بناء على أسباب معولة بأن يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي دون أن يتجه علمه إلى البقاء في نظام المعالجة الآلية للمعطيات فإن قصد الدخول أو البقاء لا يتوفر فيه .

الفرع الرابع

عقوبة الدخول و البقاء غير المصرح به

العقوبة المقررة لجريمة الدخول و البقاء غير المصرح به ، نصت على ذلك المادة 394 مكرر من قانون العقوبات ، و هي الحبس من ثلاثة إلى ستة أشهر و بغرامة مالية من 50000 دج إلى 10000 دج و تضاعف العقوبة في حالة ما إذا ترتب عن ذلك حذف (إزالة بالإنقاص أو الطمس) أو التغيير (إضافة ، تعديل) أو التخريب إلى الحبس من ستة أشهر إلى سنتين (02) و غرامة من 50000 دج إلى 150000 دج و تشدد العقوبة في حالة ما إذا كان الجاني شخصا معنويا ، و هي غرامة تعادل خمس

مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ، و هو ما نصت عليه المادة 394 مكرر إضافة إلى ما نصت عليه المادة 18 مكرر 01 من قانون العقوبات .

يكفي لتوافر الضروف المشددة ، أن تكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع ، و بين النتيجة التي تحققت ، و هي محو في النظام أو عدم قدرته على أداء وضيفته أو تعديل البيانات ، وهذه النتيجة ذاتها هي التي إعتبرها المشرع ضرفا مشددا في هذه الجريمة[78] .

المطلب الثاني

جريمة التلاعب بمعطيات الحاسب الآلي

يطلق عليها أيضا إسم جريمة المساس العمدي بالمعطيات ، و هي الجريمة المنصوص عليها في المادة 394 مكرر من قانون العقوبات ، و تتمثل هاته الجريمة في القيام بجملة من الأفعال التي تعتبر إعتداءات عمدية على المعطيات ، و تتم هذه الإعتداءات بإستعمال جملة من الوسائل ، و هذا ما سنتناوله في هذا المطلب من خلال تقسيمه إلى الفروع التالية : الفرع الأول " الركن الشرعي " الفرع الثاني " الركن المادي " الفرع الثالث " الركن المعنوي " و الفرع الرابع " عقوبة التلاعب بمعطيات الحاسب الآلي .

تنص المادة 394 مكرر 01 من قانون العقوبات الجزائري " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000 دج إلى 2000.000 كل دخل عن طريق الغش معطيات في نظام المعالجة الألية للمعطيات أو أزال أو عدل بطريق الغش ، المعطيات التي يتضمنها "[79] ،

فنلاحظ أن المشرع الجزائري قد جرم فعل التلاعب بمعطيات الحاسب الآلي سواء كان ذلك عن طريق الإدخال ، التعديل أو الإزالة ، و التي يترتب عنها تغيير في المعطيات .

---

[78] عبد الفتاح بيومي حجازي ، " الحكومة الإلكترونية و نظامها القانوني " ، (د-ط) ، دار الفكر الجامعي ، الإسكندرية ، 2004 ، ص 362 .

[79] المادة 394 مكرر 01 من قانون العقوبات .

كما نص المرسوم الرئاسي رقم 14 – 252 الذي يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 08 منه على ما يلي : " تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا و بدون وجه حق "[80] .

الفرع الثاني

الركن المادي

الركن المادي لجريمة التلاعب بمعطيات الحاسب الآلي ، يقوم الركن في هذه الجريمة التي يتكون من ثلاث أفعال هي الإدخال غير المصرح به للمعطيات داخل نظام المعالجة الآلية أو إزالة هذه المعطيات أو تقديمها بخيار صحيح و هذه الأفعال كلها تؤدي على التغيير من الحالة التي توجد عليها المعطيات محل الإعتداء أي تؤدي إلى المساس بسلامتها و تكاملها[81] .

أولا : الإدخال غير المشروع للمعطيات

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها ، سواء كانت خالية أو كان يوجد فيها معطيات من قبل ، و الإدخال غير المشروع للمعلومات أو البرامج قد يترتب عليه فضلا عن التعديل الذي يطرأ على ذاكرة الحاسب الآلي ، تدل المعلومات ذاتها أو تدميرها كما في حالة إدخال برامج خبيثة إلى نظام الحاسب الآلي[82].

ثانيا : الإزالة غير المشروعة للمعلومات (تدمير المعلومات)

نصت المادة 394 مكرر 01 من قانون العقوبات الجزائري على فعل الإزالة و يتم ذلك بإزالة المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة و تخزين المعطيات إلى المنظمة الخاصة بالذاكرة .

---

[80] المادة 08 من المرسوم الرئاسي رقم 14 –252 ، الصادر في 08 سبتمبر 2014 ، المتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ، الجريدة الرسمية العدد 57 ، المؤرخة في 20 سبتمبر 2014 .

[81] محمد خليفة ، المرجع السابق ، ص 179 .

[82] أمال قارة ، المرجع السابق ، ص 122 .

و لقد أستخدمت جميع القوانين التي جرمت الإتلاف المعلوماتي بقصد إخفاء المعلومات و محوها ، للتعبير عن تدمير المعلومات بإعتباره صورة متميزة من صور الإتلاف[83] .

حيث أنه يرى البعض أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تميزا لها و مؤدى ذلك أن إخفاء المعلومات أو الملفات على سبيل المثال ، لا يترتب على محو المعلومات التي تحتوي عليها ذاكرة الحاسب الآلي و إنما يؤدي فقط إلى التعديل في قائمة الملفات فهو لا تعديل ولا تدمير[84] .

ثالثا : التعديل غير المشروع للمعطيات

و يعني بتدمير المعطيات الموجودة داخل النظام و إستبدالها بمعطيات أخرى و يتحقق ببرامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو تعديلها و ذلك بإستخدام القنبلة المعلوماتية الخاصة بالمعطيات و البرامج الممحاة ، أو برامج الفيروسات بصفة عامة هذه الأفعال المتمثلة في الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع طائلة التجريم أي فعل آخر غيرها[85] .

في الأخير أن جريمة التلاعب بالمعطيات جريمة ضرر و جريمة مادية ، إذ لا يكفي أن تهدد سلامة المعطيات بحظر الإزالة أو التعديل أو الإدخار و إنما لابد أن يقع ضرر فعلي على هذه المعطيات يتمثل في نفس حالتها حيث أن المشرع يطلب نتيجة معينة من خلال السلوك الإجرامي في هذه الجريمة و هي تفسير حالة المعطيات ، و نتيجة جريمة التلاعب بالمعطيات بالنسبة للتعديل و الإزالة و هي نفس النتيجة التي يترتب عليها تشديد العقوبة في جريمة الدخول و البقاء غير المصرح به ، و ما يميزها أن هذه الأخيرة تتم دائما بعد دخول أو بقاء غير مصرح بهما ، كما أنها تكون غير عمدية ، بينما النتيجة في جريمة التلاعب قد تتم بعد دخول أو بقاء غير مصرح به أو أنها دائما عمدية يقصد الجاني إحداثها .

---

[83] أسامة محمد لمناعسة ، " جرائم الحاسب الآلي و الأنترنت " ن دراسة تحليلية مقارنة ، دار وائل للنشر و التوزيع ، عمان ، 2009 ، ص 73 .

[84] نائلة عادل محمد فريد قورة ، " جرائم الحاسب الآلي الاقتصادية " ، دراسة نظرية و تطبيقية ، منشورات الحلبي الحقوقية ، 2005 ، ص 341 .

[85] أمال قارة ، المرجع السابق ، ص 122 .

الفرع الثالث

الركن المعنوي

جريمة التلاعب بالمعطيات تتطلب قصد جنائي عام و هو ما يستكشف من نص المادة 394 مكرر 01 من قانون العقوبات " كل من أدخل أزال عدل بطريق الغش " ،

فمصطلح الغش يدل على ضرورة توفر قصد جنائي عام بعنصريه ، و عليه يجب أن تتجه إرادة الجاني إلى إرتكاب السلوك الإجرامي بإحدى الصور المذكورة سابقا في المادة 394 مكرر 01 إما بإدخال معطيات داخل نظام المعالجة الآلية للمعطيات أو إزالة المعطيات الموجودة به أو تعديلها مع وجوب علمه أنه غير مسموح له بذلك أو أن ذلك يتجاوز حدود صلاحياته ، أو انه يعلم أن فعله سيؤدي حتما لنتيجة معينة هي إزالة المعلومة أو تغييرها أو تعديلها رغما عن علم صاحب الحق في هذه المعطيات أو من له حق السيطرة عليها .

ولا يشترط في القصد أن يكون معين بمعطيات معينة إذا تحقق قصد الجاني الدخول لمحو المعطيات ثم تم محو أخرى و لو تم التلاعب بالمعطيات عشوائيا دون تحديد هدف إذن يحمي قانون العقوبات كل المعطيات دون الحاجة لتحديدها .

ولا تتطلب المادة 394 مكرر 01 قصد خاص إنما يكفي توافر قصد عام إذ لا تشترط فيه إلحاق الضرر بالغير إذ لا يتصرف الجاني بنية إلحاق الضرر إذ تقوم الجريمة متى قصد الجاني التلاعب بالمعطيات المتضمنة بنظام المعالجة الآلية للمعطيات 21 بالمئة من القضايا التي طرحت أمام القضاء الجزائري من 2005 إلى 2010[86].

الفرع الرابع

عقوبة التلاعب بمعطيات الحاسب الآلي

[86] مختار الأخضري ، " الإطار القانوني لمواجهة الجرائم المعلوماتية و جرائم الفضاء الإفتراضي " ، العدد 66 ، نشرة القضاة ، 2011 ن ص 68 .

من خلال إستقراء نص المادة 394 مكرر01 من قانون العقوبات الجزائري ، نلاحظ أن المشرع الجزائري قد شدد العقوبة في جريمة التلاعب بمعطيات الحاسب الآلي ، مقارنة بالعقوبة المنصوص عليها في نص المادة 394 من قانون العقوبات الجزائري و المتعلقة بجريمة الدخول أو البقاء غير المصرح به ، و ذالك نظرا إلى أن جريمة التلاعب بمعطيات الحاسب الآلي [87] تتطلب نتيجة تتمثل في تغير حالة المعطيات ، و بالتالي فهذه الجريمة هي جريمة ضرر و هي جنحة معاقب عليها بالحبس من ستة أشهر على 03 سنوات و بغرامة من 500000 دج إلى 2000000 دج .

المطلب الثالث

جريمة التعامل في معطيات غير مشروعة

تعد جريمة التعامل في معطيات غير مشروعة الصورة الثالثة من صور جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات ، و التي نص عليها المشرع الجزائري في نص المادة 394 مكرر 02 من قانون العقوبات الجزائري ، و هي أيضا أحد الجرائم و هي تمس عمدا في المعطيات المعلوماتية les donnés informatiquesو تختلف هذه الجريمة من حيث المعطيات ، على أساس الحالة التي توجد عليها المعطيات محل الجريمة و النظام الذي توجد به هذه المعطيات حيث اننا سنتناول في هذا المطلب أربعة فروع : الفرع الأول بعنوان " الركن الشرعي " و الفرع الثاني بعنوان " الركن المادي" و الفرع الثالث بعنوان " الركن المعنوي " و الفرع الرابع بعنوان " عقوبة التعامل في معطيات غير مشروعة " .

لقد نص المشرع الجزائري في المادة 394 مكرر 02 من قانون العقوبات " يعاقب بالحبس من شهرين إلى ثلاثة سنوات و بغرامة من 1000000 دج إلى 5000000 دج كل من يقوم عمدا و عن طريق الغش بما يأتي :

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

[87] المادة 394 مكرر01 من قانون العقوبات .

2 –حيازة أو إنشاء أو نشر أو إستعمال لأي غرض كان ، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم [88].

في هذه المادة عمد المشرع لتجريم مجموعة من الأفعال التي تمس بالمعطيات في حد ذاتها على خلاف الجرائم السالفة الذكر،التي تعلقت بالمعطيات الموجودة داخل نظام المعالجة الآلية و خص المعطيات التي تصلح لأن ترتكب بها إحدى الجرائم التي تمس سريتها و سلامتها أو وفرتها هذا من جهة ، كما جرم ثانيا التعامل بالمعطيات المتحصل عليها من جريمة و خص هذه الأخيرة أن تكون من إحدى الجرائم المنصوص عليها بهذا القسم .

كما يستشف من ذات المادة أن المشرع جرم فئتين من التعامل بالمعطيات لهدفين إثنين :

أولهما، تجريم التعامل في المعطيات التي يمكن أن ترتكب بها جريمة الهدف منها وقائي لمنع إرتكاب الجريمة ، وثانيهما، المتحصل عليها من الجريمة و الهدف منه الحد قدر الإمكان من الأثار و النتائج المترتبة على الجريمة الأولى و التي سبق إرتكابها للتضييق من دائرة الجناة المتعاملين بطريقة غير مشروعة فيها .

الفرع الثاني

الركن المادي

جريمة التعامل في معطيات غير مشروعة بصورتها جريمة شكلية أو جريمة خطر لا يعتد المشرع في قيامها بتحقيق نتيجة معينة ، فيكفي أن يقوم الجاني بأحد الأفعال المنصوص عليها في المادة 394 مكرر ، ليكتمل الركن المادي لهذه الجريمة .

محل جريمة التعامل في معطيات صالحة لإرتكاب جريمة كما أشارت إليه المادة 394 مكرر 02 هو المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية ، و نلاحظ أن هذه المادة تختلف عن المادتين السابقتين لهما و المتعلقتين بجريمتي الدخول و البقاء غير المصرح به و التلاعب

[88] المادة 394 مكرر02 قانون العقوبات .

بالمعطيات و ذلك في نقطتين، أولهما تتعلق بالحالة التي توجد عليها المعطيات محل الجريمة و ثانيهما، تتعلق بالنظام الذي توجد به هذه المعطيات .

فجريمة التعامل في معطيات صالحة لإرتكاب جريمة فهو أي منظومة معلوماتية ، ولا شك أن هذه الأخيرة تختلف عن نظام المعالجة الآلية للمعطيات [89].

و إن كان قانون العقوبات الجزائري قد إقتصر على المعطيات كمحل للجريمة فإن قانون العقوبات الفرنسي كان أكثر توسعا في ذلك و هو ما أقرته المادة 323 – 03 – 01 إن التعاملات المجرمة يمكن أن تقع على تجهيزات أو أدوات أو على برنامج معلوماتي أو على كل معطيات مهمة أو معدة لأرتكاب واحد أو أكثر من جرائم الدخول أو البقاء غير المصرح بهما ، أو إعاقة إفساد أنظمة المعالجة الآلية أو التلاعب بالمعطيات[90].

إن السلوك الإجرامي في جريمة التعامل في معطيات غير مشروعة يتخذ صورتين إثنين، الأولى،تتمثل في التعامل في معطيات صالحة لإرتكاب جريمة و الثانية تتعلق التعامل في معطيات متحصلة من جريمة و لا يتطلب المشرع لقيام هذه الجريمة تحقق نتيجة معينة ، و لهذا فهي تقوم بمجرد إرتكاب أحد أنواع السلوك أو الأفعال التي تنص عليها المادة 394 مكرر 02 من قانون العقوبات الجزائري .

أولا : التعامل في معطيات صالحة لإرتكاب جريمة

التعامل في معطيات صالحة لإرتكاب جريمة ، تجرمه المادة 394 مكرر 02 في البند الأول منها ، مجموعة من الأفعال الخطرة و التي تركت دون تجريم أدت إلى حدوث جرائم أخرى هذه الأفعال تشكل كافة أشكال التعامل الواقعة على معطيات الحاسب الآلي ، و التي تسبق عملية إستعمال هذه المعطيات في إرتكاب هذه الجريمة ، فمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل إلى يد الجاني فيرتكب بها جريمته ، و هذه المراحل تبدأ من تصميم هذه المعطيات و البحث فيها و تجميعها وصولا إلى جعلها في متناول الغير ، و تحت تصرفه و ذلك بتوافرها أو نشرها أو الإتجار فيها ولا يشترط ان تقع هذه الأفعال مجتمعة لتقوم الجريمة بل يكفي أن تقع إحداها فقط ، و المقصود بالتعامل هنا

---

[89] محمد خليفة ، المرجع السابق ، ص 197 .

[90] خالد أبو الفتوح ، المرجع السابق ، ص 80 .

ليس هو التعامل بمفهومه في القانون المدني ، و إنما هو تعامل بمفهوم أوسع إذ يقصد به في الجريمة محل الدراسة كل سلوك له علاقة بإعداد و إنتاج المعطيات غير المشروعة أو كل سلوك يكشف عن وجود صلة معينة بين شخص و معطيات غير مشروعة ، هذه الصلة تتمثل في القيام بأحد أنواع السلوك التي نصت عليها المادة 394 مكرر 02 و التي أطلق عليها غسم التعامل و تتمثل في السلوكيات التالية [91]، التصميم ، البحث ، التجميع ، التوفير ، النشر ، الإتجار ...

1- التصميم

هي أول عملية في سلسلة التعامل فسي المعطيات و هي تتمثل في إخراج المعطيات على الوجود أي القيام بخلق و إيجاد معطيات صالحة لإرتكاب جريمة ن و هذا العمل يقوم به المختصون في هذا المجال كمصممي البرامج و مثال هذه الجريمة تصميم برنامج يحمل فيروسا و هذا ما يطلق عليه بالبرامج الخبيثة.

2- البحث

يقصد بالبحث في نص المادة 494 مكرر 02 من قانون العقوبات الجزائري ، البحث عن الوسيلة التي يمكن أن ترتكب بها الجريمة لا يعد جريمة فمن يبحث عن سكين لا يعد مرتكبا لجريمة .

و على هذا نرجح أن المشرع يقصد بهذه العبارة البحث في كيفية تصميم هذه المعطيات و ليس مجرد البحث عن هذه المعطيات و لهذا جاءت عبارة البحث بعد عبارة التصمبم مباشرة و إن كان النص قد جاء عاما .

3-التجميع

هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول غير المصرح بها و جريمة التلاعب و يفترض هذا السلوك أن صاحبه يحتفظ بمجموعة من المعطيات التي تشكل خطرا و التي من الممكن إستعمالها في إرتكاب تلك الجرائم ، و قد أستخدمت إتفاقية بودابست مصطلح "

[91]: د/ محمد زكي أبو عامر ، " قانون العقوبات القسم الخاص " ، دار الجامعة الجديدة ، الإسكندرية ، 2005 ، ص 761 .

الحصول للإستخدام " و ما يميز هذا المصطلح عن مصطلح التجميع أن الأول يقتضي وجود نية إستخدام المعطيات المتحصل عليها ولا يشترط عددا معينا فيها بينما الثاني التجميع لا يمثل تلك النية و يشترط تعدد المعطيات **التوفير: (الوضع تحت التصرف أو العرض)**[92]

من الأفعال التي تجرمها المادة 394 مكرر 02 من قانون العقوبات أيضا فعل التوفير أي توفير معطيات يمكن أن ترتب بها جريمة دخول أو بقاء أو جريمة تلاعب و تعاقب المادة 323 – 03 – 01 على نفس السلوك تحت مصطلح Ceder كما تعاقب عليه المادة 06 من إتفاقية بودابست تحت عبارة أي أشكال للوضع تحت التصرف ، و المراد بذلك و تقديم المعطيات و إتاحتها لمن يريدها ، أي جعلها في متناول الغير و وضعها تحت تصرفه .

ثانيا : التعامل في معطيات متحصلة عن جريمة

الصورة الثانية من صورتي التعامل في معطيات غير مشروعة هي معطيات متحصلة عن جريمة و تتحقق الجريمة في صورتها بواحد من أربعة أفعال هي : حيازة معطيات متحصلة من جريمة أو إفشاءها أو نشرها أو إستعمالها أي أنه يكفي تحقق واحد من هذه الأفعال فقط لكي يقوم السلوك الإجرامي و تتمثل في الحيازة ، النشر و الإستعمال ... ، أما النتيجة الإجرامية لا تتطلب حدوث نتيجة و لا تتطلب تحقق ضرر فعلي و حال يقع على معطيات ما أو على أنظمة معالجة ، فهو أينما يجرم تلك الأفعال ليس بوصفها أفعالا خطيرة يمكن أن تؤدي معالجتها ، فهو إنما يجرم تلك الأفعال ليس بوصفها أفعالا خطرة يمكن أن تؤدي إلى ضرر مباشر و حاد ، و إنما يجرده بوصفها أفعالا خطرة يمكن أن تؤدي إلى ضرر فعلي .

الفرع الثالث

الركن المعنوي

[92] محمد زكي أبو عامر، المرجع السابق ، ص 762 .

لقيام جريمة التعامل في معطيات غير مشروعة يجب توفر القصد الجنائي العام ، أي يجب أن تتجه إرادة الجاني عمدا إلى إرتكاب جريمة التعامل في معطيات غير مشروعة مع علمه بعدم مشروعية التعامل فيها ، كما يتطلب قيام هذه الجريمة توافر القصد الجنائي الخاص أيضا .

أولا : القصد الجنائي العام

لا شك أن جريمة التعامل في معطيات غير مشروعة جريمة عصرية و هذا ما نصت عليه المادة 394 مكرر 02 من قانون العقوبات الجزائري و لابد من قيامها توافر القصد العام و هذا الأخير يقوم على العلم والإرادة.

1- العلم

فلا بد أن يعلم الجاني بكل العناصر التي تدخل في بناء الجريمة إذ يلزم أن يعلم أنه يقوم بالتعامل في معطيات غير مشروعة ولا بد أن يعلم بما يحمله سلوكه من قدرة على تهديد المصلحة المحمية ، و ذلك بأن يعلم أن من شأن المعطيات التي يتعامل فيها أن تستعمل في إرتكاب الجرائم ، و هذا بالنسبة للصورة الأولى من الجريمة أو يعلم أن من شأن تعامله في المعطيات المتحصلة من الجريمة أن يزيد من الضرر المترتب على تلك الجريمة أو لابد أن يعلم الجاني الصفة غير المشروعة للمعطيات ، أي يعلم بأنه يمكن أن ترتكب بها جريمة أو أنها متحصلة من جريمة فإذا إعتقد أنها معطيات عادية لا علاقة لها بالجريمة إنتفى عنها القصد الجنائي .

2- الإرادة

و كذلك لابد من توافر الإرادة لقيام القصد الجنائي ، إذ رغم علم الجاني بالصفة غير المشروعة للمعطيات فإنه يقوم بإرادته بالتعامل فيها ، و الإرادة هنا تنصب على السلوك الإجرامي فحسب و هو مختلف أشكال التعامل السابق بيانها ، و ذلك أنها لا توجد نتيجة تعتبر بها في بناء الجريمة كي تطالها الإرادة و بالتالي فهذه الأخيرة تقتصر على السلوك فحسب[93] .

ثانيا : مدى ضرورة تو افر القصد الخاص

[93] محمد خليفة ، المرجع السابق ، ص 112 .

إن جريمة التعامل في معطيات غير مشروعة تتطلب توافر القصد الجنائي الخاص الذي يتناول صورتين:

1- القصد الخاص في التعامل في معطيات صالحة لإرتكاب الجريمة

لا يكفي لقيام جريمة تعامل في معطيات صالحة لإرتكاب جريمة أن يتوفر لدى الفاعل القصد العام وحده و إنما يلزم فصل عن هذا القصد أن يتوافر لدى الفاعل القصد الخاص أي إتجاه العلم و الإرادة إلى وقائع معينة لا تدخل في تكوين أركان الجريمة ، أي أن التعامل في المعطيات الصالحة لإرتكاب الجريمة لا بد أن يكون بقصد التمهيد أو الإعداد لإستعمالها في إرتكاب الجريمة و مع هذا فاستعمال هذه المعطيات في إرتكاب جريمة ليس ركنا في جريمة التعامل هذه فقد لا يقوم أحد في إستعمال هذه المعطيات و مع ذلك تقوم الجريمة إذا توافر قص الإعداد و التمهيد و إستعمال هذه المعطيات في إرتكاب الجريمة .

2- مدى إشتراط القصد الخاص في التعامل في معطيات متحصلة من جريمة

رأينا أن جريمة التعامل في صورتها الأولى التعامل مع معطيات صالحة لإرتكاب جريمة ، تتطلب قصدا خاصا ، نظرا لأن المعطيات بها قد يتم التعامل فيها لأغراض مشروعة ، و هذا ما لا يوجد في الصورة الثانية للجريمة و هي واحدة ، فكلها متحصلة من جريمة و صفتها الثانية هذه تجعل من القصد العام كافيا لقيام الجريمة ، إذ لا يسأل الفاعل عن قصده الخاص من التعامل في هذه المعطيات مادام يعلم أنها متحصلة من جريمة و هذا ما يكون القصد العام فليس ما يبرر طلب المشرع لقصد خاص من هذه الناحية [94].

الفرع الرابع

عقوبة التعامل في معطيات غير مشروعة

فيما يخص عقوبة " التعامل في معطيات غير مشروعة " هو الحبس من شهرين إلى 03 سنوات و بغرامة من 1000000 دج إلى 5000000 دج و هو ما نص عليه المشرع الجزائري في نص المادة 394

[94] محمد زكي أبو عامر، المرجع السابق ، 765 .

مكرر 02 بقولها" يعاقب بالحبس من شهرين (02) إلى 03 سنوات و بغرامة من 1.000.000 دج إلى 10.000.000 دج كل من يقوم عمدا و عن طريق الغش بما يلي :

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

2 – حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان ، المعطيات المتحصل عليها في هذا القسم[95].

إضافة إلى العقوبات التكميلية التي يقضي بإغلاق المواقع محل الجريمة ومصادرة الأجهزة و البرامج و الوسائل التي أستعملت في الجريمة المنصوص عليها في المادة 394 مكرر 06 و جاءت المادة كما يلي : " نذكر فيها أنه مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم بالعقوبات المقررة على الجنحة ذاتها "[96].

الفرع الثاني

الركن المادي

يعرف الركن المادي للجريمة " سلوك إجرامي معين تطلبه القانون كمناط للعقاب على هذه الجريمة ، على أن تتحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه العقاب على الجريمة ، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سببية وهو ما يطلق عليه الإسناد المادي ."[97] ويقصد كذلك بالركن المادي للجريمة "كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا ، يؤدي إلى نتيجة تمس حقا من الحقوق ، التي يكفلها الدستور والقانون ." ويتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي

---

[95] : المادة 394 مكرر02 من قانون العقوبات .

[96] : المادة 394 مكرر06 من قانون العقوبات .

[97] عبد الله بن محمد كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، أطروحة ماجستير، كلية الدراسات العليا، تخصص التشريع الجنائي الإسلامي، جامعة نايف للعلوم الأمنية، الرياض، 2013، ص 40 .

مرتكب مثلا:(جريمة الغش المعلوماتي، الركن المادي فيها وتغير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية.)[98]

ويمكن تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر :

ويعرف السلوك الإجرامي في الجريمة المعلوماتية بأنه " فعل أو امتناع عن فعل يؤدي إلى الإضرار بمعلومات مخزنة على إحدى الحواسيب الآلية ، والتي تؤدي إلى إهدار، أو إنقاص قيمة المعلومات وتسبب ضرر الآخرين" ، فالسلوك الإجرامي في الجرائم المعلوماتية لابد أن يتم من خلال أجهزة الحاسب الآلي ، أو شبكة الانترنت، [99] ذلك أن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية و اتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته ، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة ، فيقوم بتحميل الحاسب ببرامج إختراق ،أو أن يقوم بإعداد هذه البرامج بنفسه ،وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف ،كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.[100]

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث ،فالسلوك قد أحدث تغييرا ملموسا ، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج ، بغض النظر عما يمكن ، أن يحدثه السلوك الإجرامي من نتائج أخرى ،علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقق نتيجتها مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل . [101]

وللنتيجة الإجرامية مدلولان أحدهما المدلول المادي والآخر المدلول القانوني ، فالمدلول المادي يعني الآثار المادية التي تحدثها الجريمة في العالم الخارجي، ويرتب القانون على حصولها عقوبة ،وبالنسبة

---

[98] عاقلي فضيلة، المرجع السابق، ص 120 .

[99] عبد الله بن محمد كريري، المرجع السابق، ص 41 .

[100] محمد علي قطب، الجريمة المعلوماتية وطرق مواجهتها، ج2، الأكاديمية الملكية للشرطة، مملكة البحرين، مارس 2010، ص 70 .

[101] عاقلي فضيلة، المرجع السابق، ص 119 .

للمدلول القانوني وهو المصلحة المحمية بنص القانون ، وما إذا كانت قد أضرت أم لا فإن تحقق المساس بهذه المصلحة وقعت النتيجة الإجرامية في صورتها القانونية .

وبالرجوع إلى التشريع الجزائري فان الدخول غير المصرح إلى نظام المعالجة الآلية للمعطيات يعد جريمة شكلية لأنها لا تشترط تحقق النتيجة، فبمجرد الوصول إلى المعلومات المخزنة تقوم الجريمة، وقد نصت المادة 394 مكرر من قانون العقوبات الجزائري على أنه "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6اشهر إلى سنتين والغرامة من50.000 إلى 150.000 دج".

والملاحظ أن المشرع الجزائري يعاقب على الشروع في الجريمة حتى ولو لم تحقق هذه الجريمة نتيجة وذلك من خلال استعمال عبارة " **أو يحاول** " في نص المادة 394 مكرر.

الفرع الثاني

الركن المعنوي

الركن المعنوي "الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني"[102]، و يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطا أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي.[103] ولاشك أن بقاءه داخل نظام الحاسب الآلي بعد دخوله عن طريق الخطأ وتبينه ذلك لا يختلف من حيث التجريم عن الدخول غير المشروع إلى نظام الحاسب الآلي . [104]

---

[102] محمد علي قطب، المرجع السابق، ص 71 .

[103] يوسف جفال، المرجع السابق، ص 17 .

[104] عبد الله بن محمد كريري، المرجع السابق، ص 46 .

و يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما، العلم والإرادة، فالعلم هو إدراك الفاعل للأمور أما الإرادة فهي اتجاه السلوك الإجرامي لتحقيق النتيجة .

الأصل أن الفاعل في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام ،إذن فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لا يمنع أن بعض الجرائم الالكترونية يتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الانترنيت و جرائم نشر الفيروسات عبر الشبكة) .وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي. [105]

و الشروع في الجريمة كالجريمة نفسها إذ أن العقوبة المطبقة على الشروع في الجريمة هي نفسها عقوبة الجريمة التامة ، ويراد بالشروع في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة ، كانت لتقع بالفعل لولا تدخل عامل خارج عن إرادة الفاعل حال في اللحظة الأخيرة دون وقوعها[106] وهو ما نص عليه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات حيث اعتبر العقوبة المطبقة على الشروع في الجريمة هي نفسها المطبقة على الجريمة التامة .[107]

المبحث الثالث

المجرم الإلكتروني

لاشك أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير ، يعد في نظر القانون مجرما ويتعرض للعقاب إذا ما إقترف جريمته وإذا كنا في مجال الإجرام المعلوماتي

---

[105] عاقلي فضيلة، المرجع السابق، ص 120 .

[106] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، (د/ ط)، 2009، ص 184 .

[107] مختارية بوزيدي، ماهية الجريمة الإلكترونية، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري 09-3-2017، ص 7.

فيجب علينا أن ننظر إلى المجرم المعلوماتي من حيث الظروف التي دفعته لإرتكاب جريمته وأسبابها وصفاته حتي يمكن إعادة تأهيله إجتماعيا .

المطلب الأول

سمات المجرم الإلكتروني

تسبق الحاجات عادة دوافع ، فالحاجة تنشأ من الشعور بالنقص أو الحرمان من شيء ما لدى الفرد، مما يؤدي إلى التأثير في القوى الداخلية لديه ، بغرض إشباع هذه الحاجات التي يحقق تواجدها حالة من الرضا النفسي ، وتنوع دوافع الإقدام على الجريمة الإلكترونية بإختلاف منفذيها، وتبعا لطبيعة ودرجة خبرته في مجال المعلوماتية ، كما يتميز المجرم الإلكتروني بمجموعة من الخصائص تجعله متفردا ومتميزا عن المجرم التقليدي .

الفرع الأول

دو افع إرتكاب الجريمة المعلوماتية

يمكن تصنيف هذه الدوافع إلى صنفين ، دوافع شخصية ودوافع خارجية.

1-**الدو افع الشخصية**: يمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى دوافع مادية

وأخري ذهنية[108].

أ-الدو افع المادية : من أهمها :

*- **تحقيق الربح وكسب المال** : الدافع الذي يدفع الجناة لإرتكاب جرائمهم ضد المؤسسات والشركات المالية الإضرار بهذه الشركات والحصول على منافع مادية سواء بالمتاجرة بأسرارها الصناعية ،أو بالإعتداء على حقوقها في الإنتاج ، غالبا ما يكون النفع المادي الذي سيحصل عليه الجاني من سيطرته على المعلومات لاسيما أن المعلوماتية صارت صناعة رائجة أسست لها شركات ومؤسسات متخصصة

[108]-المرجع نفسه ، الصفحة نفسها .

*- **البطالة** : ترتكز البطالة بنسبة كبيرة في فئة الشباب ، الأمر الذي يدفع بعضهم ، نحو البحث عن طرق الكسب السهل والسريع للمال ولو بطرق غير مشروعة .

ب-الدو افع الذهنية :

ذلك أن مختلف البرامج العلمية لها من الصعوبة في إقتحامها أو تخريبها وتثير التحدي في كيفية إتلافها ، وقد إنتبهت الشركات العالمية لوجود مجموعة من الأشخاص الذين يتمتعوا بقدر من الذكاء العلمي الذي يمكنهم من إرتكاب هذه الأفعال الإجرامية إلا أن تلك الشركات كانت تتابع هؤلاء الأفراد بعد القبض عليهم وللإستفادة منهم كانت تقوم بتوظيفهم لتسخير تلك المهارات في معالجة البرامج المعلوماتية .[109] ذلك أنه غالبا مايكون الدافع لدي مرتكبي الجرائم عبر الأنترنت الرغبة في قهر النظام والتفوق على الوسائل التقنية وتعقيدها ، وقد يرتبط بحب التعلم والإستكشاف .[110] وذلك دون أن يكون لهم نوايا آثمة ، فيتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها ، ويعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم ، وإنما بغرض المزاح فقط ولكن قد تنتج عنها نتائج ترقى إلى درجة الجريمة .

2-الدو افع الخارجية :

يمكن أن يتأثر المجرم المعلوماتي ببعض المواقف تدفعه لإرتكاب الجريمة ويمكن إبراز أهم هذه الدوافع فيما يلي :

أ- الإنتقام من رب العمل وإلحاق الضرر به :

لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ، يتعرضون لضغوطات نفسية كبيرة ، ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة ، هذه الأمور مثلت في حالات كثيرة قوة محركة لبعض العاملين لإرتكاب جرائم

---

[109] نايرنبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012، ص 24 .

[110] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص 33 .

الحاسوب ، باعثها الإنتقام من المنشأة أو من رب العمل ،وتحديدا جرائم إتلاف البيانات والبرامج ، وهناك أمثلة كثيرة كان دافع الجناة فيها إشباع الرغبة بالإنتقام ، وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس ، والتكنيك الغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لإرتكاب جرائمها .[111]

ب-المنافسة :

محاولات الشركات المنافسة الحصول على معلومات تقنية حديثة أو أسرار تكنولوجية أو عسكرية أو معلومات عن البنوك والمعاملات المالية مثل : الأسهم والسندات المتعامل بها في البورصات العالمية ، وذلك بواسطة أشخاص مؤجرين لهذا الغرض .

هذا النوع كثير التكرار في الجرائم المعلوماتية ، وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية ، أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها ، فيقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية ، وعادة ما يمارسون التنصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم . وينتشر هذا الدافع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة .

ج- التهديد الأمني الوطني والعسكري.

بعض الجرائم الالكترونية الهدف منها يرجع لأسباب ودوافع سياسية كتهديد الأمن القومي و العسكري ، حيث سخرت شبكة الأنترنت في الصراعات السياسية الدائرة اليوم فمنذ سنوات ظهرت هناك محاولات لإختراق شبكات حكومية في مختلف أنحاء العالم ، ومن ذلك ظهور ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني والحر بالمعلوماتية كما هو حاصل بين الدول المتقدمة إلكترونيا.

الفرع الثاني

سمات المجرم الإلكتروني

[111] أمير فرج يوسف، المرجع السابق، ص 129 .

يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ومن أهمها :

1-المهارة والتخصص :

تنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدرا من المهارة يتمتع بها الفاعل والتي يكتسبها عن طريق الدراسة المتخصصة في هذا المجال ، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات ، أو بمجرد التفاعل الإجتماعي مع الآخرين .[112] حيث تبين في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى ، مما يعكس أن المجرم الذي يرتكب الجرائم الإلكترونية هو مجرم في الغالب متخصص في هذا النوع من الإجرام .[113] إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو أن تكون لديه خبرة كبيرة فيه ، بل إن الواقع العملي قد أثبت أن جانب من مجرمي المعلوماتية ، لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال .[114]

2-المعرفة :

تتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها ، وإمكانيات نجاحها وإحتمالات فشلها ، إذا أن المجرم الإلكتروني بإستطاعته أن يكون تصورا كاملا لجريمته ، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته .

3- إرتفاع مستوى الذكاء لدى المجرم الإلكتروني :

---

[112] طارق إبراهيم الدسوقي عطية، المرجع السابق، 176 .

[113] عمر عبد العزيز موسى الدبور، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية، المؤتمر الدولي الرابع عشر الجريمة الإلكترونية من 24 – 25 مارس 2017، طرابلس، لبنان، ص 219 .

[114] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 176 .

إجرام الأنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف ، فمجرم الأنترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة ، لايعرفها أحد سواه وذلك من أجل إختراق الحواجز الأمنية في البيئة الإلكترونية ثم نيل مبتغاه .

4- الوسيلة :

يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بالبيانات والمعلومات والبرامج [115] هي في أغلب الحالات تتميز نسبيا بالبساطة وسهولة الحصول عليها .

5- السلطة :

يقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي في جريمة تكنولوجيا المعلومات الحديثة والتي تمكنه من إرتكاب جريمته ، وقد تتمثل هذه السلطة في الحق في إستعمال الجهاز الذي يحوي مزايا نظام المعلومات الإلكترونية أو إجراء بعض المعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على أنظمة المعلومات ، وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية ، كما في حالة إستخدام شفرة الدخول الخاصة بشخص آخر .[116]

6- الصبر :

إن الوصول إلى أنظمة المعلومات في الكمبيوتر واختراق تحصيناتها الدفاعية والرقابية يتطلب في الغالب إجراء عدة محاولات تستغرق مددً ا طويلة ، كما أن أكثر الاختراقات تتم عن طريق تقنية المحاولة والخطأ ، والتي تستلزم إجراء عدد من المحاولات ، واستخدام عدد كبير من الأدوات و البرامج للقيام بذلك ،

---

[115] محمد أمين شوابكة، جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1، 2009، ص 19 .

[116] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الوقعة على الأشخاص والحكومة، ص 109 .

كما أن اختيار التقنية المناسبة والعدد والبرامج التي تتطلبها مثل هذه الإختراقات ، واختيار الوقت والمكان المناسبين لإجراء الاختبارات ،و إتباع الطرق المناسبة لتلقي عمليات التتبع وتقفي آثار المعتدي ، كالانتقال من شبكة إلى أخرى حتى الوصول إلى الهدف كل ذلك يتطلب درجة عالية من الذكاء لدى منفذ مثل هذه العمليات.

7- المجرم الإلكتروني متكيف اجتماعيا:

المجرم الإلكتروني لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل إنه إنسان متكيف إجتماعيا , ذلك أنه أصلا مرتفع الذكاء و ذلك يساعده على التكيف الاجتماعي ذلك أن الكثيرين يرون أن الذكاء ما هو إلا القدرة على التكيف ولا يعني ذلك التقليل من شأن المجرم المعلوماتي بل إن خطورته الإجرامية قد تزداد إذا زاد تكيفه اجتماعيا مع توافر الشخصية الإجرامية لديه ، و أغلب المجرمين المعلوماتيين أعمارهم تتراوح عادة ما بين 18 و 46 سنة والمتوسط العمري لهم 25 سنة [117].

8-الحرص الشديد وخشية الاكتشاف:

يتصف المجرمون عبر الأنترنت بالخوف من كشف جرائمهم وإفتضاح أمرهم ، وبالرغم من أن هذه الخشية تصاحب المجرمين على إختلاف أنماطهم إلا أنها تميز مجرمي الأنترنت بصفة خاصة لما قد يترتب على كشف أمرهم من إرتباك مالي وفقد المركز الوظيفي في كثير من الأحيان .

9- مجرد عائد الإجرام :

يتميز المجرم الإلكتروني بأنه عائد للجريمة، دائما فهو يوظف مهاراته في كيفية عمل الحواسيب، وكيفية تخزين البيانات والمعلومات والتحكم في الأنظمة. إذ يوجد شعور لدى مرتكب فعل الإجرام الإلكتروني أن ما يقوم به لا يدخل في عداد الجرائم، ولا يعاقب عليها قانونيا.[118]

10-الميل إلى التقليد :

---

[117] حكيم سياب، السمات المميزة لجرائم المعلوماتية عن الجرائم التقليدية، جامعة 20 أوت 1955، سكيكدة، ص 224.

[118]- عطوي مليكة، الجريمة المعلوماتية، مجلة حوليات جامعة الجزائر، العدد 21، جوان 2012، ص 12 .

ذلك لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية ، مما يؤدي به الأمر إلى إرتكاب الجرائم ، لاشك أن ذلك نتيجة لعدم الإستواء في شخصية الفاعل الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط به ، ويتنهي به الأمر إلى إرتكاب الجريمة .

11- التخطيط والتنظيم :

في عالم الشبكات الإلكترونية وخاصة العالمية للأنترنت ، ترتكب أغلب جرائم المعلومات من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ، يتم العمل بينهم وفقا لتخطيط وتنظيم سابق على إرتكاب الجريمة ، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر يساهم في إرتكاب الجريمة ،فمثلا تحتاج جريمة نسخ برامج الحاسب الآلي إلى شخص يقوم بنسخ تلك البرامج وتحتاج أيضا إلى من يقوم بعملية البيع .

المطلب الثاني

أنواع المجرمين الإلكترونيين

لقد ورد في العديد من الدراسات تصنيف لمجرمي الأنترنت إلا أن التصنيف الذي جاء به Dividicove Karl Seger and WiliamVonstrch, في مؤلفهم جرائم الكمبيوتر الصادر عام 1995 من أفضل التصنيفات حيث إعتمد على الغرض وليس على أساس التكنيك الفني المرتكب في الإعتداء التي ولقد تم تصنيف مجرمي المعلوماتية إلى ثلاث طوائف وهم: المخترقون، المحترفون والحاقدون .

الفرع الاول

المخترقون أو المتطفلون

يرتكب أفراد هذه المجموعة هذا النوع من الجرائم بهدف التحدي والابداع حيث انهم ينصبون أنفسهم أوصياء على أمن الكمبيوتر في المؤسسات المختلفة ويتميزون بالتعاون بينهم فهم يتبادلون المعلومات ويتشاركون في وسائل الاختراق وآليات نجاحها.

والسمة الغالبة على أعضاء هذه الطائفة صغر السن وقلة الخبرة وعدم التميز بين الأنظمة محل الاختراق، ولكن هذا لم يمنع مجرموها من اختراق مختلف أنواع نظم المعلومات التابعة للشركات المالية والتقنية والبنوك والمؤسسات الحكومية ومؤسسات الخدمة العامة.[119]

1-الهاكرز hackers :أو المتسلل

هو شخص بارع في إستخدام الحاسب الآلي وبرامجه ولديه فضول في إستكشاف حسابات الآخرين وبطرق غير مشروعة أو بهدف إكتساب الخبرة أو لمجرد القدرة على إختراق هذه الأنظمة [120] ،وهم عادة من الشباب الفضوليين الذين يسعون إلى التسلية ولايشكلون خطورة على الصناعات وأنظمة المعلومات .

فهم متطفلون يتحدون أمن النظم والشبكات، لكن لا تتوافر لديهم دوافع حاقدة او تخريبية، وانما ينطلقون من دوافع التحدي واثبات المقدرة. فهم يتخذون من الجرائم الالكترونية والقرصنة هواية أو فضول ليس أكثر وتكون غالبا من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الالكترونية والحاسوب.[121]فغرضهم هو التوصل الى الدخول غير المصرح به الى نظم الحاسوب، حيث أن دوره يقتصر في التسلية لا غير فهو غير مؤذ، مثل ما حدث بنظام شركة مايكروسوفت الأمني في اكتوبر 2000 حيث قامت مجموعة مجهولة من اختراقه دون أن تخربه .[122]

---

[119] هروال هبة نبيلة، جرائم الانترنيت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بالقايد، تلمسان، 2013-2014، ص 52.

[120] نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقانون المقارن، المؤتمر الدولي الرابع عشر الجريمة الإلكترونية، 24-25 مارس 2017، طرابلس، لبنان، ص 101 .

[121]عاقلي فضيلة، الجريمة الالكتروبية واجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الرابع عشر الجريمة الالكترونية، طرابلس، لبنان، 24 الى25 مارس2017، ص 120.

[122]هروال هبة نبيلة، المرجع السابق، ص، 52.

وعادة ما يكونون من العاملين بنفس جهة الضحية التي تثق بهم ولا تشك في نزاهتهم منتهزين في ذلك جهل موظفيها وكبار مديريها بعلوم وتقنيات الحاسوب.[123]

2- الكراكرز crakers أو المقتحم :

تعرف هذه الطائفة بالمجرمين البالغين ،أو المخربين المهنيين ،وأعمارهم بين 25-45 عاما ، ومن أبرز سمات و خصائص أفراد هذه الطائفة ، بأنهم ذوي مكانة في المجتمع وأنهم دائما ما يكونون من المتخصصين في مجال التقنية الإلكترونية أي انهم يتمتعون بمهارات ، ومعارف فنية في مجال الأنظمة المعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات ،

فإعتداءاتهم تعكس ميولا إجرامية خطرة تنبئ عن رغبتهم في إحداث التخريب ، ويتميز هؤلاء بقدراتهم التقنية الواسعة ،وخبراتهم في مجال الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول ،فقد يحدثون أضرارا كثيرة وعادة ما يعود المجرم المحترف للجريمة عبر الأنترنت إلى إرتكابها مرة أخرى ،حيث أنهم لا يتفانون في ارتكاب جريمتهم تحت أي ظرف كان ، ويمثل هذا الأخير التهديد المباشر والكامل والخطير للمصالح عبر الأنترنيت اذ يتسلل بصورة خفية الى مواقع مختارة بعناية لارتكاب جريمته سواء كانت في صورة الاتلاف أو التخريب أو الارهاب أو الابتزاز أو العدوان على الأموال بالسرقة والنصب[124]، وقد ساهم هؤلاء المخترقون في تطوير نظم الأمن في عشرات المؤسسات في القطاعين الخاص والعام بالاضافة الى الاستعانة بخبراتهم في فحص وتدقيق مستوى أمن نظم الكمبيوتر والمعلومات[125] .وتميز هذه الفئة بسعة الخبرة والادراك الواسع للمهارات التقنية، لذلك فقد اثبت الواقع العملي أن الهاكرز يستعين بالكراكرز اذا ما صادفه اي نوع من أنواع الحماية، وغالبا ما يكون هدف هذه الفئة هو الحصول على المال او بغرض الشهرة

3- صغار نوابغ المعلوماتية

---

[123] المرجع نفسه، ص 47.

[124] هروال هبة نبيلة، المرجع السابق، ص، 53.

[125] نفس المرجع، ص 124.

هم فئة من صغار السن مولعون بالثورة المعلوماتية بسبب إنتشار الحاسبات الآلية ، لذلك كان أولئك الشباب يرتكبون الجرائم المعلوماتية عن طريق إستخدام الحاسبات الآلية الخاصة بهم أو بمدارسهم ،وهذه الطبقة من الشباب لديهم قدر لابأس به من الخبرة المعلوماتية ، ومن ثمة فهم يمارسون مواهبهم في إستخدام الحاسب الآلي بغرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية سواء الخاصة بالوزارات أو الشركات العملاقة أو الشركات التجارية أو المؤسسات المصرفية ، وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب خاصة إذا كان من بينهم من لديه علم ومعرفة بعملية البرمجة ،فالجرائم التي يرتكبها العابثون بالحاسوب هي جرائم تدمير واتلاف البرامج والبيانات والمعلومات الخاصة بالغير والمخزنةعلى الحاسوب وادخال الفيروسات لتخريب محتوياته، وكذلك جرائم تعديل أو حذف أو تغيير البرامج والبيانات والمعلومات المخزنة على الحاسوب للغير بشكل غير مشروع لمحاولة الوصول الى نقل أموال من حساب شخص آخر الى حسابه الخاص.[126] ومع ذلك فهؤلاء الشباب قد تكون غايتهم في النهاية مجرد التسلية والملاحظة وليس لديهم دوافع لإرتكاب أفعال إجرامية ، ولكن لايجب أن نستخف بهم لأن خطر إنزلاق هذه الفئة إلى الإحتراف هو إحتمال قائم ، وعندئذ يتحول من مجرد هاوي صغير إلى محترف وخير مثال على ذلك ماحدث في الولايات المتحدة الأمريكية حيث قام طلاب المدرسة الثانوية في مدينة " مانهاتن " بإختراق شبكة إتصالات البيانات الكندية وتدمير ملفات زبائن الشركة .

الفرع الثاني

المحترفون

يقصد بهم المخترقون ذوي النوايا الاجرامية في الاتلاف أو التخريب باستخدام الفيروسات أو القنابل المنطقية، وهم يتميزون بأنهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنيات الحاسب وشبكات الحواسيب، وهم يمثلون التهديدات المباشرة للأنشطة والمصالح، ويتميز أفراد هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية وبالتنظيم والتخطيط للأنشطة المرتكبة لذا

[126] خالد عياد الحلبي، المرجع السابق، ص،36.

فهي تعد الأخطر من بين الفئات الأخرى، وتهدف إعتداءات أفراد هذه الطائفة في الأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم أو سخرتهم مثل: المجموعات الإجرامية التي أصبحت تستغل الأنترنت كوسيلة بديلة للكسب المادي غير المشروع .

هذا إلى جانب المعرفة التقنية المميزة لهذه الطائفة والتنظيم العالي والتخطيط السليم المنوي إرتكابها فإن أفرادها يتميزون أيضا بالتكتم فلا يتبادلون المعلومات المتعلقة بأنشطتهم ، بل العكس يحاولون تطوير معارفهم بسرية تامة ويحاولون ماأمكن عدم كشف طرقهم التقنية لإرتكاب جرائمهم ، والفئة العمرية لهذه الطائفة تتراوح مابين 25 – 40 عام أي أنهم من الشباب .

وقد تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية أو التعبير عن موقف فكري أو نظري أو فلسفي كما لو إستخدمتها الجماعات الإرهابية أو المتطرفة في نشر أفكارها ويعمل المنتمون الى هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة أو على الأقل يشترك في تنفيذ النشاط الاجرامي أكثر من فاعل. وأفرادها يتم تصنيفهم وتقسيمهم إلى مجموعات متعددة إما تبعا لتخصصهم في نوع معين من الجرائم أو تبعا للوسيلة المتبعة من قبلهم في إرتكاب الجرائم حيث نجد:

1-الدعاة المتطرفون EXTREME ADVOCATES:

تتكون هذه الطائفة من مجموعة من الأشخاص لديهم معتقدات وأفكار إجتماعية أو سياسية أو دينية أويرغبون في فرض هذه المعتقدات باللجوء إحيانا إلى النشاط الإجرامي ، ويرتكز نشاطهم بصفة عامة في إستخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى مايدعون إليه ، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوروبا بإسم "**الألوية الحمراء ""THE RED BRIGADES**بتدمير مايزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها .

2-محترفو التجسس :ESPIONS

هؤلاء مهمتهم إستخبارية تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها ،سواء كانو يعملون لمصلحة دولهم ،أو لمصلحة بعض الأشخاص ،أو الشركات التي تتنافس فيما بينها، فمن مقتضيات عملهم عدم ترك أي دليل وراءهم ، وذلك لكونهم أشخاص من أصحاب الكفاءات ،ويتمتعون بقدرة عالية على التعامل مع الحاسب الآلي ، إلى جانب قدرتهم على طمس الأدلة التي تتخلف عن جرائمهم . [127]كما يمكن لهم من خلال عمليات التجسس التي تقوم بها الأجهزة الاستخباريةالحصول على أسرار ومعلومات الدولة ومن ثم افشائها الى دول أخرى معادية أو اسغلالها لما يضر المصلحة الوطنية لتلك الدولة.

3- محترفو السطو على أموال البنوك:

عن طريق القرصنة والتي تستهدف المواقع البنكية من أجل تحويل الأموال ثم تمريرها عبر سلسلة من الحسابات بعد توظيف أصحابها في هذا الشأن ، ظهرت بعض الحالات المماثلة ، حيث قام شخص جزائري بتصميم صفحة ويب خاصة ببنك أجنبي ليقوم بعد ذلك ببيعها لشبكة من القراصنة الذين قاموا بدورهم بإيوائها في الشبكة العنكبوتية من أجل إيهام الزبائن بأنها فعلا الصفحة الرسمية لبنكهم وبعدما تمكنوا من تحويل إرتباطات هؤلاء الزبائن وبعده الحصول على المعطيات المتعلقة بحساباتهم البنكية التي إستعملت في تحويل أرصدتهم[128] .

الفرع الثالث

الحاقدون

هذه الطائفة يغلب عليها عدم توافر أهداف وأعراض الجريمة المتوفرة لدى الطائفتين المتقدمتين فهم لا يسعون إلى إثبات القدرات التقنية والمهارية وفي نفس الوقت لا يسعون إلى مكاسب مادية أو

---

[127] محمد حماد مرهج الهيتي، المرجع السابق، ص 82 .

[128] مختار الأخضري، المرجع السابق، ص 129 .

سياسية إنما يحرك نشاطهم الرغبة في الإنتقام والثأر كأثر لتصرف صاحب العمل معهم ،أو لتصرف المنشأة المعنية معهم عندما لا يكونون موظفين فيها ،

ولهذا فإنهم ينقسمون إما إلى مستخدمي النظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة ،وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم ، وتغلب على أنشطتهم من الناحية التقنية إستخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم وإتلاف كل أو بعض معطياته ،

ومن ميزاتها عدم توافر التفاعل بين أعضائه كما أنهم لا يفاخرون بأنشطتهم بل يعمدون الى اخفائها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قامو بارتكابها لتوفر ظروف وعوامل تساعد في ذلك، ولكن بالرغم من أن سمات أفراد هذه الطائفة أقل خطورة من غيرهم من مجرمي التقنية، الا أن ذلك لا يمنع أن تكون الأضرار التي نجمت عن أنشطة بعضهم جسيمة قد تلحق خسائر فادحة بالمؤسسات المستهدفة.[129] وليس هناك ضوابط محددة بشأن أعمار هذه الطائفة .[130] ويمكن توضيح ذلك كما يلي :

1-الموظفون العاملون بمراكز الحاسب الآلي :

وهم يمثلون الغالبية العظمى من مرتكبي الجرائم المعلوماتية ،وذلك بحكم سهولة إتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية .[131]

2- **الغرباء :**

وهم أشخاص أجانب عن تلك المؤسسة ويندرج تحت هذه الطائفة المستخدمون الذين ليس لهم تصريح بالعمل على النظام المعلوماتي الخاص بتلك المؤسسة أو الشركة وفي الغالب يكون التخريب

---

[129] سمير شعبان، المرجع السابق، ص، 125.

[130] محمد أبو العلا عقيدة، ظاهرة الإجرام الإلكتروني ومخاطرها ،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية 26- 28 نيسان 2003، مركز البحوث والدراسات، الإمارات العربية المتحدة، ص 23-24.

[131] حكيم سياب، المرجع السابق، ص 223 .

هو هدف هؤلاء الدخلاء أي أنهم يقومون بالدخول على الكمبيوتر بغرض إرتكاب جرائم التخريب أو قد يكون المكسب المادي هو الهدف من عملية الدخول .[132]

الفصل الثاني

الأحكام الإجرائية للجريمة الإلكترونية

إنّ تجريم بعض السلوكيات و تقرير جزاءات تسلّط على مرتكبيها يستوجب إسناد هذا الفعل للمتهم بناء على معطيات و أدّلة إثبات تفيد ارتكابه للفعل المحظور قانونا ، و تتمّ المتابعة الجزائية للشخص المتهم بعد تحريك الدعوى العمومية من طرف الجهات المؤهلة قانونا أين يتم إجراء التحري و جمع الأدّلة ثم التحقيق القضائي وهو ما يطلق عليه المواجهة الإجرائية ، فيتقرر بناء على المعطيات و الأدّلة المتوصل إليها متابعة الشخص سواء الطبيعي أو المعنوي و تقرير الإدانة أو البراءة ، وذلك حماية للمصلحة العامة للدولة و الأفراد ، وطبيعة الدليل التي تثبت به هذه الجريمة يستمد من العالم الافتراضي الذي يعتد على الأرقام و هو ما يطلق عليه الدليل الرقمي ،

[132] بن منصور صالح ،كوش أنيسة، المرجع السابق، ص 38 .

و نبيّن في المبحث الأوّل من هذا الفصل إجراءات الدعوى العمومية ثمّ نعرج على الدليل الرقمي وحجيته في الإثبات وهذا في مطلبين على التوالي ، وخصصنا المبحث الثاني للعقوبات المقررة لهذه الجريمة رغم أنّها تدخل في الأحكام العامة إلاّ أنّنّا ارتأينا إدراجها في هذا الفصل ، لأنّها النتيجة الحتمية لتحريك الدعوى العمومية و انتهاء إجراءات البحث و التحري و التحقيق القضائي أين تتقرر المحاكمة و توقيع العقوبة .

إن الاستخدام غير المشروع لتقنية الحاسب الآلي والانترنت رتب العديد من الإشكاليات الإجرائية في مجال إجراءات الملاحقة الجنائية التي تتبع من أجل كشف الجريمة وإقامة الدليل على وقوعها ونسبتها إلى مرتكبيها الذين يتوسلون بالتقنية المتطورة في ارتكابها وفي إخفاء معالمها وعدم ترك أية آثار مادية دالة عليها ، وهذه صعوبة مع الصعوبات الأخرى التي تواجه الحصول على الدليل والتي سيأتي تفصيلها لاحقا ؛ جميعها أدت إلى تدخل مشرعي بعض الدول لمواجهة هذا النوع من الجرائم ، وذلك بإصدار قوانين خاصة بملاحقتها وتنظيم الإجراءات التي تناسبها دون مساس بحقوق الأفراد وحرياتهم الأساسية.

دراستنا لإجراءات جمع الأدلة سوف تقتصر على أربع وسائل وهي المعاينة والتفتيش وضبط الأشياء وندب الخبراء ، نبدأ كلاً منها بنبذة موجزة عن القواعد العامة المتعلقة بها ، وننبه بالرجوع إلى المراجع العامة ذات العلاقة ، نظرا لضيق مساحة هذا البحث ، على أمل أن لا يكون في نهجنا هذا إخلال بمنهجية البحث أو قصور في التقديم والطرح ، ثم نبحث تلك الإجراءات من المنظور الذي يعتمد عليها فيه بالنسبة للجرائم الإلكترونية التي تمثل ضربا من ضروب الذكاء الإجرامي الجديد والتي باتت تتخذ أنماطا جديدة لا يجدي معها اتّباع الإجراءات التقليدية ، لما تثيره طبيعتها غير المادية من إشكاليات وما تؤديه التقنية الحديثة من دور في ارتكابها ، وما توفره لها من مسرح غالبا ما يكون أقل ظهورا لحقائق موضوع البحث وأدلته ، وذلك لوقوعها في عالم افتراضي ، وطبيعة أدلتها غير ملموسة [133] .

المبحث الأوّل

[133]- ولهذا نصت المادة 15 من اتفاقية بودابست الخاصة بجرائم الحاسب الآلي والانترنت ، على إجراءات أغالبها مستحدثة وغير مألوفة يعبر عنها بمصطلحات بيئة التقنية ، وهي إجراءات تتناسب مع طبيعة الجرائم الإلكترونية تراعى فيها حرية الأفراد الشخصية وتكفل حقوقهم الأساسية.

المواجهة الإجرائية للجريمة

تبدأ المواجهة الإجرائية إمّا بالإخطار أو الإبلاغ من قبل الأشخاص الطبيعية أو الاعتبارية أو موظفي المؤسسة المالية أو جهات الاستدلال أو الشرطة عند تلقي البلاغات [134]، و بعد ذلك تبدأ الهيئات المختصة في جمع المعطيات و الأدّلة المتعلقة و المحيطة بالجريمة بغرض الحصول على أدّلة الإثبات وفق الإجراءات المقررة في القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها[135]، كما أنّ طبيعة الدليل الرقمي المعتد به في الجريمة الإلكترونية يثير إشكالية حجيته في الإثبات ، لذا سوف نتطرق إلى مراحل الدعوى العمومية في مطلب أوّل ثمّ في مطلب ثاني حجية الدليل الرقمي .

المطلب الأوّل

مراحـل الدعــوى العمــوميــة

إن مراحل الدعوى العمومية ثلاث ن مرحلة الإستدلالات و مرحلة التحقيق اقضائي و مرحلة المحاكمة والتي من خلال تلك المراحل و مختلف وسائل جمع الأدلة الجنائية يتقرر الحكم بالإدانة أو بالبراءة ،

و سوف نبيّن الإجراءات التي تتمّ في كلّ من مرحلة جمع الاستدلالات و التحقيق كونهما تثيران العديد من الإشكالات في ظلّ الجرائم الرقمية ، خاصة و أنّ المشرع الجزائري لم يضع أحكاما خاصة ، في حين أنّ مرحلة المحاكمة لا يذكر فيها أيّ جديد .

الفرع الأوّل

مرحلة جمع الاستدلالات

تمرّ الدعوى العمومية بمرحلتين التحقيق القضائي و الثانية تعرف بالمحاكمة ، و تسبق هاتين المرحلتين ، مرحلة أوّلية تعرف بأعمال الاستدلال تهدف إلى التمهيد للتحقيق الابتدائي و جمع

---

[134] إبراهيم محمود محمد بن عبد الرحمان ، جريمة غسل الأموال في القانون الإماراتي و المقارن - دراسة مقارنة - رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، 2009 ص 361

[135]قانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج رعدد 47 الصادرة بتاريخ 2009/08/16 .361

المعلومات عن الجريمة و البحث عن مرتكبيها بأساليب محدّدة قانونا [136]، تهدف إجراءات الاستدلال إلى جمع معلومات متعلّقة بالجريمة و المساهمين فيها لتوضيح المعطيات لسلطة التحقيق كي تتصرّف على وجه معيّن [137].

أوّلا : الهيئات المختصة بجمع الاستدلالات

الأصل أنّ الضبطية القضائية هي المختصة في جمع الاستدلالات و التحري عن مختلف الجرائم إلاّ أنّ الجريمة الإلكترونية لها خصوصيتها من الناحية الإجرائية لذا نصّ المشرع الجزائري على إنشاء هيئة متخصصة .

1-الضبطية القضائية

تنص المادة 12 فقرة 01 من قانون الإجراءات الجزائية المعدّلة و المتمّمة بموجب المادة 04من القانون 15/17 المؤرخ في 2017/03/27 [138]، و التي نصّها ما يلي :

" يقوم بمهمة الشرطة القضائية ، القضاة و الضباط و الأعوان و الموظفون المبيّنون في هذا الفصل .." يتضح من نص المادة أنّ هذه الفئات هي :

ضباط الشرطة القضائية : حدّدتهم المادة 15 من الأمر 02/15 الصادر في 2015/07/23 [139]المعدل و المتمم لقانون الإجراءات الجزائية التي تنص :" يتمتع بصفة ضابط الشرطة القضائية :

- رؤساء المجالس الشعبية البلدية .
- ضباط الدرك الوطني .
- الموظفون التابعون للأسلاك الخاصة للمراقبين و محافظي ضباط الشرطة للأمن الوطني .

---

[136] لعوارم وهيبة، المرجع السابق، ص 311.

[137] لعوارم وهيبة، نفس المرجع ، ص 312 .

[138]قانون 15/17 المؤرخ في 2017/03/27 يعدل و يتمم الأمر 155/66 المؤرخ في 08 يونيو 1996 و المتضمن قانون الإجراءات الجزائية ، ج ر عدد 20 المؤرخ في 2017/03/29 .

[139]الأمر 02/15 المؤرخ في 23 يوليو 2015 المعدل و المتمم لأمر 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، ج ر عدد 40 الصادرة بتاريخ 2015/07/23 المو افق عليه بموجب القانون 17/15 المؤرخ في 2015/12/13 .

-ذوو الرتب في الدرك،ورجال الدرك الذين أمضوا في سلك الدرك الوطني ثلاث سنوات على الأقل بهذه الصفة و الذين تمّ تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية و الجماعات المحلية،بعد موافقة لجنة خاصة.

- ضباط و ضباط الصف التابعين للمصالح العسكرية للأمن الذي تمّ تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل .

يحدّد تكوين اللجنة المنصوص عليها في هذه المادة و تسييرها بموجب مرسوم "

تدخل المشرع بموجب نص المادة 15 مكرر فقرة 01 [140] التي جاء بها القانون 07/17 المعدل لقانون الإجراءات الجزائية و حصر مهام مصالح الأمن العسكـري في الجرائم الـماسة بأمـن الدولة لكي يتـفرغ للعمل المخابراتي لحماية أمن الدولة.

أعوان الشرطة القضائية الذين عددتهم المادة 19 ق إ ج [141]

فئة الولاة : نصت عليهم المادة 28 ق إ ج [142]و يتدخل الولاة في حالة الاستعجال شرط العلم بعدم إخطار الضبطية القضائية .

3- قضاة التحقيق و النيابة العامة

يستفاد من نص المواد 12 و 36 و 38 و 56 ق إ ج أنّ إجراءات البحث و التحري عن الجرائم من صلاحيات جهات التحقيق [143] ،ممّا يفيد أنّ قاضي التحقيق و النيابة لها صلاحيات الضبطية القضائية .

* إلى جانب هذه الفئات هناك فئات محددة في قوانين خاصة .

---

[140]تنص المادة 15 مكرر فقرة 01 من قانون 07/17 المعدل و المتمم لقانون الإجراءات الجزائية :" تنحصر مهمة الشرطة القضائية لضباط و ضباط الصف التابعين للمصالح العسكرية للأمن في الجرائم الماسة بأمن الدولة المنصوص عليها في قانون العقوبات ".

[141]المادة 19 الأمر 10/95 المؤرخ في 1995/02/25 "يعدّ من أعوان الضبط القضائي موظفو مصالح الشرطة وذوو الرتب في الدرك الوطني ورجال الدرك و مستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية"

[142] ارجع نص المادة 28 من قانون الإجراءات الجزائية .

[143] سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ،رسالة ماجستير، جامعة الحاج لخضر، باتنة ، 2013/2012 .ص103.

تختص الضبطية القضائية بإجراءات البحث و التحري و جمع الأدلة و المعاينة كأصل عام في حدود مقر عملهم ، إلاّ أنّه يمكن تمديد اختصاصهم في حالة الاستعجال إلى كافة دائرة اختصاص المجلس القضائي بطلب من القاضي المختص قانونا بعد إخطار وكيل الجمهورية الذي يباشرون المهام في دائرة اختصاصه، و يكون للضبطية القضائية اختصاص وطني فيما في إطار جرائم محددة على سبيل الحصر ضمن نص المادة 16 فقرة 07 من قانون الإجراءات الجزائية التي وسّعت مجال الاختصاص للضبطية في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ثانيا :الإجراءات المنوطة بالضبطية القضائية

تقوم الضبطية القضائية في مرحلة جمع الاستدلالات بعدد من الإجراءات خوّلت لها بموجب قانون الإجراءات الجزائية و قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال من بينها : المعاينة ، الاعتراض على الاتصالات السلكية و اللاسلكية ، التسرّب ، المراقبة الإلكترونية .

1-المعاينة

هى إجراء يتم بمقتضاه الانتقال إلى مكان وقوع الجريمة لجمع الأشياء المتعلقة بالجريمة ومعاينة آثار وقوعها .

بمعنى أنّها إثبات حالة الأماكن و الأشخاص و كلّ ما يساعد في كشف الحقيقة وهي تتطلب أن ينتقل ضابط الشرطة القضائية لإثبات حالة الأماكن و ما يوجد فيها من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة [144]والمعاينة قد تتم من قبل النيابة العامة أو من قاضي التحقيق أو المحكمة[145].

---

[144] بوزينة أمحمدي آمنة ،إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية و قانون الوقاية من جرائم الإعلام)، ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر، 29 مارس 2017 ، ص 60 .

[145]تكون المعاينة في هذه الحالة إجراء استدلال - المادة 42 ق إ ج ، كما قد تكون إجراء في إطار التحقيق عندما يكون الملف أمام جهات التحقيق – المادة 79 من ذات القانون- ،كما يخوّل القانون للمحكمة الانتقال لإجراء المعاينة - المادة 235 ق اج - .

تكون المعاينة كذلك في الجرائم الإلكترونية ، إلاّ أنّ الأمر يختلف كون الانتقال يكون بالضرورة عبر العالم الافتراضي[146] وينبغي في هذا الإطار التعامل مع مسرح الجريمة الإلكترونية على أنّه مسرحان:

- مسرح تقليدي ،يقع خارج بيئة الحاسوب و الانترنيت و يتكوّن من المكوّنات المادية المحسوسة للمكان الذي وقعت فيه الجريمة مثل آثار البصمات و وسائط التخزين .

- مسرح افتراضي ، يقع داخل البيئة الإلكترونية و يتضمن البيانات الرقمية التي توجد داخل الحاسوب و شبكة الانترنيت و ذاكرة الأقراص الصلبة [147]، يوصي الخبراء بوجوب اتباع و مراعاة قواعد فنية [148]، تحرير محضر بأعمال المعاينة تحت طائلة بطلان الحكم الذي يستند للمعاينة [149].

وفى كل الأحوال فالأدلة الناتجة من معاينة مكان الجريمة تخضع - كسائر الأدلة الأخرى التي تطرح في الجلسة - لتقدير قاضي الموضوع طبقا لمبدأ حرية الإثبات ، فإن أطمأن أستند إليها في حكمه ، وإذا لم يطمئن يقوم بطرحها جانبا دون معقب أو رقابة عليه من المحكمة العليا.

2- اعتراض المراسلات السلكية و اللاسلكية

عزّز المشرع الجزائري اختصاصات الضبطية القضائية بموجب تعديل قانون الإجراءات الجزائية رقم 22/06 المؤرخ في 2006/12/20 [150] بآليات جديدة للتحري و التحقيق في بعض الجرائم الواردة على سبيل الحصر منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، و من بين هذه الأساليب اعتراض المراسلات الذي يعرّف بأنّه "عملية مراقبة سرية المراسلات السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدّلة أو المعلومات حول الأشخاص المشتبه فيهم ارتكابهم أو مشاركتهم في ارتكاب جريمة" ، ونصّ المشرّع الجزائري على هذا الإجراء ضمن نص المادة 65

---

(146) عمر محمود أبوبكر يونس ،المرجع السابق ،ص 895 .

(147) عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن ، دار الجامعة الجديدة ، الإسكندرية ، 2010 ، ص 84 .

(148) بوزينة أمحمدي آمنة، المرجع السابق ، ص 61

(149) لعوارم وهيبة ، المرجع السابق ، ص 344

150 المعدل و المتمم للأمر رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية ، ج ر عدد 84 الصادرة بتاريخ 2006/12/24 .

مكرر 05 ق إ ج [151]، وقد أجاز المشرع الجزائري هذا الإجراء وفق شروط موضوعية وشكلية يجب توافرها :

أ- **الشروط الشكلية:** و تتمثل هذه الشروط فيما يلي :

- وجود إذن مكتوب تحت طائلة البطلان صادر من وكيل الجمهورية المختص يسمح بالتعرف على الاتصالات المطلوب التقاطها يسلّم لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق[152]،و هذا ما نصت عليه المادة65 مكرر07 ق إج.

- تحرير محاضر بالعمليات التي قام بها ضابط الشرطة القضائية إعمالا لنص المادة 65 مكرر 09 ق إ ج مع التزام أعوان و ضباط الشرطة القضائية القائمين على هذا الإجراء بالسر المهني .

ب-الشروط الموضوعية : و تتمثل في شرطين أساسيين :

- التسبيب ، يجب على القاضي أو وكيل الجمهورية المختص إظهار جميع الأدّلة القانونية الدافعة لإصدار الإذن المكتوب.

- تحديد نوع الجريمة : و هي محددة على سبيل الحصر في المادة 65 فقرة 05 من ق اج أي تبيان أن الجريمة إلكترونية .

3- التسرب أو الاختراق

نظمّ المشرع الجزائري أحكام هذا الإجراء هو الآخر ضمن قانون 22/06 المؤرخ في 20 ديسمبر 2006 و عرّفته المادة 65 مكرر 12 ق إ ج " التسرب هو قيام أحد عناصر الضبطية القضائية الموكلة له مهمة التحقيق في الجريمة بمراقبة الأشخاص المشتبه فيهم أو التوغل داخل الجماعة الإجرامية بإيهامهم أنّه شريك ".

لما كان هذا الإجراء من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيه فقد أحاطه المشرع بعدّة شروط شكلية و أخرى موضوعية :

---

[151]تنص المادة 65 مكرر 05 ق إ ج " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوزلوكيل الجمهورية المختص أن يأذن بما يأتي :- اعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية أو اللاسلكية ... "

[152] لعوارم وهيبة ، الجريمة المنظمة في تبييض الأموال عبر الوسائط الإلكترونية ، المرجع السابق ، ص 357 .

أ- الشروط الشكلية ،

تتمثل في شرطين ، أولاهما الإذن المكتوب من قبل وكيل الجمهورية المختص ،الذي يلتزم بالإشراف و مراقبة نجاح العملية ، و ثانيهما صفة القائم بعملية التسرب ، والتي حددتها المادة 65 مكرر12 ق إ ج [153].

مع الإشارة أن المشرع الجزائري أجاز للعنصر المتسرب رغم انتهاء مدّة التسرب أو صدور أمر بوقف عملية التسرب أن يواصل مهامه لمدّة لا تتجاوز أربعة أشهر و هذا ما نصت عليه المادة 65 مكرر 17 من ق ا ج.

ب- الشروط الموضوعية ،

وهي التسبيب و تحديد نوع الجريمة ، فتسبيب الإذن يعني تبيان أسباب اللجوء لهذا الإجراء فيجب أن يكون الإذن مسببا تحت طائلة البطلان طبقا لنص المادة 65 مكرر 15 ق إ ج [(154)] أما تحديد نوع الجريمة، يعني الإشارة إلى الجرائم المحددة في المادة 65 مكرر 05 ق اج .

وتجدر الإشارة إلى أنّه يمنع على ضباط الأعوان المتسربين أن يحرضوا على ارتكاب جريمة وهذا ما نصت عليه المادة 65 مكرر 12 /2 ق إ ج ، و يمنع أيضا الكشف عن الهوية الحقيقية للمتسرب و من قام بذلك فقد قرّر له عقوبات بنص المادة 65 مكرر 16 .

4- المراقبة الإلكترونية

أضفى المشرع الجزائري الحماية القانونية دستوريا للبيانات ذات الطابع الشخصي ضمن التعديل الدستوري لسنة 2016 [(155)] بموجب المادة 46 من دستور 2016[(156)]، وبذا يكون قد خوّل السلطة القضائية بناء على قرار معلل وفق إجراءات مبيّنة المساس بالبيانات الشخصية في حالة ما إذا اقتضت المصلحة العامة ذلك، و قد جاء بهذا الإجراء قانون 04/09 المؤرخ في 05 أوت 2009

---

[153] ارجع نص المادة 65 مكرر12 من قانون الإجراءات الجزائية .

[(154)]ارجع المادة المادة 65 مكرر11 من ق .اج.

[(155)] قانون رقم01/16 المؤرخ في 06 مارس2016المتضمن التعديل الدستوي،ج رعدد 14 الصادرة بتاريخ 2016/03/07.

[(156)]أضاف المشرع بموجب التعديل الدستوري الوارد في القانون 01/16 الفقرتين الثالثة و الرابعة للمادة 46 " ... لا يجوز بأيّ شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ، ويعاقب القانون انتهاك هذا الحكم ".

المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتهما ، فإكتفى من خلاله بتحديد مفهوم الاتصالات الإلكترونية بموجب المادة 02 فقرة "و" [157].

فيقصد بمراقبة شبكة الإتصالات " ذلك العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات و معلومات عن المشتبه فيه سواء شخص أو مكان أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأيّ غرض آخر " [158].

و بالتالي فإنّ التقنيات التكنولوجية المستخدمة في إطار المراقبة الإلكترونية هي : اعتراض المراسلات الإلكترونية ، تسجيل الأصوات ، التقاط الصور ، تفتيش المنظومات المعلوماتية و حجزها [159]، و القيام بالمراقبة الإلكترونية يتم وفق شروط شكلية و أخرى موضوعية :

فالشروط الشكلية ، تتمثل في :

- وجود إذن مكتوب من السلطات المختصة ما يستفاد من نص المادة 04 فقرة 02 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتهما، ويتم الحصول على هذا الإذن من وكيل الجمهورية أو قاضي التحقيق المختص إقليميا [160]،

- ممارسة الرقابة تحت مراقبة جهة التحقيق المختصة : وهذا ما نصت عليه المادة 41 من المرسوم الرئاسي 26/15 المؤرخ في 2015/10/08 [161]، الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

- خضوع الموظفين المكلفين بالمراقبة الإلكترونية لأداء اليمين ، وهذا ما نصت عليه المادتين 27 و 28 من ذات المرسوم.

ب- أما الشروط الموضوعية فهي ،- التسبيب ، بمعنى أن تكون هنـاك ضـرورة اقتضت هذا الإجراء و هو ما أكدّه المشرع في الفقرة " ج "من المادة 04 من قانون 04/09 " ... لمقتضيات التحريات و

---

[157] تنص المادة 02 فقرة "و"من قانون 04/09" الاتصالات الإلكترونية، أي تراسل أو إرسال أو استقبال علامات أو إشارات أوكتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أيّ وسيلة الكترونية ".

[158] لعوارم وهيبة ، الجريمة المنظمة في تبييض الأموال عبر الوسائط الإلكترونية ، المرجع السابق ، ص،363.

[159] بوزينة أمحمدي آمنة ، المرجع السابق، ص 76 .

[160] غير أنّ الوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب أو الجرائم الماسة بأمن الدولة فإنّ الأمر يتم استصداره من النائب العام لدى مجلس قضاء الجزائر.

[161] را جع نص المادة 41 من المرسوم الرئاسي 26/15 المؤرخ في 2015/10/08 ، ج رعدد 53 الصادرة بتاريخ 10 أكتوبر 2015 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها.

التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية

- تحديد نوع الجريمة ، و هي الحالات المحددة في المادة 04 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال[162]،

إنّ تكريس المشرع لإجراء المراقبة الإلكترونية خطوة جريئة لكونه يمسّ بالخصوصيات الشخصية للأفراد [163]، لكن استعمال البيانات الشخصية المتحصل عليها يتوقف في حدود ضرورات التحقيق وهذا ما كرسته المادة 09 من قانون 04/09 " تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به ، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون ، إلاّ في الحدود الضرورية للتحريات أو التحقيقات القضائية " .

الفرع الثاني

مرحلة التحقيق القضائي

تبدأ مرحلة التحقيق القضائي بإحالة الملف على التحقيق من طرف النيابة بموجب طلب افتتاحي لإجراء تحقيق بموجب المادة 38 ق إ ج[164]، و التحقيق وجوبي في الجنايات و جوازي في الجنح و يمكن أن يكون في المخالفات إذا طلبه و كيل الجمهورية طبقا للمادة 66 ق إ ج، و تتسم هذه المرحلة بالحياد و بضمانات واسعة للمتهم اعتمادا على قرينة البراءة[165]،كما تمتاز بالسريّة اتجاه الجمهور و المواجهة بين الأطراف وكذا خاصيّة التدوين.

أولا : جهات التحقيق

---

[162]تنص المادة 04 من قانون 04/09 على أنّه "يمكن القيام بعمليات المر اقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية : أ - للوقاية من الأفعال الموصوفة بجر ائم الإرهاب أو التخريب أو الجر ائم الماسة بأمن الدولة ، ب- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسا الدولة أو الاقتصاد الوطني ، ج-لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المر اقبة الإلكترونية، د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة ...".

[163] سعيداني نعيم ، المرجع السابق ، ص 184 .

[164] تنص المادة 38 ق إ ج " ... و يختص بالتحقيق في الحادث بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73 ".

[165] تنص المادة 2/1 من قانون 07/17 " أنّ كلّ شخص يعتبر بريئا ما لم تثبت إدانته بحكم قضائي حائز لحجية الشيء المقضي فيه "

يختص بالتحقيق القضائي قاضي التحقيق و يكون مختصا بالنظر في وقائع الأفعال المرتكبة حسب مكان وقوعها أو مكان إقامة المتهم أو مكان القبض عليه ، حسب نص المادة 1/40 ق إ ج [166].

لكن في الجريمة الإلكترونية و بعض الجرائم الأخرى المحددة حصرا بموجب المادة 2/40 ق إ ج يجوز تمديد الاختصاص المحلي إلى محاكم أخرى [167]

و كذا المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[168]وهذا بالنسبة لكل من المحاكم التالية : "محكمة سيدي أمحمد ، محكمة الجزائر ، قسنطينة ، ورقلة ، وهران "، و أطلق على هذه المحاكم تسمية الأقطاب كما يجوز لقاضي التحقيق القيام بجميع إجراءات التحقيق في نطاق اختصاص المحاكم المجاورة لنطاق اختصاصه وفق المادة 80 ق اج .

ثانيا : وسائل التحقيق أو جمع الأدلة

وسائل جمع الأدلة أو التحقيق هي مجموعة من الأعمال التي يرى المحقق ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات ، وهي لم ترد على سبيل الحصر ، لذلك يجوز للمحقق أن يباشر أي إجراء آخر يرى فيه فائدة للإثبات طالما أنه لا يترتب على اتخاذه تقييد لحريات الأفراد أو مساس بحرمة مساكنهم .

وقسم الفقه هذه الوسائل أو الإجراءات إلى نوعين الأول يهدف إلى جمع وفحص الأدلة المثبتة لوقوع الجريمة ونسبتها إلى فاعلها كالمعاينة والخبرة و التفتيش وضبط الأشياء المتعلقة بالجريمة وسماع الشهود والاستجواب ؛ والثاني هو اتخاذ الوسائل اللازمة قبل المتهم لمنعه من التأثير في التحقيق أو في

---

[166] تنص المادة 40 /1 ق إ ج " يتحدّد اختصاص قاضي التحقيق محليّا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقتر افها أو بمحل القبض على أحد هؤلاء الأشخاص حتى و لو كان هذا القبض قد حصل لسبب آخر".

[167] تنص المادة 40 /2 ق إ ج " يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جر ائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجر ائم الماسة بأنظمة المعالجة الآلية للمعطيات و جر ائم تبييض الأموال و الإرهاب و الجر ائم المتعلقة بالتشريع الخاص بالصرف ".

[168] مرسوم تنفيذي 348/06 المؤرخ في 2006/10/05 يتضمن تمديد الإختصاص المحي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق ، ج رعدد 63 الصادرة بتاريخ 2006/10/08 المعدل والمتمم بالمرسوم تنفيذي 267/16 المؤرخ في 2016/10/17 ج رعدد 62 الصادرة بتاريخ 2016/10/23 .

العبث أو إزالة الآثار المستفادة من الأدلة ، وهي ما يطلق عليها الإجراءات الاحتياطية قبل المتهم ، كالأمر بالحضور والأمر بالقبض والحبس المؤقت .

فما هي الوسائل التي منحها القانون لسلطات التحقيق في مواجهة الجريمة الإلكترونية و الكشف عنها و عن مرتكبيها .

1- التفتيش

التفتيش هو البحث عن أشياء تفيد الكشف عن جريمة وقعت ونسبتها إلى المتهم ، كما عرف بأنه " البحث في مستودع سر شخص عن أشياء تفيد الكشف عن الجريمة ونسبتها إلى المتهم " [169].

والتفتيش وفقا للقواعد قانون الإجراءات الجنائية التقليدية ينقسم من حيث محله قسمين : الأول تفتيش ينصب على المنازل ، وتفتيش يقع على الأشخاص ، وتفتيش المنازل هو إجراء من إجراءات التحقيق بمقتضاه يقوم المحقق أو من يأذن له من رجال الضبطية القضائية بالبحث في منزل شخص معين على أشياء تتعلق بجناية أو جنحة قامت قرائن قوية على حيازته لها ، والثاني هو إجراء من إجراءات التحقيق أيضا يقصد به ضبط ما يحوزه الشخص من أشياء تفيد كشف الحقيقة ، وتفتيش المنازل بمعرفة سلطة التحقيق يختلف من حيث شروطه عن التفتيش الذي يجريه مأمور الضبط القضائي استثناء في الجرائم المتلبس بها .

وبخصوصية التفتيش في البيئة الرقمية ، فإنّه ينصب على جهاز الحاسب الآلي الذي يعمل طبقا لتعليمات محددة سلفا يستقبل البيانات ويخزنها ويقوم بمعالجة واستخراج النتائج المطلوبة ، وهو متصل بالشبكة للحصول على المعلومات وتبادلها عبر الشبكات والبريد الإلكتروني ، ولهذا فإن التفتيش في الجرائم الإلكترونية له طبيعة خاصة ومتميزة ، إلا أنه يخضع في إجراءاته للضوابط التي حددها قانون الإجراءات الجنائية وما يستلزمه من وقوع الجريمة واتهام شخص أو أشخاص معينين بارتكاب جريمة ، وأن تكون هناك دلائل أو قرائن على ما يفيد في كشف الحقيقة في أجهزة الحاسب الآلي والإنترنت خاصة بالمتهم أو غيره من الأشخاص ، وإذا ما توافرت تلك الشروط ، فإنه يجوز لسلطة التحقيق تفتيش جهاز الحاسب الآلي وملحقاته المكونة له المادية والمعنوية ، وذلك من أجل ضبط أدلة

[169] مأمون محمد سلامة ،الإجراءات الجنائية في التشريع الليبي ، ج1 ، ط1، منشورات الجامعة الليبية ، 2000، بنغازي ، ص481.

الجريمة ، وما يحتمل أن يكون قد استعمل في ارتكابها أو نتج عنها أو وقعت عليه ، وكل ما من شانه أن يكشف عن الجريمة [170].

أقرّ المشرع الجزائري هذا الإجراء كغيره من المشرعين المقارنين تغليبا لمصلحة المجتمع على مصلحة الأفراد وفق قيود وضوابط تضمن عدم التعدّي على حريّة الأشخاص وحرمة مساكنهم إلاّ في حدود حاجة التحقيق [171]و لصحة الإجراء يشترط توافر شروط موضوعية وشكلية .

أ - الشروط الموضوعية :

وتتعلق بسبب التفتيش و محل التفتيش

- **سبب التفتيش**[172] : أجاز إمكانية اللجوء إلى التفتيش إمّا للوقاية من حدوث الجرائم أو توّفر معلومات باحتمال وقوع الجرائم المحددة في المادة 04 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتهما.

- **محل التفتيش** : يتكوّن النظام المعلوماتي من مكوّنات مادية(HARD WARE)و مكونات منطقية (SOFT WARE) ، و تخضع المكونات المادية للنظام للتفتيش بموجب نص المادة 44 من قانون الإجراءات الجزائية [173] ، كون المشرع استعمل عبارة أشياء و التي يقصد بها المكونات المادية ، أمّا فيما يخص تفتيش المكوّنات المعنوية أجاز المشرع الجزائري تفتيشها بموجب المادة 05 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال [174]

.

ويفترض أن لا يكون الأمر بالتفتيش أمرا عاما ، وإنما يكون الهدف منه محددا تحديدا دقيقا وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية ، بحيث لا يترك ذلك للسلطة التقديرية لرجل

---

[170] عبد الفتاح بيومى حجازى ، مبادئ الإجراءات الجنائية في جر ائم الكمبيوتروالإنترنت ، مرجع سابق ، ص 380 .

[171] لعوارم وهيبة ، المرجع السابق ، ص 345 .

[172] راجع نص المادة 05 من قانون 04/09 .

[173]تنص المادة 44 ق إ ج " لا يجوزلضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهرأنّهم ساهموا في الجناية أوأنّهم يحوزون أور اقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة ..."

[174] تنص المادة 05 من قانون 04/09 "... الدخول بغرض التفتيش و لو عن بعد إلى : أ- منظومة معلوماتية أوجزء منها وكذا المعطيات المعلوماتية المخزنة فيها . ب- منظومة تخزين معلوماتية ... "

الشرطة الذي سيقوم بتنفيذ الأمر ، وأن لا يكون الأمر بالتفتيش كأمر عام بالتفتيش لضبط الأشياء المتعلقة بالحياة الخاصة أو بالتعبير عن الرأي ، ومنها أجهزة الحاسب الآلي - التي تحتوي بيانات شخصية أو بيانات لا تتعلق بالجريمة – فهذه الأجهزة يجب أن تكون موصوفة في أمر التفتيش بصورة دقيقة .

و جاء تعديل قانون الإجراءات الجزائية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006 و تحديدا تعديل المادة 45 و الفقرة 03من المادة 47 و الفقرة 03 من المادة 64 ، أين أسقط المشرع بموجب هذه النصوص الضمانات عند إجراء التفتيش بمناسبة تحقيق في جريمة معلوماتية، بمعنى أنّ التفتيش و لو في غياب المشتبه فيه و في أيّ ساعة من اليوم ودون الحصول على موافقته [175].

إتضح موقف المشرع الجزائري من خلال القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، إذ نص صراحة على جواز تفتيش أنظمة الحاسب الآلي وذلك بموجب المادة 05منه " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية ، الدخول بغرض التفتيش ولو عن بعد منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها، و كذا منظومة تخزين معلوماتية ."

***- التفتيش عن بعد ،**

مما لاشك فيه أن الطبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش في الجرائم الإلكترونية ، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش، كما قد يكون الموقع الفعلي للبيانات والمعلومات ضمن الاختصاص القضائي لدولة أخرى، وهو ما يعقد ويصعب من عملية التفتيش وضبط الأدلة الجنائية الرقمية ، وعلى هذا الأساس يمكن التفرقة بين فرضيتين :

[175] سعيداني نعيم، المرجع السابق ، ص 145 ،148.

- حالة وجود جهاز متصل بجهاز المتهم داخل الدولة: تكمن المسألة في هذه الحالة في تجاوز الاختصاص المكاني للسلطة المختصة بالتفتيش، كما أنه يعتبر بمثابة العدوان على حقوق الأفراد وحرياتهم، وذلك عند قيام سلطة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة .

وبناء على هذا الاحتمال الذي يشكل عائقا أمام السلطات القائمة على التفتيش وضبط الأدلة الجنائية الرقمية ، عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش أنظمة الحاسب الآلي، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة، وهو ماذهب إليه المشرع الجزائري حيث نصت الفقرة الثانية من المادة 05 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة المختصة بذلك ...".

- وجود جهاز متصل بجهاز المتهم خارج الدولة : من المشاكل التي تواجه سلطات التحقيق في جمع الأدلة الإلكترونية قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية وذلك بغرض عرقلة التحقيق ومن ثم سير العدالة، ونتيجة لذلك أدخلت تعديلات على قانون الإجراءات الجنائية لتجيز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة ومن ذلك المشرع الفرنسي. أما بالنسبة للمشرع الجزائري فقد حلت هذه المشكلة وذلك بموجب القانون 09-04 وذلك من خلال تعاون السلطات الأجنبية وفقا لمبدأ المعاملة بالمثل في إطار اتفاقيات دولية بهذا الصدد[176] وهذا مانصت عليه المادة05فقرة 3 من القانون 09-04

ب-الشروط الشكلية

- وجود إذن مكتوب صادر عن الجهة القضائية المختصة : لم ينّص المشرع الجزائري على هذا الشرط ضمن القانون 04/09 غير أنّه تطبيقا لمعيار الخصوصية التي يحميها الدستور ،فإنّ

[176] بوبكر رشيدة ، المرجع السابق ، ص 402.

النظام المعلوماتي و ما يحويه من أسرار و خصوصيات الأشخاص تستوجب وجوب إذن من السلطة القضائية المختصة [177] وهذا ما نصت المادة 45 ق إ ج [178].

2-الخبرة القضائية

الخبرة هي إجراء يتعلق بموضوع يتطلب إلماماً بعلم أو فن معين لإمكان استخلاص الدليل منه ، لذلك فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منه الخبير رأيه .

وللمحكمة أثناء تحقيقها النهائي أن تنتدب الخبراء وذلك إذا ما عرضت أثناء المناقشة مسألة تحتاج لرأي فني أو تقني .

و يعتبر تقرير الخبير من الأدلة ، أما إجراء ندب الخبير فهو من إجراءات جمع الأدلة ، ولذلك إذا ما بوشر بمعرفة سلطة التحقيق تحركت به الدعوى العمومية باعتباره إجراء من إجراءات التحقيق .

والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره ، ولذلك فإن الخبير يأخذ حكم الشاهد ويجوز استدعاؤه لسماع شهادته ومناقشته في التقرير الذي أعده وتقدم به ، غير أن الخبير يختلف عن الشهود من حيث الوقائع التي يشهد بها ، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها أما الخبير فشهادته فنية أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة ويترتب على ذلك أنه لا يجوز سماع الخبير كشاهد إذا كان إجراء الخبرة قد وقع باطلا[179] .

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

والقاعدة أن المحكمة هي الخبير الأعلى ، ولذلك فتقارير الخبراء تخضع دائما لتقديرها ، فلها أن تطرحها كلية ولها أن تأخذ برأي خبير دون الآخر ، كما أن للمحكمة سلطة الجزم في المسائل التي تتسق ووقائع الدعوى حتى ولو كان تقرير الخبير لم يجزم فيها برأي ، وإذا اختلف خبيران في الرأي فليست المحكمة ملزمة بمواجهتهما وإنما تملك ترجيح أحدهما علي الآخر وفقا لاقتناعها وما تراه مؤيدا بوقائع

---

[177] سعيداني نعيم ، المرجع السابق ، ص 157 .

[178] راجع نص المادة 45 إجراءات جزائية .

[179] مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، الجزء الأول ، المرجع السابق ، ص 603 -605 .

الدعوى ، وهي في ذلك غير ملزمة ببيان أسباب الترجيح كما أنها غير ملزمة بمناقشة التقارير الأخرى طالما لم تر محلا ولم يطلب الخصوم منها شيئا من ذلك ، وللمحكمة السلطة التقديرية أيضا أن تأخذ ببعض ما ورد بتقرير الخبير وتطرح الجزء الآخر دون إبداء أسباب لذلك اللهم إلا في المسائل الفنية فلا يجوز تفنيدها إلا بأسانيد فنية .

وإذا كان لندب الخبراء أهمية في الجرائم التقليدية ، فإن أهميتها أكثر وضرورتها أشد في إجراءات جمع أدلة المكونات المعنوّية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات ، غير أن ذلك لا يعني عدم الاكتراث بمسألة تأهيل سلطات الملاحقة وتزويد أفرادها بالمعرفة العلمية والتقنية ليكونوا على دراية فيما يستلزم ندب الخبراء وفهم ما يقدمونه من آراء ، ولذلك نجد الكثير من الدول المتقدمة قد اهتمت بتدريب المحققين في الجرائم الإلكترونية ، كما دعا المجلس الأوروبي في إحدى توصياته سنة 1999 إلى ضرورة تدريب الشرطة وأجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات واستخدامها لتحقيق التوازن بين وسائل ارتكاب الجريمة وبين سبل مواجهتها ، وعقدت كذلك المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمحققي جرائم الحاسب الآلي.[180]

إهتم المشرع الجزائري بتنظيم الخبرة في المواد من 143إلى 156 من ق إ ج ، وإعتبرها من إجراءات التحقيق، حسب نص المادة 143 منه، وعملية ندب الخبراء غير محدّدة بنطاق موضوعي محدّد و إنّما مطلقة و من ثمة يستطيع قاضي التحقيق تحديد كافة المسائل التي يرى ضرورة عرضها على الخبير [181]، وقد نص على هذا الإجراء المشرع الجزائري في المادة 05 فقرة الأخيرة من قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها [182].

---

[180] لعوارم وهيبة ، المرجع السابق ، ص 351 .

[181] عمر أبو بكر يونس، المرجع السابق ، ص 892 .

[182] تنص المادة 05 فقرة أخيرة من قانون 04/09 "...يمكن السلطات المكلفة بالتفتيش تسخير كلّ شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنّها قصد مساعدتها و تزويدها بكلّ المعلومات الضرورية لإنجاز مهمتها".

كما قام بإنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و التي حدّدت مهمتها انجاز الخبرات القضائية التي تطلبها السلطة و الشرطة القضائية [183].

و قد صدر المرسوم الرئاسي 26/15 المؤرخ في 08 أكتوبر 2015 الذي يحدّد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها و التي تعدّ سلطة إدارية مستقلة لدى وزير العدل [184]و بعد انتهاء الخبير من أبحاثه و فحوصاته يعدّ تقريرا يضمنه النتائج المتوصل إليها و يتم إيداعه لدى الجهة الآمرة بالتحقيق.

4- ضبط الأشياء

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الجريمة ، وسائله متعددة منها التفتيش والمعاينة وتكليف الحائز للشيء بتقديمه للمحقق .

وإذا ما سفر التفتيش الذي يجريه مأمور الضبط عن آثار أو أشياء تفيد في كشف الجريمة أو تكون قد استعملت في ارتكابها ، وجب على مأمور الضبط القضائي ضبط هذه الأشياء ، ومن باب أولى لسلطة التحقيق أن تضبط جميع الأشياء المتعلقة بالجريمة ، ومن أجل ذلك ، أجاز المشرع التفتيش لتتمكن سلطة التحقيق من إجراء الضبط الذي يعد في هذه الحالة إجراء من إجراءات التحقيق .

ويمكن أن يكون موضوعا للضبط من قبل سلطة التحقيق جميع الأشياء التي تفيد في كشف الحقيقة المتعلقة بالجريمة ، ويجب أن تكون هذه الأشياء مادية ، فسلطة التحقيق لها ضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات لدى مكاتب البريد كافة والتلغراف ، كما يجوز لها أيضا مراقبة المحادثات التليفونية متى كان لذلك فائدة في ظهور الحقيقة ، وإذا كان القائم بالتحقيق أحد أعضاء النيابة العامة ، فيلزم للقيام بهذا الإجراء استصدار أذن من القاضي الجزئي ، وقياسا على ذلك يجوز لسلطة التحقيق أن تضبط أيضا لدى البنوك والمؤسسات المختلفة الأوراق والأشياء المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة ، وحظر المشرع على سلطة التحقيق أن تضبط لدى المدافع عن المتهم أو الخبير الاستشاري الأوراق والمستندات التي سلمه المتهم لهما لأداء المهمة التي عهدت إليهما بها ، وكذلك المراسلات المتبادلة بينهما في القضية .

---

[183] لعوارم وهيبة ، المرجع السابق ، ص 352 .

[184] بوزينة أمحمدي يآمنة ، المرجع السابق ، ص 78

أولا- ضبط المكونات المادية

الأصل في الضبط أنه يرد على الأشياء المادية التي تصلح لوضع اليد عليها ، ولهذا لا يثير ضبط المكونات المادية للحاسب الآلي وملحقاته أيه إشكالية باعتبارها أشياء مادية ، وبالتالي يجوز ضبط الأسلاك ومفاتيح التشغيل وحدة الإدخال والمودم ووحدة الذاكرة ووحدة التحكم ، وبما في ذلك مخرجات الحاسوب الموجودة في صورة مخرجات ورقية أو وسائط وأوعية التخزين المادية كالأقراص والأشرطة المغناطيسية ، حيث يتم ضبط الأداة أو الوسيط الذي يتم فيه التخزين .

ثانيا- ضبط المكونات المعنوية

يستخلص من صياغة التشريعات الجنائية لمفهوم الضبط أنه يقتصر على الأشياء المادية و كان ذلك مثار الجدل حول ما إذا كان يجوز ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج ، وما تحتويه صناديق البريد الإلكترونية من رسائل وصور وبيانات ؟

الجدل لا يزال محتدما إلى يومنا هذا بين المؤيد والرافض لإمكانية ضبط البيانات المعالجة إلكترونيا منفصلة عن دعامتها المادية ، كتلك التي يتم عرضها على شاشة الحاسب الآلي ، فذهب اتجاه إلى أنه من غير الممكن ضبط البيانات إلكترونيا لانتفاء الطابع المادي لهده البيانات ، ذلك أن بيانات الحاسب الآلي ليست كمثل الأشياء المحسوسة ، وبالتالي لا تصلح لأن يرد عليها الضبط ، وأخذت بعض تشريعات الدول بهذا الاتجاه منه كألمانيا ورومانيا واليابان وجانب من الفقه الفرنسي ؛ وذهب اتجاه ثان إلى أنه وإن كانت الغاية من التفتيش هو ضبط الأدلة المادية ، إلا أن هذا المفهوم يمكن أن يمتد ليشمل البيانات المعالجة الإلكترونية مجردة . ويجد هذا الاتجاه تجسيده التشريعي في قوانين بعض الدول مثل كندا واليونان والولايات المتحدة الأمريكية التي قضت بإعطاء سلطات التحقيق مكنة القيام بأي شيء يكون ضروريا لجمع الأدلة وحمايتها ، بما في ذلك المكونات المعنوية للحاسب الآلي ، وإن كان لا يتصور ضبطها باعتبارها أشياء غير محسوسة ، فإنه من الممكن ضبطها إذا أصبح لها كيان مادي ، كضبط القطعة الصلبة كأداة تخزينية للدليل و المعلومات والبيانات المراد ضبطها على ورق أو تسجيلها في أشرطة أو أقراص أو نسخها في ملفات ، إذ في هذه الحالة تتحول المكونات المعنوية للحاسب الآلي إلى أشياء مرئية ومقروءة وتكتسب كيانا ماديا يمكن بواسطته ضبطها ونقلها من مكان لأخر ،

والقول نفسه يطبق بشان الرسائل الالكترونية ، فللمحقق أن يضبط الرسائل المخزنة بالبريد الالكتروني عن طريق طباعة الرسالة التي يريد ضبطها ، أو تسجيلها في ملف أو قرص .

وهناك اتجاه ثالث وأخير يرى أنصاره ، بأنه لا فائدة من تطبيق نصوص الإجراءات الحالية المتعلقة بالضبط على البيانات المعالجة إليكترونيا بصورتها المجردة عن دعامتها المادية ، بل لابد من تدخل المشرّع لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط ، ليشمل

البيانات المعالجة بصورتها غير الملموسة [185].

ثالثا : الأمر بتقديم الأشياء المراد ضبطها أو الاطلاع عليها

لسلطة التحقيق أن تأمر الحائز لشيء تري ضبطه أو الاطلاع عليه بتقديمه ، والفرض هنا أن الحائز قد يكون موظَّفَ مكتب البريد أو التلغراف ، كما قد يكون شخصاً آخر، ويستوي أن يكون فردا عاديا أو موظفا حكوميا يحوز شيئا متعلقا بالجريمة أو يفيد في كشفها بمناسبة أو بسبب وظيفته ، والمفروض أن الشيء موضوع الحيازة لا يكوّن جريمة في حد ذاته وإلا جاز تفتيشه ، وقد خول القانون لسلطة التحقيق هذا الحق بدلا من أن تلجأ إلى إجراء تفتيش منزل غير المتهم بعد الحصول على إذن القاضي الجزئي إذا كان التحقيق تباشره النيابة العامة .

كما راعى المشرع أيضاً أنه قد لا يمكن ضبط هذه الأشياء بسبب إخفاء الحائز للأوراق أو الأشياء في مكان ما لم يتم التوصل إلى اكتشافه ، فجعل المشرع من الامتناع عن تقديم الأشياء التي في حيازة الشخص الذي يؤمر بتقديمها من قبل سلطة التحقيق جريمة معاقبا عليها في قانون العقوبات ، اللهم إذا توافر بالنسبة للحائز حالة من الحالات التي يخوله القانون فيها الامتناع عن أداء الشهادة .

وبالنسبة للمشرع الجزائري فإنه وطبقا لأحكام **المادة 6** من القانون **09-04** على أنه عندما يتوصل المحققون أثناء إجراء التفتيش في منظومة معلوماتية إلى وجود معطيات أو بيانات من شأنها الإفادة في التحقيق وضبط الأدلة للكشف عن الجريمة الإلكترونية ، ومرتكبيها فأنه يمكن لهم حجز المنظومة المعلوماتية برمتها إذا كان ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات وذلك بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق أو ضبطها على الشاشة وذلك

[185] هشام محمد فريد رستم ، المرجع سابق ، ص96 .

لتسهيل قراءتها والتعامل معها وهذا ما أشارت إليه المادة 6 من خلال عبارة " دعامة تخزين إلكترونية تكون قابلة للحجز"، والملاحظ أن المشرع الجزائري إستعمل مصطلح " الحجز" وليس مصطلح "الضبط " ذلك أن مصطلح الحجز يتلائم مع الأشياء غير المادية.

إن عملية ضبط البيانات المعالجة إلكترونيا تواجهها عدة صعوبات منها حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها، و وجود بيانات في شبكات أو أجهزة تابعة لدولة أجنبية كما يشمل التفتيش والضبط أحيانا إعتداء على حقوق الغير، أو على حرمة حياتهم الخاصة، فيجب إتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات[186].

المبحث الثاني

الإثبات الجنائي الإلكتروني

الإثبات في المواد الجنائية يخضع لقواعد تختلف عن تلك التي تحكم الإثبات في المواد المدنية ، وذلك لاعتبارات قد ترجع إلى اختلاف موضوع الإثبات بين تلك المواد ومنها ما يرجع إلى أهمية الدعوى الجنائية ، وأن القواعد التي تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة جريمة تمثل اعتداء على الجماعة وتهم المجتمع بأسره .

ومن القواعد التي تحكم الإثبات في المسائل الجنائية ثلاث : أولها حرية القاضي في تكوين عقيدته ، بمعنى أن له أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة والكشف عنها دون أن يتقيد في ذلك بإتباع وسائل معينة للكشف عن الحقيقة ،

كما أن له مطلق الحرية في تقدير أدلة الدعوى ، فله أن يأخذ بها وله أن يطرحها ، كل ذلك بناء على تقييمه لها وقناعته بما ينتهي إليه من مجموع ما طرح من أدلة في الجلسة ؛ وأن يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته مما يطرح أمامه على بساط البحث في الجلسة دون إلزام عليه بالتقيد بطريق معين من طرق الإثبات ، إلا إذا أوجب القانون عليه ذلك ، أو حظر عليه سلوك طريق معين في الإثبات يستمد قناعته من أي ورقة سواء كانت رسمية أو عرفية يستخلص منها ما يطمئن إليه ضميره ووجدانه ويطرح ما لا يطمئن إليه ، شأنه في ذلك شأن سائر الأدلة الأخرى التي قد تطرح أمامه ؛

[186] لعوارم وهيبة ، المرجع السابق ، ص 359.

وثاني القواعد التي تحكم لإثبات في المسائل الجنائية الدور الإيجابي للقاضي الجنائي في البحث عن الحقيقة فإنه ليس مجرد موازنة للأدلة المثبتة للإدانة أو البراءة ، وإنما عليه التحري عن الحقيقة والكشف عنها ، وهو في ذلك يختلف عن القاضي المدني الذي يكون دوره في الدعوى المدنية المنظورة أمامه سلبيا ومقتصرا على الموازنة بين أدلة الخصوم؛ وآخر القواعد التي تحكم الإثبات في المسائل الجنائية قاعدة عبء الإثبات في المواد الجنائية يقع على سلطة الإدعاء العام من منطلق أن الأصل في الإنسان البراءة ، وعلى من يدعي عكس ذلك إثباته .

ولا شك في أن مجموع هذه القواعد لا اختلاف فيها بين الجرائم التقليدية والجرائم الإلكترونية ، إلا أن الطابع الخاص الذي تتميز به الجرائم الإلكترونية أن محل أو موضوع بعضها يكون غير مادي ، إضافة إلى أن إثبات هذه الجرائم يحيط به كثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم بحسب أنها جرائم فنية تتطلب تقنية معينة في مجال الحاسبات الآلية والإنترنت ، وهي على الرغم من أنها – غالبا – ما تكون جريمة هادئة لا عنف فيها ولا تترك أشياء مادية تدرك بالحواس ، لكونها عبارة عن أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات ، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[187] .

وإلى جانب إمكانية ارتكابها عبر الوطنية باستخدام شبكات الاتصال ، فإن المجني عليه الذي عادة ما يكون مؤسسة مالية أو مشروعاً صناعياً ضخماً يحاول - في الغالب - كتم حصول الجريمة والإحجام عن البلاغ عنها أو مساعدة السلطات المختصة في إثباتها والكشف عنها حتى لا يتم تقليدها من قبل الآخرين ، وخشية من أن يترتب على شيوع العلم بوقوعها إساءة واهتزاز لسمعته وثقة المساهمين والعملاء .

دليل الإثبات هو " الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه "[188] .

---

[187] محمد على العريان ، المرجع السابق، ص 53و54 .

[188] مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، الجزء الثاني ، منشورات المكتبة الوطنية ، الطبعة الثانية ، بنغازي ،2000 ، ص 176 .

وقد تعارف الفقه والقضاء على الأدلة التي يمكن للقاضي الاستناد إليها دون أن يحول ذلك عن الاستناد إلى أدلة أخرى ، وهذه الأدلة هي الاعتراف والمعاينة والمحررات وشهادة الشهود والخبرة والقرائن ، غير أن هذه الأدلة تبدو في الأعم قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية الذي يتوسل بنبضات اليكترونية غير مرئية العبث بالدليل أو محوه بالكامل في وقت قصير جدا ، يتعذر معه كشفها إلا بطريق الصدفة .

المطلب الأوّل

مفـهوم الدلـــيل الإلكتروني

الكتابة لا تعدو كونها رموزاً تعبر عن الفكر و القول ، و قد ظلت العلاقة بين الكتابة و الدعامة الورقية المدونة عليها علاقة وثيقة لفترة طويلة من الزمن ، حيث كان يسود الاعتقاد بأن الكتابة تساوي الورق ، كل ذلك علي الرغم من أنه لا في اللغة و لا في القانون ما يتطلب أن تكون الكتابة علي الورق فقط ، بل من الجائز أن تكون علي الورق أو الجلد أو القماش أو الحجر أو الخشب أو علي دعامة أخري مادية كانت أو رقمية .

والدليل الكتابي هو المحرر ، ويمكن تعريفه بأنه " مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الأفكار والمعاني "[189] ،

والمحررات رسمية كانت أو عرفية التي تثبت وقوع الجريمة سواء أكانت هذه المحررات موضوع السلوك الإجرامي ذاته كما في جريمة التزوير أو التهديد كتابة ، أم كانت تتضمن دليلا على ارتكاب الجريمة ، فهذه بطبيعتها تخضع لمطلق تقدير المحكمة التي لها أن تأخذ بها أو تطرحها دون أن تكون ملزمة بتسبيب طرحها لها[190].

وهناك ما يسمي بالدليل الرقمي ، و هو ما يعرف بأنه " الدليل الذي يجد له أساساً في العالم الافتراضي إلي الجريمة "[191] ، وعرف أيضا بأنه " الدليل المأخوذ من أجهزة الحاسب الآلي في شكل

---

[189] محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، ج1 ، ط 1 ، دار النهضة العربية ، القاهرة، 1988 ، ص483 .

[190] مأمون محمد سلامة ، الجزء الثاني ، مرجع سابق ، ص 193 .

[191] عمر محمد أبوبكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، دار النهضة العربية ، القاهرة ، 2004 ، ص 969 .

مجالات و نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجية خاصة ، [192] .

الفرع الأول

تعريف الدليل الإلكتروني

تعددّت التعريفات التي قيلت بخصوص الدليل الرقمي و تباينت بين التوسع و التضييق و يرجع ذلك للبيئة التي ينشأ فيها الدليل الرقمي فهناك من يعرّفه من منظور تقني بحت ، وهناك من يراه من جانب قانوني مرّكزا على اجراءات استخلاصه و مدى اعتماده كوسيلة اثبات[193] .

إذا يمكن تعريفه بأنّه" معلومات مخزنة في أجهزة الحاسوب و ملحقاته من دسكات و أقراص مرنة و غيرها من وسائل تقنية المعلومات كالــطابعات و الفاكسات أو متنقلة عبر شــبكات الإتصال و التي يتم تجــميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة بهدف اثبات وقوع الجريمة و نسبتها إلى مرتكبها"[194].

كما عرفته مجموعة العمل العلمية للأدلة الرقمية The SienticWorking Group on Digital "معلومات ذات قيمة إثباتية مخزنة أو منقولة في شكل ثنائي"[195].

وقد يتخذ الدليل الرقمي أحد الصور التالية : الصورة الرقمية ، التسجيلات الصوتية ، النصوص المكتوبة، و يشمل الرسائل الإلكترونية و البيانات المسجلة بأجهزة الحاسب الآلي [196].

الفرع الثاني

خصائص الدليل الإلكتروني

يتميّز الدليل الرقمي بعدّة خصائص منها :

---

[192] ممدوح عبد المجيد عبد المطلب ، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم علي الكمبيوتر، بحث منشورعلي الإنترنت ، الموقع الإلكتروني Dpolice.Maktoobblog .

[193] نورالهدى محمودي ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ، مجلة الباحث للدراسات الأكاديمية ، المجلد الأول ، العدد الحادي عشر، جامعة الحاج لخضرباتنة ، الجزائر، جوان 2017، ص 912 .

[194] عائشة بن قارة ، المرجع السابق ، ص 61 .

[195] سعيداني نعيم ، المرجع السابق ، ص 121 .

[196] المرجع نفسه ، ص 127، 128 .

1-دليل علمي

فهو منطقه الذي يجب ألا يخرج عليه إذ يجب عدم تعارضه مع القواعد العلمية السليمة و هي ذات الطبيعة التي يتوافر عليها الدليل الرقمي [197]،و ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القانون المقارن " أنّ القانون مسعاه العدالة ، أمّا العلم مسعاه الحقيقة " [198].

2- دليل تقني

يحتاج الدليل الرقمي إلى مجال تقني يتعامل معه كونه من طبيعة تقنية المعلومات [199]و مستوحى من البيئة الرقمية أو التقنية و تتمثل هذه الأخيرة في إطار الجرائم الإلكترونية في العالم الإفتراضي وتنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها و حجمها و مكان تواجدها غير المحدد ، فالدليل الرقمي ذو طبيعة ديناميكية فائقة السرعة و ينتقل من مكان إلى آخر عبر شبكات الإتصال[200] .

3-دليل يصعب التخلص منه

تعدّ من أهم خصائص الدليل الإلكتروني ، إذ أنّها قابلة للإسترجاع بعد محوها وإصلاحها بعد اتلافها و إظهارها بعد إخفائها ممّا يؤدي إلى صعوبة الخلاص منه [201] ، إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تمّ إلغائها أو إزالتها من الحاسوب [202].

4-دليل قابل للنسخ

إذ يمكن استخراج نسخ من الأدّلة الجنائية الرقمية مطابقة للأصل و لها نفس القيمة العلمية ممّا يشكلّ ضمانة هامة للحفاظ على الدليل من الفقدان و الإتلاف أو التغيير [203] .

*توجد خصائص أخرى للدليل الرقمي من بينها أنّه متنوع و متطور و يمتاز بسعة تخزينية عالية ، وهذه الخصائص هي التي تطرح إشكالية قبول الدليل الرقمي في الإثبات .

---

[197] عمر محمد أبو بكر بن يونس ، المرجع السابق ، ص 977 .

[198] عائشة بن قارة مصطفى، المرجع السابق ، ص 62 .

[199] عمر محمد أبو بكر يونس ، المرجع السابق ، ص 977

[200] عائشة بن قارة مصطفى ، المرجع السابق ، ص 62 .

[201] المرجع نفسه ، ص 63 .

[202] عمر محمد أبو بكر يونس ،المرجع السابق ، ص 983 .

[203] عائشة بن قارة مصطفى ، المرجع السابق ، ص 64.

صعوبات جمع الأدلة :

على الرغم من اتجاه العديد من التشريعات الجنائية إلى وضع قواعد موضوعية لمواجهة الجرائم الإلكترونية وإجراء تعديلات في القواعد الإجرائية بتطوير أساليب كشف وضبط هذه الجرائم بما يحقق متطلبات العدالة الجنائية ، وحتى لا تكون القواعد الإجرائية عائقا أمام سلطات التحقيق في كشف وملاحقة مرتكبي الجرائم في مجال تقنية المعلومات والاتصالات ، فإن التحقيق في الجرائم الإلكترونية يظل يواجه العديد من التحديات والصعوبات مثل :

أولا. صعوبات تتعلق بالحصول على الدليل

إن إقامة الدليل على وقوع الجريمة الإلكترونية ونسبتها إلى متهم معين تكتنفه إشكاليات وصعوبات لا تتعلق فقط بتقديم الأدلة غير المادية ، ومدى حجيتها أمام القضاء ، وهى من المسائل المهمة في مجال تطوير الإثبات الجنائي في هذه الجرائم ، وإنما تتعلق أيضا بصعوبات الحصول على هذا النوع من الأدلة ، وهو ما نعنيه ونقتصر الإشارة إلي أهم هذه الصعوبات :

1. إخفاء الدليل

نتيجة ضعف الأنظمة الرقابية يتمكن مرتكبو الجرائم الإلكترونية من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته ، أو دس برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل ، ومن ثم إخفاء ما قاموا به أو محو الدليل عليه ، بحيث يتعذر إعادة عرض أعمال التسلل والدخول ، وهكذا يستطيع الجناة في الجرائم الإلكترونية إخفاء جرائمهم وطمس آثارها في وقت قياسي من القصر وقبل أن تصل إليه سلطة التحقيق ، الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل ، ومن أمثلة سهولة محو الدليل المعلوماتي في وقت قصير، انه أثناء إجراء المحاكمة للمسؤولين عن أحد المشروعات بألمانيا طلبت سلطات التحقيق المساعدة القضائية من السلطات السويسرية من أجل ضبط البيانات التي توجد في النظام ألمعلوماتي لإحدى الشركات السويسرية ، وأثناء سير الإجراءات تمكن الجناة من محو البيانات التي كانت من الممكن أن تستخدم كدليل ، ولكن لحسن الحظ بعد ضبط الدعامات والأقراص الصلبة وأسطوانات الليزر، تمكن الخبراء بطرق فنية من استعادة البيانات التي كانت مسجلة عليها.

2- غياب الدليل ضد متهم معين

تختلف الجريمة الإلكترونية عن الجريمة التقليدية ، بأن الجريمة الأولى لا تحتاج لارتكابها أي من أنواع العنف إلا فيما ندر ، وإنما هي معالجة بواسطة إدخال بيانات معلومات خاطئة أو محظورة ضمن البرامج ، أو تحريف أو تعديل البيانات والمعلومات المخزنة أصلا في الحاسب الآلي ، أو إرسال برامج تخريبية أو التجسس على البيانات والمعلومات المخزنة ونسخها ... الخ ، وإذا ما صادف واكتشفت هذه الأفعال وجمعت الأدلة على وقوعها ، فإن هذه الأدلة قد لا تفصح عن صلة شخص معين بالجريمة المرتكبة ، نظرا لأن معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها ، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدرجة بالأنظمة ، وتعمد الجناة إلى إخفاء هويتهم ، وخير مثال على الصعوبات التي تشكلها ضخامة كم البيانات والمعلومات وتأثيرها السلبي على جمع الأدلة بشان الجريمة المعلوماتية وملاحقة المجرمين الواقعة التي شاهدتها ألمانيا الاتحادية عام 1971ف حيث اكتشفت شركة طلبيات بريدية (Order –fimmail) سرقة أشرطة ممغنطة تحتوي على (300,000) عنوانا لعملائها واستصدرت من المحكمة أمرا يسمى وقف الإعمال ، وذلك باستعادة كل هذه العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من الذين ارتكبوا السرقة ، وتنفيذا لذلك سمحت الشركة المنافسة لمساعد مأمور التنفيذ ، أن يدخل مقر الحاسب الآلي الخاص بها ، وذلك للحصول على تلك العناوين ، ووجد نفسه وسط كم هائل من الأشرطة والأقراص الممغنطة التي لا يدري عنها شيئا ، ولا يمكن فحص محتوياتها أو لديه القدرة على ذلك فغادر مقر الشركة دون أية معلومات ، إلا أن الشركة المنافسة قامت من تلقاء نفسها بعد أيام ، بتسليم بيانات العناوين إلى الشركة المعتدى عليها وإن كان ذلك لا يمنع من نسخ هذه الشرائط قبل تسليمها ، الأمر الذي يفرغ أمر المحكمة من مضمونه[204] .

3- إعاقة الوصول إلى الدليل

يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمته وضبط أدلتها باستخدام تقنيات التشفير أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام ، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها ، وقد أثبتت التحقيقات في بعض الجرائم الإلكترونية بألمانيا وجود صعوبات تواجه البعض من هذه التحقيقات

[204] هشام محمد فريد رستم ، المرجع السابق ، ص19 .

نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم ، ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير، كوسيلة لمنع ضبطه والإيقاع به ، واقعة حدثت في الولايات المتحدة عام 1996 ، إذ كان المشتبه به مشغلا للوحة إعلانات bbs ، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الالكترونية ، حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به ، فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب ، وقاموا بكتابة برنامج يحاول تشغيل النسخة الاحتياطية ، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهوله إلى أسماء المستفيدين وأرقامهم ، ولكن لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به ، خاصة وأنها كانت مشفرة ، ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة ، ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها ، ولكن التشفير حال دون ذلك .

وللوصول إلى كلمة المرور قام المحققون بإنشاء رقمين جديدين من أرقام المستفيدين ، لهم أسماء مختلفة ، ولكن لهم نفس كلمة المرور، وبهذه الطريقة وبتتبع كلمتي المرور المتشابهتين أمكن العثور على مكان وجود كلمات المرور على القرص الصلب ، ووضع المحققون يدهم على كلمة المرور الخاصة بالمتهم في ملف المستفيدين ، ثم قاموا بإحلال كلمة المرور السابق استخدامها مع المستفيدين الوهميين مكان كلمة المرور الخاصة بالمشغل (وهي مشفرة كما هي) ، وبذلك أمكن الدخول إلى الحاسب باستخدام اسم المشغل مع كلمة المرور الخاصة بالمستفيد الوهمي[205] .

ثانيا .صعوبات تتعلق بالجانب الفني

من المسائل التي تعوق عمليات البحث والتحقيق في الجرائم الإلكترونية نقص في المعرفة التقنية الحديثة والمتجددة لدى القائمين بالبحث والتحقيق في هذه الجرائم ، مما يجعل منهم غير قادرين على أداء واجبهم على الوجه المطلوب ، إذ إن نقص الخبرة والكفاءة ، سواء في أجهزة الشرطة أو الادعاء يعد من الأسباب الرئيسية في الإخفاق في كشف الجرائم الإلكترونية وجمع أدلتها ، ويظهر ذلك بشكل واضح في الدول التي لا تزال تتعامل مع هذه الجرائم بإجراءات البحث والتحقيق التقليدية وتفتقر سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها ، وبديهيا

[205] حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2000 ف، ص 233_234

أنه في حالة عدم توافر التأهيل والخبرة وشُحِّ الإمكانيات التقنية على وجه الخصوص ، فلا يمكن أن نتصور أي وجه للتعامل مع هذه الجرائم ، وبالتالي ستكون النتائج سلبية لا محالة ، ما لم تضع الدول برنامج تدريب وتأهيل لرجال الشرطة على أساليب الوقاية من جرائم الحاسب الآلي ووضع التدابير المانعة لوقوعها، والقيام بالتحري عما ارتكب منها وكشفها ، وأيضا كيفية التعامل مع الأدلة وضبطها ، والاستعانة بذوي التخصصات الدقيقة المتعمقة في أنظمة الحاسب الآلي والإنترنت وشبكات الاتصال الأخرى .

ثالثا : إجراءات ضبط الدليل الرقمي

الضبط هو النتيجة الطبيعية التي ينتهي إليها التفتيش و هي ضبط الأدّلة التي يتم الحصول عليها أثناء إجراءات التفتيش، فالضبط هو غاية التفتيش و الأثر المباشر الذي يسفر عنه[206]،و يختلف الضبط في الجريمة الإلكترونية عن غيرها من الجرائم التقليدية كون أنّهذه الأخيرة ترد على أشياء مادية ملموسة في حين أنّ الدليل في الجريمة الإلكترونية يرد على أشياء ذات طبيعة معنوية و هي البيانات ، المراسلات و الإتصالات الإلكترونية [207]فالبيئة الإفتراضية لا تنتج سكينا أو سلاحا ناريا و إنّما تنتج نبضات رقمية تشكلّ قيمة وجوهر الدليل الرقمي ... هذا ما آثار جدلا فقهيا حول إمكانية ضبط الأدلة الرقمية غير أنّ ضبط الأدلة المادية للحاسوب لا يثير أيّ مشاكل في الفقه المقارن[208].

و بما أنّ التفتيش يشمل المكونات المعنوية للحاسوب و بالتالي يجب ضبط الأدلة التي تمّ الوصول إليها ، و تدّخل المشرع الجزائري في هذا الإطار بموجب نص المادة 06 التي جاءت تحت عنوان "حجز المعطيات المعلوماتي"من قانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا

---

[206] المرجع نفسه ، ص 114 .

[207] عائشة بن قارة مصطفى ، المرجع السابق ، ص 114 .

[208] سعيداني نعيم ، المرجع السابق ، ص 158 ، 159

الإعلام و مكافحتها [209]، ممّا يفيد جواز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتواها [210] .

و قدبيّن المشرع الجزائري طريقة ضبط الأدلة الرقمية التي قد تتخذ إحدى الصورتين:

الصورة الأولى :عن طريق نسخ المعطيات محل البحث على دعامة تخزين الكترونية على أن تكون هذه المعطيات مهيأة بشكل يجعلها قابلة لحجزها و وضعها في أحراز حسبما هو مقرر في قواعد التحريز المنصوص عليها في قانون الإجراءات الجزائية .[211]

الصورة الثانية:تتمثل في الإستعانة بالتقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ، و تتبع هذه الطريقة في حالة استحالة ضبط هذه المعطيات وفق الصورة الأولى لأسباب تقنية [212].

بعد ضبط البيانات يتم تحريزها و تأمينها فنيّا لتقديمها ضمن الملف و يتم ذلك وفق الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث و التغيير [213]،و هذا ما أشارت إليه المادة 06 فقرة 03من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، ومن هذه الإجراءات على سبيل المثال[214]:

- أخذ نسخة احتياطية عن المعطيات و العمل عليها لضمان عدم المساس بالدليل الأصلي .

---

[209]تنص المادة 06 من قانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و مكافحتها التي جاءت تحت عنوان " حجز المعطيات المعلوماتي " أنه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنّه ليس من الضروري حجز كلّ المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

يجب في كلّ الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية . غير أنّه لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات ، قصد جعلها قابلة للإستغلال أغراض التحقيق ، شرط أنّ لا يؤدي ذلك إلى المساس بمحتوى المعطيات " .

[210] لعوارم وهيبة ، المرجع السابق،ص 350.

[211] سعيداني نعيم ، المرجع السابق ، ص 163 .

[212]المرجع نفسه ، ص 163 .

[213] نور الهدى محمودي آمنة، المرجع السابق ، ص 932 .

[214] في هذا الإطار نجد الهيأة الدولية لدليل الحاسب الآلي(IOCE)وضعت عدّة ضوابط لعلمية ضبط الدليل الرقمي منها ألا تكون الإجراءات المتخذة في تحريز الدليل الرقمي سببا في تغيي طبيعة هذا الدليل و ان تكون جميع الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها أو نقلها موثقة توثيقا كاملا مع المحافظة عليها و توفيها للمراجعة ، وهو الأمر الذي أوردته كذلك الفقرة03من المادة19من الإتفاقية الأوربية للجريمة المعلوماتية. سعيداني نعيم ،المرجع السابق ، ص 164

- عدم تنفيذ برامج على الحاسوب مسرح الجريمة لتفادي اتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات و عدم السماح للمشتبه به بالتعامل مع الحاسوب .
- ضبط الدعائم الأصلية للمعلومات و عدم الإقتصار على ضبط نسخها .
- عدم ثني القرص لأنّ ذلك يؤدي إلى تلفه و فقدانه للمعلومات المسجلة عليه .
- عدم تعريض الأقراص و الأشرطة الممغنطة لدرجات حرارة عالية و لا إلى الرطوبة [215].

* بعد انتهاء اجراءات ضبط الدليل الرقمي يتمّ تقديمه ضمن ملف القضية بغرض إسناد الفعل المجرم إلى المتهم أو إثبات براءة هذا الأخير ، ممّا يثير اشكالية حجية الدليل الرقمي كون طبيعته تختلف عن الدليل المادي الملموس المعتاد وهذا ما سنتطرق له .

المطلب الثاني

حجية الدليل الإلكتروني

في نطاق جريمة تبييض الأموال عبر الوسائط الإلكترونية يكون الدليل الرقمي هو الأوفر ، و وجود دليل يثبت وقوع الجريمة و نسبها إلى شخص معيّن غير كاف لإدانة المشتبه فيه و مرّد ذلك أنّه يلزم أن تكون الأدلة ذات قيمة قانونية [216]، وقد مكنّ المشرع الجزائري القاضي الجنائي بسلطة تقديرية واسعة في مدى قبول أو استبعاد الدليل تحت قيود و ضوابط للوصول إلى الحقيقة ، لذا تطرقنا في الفرع الأول حجية القبول ، و في الفرع الثاني حجية التقدير .

الفرع الأول

حجية قبول الدليل الإلكتروني

---

[215] عائشة بن قارة ، المرجع السابق ، ص 117 وسعيداني نعيم ، المرجع السابق - ص 163 ،164 .

[216] سعيداني نعيم ، المرجع السابق ، ص 207 .

يتعيّن على القاضي لقبول الأدلة الرقمية كأساس للحقيقة توافر بعض الشروط من حيث يقينية هذه الأدلة و مشروعية الدليل الرقمي .

1- وجوب يقينية الأدلة الرقمية و غير قابيتها للشك

يتحقق اليقين للأدلة الرقمية بإخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمكنّ من فحصه للتأكدّ من سلامته و كذا صحة الإجراءات المتبعة في الحصول عليه من أجل تفادي تلك العيوب التي قد تشوبه [217] و تتمثل وسائل تقييم الدليل الرقمي فيمايلي :

أ-تقييم الدليل الرقمي للتحقق من سلامته من العبث : و يتمّ ذلك بأحد الطرق التالية:

-فكرة التحليل التناظري الرقمي : و يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية بالإستعانة بعلوم الكمبيوتر التي تساعد على تقديم المعلومات الفنية التي تساهم في فهم مضمون و كينونة الدليل الرقمي ، و يستعان بهذه الطريقة للكشف عن وجود تلاعب في مضمون الدليل الرقمي من عدمه[218].

-استخدام عمليات حسابية خاصة تسمى بالخوارزميات :وذلك في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة العبث بها.

-استعمال الدليل المحايد:وهذا النوع من الأدّلة مخزن في البيئة الإفتراضية و لا علاقة له بالجريمة لكنّ يساعد في التأكد من سلامة الدليل الرقمي المقدم

- الخبرة التقنية : فالقاضي الجزائي يمكن له أن يستعين في هذه المسائل بوسائل الخبرة للبحث في مصداقيته في مجال المعالجة الآلية للمعطيات و تحقيق اليقينية [219].

ب- تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه

سبق و أن رأينا أنّ هناك شروط موضوعية و شكلية يجب توافرها أثناء مباشرة أحد إجراءات جمع الأدلة،وإن كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة لكنّها محتملة الوقوع ، فالدليل الرقمي من الممكن أن يتم العبث به للخروج به على نحو يخالف الحقيقة و ليس في إمكان أيّ

---

[217] سعيداني نعيم ، المرجع السابق ، ص 216 ،217 .

[218] المرجع نفسه ، ص217 .

[219] المرجع نفسه ، ص 217 .

كان إدراك ذلك باستثناء ذوي الإختصاص فيظهر و كأنّه نسخة أصلية في تعبيرها عن الحقيقة [220]، و يتم التأكد من سلامة الإجراءات من حيث انتاجها لدليل تتوافر فيه المصداقية ، وفق مجموعة من الخطوات أهمها:

- اخضاع الآداة المستخدمة لعدّة تجارب للتأكد من دقتها في إعطاء النتائج .
- الإعتماد على الآدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل [221].

2 -مشروعية الدليل الرقمي

يكون الدليل الرقمي مشروعا إذا تمّ الحصول عليه احتراما للأحكام الإجرائية الشكلية و الموضوعية و إذا تمّ مخالفتها فإنّ الدليل لا يعتدّ عليه و لايستند القاضي إليه في تسبيب حكمه ، و الخطوة الأولى التي يتخذها القاضي هو التأكد من مراعاة الدليل الجنائي لقاعدة مشروعية الحصول عليه وهو ما يقتضي التطرق إلى مشروعية وجود الدليل الرقمي و مشروعية الحصول عليه [222]:

أ- مشروعية وجود الدليل الرقمي

يقصد بمشروعية الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الإستناد إليه في تكوين قناعته تبعا لنظام الإثبات السائد في الدولة ، إذ تختلف النظم القانونية في موقفها من حيث الأدلة[223]، و المشرع الجزائري بدوره لم يضع نصوصا خاصة تحظر على القاضي قبول أو عدم قبول أيّة دليل بما في ذلك الدليل الرقمي لاستناده على مبدأ حرية الإثبات الجزائي الذي يعتبر تجسيدا لمبدأ نظام الإثبات الحرّ الذي لا يثر إشكالية مشروعية الدليل الرقمي من حيث الوجود كون المشرع لم يحصر الأدلة الجنائية ، فالأساس هو حرية القاضي في قبول أو استبعاد أيّ دليل وفقا لقناعته[224]،

و لم يتضمن قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها أيّة أوضاع خاصة ، و ترك الأمر للقواعد العامة التي تفيد

---

[220] لعوارم وهيبة،المرجع السابق، ص 376.

[221] سعيداني نعيم ، المرجع السابق ، ص 218 .

[222] لعوارم وهيبة، المرجع السابق ، ص 371 .

[223] سعيداني نعيم ، المرجع السابق ،ص 208 .

[224] لعورام وهيبة ، المرجع السابق ، ص 371 .

أنّ الأصل في الأدّلة مشروعية وجودها فالدليل الرقمي مشروعا من حيث الوجود وفقا لمبدأ الشرعية الإجرائية ، و لا يأخذ القاضي إلاّ بالدليل الذي تمّ الحصول عليه وفقا لطرق مشروعة [225].

2- مشروعية الحصول على الدليل الرقمي

الدليل الجزائي بما يتضمنّه من أدّلة مستخرجة من وسائل إلكترونية لا يكون مشروعا إلاّ إذا تمّ الحصول عليه و تقديمه للقضاء بالطرق التي رسمها القانون ، فإذا تمّ الحصول على الدليل خارج الأحكام القانونية لا يعتد بقيمته مهما كانت دلالته الحقيقية و ذلك لعدم مشروعيته[226]، فإذا خالفت إجراءات جمع الدليل القواعد الإجرائية التي تنّظم كيفية الحصول عليه فإنّ الإجراءات تكون باطلة و بالتبعية بطلان الدليل المستمد منها ،و يصبح الدليل غير صالح للإعتماد عليه في الإدانة في المواد الجنائية [227]، و القاعدة أنّ الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة وهو الرأي الذي تبنّاه المشرع الجزائري في نص المادة 191 من ق إج ج [228].

أمّا بالنسبة لدليل البراءة فقد ثار خلاف فقهي بين من يرى أنّ المشروعية مطلوبة في جميع الأدلة سواء كانت أدلّة إدانة أو براءة ، و إتجاه آخر يحصرها في أدلة الإدانة فقط و طائفة أخرى عدّدت حالات دون الأخرى بخصوص دليل البراءة غير المشروع ، و الراجح من بين هذه الإتجاهات هو الإتجاه الذي يقصر المشروعية على دليل الإدانة فقط دون البراءة لأنّ دليل البراءة غير المشروع إن تمّ استبعاده سيؤدي لا محالة إلى إدانة بريء وهو ما لا يستقيم مع المنطق و العدل [229]،و كذا مع أحكام المادة الأولى فقرة 06 ".. أن يفسر الشك في كلّ الأحوال لصالح المتهم .." ، و كذا مبدأ "براءة مذنب خير من إدانة بريء" .

ثانيا : حجية تقدير الدليل الرقمي

---

[225] سعيداني نعيم ، المرجع السابق ، ص 210 .

[226] لعوارم وهيبة ،المرجع السابق، ص 373.

[227] سعيداني نعيم ، المرجع السابق ، ص 211 .

[228] نص المادة 191 من قانون الإجراءات الجزائية" تنظر غرفة الإتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به ، وعند الإقتضاء ببطلان الإجراءات التالية له كلها أوبعضها ولها بعد الإبطال أن تتصدى لموضوع الإجراء أوتحيل الملف إلى قاضي التحقيق نفسه أولقاض غيره لمواصلة اجراءات التحقيق "

[229] لعوارم وهيبة، المرجع السابق ، ص 375

يحكم الإثبات الجنائي في القانون الجزائري حرية القاضي و اقتناعه الشخصي وفقا لما جاء في نص المادة 212 من قانون الإجراءات الجزائية [230]، غير أنّ هذه الحرية القاضي تخضع لقيوم و ضوابط التي تشكلّ شروطا لإعمال هذا المبدأ و التطبيق الأمثل له و هذا ما نصت عليه ذات المادة[231] إذ يتعيّن مناقشة الدليل الرقمي تطبيقا لمبدأ شفوية المرافعة ، فإذا كانت مخرجات الوسائل الإلكترونية تعدّ أدّلة إثبات قائمة فإنّه يجب مناقشتها في حضور الخصوم [232] ، و لذا يتعين التطرق إلى سلطة القاضي في تقدير الدليل ، ومناقشة الدليل في جلسة المحاكمة .

1- سلطة القاضي الجزائي في تقدير الدليل الرقمي

حرية القاضي في الإقتناع تلزمه ببسط سلطانه على كلّ الأدّلة دون استثناء حتى على الدليل الرقمي لأنّ إعطاء القوة الثبوتية للدليل الرقمي يعدّ بمثابة الرجوع إلى المذهب المقيّد[233]، فالأدّلة المتحصل عليها من الوسائل الإلكترونية يخضع لمبدأ حرية القاضي في تكوين قناعته ، و حجية الأدّلة الرقمية تدخل ضمن مسألة قبول الأدّلة العلمية في الإثبات[234]وفق ما تقتضيه المادة 212 من قانون الإجراءات الجزائية ،فالدليل العلمي مهما تقدّمت طرقه وعلت قيمته العلمية و الفنيّة في الإثبات إلاّ أنّه يحتاج إلى قاضي يتمتع بسلطة تقديرية تسمح للقاضي تقدير الدليل الصحيح من الخاطئ و الدليل المغشوش و المتعمّد الغلط فيه [235].

و لا يخضع القاضي في تقديره للأدّلة لرقابة المحكمة العليا و مقيّد باليقين لاستبعاد قرينة البراءة و اليقين المستوجب في الأدلة الرقمية هو المعرفة العلمية في مجال الإلكترونيات[236]، إلاّ أنّ نقص الثقافة المعلوماتية للقاضي الجزائري يحتّم عليه الاستعانة بأهل الاختصاص من الخبراء و

---

[230] تنص المادة 212 ق ا ج " لا يسوغ للقاضي أن يبني قراره إلاّ على الأدّلة المقدمة له في معرض المر افعات و التي حصلت المناقشة فيها حضوريا أمامه".

[231] لعوارم وهيبة ، المرجع السابق، ص 921.

[232] نور الهدى محمودي ، المرجع السابق ، ص 919 .

[233] سعيداني نعيم ، المرجع السابق ، ص 228 .

[234] أجاز المشرع الجز ائري إثبات الجر ائم بأيّ طريق من طرق الإثبات عدا بعض الجر ائم التي اشترط لإثباتها أدّلة قانونية محدّدة مسبقا و على سبيل الحصر المادتين 341 ،342 من قانون العقوبات كما أعطى بعض المحاضر حجية الكاملة كمحاضر المعاينة الجمركية التي تعتبر صحيحة إلى غاية إثبات العكس. نور الهدى محمودي ، المرجع السابق، ص 920 .

[235] المرجع نفسه ، ص 920 .

[236] لعوارم وهيبة ، الجريمة المنظمة في تبييض الأموال عبر الوسائط الإلكترونية - دراسة مقارنة -،المرجع السابق ، ص 380.

الفنيين في هذا المجال للبحث عن الدليل و مصداقيته ممّا يؤدي إلى انكماش دور القاضي الجزائي في التقدير و لا يبقى للقضاة سوى الإذعان لرأي الخبراء المختصين [237]، و بالتالي فإنّ توافر الدليل لا يعني أنّ القاضي ملزم بالحكم بناء على هذه الأدّلة مباشرة و إنّما يجب أن يبسط رقابته على هذه الأدلة العلمية... و التأكد من مشروعيتها و أن يتمّ تضمين ملف الدعوى الدليل الذي يطرح للمناقشة أثناء المرافعات الشفوية[238].

ثانيا: وجوب مناقشة الأدلة الرقمية في الجلسة

بالرجوع إلى نص المادة 212 من ق إج ج ، يتعيّن مناقشة الدليل الرقمي تطبيقا لمبدأ شفوية المرافعة، فإذا كانت مخرجات الوسائل الإلكترونية تعدّ أدّلة إثبات قائمة في ملف القضية في الجريمة المعلوماتية فإنّه يجب مناقشتها في حضور الخصوم [239] ، و الحديث في هذه المسألة يجرنا إلى مناقشة مدى تأثير الأصالة الرقمية للدليل الرقمي على مبدأ قبوله من طرف القضاء ، إذ تبرز هذه الإشكالية عندما يتم حذف الدليل الرقمي عن بعد فيكون ما تبّقى منه مجرد نسخة فقط يتم التوّصل إليها عن بعد مثلا عن طريق المراقبة الإلكترونية [240]أو يتم استرجاعه وفق تقنيات خاصة .

و الدليل الرقمي لا يعبرّ عن قيمة أصلية بمجرّد الحصول عليه من العالم الافتراضي ممّا يثير إشكالية أصالته خاصة أنّ الدليل الرقمي يتم استنباطه و مستوحى من قاعدة مجهولة أو خدمات غامضة مثل خدمات الهكرز(قراصنة الانترنيت) و يتم استخدام برمجيات ذات تقنيات عالية تعمل على إخفاء آثار الدليل في العالم الافتراضي ، فالدليل الرقمي له طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي [241].

بالرجوع إلى التشريعات المقارنة نجدها اعتمدت منطق الافتراض أكثر من السعي إلى الحقيقة في معنى إقرار العدالة في إطار الدليل الرقمي ، فالاعتراف بأصالة الدليل الرقمي كان اعترافا قانونيا

---

[237] سعيداني نعيم ، المرجع السابق ، ص 220.

[238] لعوارم وهيبة ، الجريمة المنظمة في تبييض الأموال عبر الوسائط الإلكترونية - دراسة مقارنة -، المرجع السابق ، 377 ،378 .

[239] نور الهدى محمودي ، المرجع السابق ، ص 919 .

[240] سعيداني نعيم ، المرجع السابق ، ص 219 .

[241] عمر محمد أبو بكر يونس ، المرجع السابق ، ص 973

فقط ، فالعلاقة قائمة بين التشريع و بين الافتراض في طبيعة الدليل الرقمي ، و الافتراض هو الأصالة هنا. [242]

وجب على المشرع الجزائري تقنين هذا النوع من المسائل المهمة لاسيما أمام استبعاد هذا النوع من الأدّلة [243].

الفرع الثالث

الإجراءات الحديثة لجمع الأدلة في اتفاقية بودابست

استشعارا بصعوبة الحصول على أدلة الجرائم الإلكترونية وضبطها بالوسائل التقليدية تضمنت اتفاقية بودابست بشأن جرائم الحاسب الآلي والإنترنت مجموعتين من الإجراءات الجديدة إحداهما تتعلق بالإجراءات الممهدة لجمع الأدلة ، والثانية الإجراءات الخاصة بجمع الأدلة .

الإجراءات الممهدة لجمع الأدلة : وهي نوع من المراقبة والمتابعة لاستخدام تقنية الاتصالات (الحاسب الآلي والإنترنت) ، ويتولى القيام بهذه الإجراءات مقدمو خدمات الحاسب الآلي والإنترنت بتكليف من السلطة المختصة ومباشرة هذه الإجراءات لا يعد تحريكا للدعوى .

وتنقسم الإجراءات الممهدة إلى نوعين : النوع الأول إجراءات التحفظ السريع على مضمون البيانات المخزنة[244]، وهذا النوع يتمثل في أمرين : الأمر الأول هو إصدار أوامر إلى مقدمي الخدمات من أفراد وشركات بالحفاظ على البيانات المخزنة بمنظومة الحاسب الآلي والإنترنت لفترة زمنية معينة [245]. ؛ والأمر الثاني هو تمكين السلطة المختصة بالتحقيق لمعرفة مضمون البيانات التي أرسلها أو استقبلها المشترك ، سواء عن طريق مقدمي الخدمة أو من خلال ما أسفر عنه التفتيش ؛ أما النوع الثاني من الإجراءات الممهدة لجمع الأدلة فهو إجراءات التحفظ السريع على البيانات المتعلقة بخط سير البيانات[246] ، وقصد بها إلزام مقدمي الخدمات أفرادا أو شركات بالحفاظ على البيانات والمعلومات المخزنة ووقت إرسالها ووقت استقبالها ، ومن قام بنقلها ، وذلك يساعد على التعرف على مرتكب

---

[242] المرجع نفسه ، ص 973 ، 974 .

[243] لعوارم وهيبة، المرجع السابق ، ص 373 .

[244] المادة 16 من اتفاقية بودابست .

[245] حددت اتفاقية بودابست هذه المدة بما لا يتجاوز 90 يوما .

[246] المادة 17 من اتفاقية بودابست .

الجريمة الإلكترونية والمساهمين معه في ارتكابها ، وقد استجاب بعض المشرعين لما قررته اتفاقية بودابست في مادتها 1/17 و2 .

إجراءات جمع الأدلة ومن أهمها :

أولا - إصدار أمر بتقديم بيانات محددة[247] :

ويقصد به أن تصدر السلطة المخولة أمرا إلى مقدم الخدمة أو أي شخص في حيازته أو تحت سيطرته بيانات معينة أن يقوم بتقديمها ، سواء أكانت هذه البيانات تتعلق بالمحتوى أم بخط السير .

ثانيا - تفتيش وضبط البيانات المخزنة[248] :

ويقصد به البحث عن طريق التفتيش والضبط عن البيانات المخزنة في النظام المعلوماتي للحاسب الآلي أو في دعامة تخزين المعلومات ، سواء كانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات .

وقد حصرت المادة 19 من اتفاقية بودابست الإجراءات الخاصة بجمع الأدلة في : التفتيش أو الدخول المشابه ، الضبط أو الحصول ويشمل الضبط أو الحصول إلى البيانات ، وأيضا التحقق والتحفظ على نسخة من البيانات ، وكذلك المحافظة على سلامة البيانات ، وأخيرا منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتى .

ويمكن تقسيم هذه الإجراءات إلى نوعين من الإجراءات :

أ- **إجراءات تحفظية :**

تهدف إلى الحفاظ على البيانات المخزنة التي ترى الجهة المختصة أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتى للحاسب الآلي أو في دعامة التخزين ومنع الوصول إليها أو إلغائها أو التصرف فيها

ب- **إجراءات ضبط :**

وهي إجراءات لاحقة للتفتيش والدخول ، ويقصد بها جمع البيانات سواء بأخذ دعامة تخزين المعلومات ذاتها أو بعمل نسخة من البيانات المخزنة بها أو بالنظام المعلوماتي للحاسب الآلي في ورق أو أقراص .

---

[247] المادة 18 من اتفاقية بودابست .

[248] المادة 19 من اتفاقية بودابست .

ثالثا - التجميع في الوقت الفعلي لبيانات خط سير البيانات[249] :

ويقصد به تجميع أو تسجيل - عن طريق وسائل معينة موجودة على أرض الدولة - البيانات المتعلقة بخط سير البيانات في الوقت الصحيح ؛

وكذلك إلزام مقدم الخدمة في حدود قدرته الفنية بجمع وتسجيل البيانات المتعلقة بخط سير البيانات في الوقت الصحيح .

ويهدف هذا الإجراء الخاص بالتجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي قد تقوم به السلطة المختصة في الدولة أو ينفذه مقدمو الخدمة بناء على أوامر صادرة من السلطة المختصة بهذا الإجراء إلى تسهيل مهمة الجهات القائمة بجمع الأدلة .

و يختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي نصت عليه المادة (16) من اتفاقية بودابست في أن البيانات في حالة التحفظ موجودة لدى مقدم الخدمة أي مخزنة بالنظام المعلوماتي للحاسب الآلي أو في دعامة التخزين ، بينما في حالة التجميع أو التسجيل فالبيانات ليست مخزنة

وتهدف هذه الإجراءات إلى تجميعها أو تسجيلها وقت مباشرة الاتصال .

الخاتمة

اختيارنا للجريمة الإلكترونية والتغلب على تحدياتها كموضوع لهذه المطبوعة كان لأهميته وللتعرف على أبعاده وتنظيم قواعده بعد أن شغل هذا الموضوع بال المواطن ومؤسسات المجتمع والمهتمين بالدراسات القانونية ووقفت حياله أغلب التشريعات العربية عاجزة عن تجاوز تحدياته بسن تشريع خاص ومتطور لمواجهة هذا النوع من الجرائم والتصدي له أو كحد أدنى تعديل نصوص قائمة بما يتلاءم معه ويواكبه في تطوره وتجديداته في إطار مبدأ شرعية الجرائم والعقوبات ، بحيث لا تقل مراميه وأهدافه عن ما تضمنته توصيات هذه الورقة البحثية التي نلخصها في الآتي :

1- سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية ، على أن يكون شاملا للقواعد الموضوعية والإجرائية ، وعلى وجه الخصوص النص صراحة على تجريم الدخول غير المصرح به إلى

---

[249]- المادة 20 من اتفاقية بودابست .

الحاسب الآلي وشبكات الاتصال (الإنترنت) والبريد الإلكتروني ، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة ، أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت ، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات .

2- تكريس التطور الحاصل في نطاق تطبيق القانون الجنائي من حيث الزمان والمكان ، وتطوير نظام تقادم الجريمة الإلكترونية .

3- اعتبار بعض صور المساهمة في دورها وآثارها من قبيل الجرائم المستقلة .

4- الاعتراف في بعض الحالات بحجية للتشريعات والأحكام الجنائية غير الوطنية .

5- منح سلطات الضبط والتحقيق الحق في إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها ، على أن تمتد هذه الإجراءات إلى أية نظم حاسب آلي آخر له صلة بمحل الجريمة .

6- تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة .

7- نشر الوعي بين المواطنين وخاصة الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات.

8- تفعيل دور المجتمع المدني والمؤسسات للقيام بدوره التوعوي والوقائي من الوقوع في براثن الرذيلة والممارسات الخاطئة .

9- إعداد أنظمة ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية.

تم بعون الله

قائمة المراجع

أولا : الكتب

1- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية والأدبية، ط1،2013 .

1- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان.

2- زبيحة زيدان،الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011 .

3- أمير فرج يوسف،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، ط1، 2011.

4- خثير مسعود،الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، طبعة 2010 .

5- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن ط1، 2011.

6- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، طرابلس، 2012 .

7- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية ، 2009

8- عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري و القانون المقارن ، دار الجامعة الجديدة ، الإسكندرية ، 2010 .

9- سامي جلال فقي حسين ، التفتيش في الجرائم المعلوماتية - دراسة تحليلية - ، دار الكتب القانوني - دار شتات للنشر و البرمجيات ، مصر ، 2011 .

10-مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، ج1 ،ط 2، منشورات المكتبة الوطنية ، بنغازي ،2000 .

11-مأمون محمد سلامة ، الإجراءات الجنائية في التشريع الليبي ، ج 2 ،ط2، منشورات المكتبة الوطنية ، بنغازي ، 2000.

12-محمود نجيب حسني ،شرح قانون الإجراءات الجنائية ، ج 1 ، ط 1 ، دار النهضة العربية ، القاهرة 1988 .

13-جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، 2001 .

14-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، دد ن ،2009 .

15-عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، المحلة الكبرى،2007 .

16-عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار الكتب القانونية، مصر ط1، 2009.

17-عمر سالم ، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن ، دار النهضة العربية ، الطبعة الأولى ، القاهرة ، 2000 .

18-محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2004 .

19-مدحت رمضان ، جرائم الاعتداء علي الأشخاص والانترنت ، دار النهضة العربية ، القاهرة ، 2000 .

20-هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، 1962 .

21-هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، د سن ، د ب ن ، 1994 .

22-هلالي عبد اللاه احمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقاً عليها) ،ط1 ، دار النهضة العربية، القاهرة ، 2007 .

23-هلالي عبد اللاه احمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دراسة مقارنة ،ط1، دار النهضة العربية ، القاهرة ، 1997 .

ثانيا : الرسائل و المذكرات

1- عبد الله دغش العجمي،المشكلات العلمية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

2- عمر محمد أبو بكر بن يونس ،الجرائم الناشئة عن استخدام الأنترنيت ، رسالة دكتوراة ،كلية الحقوق ، جامعة عين شمس ، 2004 .

3- ثنيان ناصر آل ثنيان، الجريمة الإلكترونية، رسالة ماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2012.

4- سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ،رسالة ماجستير، جامعة الحاج لخضر ، باتنة ، 2013/2012 .

5- إبراهيم محمود محمد بن عبد الرحمان ، جريمة غسل الأموال في القانون الإماراتي و المقارن - دراسة مقارنة - رسالة دكتوراه، كلية الحقوق ، جامعة الإسكندرية، 2009.

6- لعوارم وهيبة،الجريمة المنظمة في تبييض الأموال عبر الوسائط الإلكترونية - دراسة مقارنة -.، أطروحة دكتوراة ، كلية الحقوق ، جامعة باجي عمار ، عنابة ، 2017 .

7- عبد الله بن محمد كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، أطروحة ماجستير، كلية الدراسات العليا، تخصص التشريع الجنائي الإسلامي، جامعة نايف للعلوم الأمنية، الرياض، 2013 .

ثالثا : المجلات و الملتقيات

1- حسن طاهر داود،جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2000 .

2- محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الانترنت المنعقد الفترة من 1-3 مايو ، بكلية الشريعة والقانون بدولة الإمارات 2000 .

3- هدى حامد قشقوش، الإتلاف العمدي لبرنامج وبيانات الحاسب الآلي ، بحث مقدم لمؤتمر (القانون والكمبيوتر والانترنت) المنعقد في الفترة من 1-3 مايو2000 بكلية الشريعة والقانون بدولة الإمارات .

4- محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي ، المنعقد من 25-28 أكتوبر ، سنة 1993 .

5- نور الهدى محمودي ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ، مجلة الباحث للدراسات الأكاديمية ، المجلد الأول ، العدد الحادي عشر ، جامعة الحاج لخضر باتنة ، الجزائر ، جوان 2017.

6- عاقلي فضيلة ،الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الرابع عشر الجرائم الإلكترونية، من 24-25 مارس 2017، طرابلس لبنان .

7- محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25 -28 أكتوبر ، 1993 .

8- بوزينة أمحمدي آمنة ،إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية و قانون الوقاية من جرائم الإعلام)، ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر ، 29 مارس 2017 .

9- فضيلة عاقلي ، الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري ، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية ، مركز جيل البحث العلمي ، طرابلس 24-25 مارس 2017 .

10-هلالي عبد اللاه احمد، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي ، بحث مقدم إلي المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25-28 أكتوبر ، 1993 .

11-مختارية بوزيدي، ماهية الجريمة الإلكترونية، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري 09-3- 2017.

12-ميلود بن عبد العزيز، الجرائم الأخلاقية والإباحية عبر الانترنت وأثرها على المجتمع من منظور شرعي وقانوني، مجلة الواحات للبحوث والدراسات، العدد 17، 2012.
13-محمد علي قطب، الجريمة المعلوماتية وطرق مواجهتها، ج2، الأكاديمية الملكية للشرطة، مملكة البحرين، مارس 2010.
14-علي محمد سالم، حسون عبيد هجيج، الجريمة المعلوماتية، مجلة بابل للعلوم الإنسانية، كلية القانون، جامعة بابل، المجلد 14، العدد 6، 2007 .
15-عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض،2007.
16-مختار الأخضري، محاربة الجريمة المعلوماتية، ملتقى دولي 5-6 ماي 2010، مركز البحوث القانونية والقضائية، الجزائر.
17-سومية عكور، الجرائم المعلوماتية وطرق مواجهتها : قراءة في المشهد القانوني والأمني، الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الفترة من 2-4 / 2014/09، كلية العلوم الإستراتجية، عمان، الأردن، 2014.

رابعا : النصوص القانونية

1- قانون04-15 المؤرخ في 10 نوفمبر2004 المعدل والمتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج رعدد 71 الصادرة بتاريخ 11/10 /2004.
2- قانون 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد 44، المؤرخة في 23 جويلية 2003 .
3- القانون 03-2000 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية ،ج ر عدد 48، المؤرخة في 6 أوت 2000.
4- قانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج ر عدد 47 الصادرة بتاريخ 16 أوت 2009 .

5- قانون 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم للأمر 155/66 المؤرخ في 08 يونيو 1996 و المتضمن قانون الإجراءات الجزائية ، ج ر عدد 20 المؤرخ في 2017/03/29 .
6- قانون 16-01 المؤرخ في06 مارس2016 المتضمن التعديل الدستوي، ج ر عدد 14 الصادرة بتاريخ 2016/03/07.
7- أمر 15-02 المؤرخ في 23 يوليو 2015 المعدل و المتمم للأمر 155/66 المؤرخ في 08 يونيو 1996 المتضمن قانون الإجراءات الجزائية ،ج ر عدد 53 الصادرة بتاريخ 10 أكتوبر 2015 الموافق عليه بموجب القانون 17/15 المؤرخ في 2015/12/13 ، ج ر عدد 20 المؤرخ في 29 مارس2017 .
8- مرسوم رئاسي 15- 26 المؤرخ في 2015/10/08 ، الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر عدد 53 الصادرة بتاريخ 10 أكتوبر 2015 .
9- مرسوم تنفيذي 348/06 المؤرخ في 2006/10/05 يتضمن تمديد الإختصاص المحي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق ، ج ر عدد 63 الصادرة بتاريخ 2006/10/08 المعدل والمتمم بالمرسوم التنفيذي 267/16 المؤرخ في 2016/10/17 ج ر عدد 62 الصادرة بتاريخ 2016/10/23 .