الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة مولود معمري – تيزي وزو –
كلية الحقوق والعلوم السياسية
قسم القانون – نظام ل.م.د

الجريمة المعلوماتية في التشـــريع الجزائري

مذكرة لنيل شهادة الماستر في القانون
تخصص القانون الجنائي والعلوم الإجرامية

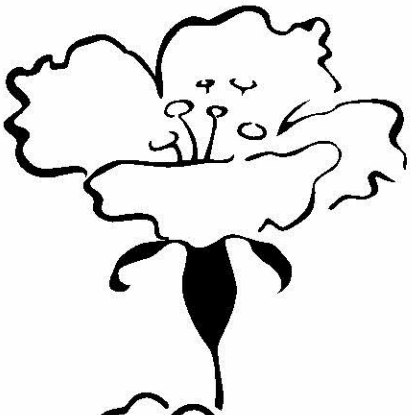
إعداد الطّالبتين:
شريد حكيمة
ربيع مايسة

إشراف الأستاذة:
أ.د. إقلولي/اولدرابح صافية

لجنة المناقشة:

الدكتور بلميهوب عبد الناصر، أستاذ محاضر"ب".....رئيسًا
الدكتورة إقلولي/اولد رابح صافية، أستاذة، .....مشرفة ومقررة
الأستاذ بوغرارة رمضان، أستاذ مساعد "ب".....ممتحنا

تاريخ المناقشة:18/07/2016



إهداء

أهدي هذا العمل إلى من أوصاني بهما ربي برا وإحسانا، والدي العزيزين، أمي وأبي أطال الله في عمرهما.

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إخواني وأخواتي إلى كل، من ساهم، من قريب أو بعيد، في إعداد هذا العمل المتواضع خاصة أختي كريمة و نوال وصديقة الغالية ليندة وعائلتها.

حكيمة

إهداء

أهدي ثمرة جهدي إلى:

منبع حياتي، التي أهدتني نور الحياة وسقتني من دفقات حبها،

التي قدمت لي آيات الحب والحنان، أطال الله في عمرها، أمي الغالية.

إلى الذي استلهمت منه معاني

الثبات وزرع في قلبي حب العلم ووهبني كل رعايته

واهتمامه، أبي العزيز أدامه الله لي .

إلى الذي ساندني و رافقني في هدا العمل، نور قلبي، نطيبي إسلام

إلى والدي نطيبي أطال الله في عمرهما.

إلى أخوي وليد وأوسامة.

إلى إخوة نطيبي أميرة وطارق.

و كل من ساهم من بعيد أو قريب في إعداد هذا العمل.

مايسة

كلمة شكر

نشكر الله سبحانه وتعالى، ابتداءً، واعترافا بالفضل والجميل. نتوجّه بالشّكر الجزيل إلى أستاذتنا المشرفة

أ.د. إقلولي/اولدرابح صافية

التي أشرفت على هذا العمل وتتبّعتنا فيه بالنصائح والإرشادات، وأخذت بيدنا أثناء إنجازه خطوة بخطوة إلى أن تمّ واكتمل.

نفع الله بها العلم وطلاّبه، وجزاها الله عني كلّ خير.

شريد حكيمة وربيع مايسة

قائمة أهم المختصرات

1- باللغة العربية:

ج. ر. ج. ج:..... جريدة رسمية للجمهورية الجزائرية.

ص ص:..... من الصفحة رقم... إلى الصفحة رقم.

ص:.....الصفحة رقم.

مقدمـــة:

عرف الإنسان الجريمة منذ وجوده على الأرض وتطورت بتطوره في مختلف المجالات، العسكرية، الاقتصادية، السياسية، الدينية والتجارية. وأدى ظهور الأنماط الجديدة والمستحدثة، التي لم يعرفها العالم من قبل، إلى توسيع وتطوير النشاط الإجرامي.

ويعود سبب هذا التوسع إلى عدة عوامل، لعل أبرزها **التقدم التكنولوجي** الذي شهدته وتشهده الإنسانية في مجالي تقنية المعلومات والاتصال، إذ أصبحت مختلف القطاعات تعتمد في أداء عملها، بشكل أساسي، على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري الدقة والسرعة في تجميع المعلومات وتخزينها ومعالجتها. ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين الدول.

إلى جانب ذلك، تقدم التكنولوجيا الحديثة للأجهزة الأمنية الكثير من التسهيلات والإمكانات التي تساهم في رفع كفاءاتها وقدرتها على التصدي للجريمة. وعليه، فمن يملك المعلومات يملك مفاتيح المستقبل لأنها ثروة لا يستهان بها ومصدر قوة سياسية واقتصادية، ومعيار يقاس عليه مدى تطور وتحضر الشعوب.

وتجدر الإشارة إلى أن الجانب الإيجابي لعصر المعلوماتية صاحبته جملة من الانعكاسات السلبية والخطيرة، أفرزتها تلك التقنية العالية بسبب إساءة استخدام الأنظمة المعلوماتية. ومن هنا ظهر ما يسمى بالجريمة المعلوماتية التي يستخدم فيها الكمبيوتر لأغراض غير شرعية مثل سرقة الأموال. كما سهلت تلك التقنية ارتكاب بعض الجرائم التقليدية فازدادت هذه المخاطر تفاقما في ظل شبكة المعلومات.

وكثر ارتكاب هذه الجريمة، في العشرية الأخيرة، في معظم دول العالم، منها الجزائر، بسبب ازدياد عدد شبكة الاتصالات وتوسعها مما يصعب تحديد حجم الخسارة الفعلية التي تسببها، من جهة، ويعقد مهمة مكافحتها، من جهة أخرى.

استدعى توسع ارتكاب الجريمة المعلوماتية تحرك الدول، على جميع المستويات، من أجل مواجهتها، فسنت تشريعات بهدف معاقبة مرتكبيها والكشف عنها قبل ارتكابها، فالتصدي لهذه الجريمة يمثل تحديا جديدا للأنظمة القانونية.

وبادرت الجزائر، على غرار باقي الدول، إلى تعزيز نظامها القانوني في سبيل التصدي للجريمة المعلوماتية بالسعي إلى وضع تشريعات تحد قدر الإمكان من حالات

ارتكابها. ومن هنا تبرز أهمية الموضوع وسبب اختيارنا له.

وبناء على كل ما سبق ذكره، رأينا طرح الإشكالية التالية: **فيما تتمثل الإصلاحات التشريعية التي كرسها المشرع الجزائري في مجال مكافحة الجريمة المعلوماتية؟**

ولدراسة هذه الإشكالية، اعتمدنا خطة ذات فصلين: تطرقنا في **الفصل الأول** إلى الطبيعة القانونية للجريمة المعلوماتية، وخصصنا **الفصل الثاني** لمكافحة الجريمة المعلوماتية في التشريع الجزائري.

الفصل الأول

الاحكام العامة للجرائم المعلوماتية

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية، نظرا للدور البارز الذي تلعبه المعلومات في الوقت الراهن في مجال تبادل المعلومات، وما تقدمه من مزايا كثيرة.

وبالرغم من كل ما حققته شبكة الانترنت من إيجابيات، إلا أنها حملت معها آثارا سلبية إلى مختلف المجتمعات نتيجة استخدامها بسوء نية، فأصبحت وسيلة لانتهاك حقوق الإنسان وحرياته نتيجة الاستغلال غير المشروع لها.

ونظرا لما سبقت الإشارة إليه، فقد اهتمت الكثير من الدراسات بمحاولة إيجاد تقسيمات للجريمة المعلوماتية. ولدراسة ذلك، يجب أن نتناول أولا تحديد مفهوم الجريمة المعلوماتية (**المبحث الأول**)، ثم ثانيا، أن نتعرض إلى تكييف الجريمة المعلوماتية (**المبحث الثاني**).

المبحث الأول
مفهوم الجريمة المعلوماتية

أثارت الجريمة المعلوماتية عدة تساؤلات في الأوساط الفقهية بخصوص تحديد مفهومها. ومن أجل تحديده، فإنه لابد من التطرق إلى مختلف التعريفات المتداولة، الفقهية والقانونية منها، وبيان الخصائص التي تقوم عليها (المطلب الأول).

ويتطلب أمر تحديد مفهوم الجريمة المعلوماتية التعرض إلى الفاعل المعلوماتي بإبراز خصائصه المميزة، أصنافه، ودوافع ارتكابه الجريمة (المطلب الثاني).

المطلب الأول
التعريف بالجريمة المعلوماتية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المرتبطة بالإعلام الآلي فهناك من يسميها: جرائم الكمبيوتر أو جرائم التقنية العالية، في حين ذهب آخرون إلى تسميتها: الاحتيال المعلوماتي أو الجرائم المستحدثة. وانعكس ذلك الاختلاف في التسمية على التعريفات المقدمة (الفرع الأول)، التي يمكن الاستناد إليها، بالرغم من ذلك، لاستنتاج خصوصية الجريمة المعلوماتية (الفرع الثاني).

الفرع الأول
محاولة تحديد المقصود بالجريمة المعلوماتية

اختلفت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع سبب ذلك إلى ارتباطها بتكنولوجيا الإعلام والاتصالات. وقد سعى الفقه والتشريع إلى إزالة الغموض الذي يكتنف المقصود بتلك الجريمة.

أولا- التعريف الفقهي:

اختلف الفقه في تعريف الجريمة المعلوماتية فانقسم إلى اتجاهين، اتجاه يضيق في تعريفها، واتجاه يوسع فيه.

1- الاتجاه المضيق في تعريف الجريمة المعلوماتية:

حصر أنصار هذا الاتجاه الجرائم في الحالات التي تتطلب قدرا كبيرا من المعرفة في مرتكبيها، فعرف الفقيه " **دفيد تمسون**" الجريمة المعلوماتية كما يلي : " **جرائم يكون متطلبا لإقترافها أن يتوفر لدى الفاعل معرفة بتقنية الحاسب** "[1].

وعرفها جانب آخر بأنها: " **كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لإرتكابه من ناحية وملاحقته من ناحية أخرى**". وحسب هذا التعريف فإنه يجب أن تتوفر، لدى الفاعل، معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة[2].

وذهب الأستاذ " **روسبلات** " إلى القول بأنها: " **نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها** "[3].

2- الاتجاه الموسع في تعريف الجريمة المعلوماتية:

ذهب أصحاب هذا الاتجاه إلى اعتبار مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يضفي عليها وصف الجريمة، فيرى فريق بأنها: " **كل سلوك إجرامي يتم بمساعدة الكمبيوتر** "، أو هي: " **كل سلوك غير مشروع أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها** " [4].

نستنتج من خلال هذين التعريفين أن الجريمة المعلوماتية هي كل نشاط إجرامي يؤدي فيه نظام الكمبيوتر دورا لإتمامه على أن يكون هذا الدور مؤثرا في ارتكاب الجريمة.

كما اعتبر الفقيهان "**ميشال وكريدو**" أن تلك الجريمة تشمل استخدام الحاسب كأداة لارتكاب الجريمة. وعرفها الفقيه الألماني "**تاديمان**" كما يلي: " هي **كل أشكال السلوك غير**

---

[1]- طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 154.

[2]- خالد ممدوح إبراهيم، **حوكمة الأنترنت**، الطبعة الأولى، دار الفكر الجامعي ،الإسكندرية ،2011، ص357.

[3]- مليكة عطوي: " **الجريمة المعلوماتية: الأسواق المالية العربية في ظل العولمة المالية وحجية الإعتراف في تكوين قناعة القاضي الجزائي**"، مجلة حوليات الجزائر، عدد 21، الجزائر 2012، ص 13.

[4]- خالد ممدوح إبراهيم، مرجع سابق، ص 357.

المشروع أو الضار بالمجتمع، و الذي يرتكب باستخدام الحاسب الآلي "[1]. نرى من خلال هذا التعريف هذا الاتجاه يعتمد وسيلة ارتكاب الجريمة.

ويوسع البعض من تعريف الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط، بأي طريقة تكن، بالحاسب يتسبب في إمكانية حصول مرتكبه على مكسب أو إمكانية تحمل المجني عليه الخسارة، وهو ما ذهب إليه الخبير الأمريكي "**باركور**" في تعريفه للجريمة المعلوماتية الذي اعتبرها بأنها: " **كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق المجني عليه أو مكسب يحققه الجاني** " [2].

نستنتج، أخيرا، أنه رغم تعدد التعريفات المقدمة بشأن الجريمة المعلوماتية، إلا أن تعريفها يقوم على العمل الرئيسي المكون لها، وليس بالاعتماد على الوسيلة المستخدمة في ارتكابها[3].

ثانيا- التعريف التشريعي:

أطلق المشرع الجزائري على الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب أحكام نص المادة 02 من القانون رقم 09-04، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الذي عرفها كما يلي: " **جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية** "[4]. ويلاحظ من خلال هذا النص أن المشرع الجزائري لم يحدد صورة السلوك المجرم الذي يرتكب أو يسهل ارتكابه ضد منظومة معلوماتية[5].

---

[1]- لعاقل فريال، **الجريمة المعلوماتية في ظل التشريع الجزائري**، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة البويرة، 2015، ص 9.

[2]- قارة أمال، **الجريمة المعلوماتية**، مذكرة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2002، ص 18 .

[3]- قارة أمال،المرجع نفسه،ص 20.

[4]- القانون رقم 09/04، **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها**، المؤرخ في 05 أوت 2009، ج.ر، عدد 47، 16 أوت 2009.

[5]- سوير سفيان، **جرائم المعلوماتية**، مذكرة لنيل شهادة ماجستر في العلوم الجنائية وعلم الإجرام، جامعة تلمسان، 2010، ص 11.

وعمل المشرع الجزائري على استحداث نصوص جديدة لقمع مرتكبي الجريمة المعلوماتية، بموجب القانون رقم 15/04 الصادر بتاريخ 2004/11/10، المعدل لتقنين العقوبات، محددا بذلك الأفعال التي تدخل ضمن هذا النوع من الجرائم الجديدة بمقتضى نصوص المواد من 394 إلى 394 مكرر 7 من التقنين المذكور[1].

الفرع الثاني

خصوصية الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من بين الجرائم المستحدثة لأنها نتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع، فهي بذلك تتميز بخصائص وسمات تميزها عن غيرها من الجرائم وجعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل.

1- الجريمة المعلوماتية جريمة عابرة للحدود:

تتسم الجريمة المعلوماتية غالبا بالطابع العابر للدول، إذ يسهل ارتكابها ما بين الدول، فالجريمة المعلوماتية تتخطى حدود الدولة التي ارتكبت فيها لتتعدى آثارها إلى دول أخرى. فيمكن ارتكاب العديد من الجرائم، من خلال النظام المعلوماتي، مثل: جرائم التعدي على قواعد البيانات، جرائم الاحتيال المعلوماتي، سرقة بطاقات الائتمان، غسيل الأموال والقرصنة[2].

يتم ارتكاب الجريمة المعلوماتية عن بعد، فهي تتعدى الحدود الجغرافية للدول نظرا للقدرة التي تتمتع بها الحاسبات الآلية في تبادل المعلومات ونقلها إلى مسافات كبيرة تصل آلاف الأميال، إضافة إلى السرعة الهائلة التي يتم بها تنفيذ الجريمة المعلوماتية مما يصعب اكتشافها[3].

2- إرتكاب الجريمة المعلوماتية من أشخاص تتطلب فيهم مهارة:

يتطلب ارتكاب الجريمة المعلوماتية أن يكون مرتكبها متمتعا بالمعرفة الفائقة والمهارة العالية والوسيلة الخاصة بهذه الجريمة، لأن الإجرام المعلوماتي هو إجرام الأذكياء، إذ يشغل

---

[1]- القانون رقم 15/04، **المتضمن تعديل قانون العقوبات**، مؤرخ في 2004/11/10، ج.ر، عدد 71، الصادرة بتاريخ 2004/11/10. 10-11-2004.

[2]-خالد ممدوح إبراهيم، مرجع سابق، ص 360.

[3]-سوير سفيان، مرجع سابق، ص 20.

المجرم ذكاءه لتنفيذ جريمته. ولذلك، فإنه غالبا ما يكون المجرم المعلوماتي من ذوي المستويات العالية[1].

3- الطابع الخفي للجريمة والسرعة في تنفيذها:

تعتبر الجريمة الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلب الأحيان، فالضحية لا يتفطن للجريمة رغم أنها قد وقعت أثناء وجوده على الشبكة ذلك أن الفاعل يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة كالاختلاس المعلوماتي أو إتلاف المعلومات.

يستخدم المجرم في ذلك أساليب عبقرية كما هو الشأن بالنسبة إلى أسلوب التلاعب بالنبضات والذبذبات الإلكترونية.

وإضافة إلى ذلك، فإن القراصنة يتبادلون المعلومات المتعلقة بأساليب إخفاء الجريمة في إطار مؤتمرات سرية، وهو ما ساعد في ابتكار طرق ووسائل في غاية التعقيد عجزت مختلف التشريعات في مواجهتها[2].

4- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها:

تتميز الجريمة المعلوماتية بأنها صعبة الاكتشاف والإثبات لأنها عبارة عن أرقام وبيانات تتغير أو تحمى من السجلات المخزنة في ذاكرة الحاسب.

وإلى جانب ذلك، لا تترك هذه الجريمة آثارا خارجية ما يؤدي إلى انعدام وجود آثار مادية ملموسة (بصمات، شواهد مادية، تخريب)، إضافة إلى سهولة محو الدليل أو تدميره[3].

---

[1]- واقد يوسف، **النظام القانوني للدفع الإلكتروني**، مذكرة لنيل درجة ماجستر في القانون العام، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011 ، ص 118.

[2]- صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة لنيل شهادة الماجستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 14 و15.

[3]- طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 171.

5- الجريمة المعلوماتية جرائم ناعمة:

تتميز الجريمة المعلوماتية بأنها جرائم ناعمة لا يشوبها أي عنف، فهي تنقل بيانات ومعلومات من حاسب إلى آخر أو السطو على أرصدة المؤسسات أو الشركات[1].

6- عدم الاتفاق على مفهوم مشترك للجريمة المعلوماتية:

يوجد اختلاف كبير بشأن إيجاد مفهوم مشترك للجريمة المعلوماتية، وذلك راجع إلى تطور ظاهرة الإجرام المرتبط بتقنيات المعلومات والاتصالات، وانعدام معاهدات دولية ثنائية أو جماعية لمواجهة الجريمة المعلوماتية. ولا شك أن هذا الاختلاف انعكس سلبا على إيجاد حلول مناسبة لتشجيع الدول على مواجهة الجرائم المعلوماتية، من جهة، والعمل على إبرام اتفاقيات ثنائية من أجل تبادل المعلومات والخبرات [2].

وقد اختلف الفكر القانوني حول تسمية الجريمة المعلوماتية ابتداء من مصطلح **إساءة** استخدام الكمبيوتر مرورا بمصطلح الاحتيال بواسطة الكمبيوتر والجرائم المعلوماتية إلى جانب جرائم الغش المعلوماتي والاحتيال المعلوماتي[3].

7- الجريمة المعلوماتية جريمة مستحدثة:

يتوقف أمر ارتكاب تلك الجريمة على توفر جهاز كمبيوتر أو أي جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية، كأجهزة فك الرموز المقرصنة التي باتت تشكل خطرا جسيما في ظل العولمة.

المطلب الثاني

الفاعل المعلوماتي

يتمتع المجرم المعلوماتي بقدر كبير من الذكاء فهو ذو نظرة غير تقليدية للجريمة، بسبب ذكائة الحاد.

ترتبط الجريمة المعلوماتية بذات الإنسان وشخصيته ودوافعه التي تحفزه على القيام بسلوك إجرامي عبر شبكة الانترنت.

---

[1]- ذياب موسى البدانية: "**الجرائم الالكترونية: المفهوم والاسباب**"، ورقة مقدمة في الملتقى العلمي،الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية ، الاردن، 2-4-2014.

[2]-خالد ممدوح إبراهيم ، **أمن الجريمة الالكترونية**، دار الجامعة، الإسكندرية ، 2010، ص 48 و49 .

[3]-خالد ممدوح إبراهيم، مرجع سابق، ص 49.

ولتوضيح ذلك سنتعرض في هذا المطلب إلى خصائص المجرم المعلوماتي (الفرع الأول)، ثم إلى أصناف المجرم المعلوماتي (الفرع الثاني)، وستناول أخيرا دوافعَ إرتكاب الجريمة المعلوماتية(الفرع الثالث).

الفرع الأول

خصوصيات شخصية المجرم المعلوماتي

يتميز المجرم المعلوماتي بمجموعة من الخصائص التي تميزه عن غيره من المجرمين والتي تتمثل أساسا في:

1-المهارة:

تعد المهارة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي التي تكتسب عن طريق الخبرة في مجال التكنولوجيا والتفاعل الاجتماعي مع الآخرين.

غير أن ذلك لا يعني بالضرورة أن يكون المجرم المعلوماتي على قد كبير من المعرفة بالعلوم. فأثبت الواقع العملي أنه من بين أخطر المجرمين المعلوماتيين من لم يكتسبوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[1].

2- المعرفة:

يقصد بالمعرفة في هذا المجال، التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانية نجاحها واحتمالات فشلها.

فيستطيع المجرم المعلوماتي تصور الجريمة كاملة لأن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالجاني يستطيع أن ينفذ جريمته على أنظمة مماثلة لتلك التي يستهدفها، وذلك قبل تنفيذ جريمته[2].

---

[1]- لعاقل فريال، مرجع سابق، ص20.

[2]- طارق إبراهيم الدسوقي عطية، مرجع سابق، ص176.

3- الذكاء والاحتراف:

يتمتع المجرم المعلوماتي بعدة مزايا منها الذكاء الذي يعتبر من أهم صفاته لأنها تمكنه من فتح الملفات قراءاتها، كتابتها محوها، تعديل أو إلغاء المعلومات التي تحتوي عليها مختلف الأنظمة المعلوماتية.

وتتجلى أهمية صفة الذكاء والاحتراف بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكاب الجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة دون أن يشوبه غموض[1].

4- الوسيلة:

تعتبر الوسيلة مجموعة الإمكانيات التي يتزود بها الجاني لإتمام جريمته، وقد تتميز أحيانا بالبساطة وسهولة الحصول عليها. كما يمكن أن تكون الوسيلة ابتكار المجرم نفسه من أجل إتمام نشاطه.

الفرع الثاني

أصناف المجرم المعلوماتي

يمكن تصنيف مجرمي المعلوماتية إلى مجموعة من الأصناف تتمثل فيما يلي:

1- صغار نوابغ المعلوماتية: (فئة صغار مجرمي المعلوماتية)

يقصد بهم فئة صغار السن ويوصفون بأنهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، خاصة في انعدام حدود جغرافية لأفعالهم، والتي تصل إلى أنظمة ومراكز المعلوماتية توجد على إقليم دولة واحدة[2].

ويرتكب هؤلاء الأشخاص هذه الجرائم غالبا دون نية الإضرار بالغير وإنما لمجرد التسلية و المزاح فقط.

وتجدر الإشارة إلى أنه رغم صغر سنهم إلا أنهم يمثلون تهديدا يمس بسياسة الدول عامة والأفراد خاصة لأنهم عرضة للتحول إلى قراصنة في المستقبل[3].

---

[1]- سعيداني نعيم ، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2013، ص 51.

[2]- عبد الفتاح بيومي حجازي، **مباديء الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت**، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية ، 2006، ص 16 .

[3]- سعيداني نعيم ، مرجع سابق، ص 54.

2- فئة القراصنة الهواة أو المخترقون:

هم المتطفلون الذين يتحدون أمن النظم المعلوماتية فيدخلون إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها.

وتتسم هذه الفئة بميزة تبادل المعلومات والخبرات فيما بين الفراصنة، وغالبا لا تكون لديهم دوافع حاقدة أو تخريبية من وراء أعمالهم و إنما ينطلقون من هدف اكتساب الخبرة والمهارة[1].

3- فئة القراصنة المحترفين:

تعد هذه الفئة من بين أخطر المجرمين لأن اعتداءاتهم تهدف إلى تحقيق الكسب المادي الهائل، وتتراوح أعمارهم من 25 إلى 45 سنة، وغالبا ما يتم ارتكاب الجرائم المعلوماتية من أشخاص المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسبات الآلية.

ويقومون بتنفيذ أعمالهم غير المشروعة بأنفسهم أو بمساعدة عدة أشخاص مما يساعد على نجاح أفكارهم. ويلاحظ أن الأضرار التي تترتب عن هذه الأفعال تكون بالغة الضرر بعكس الفئات الأخرى إذ أنهم كثيرا ما ينظر إليهم بوصفهم مستخدمين مثاليين[2].

الفرع الثالث

دوافع ارتكاب الجريمة المعلوماتية

يرجع سبب ارتكاب الجريمة المعلوماتية إلى عدة دوافع، فبعضها دوافع شخصية وأخرى دوافع خارجية, وهو ما سنتعرض إليه فيما يلي:

أولا- الدوافع الشخصية:

توجد عدة دوافع شخصية تحفز المجرم على ارتكاب الجريمة المعلوماتية، منها دوافع مالية، دوافع ذهنية أو نمطية.

1- الدوافع المالية:

---

[1]- مليكة عطوي، مرجع سابق، ص 20.

[2]- محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة الإسكندرية،2011، ص 80.

يعد هذا الدافع من بين أكثر الدوافع تحريكا للجناة لأنه يهدف إلى تحقيق الربح المالي السريع. وذلك بالاطلاع على معلومات معينة أساسية ذات أهمية خاصة، أو عن طريق المساومة على البرامج والمعلومات.

ونتيجة لوقوع الضحايا تحت الضغط بسبب حصول الجناة على معلومات متعلقة بحياتهم الخاصة، فإنهم يجدون أنفسهم مجبرين للخضوع لطلباتهم المالية[1].

2- الدوافع الذهنية أو النمطية:

يسعى المجرمون المعلوماتيون إلى إظهار مستوى تفوقهم، أن الحصول على المعلومة لا يجب أن يشوبها غموض أو قيد.

ويكون، عادة، هؤلاء في مجموعات قصد تبادل الخبرات والتجارب، إذ يبذلون كل جهدهم لتعلم كيفية اختراق المواقع الممنوعة وابتكار طرق جديدة ومعقدة. ومن بين أبرز الأمثلة عن ذلك، قيام أحد القراصنة الهواة، في أوربا بحل شفرة إحدى مراكز المعلومات في وزارة الدفاع الأمريكي وتمكنه من العبث في بياناته[2].

ثانيا- الدوافع الخارجية:

يتأثر الإنسان بدوافع خارجية نتيجة وجوده في محيط المعلومات. وتكون الدوافع التي تحفز الإنسان، على ارتكاب الجريمة المعلوماتية، سواء إما الانتقام أو الإضرار بالغير.

1 - الانتقام من رب العمل وإلحاق الضرر به:

يتعرض العاملون في قطاع التقنية لضغوطات نفسية تكون ناجمة عن المشاكل المالية ، وهو الأمر الذي يدفع إلى التفكير في البحث عن وسيلة لتحقيق الربح.

وعلاوة عن ذلك، فإن ضغط العمل يؤدي بالعمال إلى ارتكاب جرائم الحاسوب، تكون غايتها الانتقام من رب العمل، سواء كان شخصا طبيعيا أو معنويا، ومثال ذلك: قيام محاسب بالتلاعب ببرامج الكمبيوتر الخاصة بالشركة التي يعمل بها انتقاما منها[3].

---

[1]- محمد علي العريان، مرجع سابق، ص 72.

[2]- سمية مرغيش، **جرائم المساس بالأنظمة المعلوماتية**، مذكرة لنيل شهادة ماستر: تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، بسكرة، 2014، ص 10.

[3]- جعفر حسن جاسم الطائي، مرجع سابق، ص 168.

2-الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية:

تغلب الرغبة، أحيانا، في قهر النظام الرغبة في الحصول على الربح، ذلك من أجل إظهار المجرم المعلوماتي تفوقه ومستوى براعته.

وإثباتا لما سبق ذكره أعلاه، فإنه كلما ظهرت تقنية جديدة مستحدثة، فإن المجرم المعلوماتي يحاول إختراقها بإيجاد أو محاولة كشف وسيلة تحطيمها، وخاصة إذا كان المجرم مراهقا[1].

المبحث الثاني

تكييف الجريمة المعلوماتية

يقتضي أمر تحديد تكييف الجريمة المعلوماتية العمل على معرفة أساليب ارتكابها، وخاصة معرفة الأركان التي تقوم عليها لأن تخلف إحداها سيؤدي إلى انتفاء الجريمة (المطلب الأول).

وتقسم تصنيف الجريمة المعلوماتية على أصناف، فمنها جرائم واقعة على الأشخاص، جرائم واقعة على الأموال وجرائم واقعة على أمن الدولة (المطلب الثاني).

المطلب الأول

أساليب ارتكاب الجريمة المعلوماتية وأركانها

يعتمد الجناة في ارتكاب الجريمة المعلوماتية أساليب في غاية التعقيد، لا يسهل على الجهات المختصة، لدى مختلف الدول، مواجهتها (الفرع الأول).

تمثل تلك الأساليب الأفعال المادية التي تكون الركن المادي للجريمة، غير أنها لا تكتمل إلا بتحقق الركن المعنوي (الفرع الثاني).

---

[1]- لعاقل فريال ،مرجع سابق ،ص 26.

الفرع الأول

أساليب ارتكاب الجريمة المعلوماتية

تتمثل أهم أساليب ارتكاب الجريمة المعلوماتية فيما يلي:

أولا- الاختراق:

يقصد به الدخول إلى جهاز طرف آخر بدون إذن منه[1]، وذلك من أجل إطلاع المخترق بمعطيات الضحية، وعادة ما يتم ذلك عن بعد[2].

ويستخدم المجرم عدة وسائل للاختراق، منها[3]:

1- الإختراق عن طريق إستعمال نظم التشغيل.

2- الاختراق باستخدام برامج المسح والنسخ.

ثانيا- الفيروسات:

يعد استعمال فيروسات الحاسب أهم وسائل ارتكاب الجريمة المعلوماتية، تضر بالجهاز ومحتوياته. فمجرد فتح برنامج حامل لفيروس أو لرسالة بريدية مرسل معها فيروس سيؤدي إلى تخريب البيانات والبرامج الموجودة فيه[4]. ومن بين أهم الفيروسات المستعملة، نذكر منها ما يلي:

1- فيروسات التلاعب بالبيانات:

يدخل هذا النوع من الفيروس إلى البرنامج للحصول على معلومات إما قصد تعديلها أو إلغائها، ومن أمثلته: فيروس الجنس، فيروس القردة وفيروس سارز[5].

2 -القنبلة المعلوماتية:

يقسم هذا الفيروس إلى نوعين هما[6]:

---

[1]- محمد بن عبد الله بن علي المنشاوي، **جرائم الانترنت في المجتمع السعودي**، مذكرة ماجستير، كلية الدراسات العليا، الرياض، 2003، ص57.

[2]- محمد خليفة، مرجع سابق، ص 40 و41.

[3]- محمد خليفة،مرجع سابق، ص 42 و43.

[4]- محمد بن عبد الله بن علي المنشاوي، مرجع سابق، ص 61.

[5]- مليكة عطوي،مرجع سابق،ص 23 و24.

[6]-مليكة عطوي، مرجع سابق، ص 25.

أ- القنبلة المنطقية:

يستعمل لتغيير برامج نظام معين في لحظة محددة، وذلك إما لتدميره أو تفسير المعلومات والبرامج المخزونة فيه[1].

ب- القنبلة الزمنية أو الموقوتة:

تستعمل لأعمال تخريبية في مدة محددة تقاس بالساعة، اليوم والسنة. والقنبلة الزمنية هي عبارة عن برامج خفية تدمر وتتلف بها المعلومات وبرامج الأنظمة الآلية[2].

3- برامج الدودة:

ينتقل هذا الفيروس عبر شبكة الانترنت، ويتصف بقدرته على إيقاف نظام الحاسب الآلي كليا، وذلك عن طريق استغلال أي فراغ في نظام التشغيل كي يتنقل من حاسب إلى آخر[3].

الفرع الثاني

أركان الجريمة المعلوماتية

تتطلب دراسة الجريمة المعلوماتية بيان الأركان الواجب توفرها لقيامها، وهو ما سنبرزه فيما يلي:

أولا- الركن المفترض:

يعتبر الركن المفترض أول ركن يجب توفره للتمكن من البحث عن أركان الجريمة المعلوماتية. ولتحديد مفهومه يجب أن نتعرض إلى العناصر المكونة له، وهي كل من نظام المعالجة الآلية والحماية المقررة له.

1- تعريف نظام المعالجة الآلية للمعطيات:

يمثل هذا المصطلح تعبيرا تقنيا يصعب على رجل القانون إدراك حقيقته بسهولة. فلم يعرف المشرع الجزائري، على غرار نظيره الفرنسي، نظام المعالجة الآلية للمعطيات، بل أوكل مهمة ذلك إلى الفقه والقضاء.

---

[1]- حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة ماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة باتنة،2012، ص 164 و165.

[2]- حمزة بن عقون، مرجع سابق، ص 165.

[3]- مليكة عطوي،مرجع سابق،ص26.

فعرفه الفقه الفرنسي: " **كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، تتكون كل منها من الذاكرة والبرامج و المعطيات وأجهزة الإدخال و الإخراج، وأجهزة الربط، التي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات وعليه يكون هذا المركب خاضع لنظام الحماية الفنية** ".

أورد الفقه الفرنسي تلك العناصر، المادية منها والمعنوية، على سبيل المثال لا الحصر، إذ يمكن حذف بعض العناصر واستبدالها بعناصر جديدة[1].

ويتحقق نظام المعالجة الآلية للمعطيات بإرسال إشارة كهربائية نحو وحدة المعالجة المركزية، التي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراء، التي تقوم، هي الأخرى، بالبحث بهدف تسجيلها في ذاكرة القراءة والكتابة[2].

2- الحماية الفنية لأنظمة المعالجة الآلية للمعطيات:

نشب خلاف حول ضرورة وجود حماية أمنية لنظام المعالجة الآلية للمعطيات من عدمه كشرط للتمتع بالحماية الجنائية.

تجدر الإشارة إلى أنه لم يضع نص المادة 394 مكرر، من تقنين العقوبات الجزائري، شرط خضوع النظام للحماية الفنية ليتمتع بالحماية الجنائية، على عكس نص المادة 1/323، من تقنين العقوبات الفرنسي، الذي اشترطه[3].

ثانيا- خصوصية أركان الجريمة المعلوماتية:

يتوقف أمر تحقق كل جريمة على توفر أركانها، والأمر نفسه بالنسبة إلى الجريمة المعلوماتية، غير أن أركانها تتميز عن غيرها من الأركان التي تقوم عليها الجرائم الأخرى، وهو ما سنبينه فيما يلي:

1- الركن المادي للجرائم بصفة عامة:

يجب أن تتوفر العناصر، التالي بيانها، ليتكون الركن المادي لأي جريمة، وهي:

---

[1]-أمال قارة ،الجريمة المعلوماتية،مرجع سابق،ص33.

[2]-لعاقل فريال،مرجع سابق،ص28.

[3]-لعاقل فريال،مرجع نفسه،ص30.

أ-**النشاط أو السلوك الاجرامي:** هو السلوك أو النشاط الذي يقوم به الجاني لتحقيق غاية ما ويحدد له القانون العقاب الواجب التطبيق، فلا جريمة بدون ركن مادي[1].

ب-النتيجة الإجرامية: تتمثل في الأثر المادي الذي يحدثه السلوك الإجرامي في العالم الخارجي[2].

ج- الرابطة السببية: تتمثل في الفعل الذي يربط بين النشاط والنتيجة، أي أن يكون السلوك الإجرامي هو الذي أدى مباشرة إلى حدوث نتيجة[3].

2- الركن المادي في الجريمة المعلوماتية:

يتمثل في الدخول والبقاء غير المشروع، وهو على صورتين: صورة بسيطة وصورة مشددة. وتتحقق الصورة البسيطة بمجرد الدخول والبقاء غير المشروع، أما الصورة المشددة فتتحقق باقترانها بظرف مشدد، وذلك إما بتغيير أو محو المعلومات الموجودة داخل النظام[4]، وهو ما سنتناوله فيما يلي:

أ- **فعل الدخول:** يقصد به الدخول إلى العمليات الذهنية التي يؤديها نظام المعالجة الآلية للمعطيات، وذلك من أجل الحصول على معلومات سرية كما هو الشأن بالنسبة إلى أسرار الدولة والحياة الشخصية للأفراد.

يكون الجاني في هذه الحالة من الذين ليس لهم الحق في الدخول إلى النظام والتلاعب بالمعطيات.

ب- فعل البقاء: يقصد بفعل البقاء التواجد بدون وجه حق داخل نظام المعالجة الآلية للمعطيات، وهو فعل مستقل عن فعل الدخول ومعاقب عليه[5].

---

[1]- خالد ممدوح إبراهيم،مرجع سابق، ص 382 و383.

[2]- محمد على العريان، مرجع سابق، ص 176.

[3]- صغير يوسف،مرجع سابق، ص66.

[4]- أمال قار ة، الجريمة المعلوماتية،مرجع سابق ،ص 41 و42.

[5]- انظر في ذلك: تخروبت فوضيل: " جرائم المعلوماتية "، مجلة المحاماة، ناحية تيزي وزو، عدد 11، 2015، ص 51.

وتجدر الإشارة إلى أن القانون لا يعاقب الشخص على الدخول إلى النظام إذا تم عن طريق الخطأ بشرط الانسحاب مباشرة بعد الدخول، وإذا بقي داخله فهو بقاء غير مشروع ومعاقب عليه إذ توفر الركن المعنوي[1].

توجد عدة أفعال أخرى تشكل الركن المادي للجريمة المعلوماتية، ويمكن تقسيمها إلى مجموعتين، وهما كالتالي:

المجموعة الأولى: أفعال الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات: نصت المادتين 5 و8 من الاتفاقية الدولية للإجرام المعلوماتي على هذا النوع من الاعتداء[2]، في حين أغفل المشرع الجزائري ذلك، إذ أورد فقط نصا خاصا بالاعتداء على المعطيات الموجودة بداخل النظام.

واكتفى بتعريف سير نظام المعالجة الآلية، بمقتضى القانون رقم 04/09، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما يلي: " **عملية عرض للوقائع أو للمعلومات أو للمفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها** "[3].

وتشمل أفعال الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات فعلين هما:

– **فعل التعطيل (العرقلة):** لم يشترط المشرع أن يتم التعطيل بوسيلة مادية، فيمكن أن يتم بأية وسيلة تكن، كتحطيم أسطوانة[4].

– **فعل الإفساد:** يقصد به كل فعل يؤدي إلى تعطيل نظام المعالجة الآلية للمعطيات، و يجعله غير صالح للاستعمال السليم، وهو ما يؤدي إلى ظهور نتائج غير صحيحة[5].

---

[1]- أمال قارة،الجريمة المعلوماتية، مرجع سابق، ص ص42-44.

[2]- لعاقل فريال، مرجع سابق، ص 34.

[3]- راجع نص المادة 2 فقرة ج من القانون رقم 04/09 المؤرخ في 2009/8/5.

[4]- تحروبت فوضيل، مرجع سابق، ص 52.

[5]- لعاقل فريال، مرجع سابق، ص 35.

المجموعة الثانية: أفعال الاعتداء العمدي على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات: يتجسد السلوك الإجرامي في هذا النوع من الاعتداء بارتكاب واحد من الأفعال التالية:

- **فعل الإدخال:** يعني إضافة معطيات غير صحيحة إلى نظام الحاسب الآلي، ويتم ذلك عن طريق الاستعمال التعسفي لبطاقات السحب أو الائتمان، سواء كان ذلك بفعل صاحبها أو بفعل الغير.

ويتحقق ذلك الفعل أيضا بإدخال برنامج غريب (فيروس، قنبلة معلوماتية زمنية)، أو بإضافة معلومات جديدة[1].

- **فعل التعديل:** يقصد به استعمال معطيات موجودة داخل النظام أو تغييرها جزئيا أو كليا. وهو الفعل الذي يتم بتعديل البرامج والتلاعب بها[2].

- **فعل المحو:** يعني إزالة خصائص مسجلة على دعامة موجودة داخل النظام بطمسها، لأن الإزالة تفترض الوجود السابق لعملية الإدخال[3].

3- الركن المعنوي للجريمة المعلوماتية:

سنتناول الركن المعنوي للجريمة المعلوماتية لكل من الأفعال المشكلة للركن المادي، التي سبق الإشارة إليها أعلاه، كما يلي:

أ- الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات: يقوم الركن المعنوي لفعلي الدخول والبقاء بشرط توفر القصد الجنائي، من علم وإرادة. والمقصود بالقصد الجنائي في هذا المقام هو الغش[4]. ولا يتوفر الركن المعنوي في الفعلين المذكورين إذا كانا مسموحين بهما[5].

يتطلب القصد الجنائي العام أن يكون الجاني على دراية بأن تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات غير مشروعة وخطيرة . أما في حالة عدم علمه بذلك

---

[1]- آمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 121 و122.

[2]- لعاقل فريال، مرجع سابق، ص 36.

[3]- محمد خليفة، مرجع سابق، ص 184.

[4]- راجع نص المادة 394 مكرر فقرة 1 من تقنين العقوبات.

[5]- محمد خليفة ،مرجع سابق، ص 21.

ينتفي القصد الجنائي[1]. وعلاوة على ذلك، فيجب أن تتجه إرادة الجاني إلى الدخول أو البقاء غير المشروع[2].

ب- الركن المعنوي لفعل الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات: يتطلب مثل هذا الاعتداء، الذي يأخذ صورة العرقلة أو صورة إفساد النظام، توفر القصد الجنائي في الفاعل، أي أن نيته موجهة للإضرار بسير نظام المعالجة الآلية للمعطيات[3].

ج- الركن المعنوي لفعل الاعتداء العمدي على المعطيات:

يشترط لقيام جريمة الاعتداء على المعطيات، أن تكون عمدية، فيتخذ فيها الركن المعنوي صورة القصد الجنائي العام، فيجب أن يكون الجاني عالما أن أفعال الإدخال، التعديل والمحو، يترتب عليها تلاعب في المعطيات، أي أن الهدف منها هو الغش[4].

المطلب الثاني

تصنيف الجريمة المعلوماتية

تهدد الجريمة الإلكترونية شتى القطاعات، الأمر الذي جعل تصنيفها يمتاز بالصعوبة على عكس الجريمة التقليدية.

تضاربت الآراء الفقهية حول تصنيف هذا النوع من الجرائم نظرا لصعوبة حصرها بصفة دقيقة ولحداثة ظهورها وسرعة انتشارها.

وجرت العادة على تصنيف الجرائم المعلوماتية إلى ثلاثة أنواع: تلك الواقعة على الأشخاص (الفرع الأول)، تلك الواقعة على الأموال (الفرع الثاني)، وأخيرا تلك الواقعة على أمن الدولة (الفرع الثالث).

---

[1]- أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 124.

[2]- محمد خليفة ، مرجع سابق، ص 212.

[3]- لعاقل فريال، مرجع سابق، ص40.

[4]- أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 125.

الفرع الأول

الجريمة المعلوماتية الواقعة على الأشخاص

تعد سلامة الأشخاص الهدف، الأول والأسمى والأعلى، من سن مختلف التشريعات والقوانين لغرض حمايتهم من الانتهاكات التي قد يتعرضون لها ماديا أو معنويا أو جسديا.

ومع كل إيجابيات التقدم التكنولوجي على الحياة اليومية للفرد، إلا أنه سلاح فتاك في يد المجرمين، يستعملونه لارتكاب مختلف الجرائم في حق الأشخاص، ومن بينها:

أولا- جرائم القذف والسب:

تعد جرائم القذف والسب الأكثر شيوعا على شبكة الإنترنيت. يتمثل موضوعها في اتخاذ هذه الشبكة للتشهير وإفشاء الأسرار من أجل تشويه شرف وسمعة المجني عليه.

تعتبر شبكة الإنترنيت مسرحا غير محدود لارتكاب تلك الجرائم، إذ تتعدى إلى الدول والمؤسسات أو الشركات من خلال نشر أو إرسال المعلومات الخاصة بتنظيمها الداخلي دون علمها[1].

ثانيا- جريمة التهديد:

يقصد بالتهديد عامة، زرع الخوف في النفس بالضغط على إرادة الإنسان، و تخويفه من ضرر ما سيلحقه، أو يلحق غيره له صلة به.

ويمثل التهديد عبر البريد الإلكتروني وسيلة مستحدثة لزرع الرعب في نفوس الضحايا، فيبعث الجاني رسالة إلكترونية للضحية مصحوبة بعبارات الخوف والترهيب لمتلقيها[2].

---

[1]- رابحي أحسن: الجريمة الإلكترونية: النقطة المظلمة بالنسبة لتكنولوجية المعلومات "، المجلة الجزائرية للعلوم القانونية، الاقتصادية والسياسية، عدد 1، كلية الحقوق، جامعة الجزائر، مارس 2011، ص 228 و229.

[2]- سمية مرغيش، مرجع سابق، ص 27.

ثالثا: انتحال الشخصية:

تعني هذه الجريمة استخدام شخصية شخص آخر للاستفادة من سمعته أو ماله أو صلاحيته. وتتخذ جريمة انتحال الشخصية عبر الإنترنيت أحد الأسلوبين: إما انتحال شخصية الفرد أو انتحال شخصية المواقع.

يزداد خطر تكنولوجيا المعلومات من خلال ارتكاب جريمة الانتحال و لاسيما عند إبرام صفقات تجارية بأموال كبيرة مملوكة للغير، مما يؤدي إلى خسائر فادحة للضحايا، إذ هي سرقة يعاقب عليها القانون[1].

الفرع الثاني

الجريمة المعلوماتية الواقعة على الأموال

أدت وسيلة التداول المالي على شبكة الانترنت، إلى استغلال المجرمين لها بطريقة غير شرعية بارتكاب جرائم تمس بالأموال، ومن أهمها، ما يلي بيانه:

أولا- جريمة السرقة والسطو على أعمال البنوك:

تنص المادة 1/350 من تقنين العقوبات على ما يلي:

" **كل من اختلس شيئا غير مملوك له يعد سارقا** ". غير أن المشرع الجزائري، بمقتضى هذا النص، عرف السرقة بصفة عامة فقط.

يمكن أن نعرف السرقة المعلوماتية بأنها تلك التي تتم عن طريق اختلاس البيانات وقرصنة البرامج من أجل الاستفادة منها للحصول على مزايا مالية بطريقة غير شرعية.

وتعرف جريمة السطو على أعمال البنوك بأنها تلك العملية التي يعتمدها الجاني، من خلال شبكة الانترنت، لتحويل الأموال من الحسابات الخاصة للبنوك إلى حسابات أخرى بطريقة غير شرعية.

يتم ذلك بإدخال بيانات مزيفة أو بمسحها أو بتعديلها بهدف سرقة الأموال أو إتلافها أو نقلها. وعادة ما يتم اختلاس جزء صغير من أموال البنوك الطائلة لكي لا تلاحظ النقص الموجود في حساباتها[2].

---

[1]- جعفر جاسم الطائي، مرجع سابق، ص 197.

[2]- صغير يوسف، مرجع سابق، ص 47 و48.

ثانيا- جرائم التزوير:

يقصد به الاعتداء على المعلومات المخزنة في ذاكرة الحاسب الآلي إما بتغيرها، بتحريفها، أو التلاعب بها كتزوير البريد الإلكتروني أو تزوير الهوية[1].

الفرع الثالث

الجريمة المعلوماتية الواقعة على أمن الدولة

أصبحت الجريمة المعلوماتية اليوم تشكل ظاهرة خطيرة في المجتمعات الإنسانية، بل تعداه الأمر إلى أن باتت أيضا تهدد أمن الدولة.

يجب على رجال القانون مكافحة كل الجرائم التي تهدد أمن الدولة، بكل الطرق والوسائل، ومن بين تلك الجرائم، ما يلي:

أولا- الجريمة المنظمة:

يرتكب هذا النوع من الجرائم مجموعة من المجرمين، في إطار نظام في غاية التعقيد والدقة، إذ يسنون قواعد قانونية يلتزمون بها من أجل تنفيذ أنشطتهم الإجرامية.

استغلت عصابات الجريمة المنظمة الوسائل المتاحة في شبكة الانترنت في تخطيط وتوجيه العمليات إلى أهدافها بكل بساطة وسهولة، فالجريمة المنظمة عبر شبكة الانترنت غير مقيدة سواء من الناحية الزمنية أو المكانية. أصبح، نتيجة لذلك، انتشارها واسعا لا تحدها الحدود الجغرافية[2].

يعتبر الترابط الموجود بين الجريمة المنظمة وشبكة الانترنت ترابطا طبيعيا، لأنها توفر الوسائل والأهداف، مما يحفز على استغلالها لتحقيق أرباح مالية طائلة[3].

ثانيا: الجريمة الإرهابية:

يعد الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعدة عوامل اجتماعية، سياسية وتكنولوجية.

---

[1]- جعفر حسن جاسم الطائي، مرجع سابق، ص 136.

[2]- صغير يوسف، مرجع سابق، ص 56.

[3]- سمية مرغيش، مرجع سابق، ص 33 و34.

ترتكب أعمال الإرهاب عبر شبكة الانترنت، على غرار الجرائم الأخرى، عن طريق إنشاء مواقع مزيفة (افتراضية) تمثل منظمات إرهابية[1].

تقوم الجماعات الإرهابية، بتجنيد عناصر جديدة، لمساعدتها على ارتكاب الجرائم. وتستعين تلك الجماعات بفئة من الأشخاص ليست لهم القدرة على استيعاب أنهم ضمن منظمة إرهابية.

يتم ذلك عن طريق إعلان المنظمة الإرهابية، على موقعها الالكتروني، عن وجود مناصب شغل شاغرة للشباب.

تلجأ الجماعات الإرهابية، إضافة إلى ما سبق ذكره، إلى استعمال شبكة الانترنت لأغراض الدعاية، الترويج والتهديد[2].

ثالثا- جريمة التجسس:

تعرف هذه الجريمة بأنها الإطلاع على بيانات ومعلومات الغير، الموجودة في جهاز حاسوبه، بدون علم صاحبها[3]. ويتم التجسس بثلاث طرق هي: برامج المحادثة، البريد الإلكتروني أو زيارة شخص لمواقع مجهولة[4]. ويقسم التجسس إلى ثلاثة أنواع هي: التجسس السياسي، التجسس العسكري والتجسس الاقتصادي .

ينتهج مرتكبو جريمة التجسس أسلوب اختراق الأنظمة للعبث بمحتوياتها وإتلافها، مما مكن عديد الدول من الحصول على أسرار معلومات دولة ما وإفشائها لدولة أخرى، أو استغلالها بما يضر المصلحة الوطنية للدولة ضحية التجسس[5].

---

[1]- سمية مرغيش، مرجع سابق، ص 34.

[2]- صغير يوسف، مرجع سابق، ص ص 55-56.

[3]- سمية مرغيش، مرجع سابق، ص35.

[4]- جعفر حسن جاسم الطائي، مرجع سابق،ص ص199- 198 .

[5]- صغير يوسف،مرجع سابق، ص 57.

الفصل الثاني

مكافحة الجريمة المعلوماتية في التشريع الجزائري

استجابت عدة دول لوضع حماية جزائية للمعلوماتية، فأصدرت فرنسا مثلا القانون رقم 19/88 بشأن الغش المعلوماتي.

وصادقت الجزائر على بعض الاتفاقيات الدولية المتعلقة بمكافحة هذه الجريمة، وأصبحت من النظام القانوني الجزائري ومن بينها:

- اتفاقية باريس لحماية الملكية الصناعية[1].
- الاتفاقية العالمية حول حق المؤلف لسنة 1952 والمراجعة في باريس 1971/07/24[2].
- اتفاقية برن لحماية المصنفات الفكرية والأدبية لسنة 1886[3].

تتطلب دراسة مكافحة الجريمة المعلوماتية التطرق إلى جانبين: جانب متعلق بالمعالجة الموضوعية لتلك المكافحة (المبحث الأول)، وجانب آخر متعلق بالإطار الإجرائي المخصص لها (المبحث الثاني).

---

[1]- انظر النص الكامل للاتفاقية على الرابط التالي:
www.lasportal.org/ar/intellectualproperty/.../باريس/20اتفاقية.pdf

[2]- انظر النص الكامل للاتفاقية على الرابط التالي:
http://www.wipo.int/wipolex/ar/other_treaties/text.jsp?fil_id=193359

[3]- انظر النص الكامل للاتفاقية على الرابط التالي:
http://www.wipo.int/treaties/ar/ip/berne/

المبحث الأول

الإطار الموضوعي للجريمة المعلوماتية

يواجه القانون الجنائي تحديا بسبب صعوبة مواجهة الجريمة المعلوماتية. فيجد القاضي الجزائي نفسه مقيدا بمبدأ الشرعية، إذ لا يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى وإن هي أفعال خطيرة، كما هو الشأن بالنسبة إلى إساءة استخدام المنظومة المعلوماتية.

تثير مسألة الحماية الجنائية من الجريمة المعلوماتية إشكالية مدى كفاية القواعد المقررة في الجرائم التقليدية، وهو ما استدعى وضع نصوص حديثة سواء في كل من تقنين العقوبات (المطلب الأول) وقانون الملكية الفكرية (المطلب الثاني).

المطلب الأول

محاربة الجريمة المعلوماتية في إطار تقنين العقوبات

تدارك المشرع الجزائري الفراغ القانوني، من خلال تعديل تقنين العقوبات، باستحداث نصوص تجرم الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، بموجب القانون رقم 15/04.

ركز المشرع الجزائري على الاعتداءات الماسة بالأنظمة المعلوماتية (الفرع الأول)، بينما أغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي (الفرع الثاني)

الفرع الأول

جريمة المساس بأنظمة المعالجة الآلية للمعطيات

ظهرت ضرورة تدخل التشريع نظرا لتفاقم الاعتداءات الواقعة على الأنظمة المعلوماتية، خاصة أمام ضعف الحماية الفنية. فتم وضع أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08[1].

---

[1] – **الاتفاقية الدولية حول الإجرام المعلوماتي** التي أبرمت بتاريخ 2001/11/08، من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23، انظر النص الكامل للاتفاقية على الرابط التالي:
http://www.4shared.com/file/82161420...-27_.html

استدرك المشرع الجزائري الفراغ القانوني، من خلال تعديل تقنين العقوبات، في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 256/66 انتحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات** " ويشمل المواد من 394 مكرر إلى 394 مكرر 7[1].

أولا – الأفعال المعاقب عليها في تقنين العقوبات:

جرم المشرع الجزائري مجموعة من الأفعال الماسة بسلامة أنظمة المعالجة الآلية للمعطيات، وهي:

1- الاعتداء بالدخول أو البقاء غير المشروع:

يعد فعل الدخول والبقاء إلى نظام المعالجة الآلية للمعطيات أو المعلومات من أخطر الجرائم التي يمكن أن تصيب هذه الأنظمة أو المواقع.

وقد جرم تقنين العقوبات الجزائري فعل الدخول عن طريق الغش إلى مواقع إلكترونية أو البقاء غير المشروع فيها[2].

2 – الإعاقة أو تحريف تشغيل نظام معالجة البيانات:

جرم المشرع الجزائري كل فعل يهدف إلى إعاقة أو تحريف أو إفساد تشغيل نظام معالجة البيانات.

يشترط، بالإضافة إلى فعل الدخول للنظام أو البقاء فيه، إحداث استمرار في تخريب نظام تشغيل نظام معالجة البيانات[3]، سواء بتعطيله، بإفساده أو تغييبه. ويكون ذلك بأية طريقة تكن، سواء بالإعاقة المادية، كإتيان أعمال عنف على أجهزة الحاسب، أو بالإعاقة المعنوية كإدخال فيروس على البرامج [4].

3– صور أخرى للغش المعلوماتي:

---

[2] – حمودي ناصر: " **التنظيم القانون لظاهرة المعلوماتية في الجزائر: الإنجازات والتحديات** "، المجلة النقدية للقانون والعلوم السياسية، عدد 2، كلية الحقوق والعلوم السياية، جامعة مولود معمري، تيزي وزو، 2012، ص 208 و209؛ انظر نص المادة 394 مكرر من تقنين العقوبات.

[3] – قريم سكورة، **المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري**، مذكرة لنيل شهادة ماستر في القانون، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة البويرة، 2015، ص 36.

[4] – حمودي ناصر، مرجع سابق، ص 210.

جرم نص المادة 394 مكرر 2 من تقنين العقوبات الأفعال التالية: حيازة أو إفشاء أو نشر أو استعمال، لأي غرض يكن، المعطيات المتحصل عليها من إحدى الجرائم.

ونصت، من جانبها، الاتفاقية الدولية المتعلقة بالإجرام المعلوماتي على جريمة الاستخدام غير المشروع للمعطيات ومعاقبة كل من يقوم عمدا بإنتاج أو استيراد أو توزيع أو استعمال برنامج الحاسوب بغرض ارتكاب جريمة أو استعمال كلمة سر أو رموز وصول[1].

ثانيا–الجزاءات المقررة بالنسبة للجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات:

تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على كل من الشخص الطبيعي والشخص المعنوي.

1 – العقوبات المطبقة على الشخص الطبيعي: تتمثل فيما يلي:

أ – **العقوبات الأصلية:** يتبين باستقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية وجود تدرج داخل النظام العقابي، وهو كالتالي:

– **الدخول والبقاء بالغش(الصورة العادية):** العقوبة المقررة هي من 03 أشهر إلى سنة حبس و50.000 دج إلى 100.000 دج، في حالة ما إذا كانا يشكلان جريمة بسيطة.

– **الدخول والبقاء بالغش(الصورة المشددة):** العقوبة تضاعف إذ ترتب عن هذه الأفعال تغيير أو حذف لمعطيات منظومة معلوماتية مما يشكل ظرفا مشددا، وتكون العقوبة بالحبس من ستة أشهر إلى سنتين وغرامة من 500.000 دج إلى 4000000 دج[2].

– **الاعتداء العمدي على المعطيات:** طبقا لتقنين العقوبات، فالعقوبة المقررة للاعتداء العمدي على المعطيات، الموجودة داخل النظام، هي الحبس من ستة أشهر إلى ثلاثة سنوات وغرامة من 500000 دج إلى 2000000 دج. أما العقوبة المقررة، لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، إفشاء أو حيازة أو نشر أو

---

[1]- راجع نص المادة 6 من الاتفاقية.

[2] – انظر نص المادة 394 مكرر/1 من تقنين العقوبات.

استعمال المعلومات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، هي الحبس من شهرين إلى ثلاثة سنوات وغرامة من 1000000 دج إلى 5000000 دج [1].

ب – العقوبة التكميلية: نص تقنين العقوبات على العقوبات التكميلية التي يحكم بها وهي:

– **المصادرة:** تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية[2].

– **إغلاق المواقع:** تلك التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية[3].

– **إغلاق المحل أو مكان الاستغلال:** تطبق في حال ارتكاب الجريمة بعلم مالك المحل أو مكان الاستغلال كإغلاق مقهى الكتروني[4].

2 – العقوبات المطبقة على الشخص المعنوي:

نصت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي مساءلة الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أم شريكا أم متدخلا. كما يسأل عن الجريمة التامة أو الشروع فيها، بشرط أن تكون قد ارتكبت لحساب الشخص المعنوي وبواسطة أحد ممثليه أو أعضائه[5].

---

[1] – راجع نص المادة 394 مكرر 2 من تقنين العقوبات؛ لمزيد من التفاصيل انظر: حابت آمال، **التجارة الالكترونية في الجزائر**، رسالة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015، ص 397؛ صالح شنين: " **الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري** "، المجلة الأكاديمية للبحث القانوني، عدد 01، 2010، ص 73.

[2]- راجع نص المادة 157 من الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة؛ انظر أيضا، صالح شنين، مرجع سابق، ص 74.

[3] – راجع نص المادة 394 مكرر 6 من تقنين العقوبات؛ سوير سفيان، مرجع سابق، ص 99.

[4] – راجع نص المادة 394 مكرر 6 من تقنين العقوبات؛ سوير سفيان، مرجع سابق، ص 99.

[5] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 129.

نشير إلى أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين سواء بصفتهم فاعلين أم متدخلين أم شركاء في الجريمة نفسها.

قضى نص المادة 18 مكرر من القانون رقم 15/04، المتضمن تعديل تقنين العقوبات، بأن العقوبات المطبقة على الشخص المعنوي في مواد الجنح والجنايات، وهي:

– الغرامة التي تساوي من مرة إلى 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

– حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها، لمدة لا تتجاوز 5 سنوات.

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات، المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات مع مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها[1].

3– عقوبة الاتفاق الجنائي:

أخذ المشرع الجزائري بمبدأ المعاقبة على الاتفاق الجنائي[2]. العلة من ذلك، هى تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة تمس بالأنظمة المعلوماتية.

تتم هذه الجرائم عادة في إطار مجموعات، كما أن المشرع، رغبة منه في توسيع نطاق العقوبة، فقد أخضع الأعمال التحضيرية التي سبق البدء في تنفيذها للعقوبة إذا ما تمت في إطار اتفاق جنائي[3].

---

[1] – راجع نص المادة 394 مكرر 4 من تقنين العقوبات؛ أمال قارة، **الحماية في التشريع الجزائية للمعلوماتية الجزائري**، مرجع سابق، ص ص 129 – 130؛ سوير سفيان، مرجع سابق، ص 100.

[2] – انظر المادة 394 مكرر 5 من تقنين العقوبات.

[3] – حابت أمال، مرجع سابق، ص 399.

يعاقب القانون على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإذا كانت تحتوي على أكثر من جريمة واحدة التي يتم التحضير لها فتكون لها عقوبة الجريمة الأشد[1].

4 – عقوبة الشروع في الجريمة:

نص تقنين العقوبات على عقوبة الشروع في ارتكاب الجريمة الماسة بالأنظمة المعلوماتية[2].

ويهدف المشرع الجزائري من ذلك إلى توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية[3].

الفرع الثاني
جريمة التزوير المعلوماتي

اعتبرت الاتفاقية الدولية المتعلقة بالإجرام المعلوماتي أن واقعة ما تعد تزويرا إذا تضمنت تعديلا أو خلقا لمعطيات أو برامج غير مرخص بإنشائها أو تعديلها، بحيث تصبح قيمتها في الإثبات مختلفة فيما يتعلق بالمعاملات القانونية على تلك البيانات التي تعرضت للتزوير بقصد الإضرار بالغير[4].

وسنتعرض فيما يلي بيانه، على التوالي، إلى تعريف بجريمة التزوير المعلوماتي وموقف المشرع الجزائري منها.

أولا – تعريف بجريمة التزوير المعلوماتي:

تمثل المحررات محل جريمة التزوير. والمحرر هو كتابة مركبة من حروف أو علامات تدل على فكرة معينة، وللمحرر ويتخذ شكلا بحيث تكون الكتابة منسوبة لشخص

---

[1] – أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 131.

[2] – راجع نص المادة 394 مكرر 7 من تقنين العقوبات؛ حابت أمال، مرجع سابق، ص 399.

[3] – أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 133.

[4] – راجع نص المادة 7 من الاتفاقية؛ لعاقل فريال، مرجع سابق، ص 46 و47.

معين[1]. وتخرج المحررات المعلوماتية عن المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها[2].

يأخذ التزوير المعلوماتي، الذي يقع على المعلومات والمعطيات، التي يحتويها النظام المعلوماتي إحدى الصور التالية:

1 – **إدخال معلومات وهمية:** تتمثل في إدخال معلومات غير صحيحة إلى النظام المعلوماتي، لم تكن موجودة من قبل، وغالبا ما يتم إدخال هذه البيانات يهدف التشويش على صحة المعلومات أو البيانات القائمة[3].

2 – إدخال معلومات مزورة: يعني التلاعب بالبيانات أو بالمعلومات داخل النظام المعلوماتي بهدف تغيير حقيقتها، ويتم ذلك إما عن طريق تعديل هذه المعلومات أو من خلال محو جزء أو عدة أجزاء منها، أي تزوير المستندات المخزنة داخل الكمبيوتر ووضع معلومات بديلة للمعلومات الحقيقية وتزييف المخرجات. وتستهدف هذه الجريمة البيانات الممثلة للمستحقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات [4].

ينحصر النشاط الإجرامي في هذه الجريمة في تعديل أو تغيير حقيقة المعلومات واستبدالها بما يخالفها بغية الإضرار بالغير ومراكزهم القانونية الثابتة في تلك المحررات، وفي حالة انتفاء قواعد البيانات أو البرنامج لا يعد تزويرا بل يقع تحت طائلة نصوص التقليد الوارد في قانون حقوق المؤلف[5].

ثانيا – موقف المشرع الجزائري من التزوير المعلوماتي:

نص تقنين العقوبات على التزوير الخاص بالمحررات في القسم الثالث، الرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث منه، في المواد من 124

---

[1] – أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 238.

[2] – لعاقل فريال، مرجع سابق، ص 48.

[3] – عقون حمزة، مرجع سابق، ص 170.

[4] – عقوة حمزة، المرجع مرجع سابق، ص 170 و 171.

[5] – قارة أمال، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 139.

إلى 229، التي تشترط المحرر في جريمة التزوير. إلا أنه لم يتخذ موقفا لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير[1].

وحبذا لو أن المشرع الجزائري أورد نصا خاصا بالتزوير المعلوماتي، مثلما فعله نظيره الفرنسي في المادة 3/462 بنصها: " يعاقب بالحبس لمدة تتراوح بين سنة وخمس سنوات، وبالغرامة التي تتراوح ما بين ألف فرنك إلى 200000 فرنك ".

رغم علم المشرع الجزائري بالفراغ القانوني في مجال الإجرام المعلوماتي، إلا أنه أغفل تجريم التزوير المعلوماتي، كما أنه لم يتبنَى الرأي الذي تبنته التشريعات الحديثة، التي وسعت من مفهوم المحرر ليشمل كافة صور التزوير الحديثة[2].

وعليه، فقد تم الاقتراح، على المشرع الجزائري، إضافة نص إلى باب التزوير في المحررات يتناول فيه التزوير المعلوماتي على النحو التالي: " **كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر**"[3].

المطلب الثاني

قمع الجريمة المعلوماتية من خلال قانون الملكية الفكرية

رأينا البحث عن مدى إمكانية الحماية من الجريمة المعلوماتية في نصوص قانون الملكية الفكرية نظرا لنسبة الحماية المقررة من خلال النصوص التقليدية في تقنين العقوبات، وذلك بتقسيم حقوق الملكية الفكرية إلى قسمين: قسم يتعلق بالحماية في إطار قانون الملكية الصناعية (الفرع الأول)، وقسم يتعلق بالحماية في إطار قانون الملكية الأدبية والفنية (الفرع الثاني).

---

[1] – حابت أمال، مرجع سابق، ص 401.

[2] – لعاقل فريال، مرجع سابق، ص 49.

[3] – لعاقل فريال، مرجع سابق، ص 139.

الفرع الأول

قمع الجريمة المعلوماتية من خلال قانون الملكية الصناعية

يشمل قانون الملكية الفكرية عدة مجالات، منها أحكام متعلقة بالعلامات التجارية وأخرى متعلقة ببراءة الاختراع.

أولا – مواجهة الجريمة المعلوماتية من خلال أحكام العلامات التجارية:

نظم المشرع الجزائري أحكام العلامات التجارية بعدة تشريعات، آخرها، كان الأمر رقم 06/03 المؤرخ في 2003/07/19، المتعلق بالعلامات التجارية[1].

تعرف العلامات التجارية بأنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها، أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات، أو المصنوعات أو الخدمات، ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام العام والآداب العامة[2].

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد قام أصحاب البرامج بوضع أسماء مقترنة بهم. فالحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط لكن ليس الأمر كذلك بالنسبة للنسخ المعقد[3].

ثانيا– مواجهة الجريمة المعلوماتية من خلال براءة الاختراع:

عرفت المادة 02 من الأمر رقم 03-07 المؤرخ في 2003/07/19 المتضمن براءة الاختراع، أن الاختراع هو" **عبارة عن فكرة تسمح بإيجاد حل لمشكل محدد في مجال**

---

[1] – الأمر رقم 06/03 المؤرخ في 2003/07/19، **المتعلق بالعلامات التجارية**، ج.ر، عدد 44، صادرة في 2003/07/23.

[2] – حابت أمال، مرجع سابق، ص 402.

[3] – سمية مرغيش، مرجع سابق، ص 62.

التقنية، وفقا لشروط معينة والتي تتمثل في: شرط الابتكار، القابلية للتطبيق الصناعي، شرط الجدة، المشروعية "[1].

يتحصل المخترع، في حالة توفر تلك الشروط، على براءة اختراع. وهي الوثيقة التي تمنحها الدولة للمخترع، فتمنح له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض في مدة محددة، وبشروط معينة، والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية[2].

غير أن السؤال المطروح هو: **هل تستفيد برامج الحاسب من الحماية بواسطة براءة الاختراع؟**

تستبعد التشريعات المعاصرة بصفة عامة البرامج المعلوماتية من مجال الحماية بواسطة الاختراع لأحد السببين التاليين:

- سواء لتجرد البرامج من أي طابع صناعي.

- سواء لصعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة، إذ لا بدّ من توفر شرط الجدة في البرمجيات حتى تكون لدى الجهة التي تقوم بفحص طلبات البراءة. يجب أن تكون هذه الأخير على درجة عالية من الكفاءة والدراية والتميز في المجال التي تتولى بحثه، إذا ما كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا[3].

---

[1] – انظر المادة 2 من القانون رقم 03-07 المؤرخ في 2003/07/19، **المتعلق ببراءة الاختراع**، ج.ر، عدد 4، صادرة في 2003/07/23.

[2] – صغير يوسف، مرجع سابق، ص 105.

[3] – قارة أمال، الجريمة المعلوماتية، مرجع سابق، ص 197.

تجدر الإشارة إلى أن المشرع الجزائري استبعد، بموجب الأمر رقم 07/03، البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع، إذ قضى بأنه لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب[1].

الفرع الثاني

مواجهة الجريمة المعلوماتية من خلال قوانين الملكية الأدبية والفنية:

يتطلب أمر دراسة مواجهة هذه الجريمة، من خلال القوانين المتعلقة بالملكية الأدبية والفنية، خاصة منها القانون رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة[2]، التعرض إلى ما يلي:

أولا – مدى اعتبار البرنامج كموضوع من موضوعات حق المؤلف الجزائري:

يرى المختصون، أنه رغم عدم نص المشرع الجزائري صراحة على حماية البرامج المعلوماتية في إطار حق المؤلف، إمكانية الحماية بدليل الصياغة المرنة عند ذكر المصنفات المشمولة بالحماية.

وعليه، كان من الأفضل النص على البرامج صراحة ضمن قائمة المصنفات المحمية، وذلك ما فعله المشرع بموجب الأمر رقم 05/03 الذي أدمج برامج الإعلام الآلي ضمن المصنفات الأصلية[3].

ونستخلص من خلال استقراء الأمر 05/03 ما يلي:

– أن المشرع الجزائري وسع قائمة المؤلفات المحمية، فأدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي التي تمكن من القيام بنشاط علمي.

---

[1] – راجع نص المادة 7 من الأمر رقم 07/03؛ صغير يوسف، مرجع سابق، ص 106.

[2] – الأمر رقم 05/03، المؤرخ في 2003/07/19، **المتعلق بحقوق المؤلف والحقوق المجاورة**، ج.ر، عدد 44، صادرة في 2003/07/23.

[3] – قارة أمال، **الجريمة المعلوماتية في التشريع الجزائري**، مرجع سابق، ص 138.

– أن مدة الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن لحماية المصنفات الفكرية والأدبية التي حددت مدة دنيا للحماية، مقدرة بـ 50 سنة[1]، وبالتالي هذه المدة تشمل أيضا مصنفات الإعلام الآلي[2].

– تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لا سيما المصنفات المعلوماتية[3]. فكان سابقا فعل التعدي على الملكية الفكرية تجرمه المواد من 390 إلى 394 من تقنين العقوبات لكنه أخرج منه بموجب الأمر 05/03 الذي يقرر عقوبة الحبس[4].

وتجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري، من خلال الأمر رقم 05/03، تعود لأسباب أهمها، أنه من شروط الانضمام إلى المنظمة العالمية للتجارة ضرورة المصادقة على اتفاقية برن وهو ما فعلته الجزائر بموجب المرسوم الرئاسي رقم 341/97[5].

ثانيا – مدى خضوع برامج الحاسب الآلي للحماية الجزائية:

يضمن قانون حق المؤلف الحماية الجزائية لمصنفات الإعلام الآلي، بعد إدماجها صراحة ضمن المصنفات المحمية تطبيقا لبنود اتفاقية جوانب الملكية المتعلقة بالتجارة بغرض الانضمام للمنظمة العالمية للتجارة، وعلى ذلك تدخل برامج الحاسب تحت مظلة الحماية الجزائية لحق المؤلف، وهو ما يستلزم منا دراسة كل من جرائم التقليد وبرامج الحاسب الآلي في التشريع الجزائري والجزاءات المقررة لها.

---

[1] – راجع نص المادة 7 من اتفاقية برن.

[2]-راجع نص المادة 58 من الأمر رقم 05/03.

[3]-راجع نص المادة 153 من الأمر رقم 05/03.

[4] – قارة أمال، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، مرجع سابق، ص 78 و79.

[5] – مرسوم رئاسي رقم 341/97 مؤرخ في 1997/09/13، **يتضمن انضمام الجزائر مع التحفظ إلى اتفاقية بارن لحماية المصنفات الأدبية والفنية** المؤرخة في 1896/06/09 والمتممة في باريس في 1896/05/04 في 1979/09/28.

1 – جرائم التقليد وبرامج الحاسب الآلي في التشريع الجزائري: أدخل المشرع برامج الحاسب الآلي ضمن قائمة المصنفات المحمية، وهو ما يعني أن أي اعتداء يقع على الحق المالي والأدبي لمؤلف البرنامج بشكّل تقليدا. وهذا ما قضى به الأمر رقم 05/03[1].

نستنتج من خلال هذا الأمر وجود جرائم تعتبر من جنح التقليد ويمكن تصنيفها إلى ثلاثة أصناف:

الصنف الأول/ الجنح المتعلقة بالحق المعنوي للمؤلف:

- الكشف غير المشروع عن مصنف أدبي أو أداء فني[2].
- المساس بسلامة المصنف أو الأداء الفني[3].

الصنف الثاني/ الجنح المتعلقة بالحق الأدبي للمؤلف:

- استنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة.
- إبلاغ المصنف أو الأداء الفني للجمهور عن طريق التمثيل أو الأداء العلني أو البث السمعي أو عن طريق التوزيع أو أية وسيلة أخرى لبث الإشارات الحاملة للأصوات أو أي نظام من نظم المعالجة.

الصنف الثالث/ الجنح المشابهة لجنحة التقليد:

- استيراد النسخ المقلدة وتصديرها.
- بيع نسخ مزورة من المصنف.
- تأجير مصنف مقلد أو عرضه للتداول.

نستخلص مما سبق ذكره أن جريمة التقليد تتضمن اعتداء على أحد الحقوق المالية أو الأدبية دون موافقة المؤلف، وأن القصد الجنائي في جريمة التقليد يكون مفترضا[4].

---

[1] – انظر المادة 151 من الأمر رقم 03-05 المؤرخ في 2003/07/19.

[2] -راجع المادة 22 من الأمر رقم 05/03.

[3] – راجع نص المادة 25 من الأمر ذاته؛ قارة أمال، الجريمة المعلوماتية، مرجع سابق، ص 140.

[4] – قارة أمال، مرجع سابق، ص 140.

2 – العقوبات المقررة: ظهرت الحاجة لوضع جزاءات رادعة نظرا لخطورة الجرائم المرتكبة على حق المؤلف ، لذلك قرر المشرع الجزائري، بموجب الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، جزاءات على كل من يعتدي على هذا الحق[1].

وتجدر الإشارة إلى أن الأمر المذكور شدد في العقوبات على النحو التالي:

– للقاضي أن يطبق كعقوبة أصلية الحبس من 06 أشهر إلى 03 سنوات وغرامة قدرها من 500 دج إلى 01 مليون دج سواء قد حصل النشر في الجزائر أو في خارجها[2].

– للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية للإيرادات أو الأقساط المحصلة من الاستغلال غير المشروع لبرنامج (مصنف) أو أداء محمي وكل النسخ المقلدة[3].

– يمكن للقاضي، بناءً على طلب الطرف المدني، الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على ألاّ تتعدى المصاريف قيمة الغرامة المحكوم بها[4].

– للقاضي أن يضاعف العقوبات المقررة وذلك، في حالة العود، مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه لمدة لا تتعدى 06 أشهر، وإذا اقتضى الأمر تقرير الغلق النهائي[5].

تجب الإشارة إلى إجراء هام يتم من خلاله اكتشاف جريمة التقليد وهو ما يعرف بالحجز الناتج عن التقليد، بواسطته يمكن لمؤلف البرنامج المحمي أو ذوي حقوقه المطالبة بحجز الوثائق والنسخ الناتج عن الاستنساخ غير المشروع، ذلك حتى في غياب ترخيص

---

[1] – لعاقل فريال، مرجع سابق، ص 12.

[2]-راجع نص المادة 153 من الأمر رقم 05/03.

[3] – حابت أمال، مرجع سابق، ص 405.

[4]-راجع نص المادة 158 من الأمر رقم 05/03.

[5] – راجع العقوبات المقررة في المواد من 153 إلى 158 من الأمر رقم 05/03؛ قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 92.

قضائي، أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمعطيات.

وببيان جوانب الحماية الجزائية لبرامج الحاسب، من خلال حق المؤلف، فإنه يمكن التوصل إلى أنه من أجل أن تتمتع برامج الحاسب بالحماية، فيجب احترام شروط المصنف المحمي وأهمها شرط الابتكار وشرط الجدة، فإذا تخلفا، افتقدت البرامج الحماية الجزائية المقررة لها[1].

المبحث الثاني

المعالجة الإجرائية للجريمة المعلوماتية وصعوبات مكافحتها

تبنت تشريعات مختلف الدول آليات في سبيل الحد من الآثار التي تخلفها الجرائم المعلوماتية.

يتطلب ذلك وضع إجراءات كفيلة لتحقيق ذلك (المطلب الأول) لمواجهة الصعوبات التي تواجه عملية مكافحة تلك الجرائم (المطلب الثاني).

المطلب الأول

الإجراءات المكرسة في مجال محاربة الجريمة المعلوماتية

تتميز اجراءات مكافحة الجريمة المعلوماتية عن غيرها، بسبب خصوصيتها، لا سيما تلك المتعلقة باجراءات التحري (الفرع الأول). كما أن عملية المكافحة يجب أن تسند إلى جهة مختصة من أجل أن تكون فعالة (الفرع الثاني).

الفرع الأول

إرساء إجراءات تحري خاصة بالجرائم المعلوماتية

وضع المشرع ترتيبات من أجل مكافحة الجريمة الالكترونية بموجب القانون رقم 04/09، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

[1] – لعاقل فريال، مرجع سابق، ص 55.

والاتصال، المتمثلة في كل من إمكانية المراقبة الالكترونية، من جهة، ووسائل تلك المراقبة، من جهة أخرى.

أولا- حالات جواز المراقبة الإلكترونية:

يجوز اللجوء إلى المراقبة الإلكترونية بإذن من السلطة القضائية المختصة في الحالات التالية[1]:

- حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وذلك بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة 6 أشهر قابلة للتجديد.

- حالة الوقاية من اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

- دواعي التحريات والتحقيقات القضائية إذا كانت المراقبة الإلكترونية ضرورية للوصول إلى نتيجة تهم الأبحاث الجارية.

- ضرورة التعاون القضائي الدولي، لاسيما بسبب المشاكل التي تثيرها الجرائم المعلوماتية من حيث الاختصاص القضائي والقانوني، وتتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة، الاتفاقيات الثنائية ومبدأ المعاملة بالمثل. إلا أن هناك قيودا واردة على طلبات المساعدة أوردها. القانون رقم 09-04[2].

ثانيا- وسائل المراقبة الالكترونية: تتمثل وسائل المراقبة التي وضعها المشرع فيما يلي:

---

[1]-راجع نص المادة 4 من القانون رقم 04/09؛ لمزيد من التفصيل، انظر ما يلي:

بوبشير محند أمقران: " **الجوانب القانونية لمكافحة جرائم المعلوماتية والوقاية منها** "، مجلة المحاماة، ناحية تيزي وزو، عدد 11، 2015، ص 16.

[2]-راجع نصي المادتين 18 و19 من القانون رقم 04/09.

1- المعاينة: يقصد بها إثبات مباشر ومادي للآثار المادية التي خلفها إرتكاب الجريمة عن طريق فحصها[1].

يجوز اللجوء إلى المعاينة في كل الجرائم وهو إجراء هدفه الكشف وصيانة العناصر المادية المتعلقة بالجريمة. إذ تفيد في التحقيق الجاري بشأنها[2]. ولا يلتزم المحقق بدعوة محامي المتهم للحضور وإن غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطله [3].

يقوم القائم بالمعاينة بفحص الآثار المادية لبيان مدى صحتها في الإثبات، أما الجرائم الإلكترونية فليس الحال كذلك، حيث يتعذر أن يتخلف عن إرتكابها آثارا مادية. وقد تطول المدة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناتجة عنها إلى التلف، المحو أو التغيير بالعبث بها.

يراعى في معاينة الجريمة الالكترونية ما يلي[4]:

- العناية بملاحظة الطريقة التي تم بها إعداد النظام .
- ملاحظة و إثبات حالة التوصيلات و الكابلات المتصلة بكل مكونات النظام.
- قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات .
- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو المُمزقة و أوراق الكربون المستعملة و الشرائط و الأقراص الممغنطة غير السليمة.

2- التفتيش:

امتنع المشرع الجزائري عن وضع تعريف خاص بالتفتيش، فاعتبره إجراء من إجراءات التحقيق.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية قصد مساعدتها وتزويدها بالمعلومات الضرورية لإنجاز مهمتها. وذلك بتفتيش المنظومة المعلوماتية والمعطيات المخزنة التي أوردها القانون رقم 04/09[1].

---

[1]- حابت أمال،مرجع سابق، ص365.

[2]- صغير يوسف،مرجع سابق، ص 84.

[3]- حابت أمال، مرجع سابق، ص 365.

[4]- حابت أمال، مرجع سابق، ص 365.

يجوز للسلطات القضائية المختصة وضباط الشرطة القضائية في منظومة معلوماتية أو جزء منها وفي المعطيات المعلوماتية المخزنة، ويمكن تمديد التفتيش إلى منظومة معلوماتية أخرى و ذلك بعد إعلام السلطة القضائية المختصة مسبقا بذلك إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى[2].

اعتمد المشرع الجزائري، في تقنين العقوبات، التصنت كوسيلة لإجراء التقتيش في بعض من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[3].

3- الضبط:

تأتي عملية ضبط الأدلة بعد إنهاء عملية التفتيش. والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق التي تفيد في كشف الحقيقة ما كان منها ضد المشبه فيه أو ما كان في مصلحته. التحقيق في الجرائم التقلدية تعودت أن يقع الضبط على الأشياء المادية فقط[4].

أثير تساؤل عن مدى صلاحية الضبط كوسيلة لمراقبة من البيانات الالكترونية لأن الضبط هو وضع اليد على شيئ ملموس.

اختلف الفقه حول التساؤل المطروح، فانقسم إلى إتجاهين:

---

[1]-راجع نص المادة 5 من القانون رقم 04/09؛ بوبشير محند أمقران،مرجع سابق، ص17.

[2]- زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، الهدى للطباعة والنشر والتوزيع، الجزائر،2011، ص 130 و131.

[3]- صغير يوسف، مرجع سابق،ص ص 88،81؛ تنص المادة 65 مكرر 5 من تثنين الإجراءات الجزائية على ما يلي: " **إذ إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أوالإرهاب أوالجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:**

-إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.

-وضع الترتيبات التقنية دون موافقة المعنيين،من أجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه ببصفة خاصة أوسرية من طرف شخص أو عدة أشخاص في أماكن خاصة أوعمومية أو إلتقاط صور للشخص عدة أشخاص يتواجدون في مكان خاص.....".

[4]- سعيداني نعيم، مرجع سابق، ص 158.

يرى الاتجاه الأول أن بيانات أو معلومات الحاسب لا تصلح لأن تكون محلا للضبط لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلى بعد نقلها إلى كيان مادي ملموس.

ويرى الاتجاه الثاني أن تلك البيانات هي ذبذبات إلكترونية أو موجات كهرومغناطسية، تقبل التسجيل، الحفظ والتخزين على وسائط مادية. فوجودها المادي لا يمكن إنكاره[1].

تواجه عملية الضبط عدة صعوبات، منها:

- ضخامة البيانات التي من الواجب فحصها بالاستعانة بخبرات فنية عالية لتحديد البيانات التي تصلح كأدلة جنائية من عدمه.

- احتواء النظام المعلوماتي على عناصر لا يمكن فصلها مما يصعب ضبطها، لأنها تتضمن عناصر. كما يمكن أن تتواجد هذه البيانات أو المعلومات في شبكات وأجهزة تابعة لدولة أجنبية مما يستوجب الحصول على موافقتها للتعاون مع جهات التحقيق الوطنية[2].

يتضح مما تقدم أن التحري والبحث والتحقيق وجمع الأدلة في مجال الجرائم المعلوماتية تحيط به صعوبات عديدة لأنه يتميز بالغموض،إلا أنه لامناص من مواصلة البحث والتحقيق وجمع الأدلة مع التطور المستمر لوسائل البحث وسلطات التحقيق،وتدعيم التعاون الدولي في هذا المجال[3].

4- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أقر القانون رقم 03/200، المتعلق بالبريد والمواصلات السّلكية واللاسلكية، إجراء بحماية الاتصالات الورقية أو اللاسلكيكة التي تتم بين الأشخاص[4].

---

[1]- حابت أمال، مرجع سابق، ص 372 و373.

[2]- عداني نعيم، مرجع،سابق، ص 161 و162.

[3]- حابت أمال، مرجع سابق، ص 373.

[4]- أشار إليه زبيحة زيدان، مرجع سابق، ص 157؛ انظر لمزيد من التفاصيل: نايت علي عمران: " الجرائم المعلوماتية الماسة بالحياة الخاصة "، مجلة المحاماة، عدد 11، 2015، ص 27 وما بعدها.

نص المشرع الجزائري بمقتضى تقنين الاجراءات الجزائية على حالات اتخاذ هذا الإجراء، الإذن به، القائم به وطرق إجراءه[1].

يأذن المشرع الجزائري لضابط الشرطة القضائية باعتراض المراسلات، سواء أجريت عبر وسائل الإتصالات السلكية أو اللاسلكية، وبالتقاط صور المشتبه فيهم. وهي الترتيبات التي تستدعي الدخول للمساكن أو غيرها من المحلات ، وكل ذلك يكون تحت رقابة الجهات القضائية ،سواء كان في مرحلة التحقيق أو مرحلة البحث والتحري[2].

5- التسرب (الاختراق والتهوية):

نص المشرع الجزائري على التسرب، بموجب تعديله لتقنين الإجراءات الجزائية سنة 2006، في الفصل الخامس من المادة 65 مكرر 11 إلى المادة 65 مكرر 18.

يعتبر التسرب إجراء من إجراءات التحقيق الابتدائي التي منحت لضباط الشرطة القضائية في حدود وضمن الضوابط التي بينها المواد المشار إليها.

يجب أن يتم بإذن من وكيل الجمهورية أو من قاضي التحقيق، وأن يكون تحت رقابة وكيل الجمهورية.

يتضمن إجراء التسرب اختراق ضباط أو أعوان الشرطة القضائية العصابات الإجرامية باستعمال حيلهم الخاصة. ويكون ذلك تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية[3].

الفرع الثاني

إنشاء جهات متخصصة في الوقاية ومكافحة الجريمة المعلوماتية

تقرر، إلى جانب مكافحة الجرائم عن طريق جهات القضاء العادي، إنشاء جهتين أخرتين لمكافحة الجريمة المعلوماتية والوقاية منها.

---

[1]- راجع نصوص المواد من 65 مكرر 5 إلى 65 مكرر 10 من تقنين الاجراءات الجزائية؛ بوبشير محند أمقران، مرجع سابق، ص 18.

[2]- حمودي ناصر، مرجع سابق، ص 227.

[3]- حمودي ناصر، مرجع سابق، ص 229 وما بعدها.

أولا- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الآلي والاتصال ومكافحته:

أنشئت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، بموجب القانون رقم 04/09 المؤرخ في 2009/08/05[1]، لتتولى الهيئة القيام، خاصة، بالمهام الآتية:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[2].

ثانيا- الأقطاب المتخصصة:

تم إنشاء أربعة أقطاب متخصصة في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، إلى جانب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك بتمديد الاختصاص المحلي لكل من محكمة سيدي محمد، قسنطينة، ورقلة ووهران، بموجب كل من المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، من جهة، وبموجب تقنين الإجراءات الجزائية، من جهة أخرى[3].

---

[1]- راجع نص المادة 13 من القانون رقم 04/09.

[2]- راجع نص المادة 14 من القانون رقم 04/09.

[3]- بوبشير محند أمقران، مرجع سابق، ص 21؛ راجع نص المادة 329 من تقنين الاجراءات الجزائية.

يمكن للمحاكم الجزائرية أن تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرتكبة في الخارج، وإن كان مرتكبها أجنبيا، إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتجية للاقتصاد الوطني[1].

المطلب الثاني

صعوبات مكافحة الجريمة المعلوماتية

تصطدم الجهود المبذولة، عن طريق التشريعات أو من طرف سلطات التحقيق والضبطية القضائية وكذلك التعاون الدولي، للحد من الجرائم المعلوماتية بعدة صعوبات وعراقيل نظرا لتعقيدها.

وتتمثل في كل من صعوبة اكتشاف الجريمة المعلوماتية (الفرع الأول)، صعوبة إثباتها (الفرع الثاني) وصعوبات متعلقة بالجانب القضائي (الفرع الثالث) .

الفرع الأول

صعوبات متعلقة باكتشاف الجريمة المعلوماتية

يعترف العديد من المهتمين بشؤون تكنولوجيا المعلومات، خاصة الجانب المتعلق بارتكاب الجريمة، بوجود صعوبات باكتشاف الجريمة المعلوماتية.

يرجع ذلك إلى جملة من الأسباب، منها ما هو متعلق بافتقادها الآثار التقليدية وصعوبة التوصل إلى الجاني إلى جانب صعوبات أخرى نوردها فيما يلي:

أولا- افتقاد الجريمة المعلوماتية الآثار التقليدية للجريمة:

تبقى الجريمة المعلوماتية مجهولة ما لم يتم التبليغ عنها إلى الجهات المعنية بالتحقيق الجنائي. وتجدر الإشارة إلى أن الكثير من الجرائم المعلوماتية المرتكبة لا تصل إلى علم السلطات المعنية كباقي الجرائم الأخرى، فهي جرائم غالبا ما لا تترك آثارا مادية كتلك التي تتركها الجريمة العادية[2].

---

[1]- راجع نص المادة 15 من القانون رقم 04/09؛ بوبشير محند أمقران، مرجع سابق، ص 21.

[2]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم لي والانترنت**، ط.2، بهجات للطباعة والتجليد، مصر، 2009، ص 41.

تتم الجرائم المعلوماتية دون شعور القائمين على تشغيل الأجهزة الإلكترونية، كالاختلاس الذي يتم بتعديل البرامج[1].

يرجع السبب في عدم اكتشاف الجريمة إلى أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي، دون وجود أي أثر على وجود وثائق أو مستندات يتم النقل منها[2].

ثانيا- صعوبة التوصل إلى الجاني:

يدخل المجرمون إلى شبكة الانترنت باسم مستعار، سواء بإخفاء هويتهم أو انتحال شخصية أخرى، لتفادي التعرف عليهم في حال اكتشاف الجريمة.

يلجأ هؤلاء، غالبا، إلى استعمال مقاهي الانترنت لارتكاب جرائمهم، وذلك بتزييف رسائل البريد الإلكتروني لتبدو صادرة من شخص آخر، مما يزيد من صعوبة معرفة الجاني وتحديد مكان اتصاله وموقعه[3].

ثالثا- عدم الإبلاغ عنها من قبل جهات المجني عليها:

تعتبر الجريمة المرتكبة عبر الانترنت جريمة خطيرة وصعبة الاكتشاف، إلا أن ما يزيد من صعوباتها هو تكتم الجهات المجني عليها عن الإفصاح عنها وعدم إبلاغ الجهات المختصة في مكافحتها. يرجع السبب في ذلك إلى خوفها من الإطلاع على المعلومات التي لم يجر الإبلاغ عنها[4].

ويزيد أمر عدم وصول هذه الجرائم إلى علم السلطات المختصة والمعنية، بالطريقة العادية، من مهمة الكشف عنها[5].

رابعا- نقص خبرة سلطات الاستدلال:

تواجه عمليات اكتشاف الدليل في الجريمة المرتكبة عبر شبكة الانترنت، نقص الخبرة لدى رجال الظبط القضائي وأجهزة العدالة الجنائية في إلقاء القبض والكشف عن لمحاكمهم.

---

[1]- صغير يوسف، مرجع سابق، ص 117.

[2]- عبد الفتاح البيومى حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، ط.1، دار الفكر الجامعي،الإسكندرية، 2006، ص83.

[3]- جعفر حسن جاسم الطائي، مرجع سابق، ص 221.

[4]- صغير يوسف، مرجع سابق، ص 119 و120.

[5]- صغير يوسف،مرجع سابق،ص ص 120،119.

ويرجع ذلك إلى نقص الإمكانيات والتقنيات اللازمة للكشف، للتحقيق وللاستدلال نظرا لما تتسم به الجريمة المعلوماتية من سرعة.

ينعكس ذلك سلبا على إجراءات التحقيق والاستدلال في الدعوى الجنائية، وعلى هذا الأساس، فإنه من الضروري الدعوة إلى تأهيل جهات التحقيق والأمن والإدعاء والحكم لمواجهة مثل هذه الجرائم[1].

الفرع الثاني

صعوبات متعلقة بإثبات الجريمة المعلوماتية

يتم الفعل الإجرامي في حالات عدة دون أن يعلم الضحية بحدوث اعتداء واقع عليه، ويرجع ذلك إلى ما يلي:

أولا- غياب الدليل المرئي وسهولة إخفاء الدليل:

يعتبر سهولة إخفاء الدليل أو محوه أو تدميره من بين الصعوبات التي تعترض عملية الإثبات في جرائم المعلوماتية.

يقوم المتهم بتدمير الدليل الذي يثبت إدانته بسهول، إضافة إلى وجود أفعال غير مشروعة يرتكبها الجاني يكون أمرها حكرا عليه كالتجسس على ملفات البيانات المخزنة والوقوف على ما لديها من أسرار.

ويلجأ إلى نسخ ملفات بقصد استعمالها لأغراض له مصالح فيها. وقد يدخل الجاني إلى بيانات لتحريفها دون أن يؤدي ذلك إلى ترك أية آثار[2].

ثانيا- نقص الخبرة الفنية والتقنية لدى الشرطة و جهات الإدعاء والقضاء:

يشكل هذا الأمر عائقا أمام إثبات الجريمة المعلوماتية، إذ أن هذا النوع من الجرائم يستلزم تأهيلا و تدريبا، فيما يتعلق بكيفية جمع الأدلة والتفتيش فيها. ونتيجة لنقص الخبرة لدى الجهات المختصة فإنها لا تبذل جهودا لكشف الغموض عن الجريمة وضبط مرتكبيها. فالمحقق يمكن أن يدمر الدليل بمحو محتويات الأسطوانة بالخطأ[3].

ويمكن إجمال صعوبات إثبات الجريمة المعلوماتية في كل من:

---

[1]- صغير يوسف، مرجع سابق، ص 120 و121.

[2]- صغير يوسف، مرجع سابق، ص 125 و126.

[3]- عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 28.

- أنها جريمة لا تترك آثارا مادية بعد ارتكابها.
- أنها جريمة يصعب الاحتفاظ بآثرها.
- أنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية.
- أنها جريمة تعتمد على الخداع في ارتكابها وعلى التضليل.
- أنها تعتمد على قمة الذكاء في ارتكابها[1].

الفرع الثالث

صعوبات متعلقة بنقص التخصص القضائي

يفرض الطابع الدولي لجرائم الكمبيوتر التعاون بين دول عديدة بما أن الجريمة تتجاوز الحدود الإقليمية.

غير أن الواقع يعكس قصورا في ذلك مقارنة بتطور الجريمة، وهو ما سنتناولة فيما يلي:

أولا – قصور التعاون الدولي في مكافحة الجريمة المعلوماتية:

يعتبر التعاون الدولي في مجال مواجهة الجريمة المعلوماتية من بين المشاكل التي تواجه عملية مكافحة تلك الجريمة. ونذكر فيما يلي بعض الصعوبات التي تقف وراء عدم تحقيق تعاون دولي في هذا المجال.

– عدم وجود مفهوم مشترك متعلق بالجريمة المعلوماتية، ما أدى إلى تسهيل الإفلات من العقاب. أضف إلى ذلك أن وجود تعريف موحد للجريمة المعلوماتية جعل بعض الأفعال في تشريع دولة مباحة في حين جعلتها أخرى أفعالا مجرمة.

– تنوع واختلاف النظم القانونية الإجرائية، فبعض طرق التحري والتحقيق والمحاكمة التي تثبت فعاليتها وفائدتها في دولة ما قد تكون بدون فائدة في دولة أخرى، كما هو الحال بالنسبة للتسليم، المراقبة الالكترونية[2].

---

[1]- بن عقون حمزة، مرجع سابق، ص 24.

[2] – صغير يوسف، مرجع سابق، ص ص 133 – 134.

ثانيا- صعوبة تحديد القانون الواجب التطبيق:

يعتبر مبدأ الإقليمية، بمقتضى نص المادة 3 من تقنين العقوبات، الأصل في تطبيق النص الجنائي، فإذا ما ارتكب شخص ما جريمة معلوماتية داخل الدولة وخلفت آثارها في الدولة ذاتها فالقانون الواجب التطبيق هو قانون هذه الدولة مهما تكن جنسية الجاني والمجني عليه.

يترتب على تطبيق مبدأ الإقليمية أن الدولة لا تهتم إلا بالجرائم التي تقع على إقليمها، فلا تمتد إلى ما يرتكب من جرائم خارج إقليمها حتى ولو كان مرتكبها من رعايا هذه الدولة.

وقد تم وضع مبدأ الشخصية ومبدأ العينية ليغطيا القصور الذي يتميز به مبدأ إقليمية النص الجنائي في الجرائم التقليدية. غير أن الأمر ليس كذلك بالنسبة للجريمة المعلوماتية، خاصة في ظل عالمية شبكة الانترنت، لأن السلوك في هذه الجريمة يمر عبر عدة دول.

يخلف ذلك إشكالا في تحديد القانون الواجب التطبيق نظرا لاختلاف التشريعات وعدم وجود اتفاقيات فيما بينها.

ثالثا- تحديد المحكمة المختصة:

اعتمدت الآراء الفقيهة ثلاثة معايير لتحديد المحكمة المختصة بنظر الجريمة المعلوماتية:

1- معيار الإختصاص المكاني:

وضعت أغلب التشريعات ثلاثة ضوابط لتحديد الاختصاص المكاني وهي كل من مكان وقوع الجريمة، محل إقامة المتهم أو مكان إلقاء القبض عليه. و تكون المحكمة التي ترفع إليها الدعوى أولا هي المختصة مكانيا بالنظر في الدعوى[1].

2- معيار القانون الأكثر ملائمة:

يرى أنصار هذا الاتجاه بأنه نظرا للطبيعة الخاصة للجريمة المعلوماتية والأضرار الناتجة عنها التي تمتد إلى أكثر من إقليم دولة واحدة، فإن نسبة الضرر تتفاوت من دولة إلى أخرى، ويعود الاختصاص في رأيهم، في هذه الحالة، إلى محاكم الدولة التي تعرضت

---

[1]- صغير يوسف، مرجع سابق، ص 142.

لضرر أكبر عن ذلك الذي تعرضت له باقي الدول.

3- معيار الضرر المرتقب:

أدى ظهور شبكة الانترنت إلى خلق عالم افتراضي تسري فيه مختلف المواد المعلوماتية دون وجود إمكانية تحديد وجهتها. ولا يخضع ذلك العالم لأي سلطة إقليمية، مما رتب ضررا للدول المتصلة بالإنترنت وهذا هو المقصود بمعيار الضرر المرتقب[1]

أول المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشرت المعلومات أو البيانات بواسطته.

وقد وجد هذا المعيار طريقه إلى التطبيق في بعض الدول، منها فرنسا، إذ أصدرت محكمة باريس قرارا اعتبر صراحة أن الطبيعة الكونية الخاصة بشبكة الانترنت لا يجب أن تؤدي إلى تطبيق محتمل لجميع القوانين الموجودة بل إلى تطبيق القانون ذي الصلة مع مبدأ موضوعي[2].

---

[1]- صغير يوسف، مرجع نفسه، ص 144 و145.

[2]- عبد الفتاح بيومي حجازي ،مرجع سابق،ص 52

خاتمـــة:

يتجلى من خلال دراستنا للجريمة المعلوماتية بأنها من أكثر الجرائم صعوبة وخطورة، التي عرفها العالم في العصر الحديث، نظرا للمشكلة التي أفرزتها الثورة المعلوماتية.

حملت الثورة المعلوماتية إيجابيات كثيرة في مجال تسهيل تبادل المعلومات والخبرات بين دول العالم وتثقيف المجتمعات، إلا أنها لا تخلو من سلبيات ومخاطر جمة يهدد بها المجرم المعلوماتي.

تحولت التكنولوجيا المعلوماتية إلى سلاح، في يد المجرمين، لا يستهان به لممارسة نشاطهم الإجرامي وزرع الرعب في أوساط المجتمعات. يتميز هؤلاء المجرمين بذكاء حاد ومهارة عالية مما مكنهم من ارتكاب الجرائم التقليدية بطريقة حديثة.

تتسم الجريمة المعلوماتية بخصوصيات عدة أهمها: صعوبة الكشف عنها وإثباتها، وأنها جريمة عابرة للدول.

أظهر انتشار هذه الجريمة المستحدثة قصور النصوص القانونية في مكافحتها، إذ أصبحت عاجزة وغير كافية لضمان الحماية اللازمة والفعالة لمواكبة تطور هذه الجريمة.

وحاول المشرع الجزائري مواكبة، وإن كان ذلك بقدر قليل، الحركة التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الانترنت في مختلف مناحي حياة المواطن الجزائري. فبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال فإنها سعت، في بادئ الأمر. إلى سده بتعديل تقنين العقوبات، بمقتضى القانون رقم 15/04.

غير أن محدودية هذا القانون دفع بالمشرع الجزائري إلى إصدار قانون خاص، يتمثل في القانون رقم 04/09، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاتصال ومكافحتها. وكما كانت هناك محاولات أخرى خاصة في قوانين الملكية الفكرية مثل قانون حماية حق المؤلف والحقوق المجاورة.

أضف إلى ذلك، عدم تجريم المشرع الجزائري فعل التزوير المعلوماتي، ولذا، فحبذا لو يتدارك المشرع هذا الفراغ التشريعي من خلال استحداث نص خاص به أو بتوسيع مجال التزوير، عن طريق توسيع مفهوم المحرر، ليشمل أية دعامة أخرى على غرار التشريعات الحديثة ومنها التشريع الفرنسي.

يبقى المشرع الجزائري، بالرغم من هذه المحاولات، بعيدا كل البعد عن التطور القانوني على المستوى العالمي، من جهة، وعن تجريم الأساليب الجديدة في ارتكاب الجريمة المعلوماتية، من جهة أخرى ، مما يقتضي مراجعة وتطوير القوانين القائمة وإصدار المزيد من القوانين لتقوية الترسانة في هذا المجال.

و قد انتهينا من خلال هذا البحث إلى ضرورة تأكيد بعض النقاط من خلال التوصيات التالية:

- ضرورة وضع تشريع جزائري ينسق مع الأحكام القانونية الدولية في مواجهة هذه الجرائم وتنظيم الأحكام الإجرائية الخاصة بمواجهة هذه الجريمة، وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.
- منح سلطات التحقيق الصلاحية القانونية والتدريب العملي اللازم لاختراق أنظمة الحاسوب.
- اعتماد الدقة والوضوح في تحديد السلوك الاجرامي.
- ضرورة التعاون الدولي لمواجهة مشاكل صور السلوك المنحرف، المتمثل في جرائم الكمبيوتر والانترنت، عن طريق عقد الاتفاقيات الثنائية.

قائمـة المراجـع

أولا- الكتـب:

1- أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**،الطبعة الأولى، دارهومة للطباعة و النشر، الجزائر، 2009.

2- جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة المعلوماتية)**، دار البداية، عمان،2007.

3- خالد ممدوح إبراهيم، **الجريمة الإلكترونية**، دار الجامعة الإسكندرية،2010.

4-خالد ممدوح إبراهيم، **حوكمة الانترنت**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2011.

5- زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، عين الهلال للطباعة والنشر والتوزيع،الجزائر،2011.

6- طارق إبراهيم الدسوقي عطية، **الأمن المعلوماتي**، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر،الإسكندرية، 2009.

7- عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006 .

8- عبد الفتاح بيومي حجازي، **الدليل الجنائي في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت**، بهجات للطباعة والتجليد، مصر، 2009.

9- محمد على العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر،الإسكندرية، 2004.

10- محمد على العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة،الإسكندرية، 2011.

ثانيا- الرسائل والمذكرات:

1- رسالة الدكتوراه:

أ- حابت أمال، **التجارة الالكترونية في الجزائر**، رسالة لنيل شهادة دكتورا في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015.

2-مذكرات الماجستير:

أ- حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، بحث مقدم لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة باتنة، 2012.

ب- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية،قسم الحقوق، جامعة باتنة، 2013.

ج- سوير سفيان، **جرائم المعلوماتية**، مذكرة لنيل شهادة الماجستير، في العلوم الجنائية وعلم الإجرام، جامعة تلمسان، 2011.

د-صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة لنيل شهادة الماجستير، في القانون تخصص القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

هـ- قارة أمال، **الجريمة المعلوماتية**، رسالة لنيل درجة الماجستير،في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، 2002.

و- محمد بن عبد الله بن علي المنشاوي، **جرائم الانترنت في المجتمع السعودي**، مذكرة ماجستير في العلوم الشرطية، تخصص قيادة أمنية، قسم العلوم الشرطية، الرياض، 2003.

ي- واقد يوسف، **النظام القانوني للدفع الالكتروني**، مذكرة لنيل شهادة الماجستير، في القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق، جامعة مولود معمري، تيزي وزو،2011.

3- مذكرات الماستر:

أ- قريم سكورة، **المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري**، مذكرة لنيل شهادة ماستر في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم القانون العام،جامعة أكلي محند أولحاج، البويرة، 2015.

ب- لعاقل فريال، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة لنيل شهادة ماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، لبويرة، 2015.

ج-مرغيش سمية، **جرائم المساس بالأنظمة المعلوماتية**،مذكرة لنيل شهادة ماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة،2014.

ثالثا- المقالات:

1- بوبشير محند امقران ، " **الجوانب القانونية لمكافحة جرائم المعلوماتية والوقاية منها** "، مجلة المحاماة، ناحية تيزي وزو، عدد11، 2015.

2- بوزرام أحمد، " **جرائم المعلوماتية** "، محاضرة ألقيت من طرف، بوزرام أحمد وكيل الجمهورية، لدى محكمة، 2006.

3- بوعناد فاطمة زهرة، " **مكافحة الجريمة الالكترونية في التشريع الجزائري** "، مجلة الندوة للدراسات، عدد 1، 2013.

4- تخروبت فوضيل، "**جرائم المعلوماتية**"، مجلة المحاماة، ناحية تيزي وزو،عدد11،2015.

5- حمودي ناصر، " **التنظيم القانون لظاهرة المعلوماتية في الجزائر:الانجازات والتحديات** "، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2012.

6- ذياب موسى البدانية، " **الجرائم الالكترونية: المفهوم والأسباب** "، ورقة مقدمة في الملتقى العلمي، الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية و الدولية، عمان – الأردن،2-4-2014.

7- صالح شنين: " **الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري** "، المجلة الأكاديمية للبحث القانوني، عدد 01، 2010

8- عادل عبد النبي شكري، " **الجريمة المعلوماتية وأزمة الشرعية الجزائية** "، مجلة كلية الحقوق، عدد7، جامعة الكوفة، 2008.

9- مليكه عطوي، " **الجريمة المعلوماتية،الأسواق المالية العربية في ظل العولمة،حجية الاعتراف في تكوين قناعة القاضي الجزائي** "، مجلة حوليات الجزائر، عدد 1.

10- نايت علي عمران: " **الجرائم المعلوماتية الماسة بالحياة الخاصة** "، مجلة المحاماة، عدد 11، 2015.

رابعا- الاتفاقيات الدولية:

1- اتفاقية برن لحماية المصنفات الفكرية والأدبية لسنة 1886، المنشورة على الرابط التالي: http://www.wipo.int/treaties/ar/ip/berne/، التي انضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 341/97، المؤرخ في 1997/9/13.

2- الاتفاقية العالمية حول حق المؤلف لسنة 1952 والمراجعة في باريس 1971/07/24، المنشورة على الرابط التالي: ttp://www.wipo.int/wipolex/ar/other_treaties/text.jsp?fil_id=193359

3-اتفاقية باريس لحماية الملكية الصناعية، المنشورة على الرابط التالي:

www.lasportal.org/ar/intellectualproperty/.../باريس/20اتفاقية.pdf

4- **الاتفاقية الدولية حول الإجرام المعلوماتي** التي أبرمت بتاريخ 2001/11/08، من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23، المنشورة على الرابط التالي: http://www.4shared.com/file/82161420...-27_.html

خامسا- النصوص القانونية:

1- الأمر 05/03، المؤرخ في 2003/7/19، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر،عدد 44، صادرة بتاريخ 2003./7/23

2- الأمر رقم 06/03، المؤرخ في 2003/7/19، المتعلق بالعلامات التجارية، ج.ر، عدد 44، صادرة بتاريخ 2003/7/23.

3- الأمر رقم 07/03، المؤرخ في 2003/7/19، المتعلق ببراءات الاختراع، ج.ر، عدد 44 ،صادرة بتاريخ 2003/7/23 .

4-القانون رقم 15/04، المؤرخ في 2004/11/10،يعدل ويتمم الأمر رقم 156/66 المتضمن تعديل تقنين العقوبات ،ج.ر، عدد 71، صادرة بتاريخ2004./11/10

5- القانون رقم 04/09، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، عدد 47، صادرة بتاريخ 16 أوت 2009.

7-مرسوم رئاسي رقم 97-341 مؤرخ في13 -09-1997،يتضمن إنضمام الجزائرمع التحفظ إلى إتفاقية بارن لحماية المصنفات الأدبية والفنية المؤرخة في 04-6-1896 والمتممة في باريس في 04-05-1896في 28- 091979

فهرس

الفصل الثاني

مكافحة الجريمة المعلوماتية في التشريع الجزائري.....30