الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي
جامعة عين تموشنت
كلية الحقوق والعلوم السياسية
قسم الحقوق

المعلوماتية وجرائم الإعتداء على الأموال

مذكرة مكملة لنيل شهادة الماسترفي الحقوق - تخصص: قانون خاص

من إعداد الطلبين:

- خلوف الحاج
- مجاهد سعيد

تحت إشراف: د. مهداوي محمد صالح

لجنة المناقشة:

الرئيس	روان حسن كمال	أستاذ محاضر "ب"	جامعة عين تموشنت
المشرف	مهداوي محمد صالح	أستاذ	جامعة عين تموشنت
الممتحن	رويس عبد القادر	أستاذ مساعد "ب"	جامعة عين تموشنت

السنة الجامعية:2023 - 2024

بســـــــم الله الرحمـــــــــان الرحيـــــــم

الإهـــــــــــــداء

إلى من لا يمكن للكلمات أن توفي حقها

إلى من لا يمكن للأرقام أن تحصي فضائلها

إلى والدينا الأعـــــزاء أدامهم الله لنا

إلى كل الإخوة والأخوات والأصدقاء والزملاء الأكارم

إلى كل أساتذتنا بكلية الحقوق بجامعة "بلحاج بوشعيب"

شكر وتقـــدير وعـرفان

الحمد لله الذي بنعمته تتم الصالحات

نتقدم بأسمى عبارات الشكر والتقدير و الاعتراف بالفضل

للمشرف الأستاذ "مهداوي محمد صالح"

الذي رافقنا بإرشاداته القيمة وتوجيهاته السديدة وسعة صدره

طيلة المدة التي استغرقناها لإتمام هذا البحث المتواضع

نفعنا الله بعلمه وجزاه عنا خير جزاء

كما نتوجه بالشكر الجزيل إلى الأساتذة أعضاء لجنة المناقشة

وإلى كل من ساعدنا من قريب أو بعيد

وكان لنا سندا في هذا العمل المتواضع.

قائمة أهم المختصرات

- ص: صفحة
- ط: طبعة
- م: المـــادة
- ج: الجـزاء
- ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية
- ق. ع .ج: قانون العقوبات الجزائري
- ق. إ.ج: قانون الإجراءات الجزائية الجزائري

éd:édition

Op. cit:ouvrage précédemment cité.

P: page

مقـــــدمـــــــة

أصبحت الثورة العلمية في مجال المعلومات والاتصال حجر الزاوية في حياة الأفراد والدول حيث تعتمد جميع القطاعات في وقتنا الحالي بشكل أساسي على استخدام الأنظمة المعلوماتية، نظرا لما تتميز به من دقة وسرعة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها، وعلى الرغم من المزايا الهائلة التي تقدمها هذه الأخيرة إلا أنه قد صاحبتها انعكاسات سلبية، حيث أن هناك أصحاب النفوس الضعيفة من يستغل التقنية الحديثة في مارب غير مشروعة ما أدى إلى ظهور إجرام جديد يرتكب في فضاء إلكتروني يسمى الجريمة المعلوماتية، والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي ويستمد هذا النوع المستحدث من الإجرام نشاطه من الإمكانات الهائلة للحاسب الآلي والبرامج، وتطور شبكة الإنترنت والتطور الثقافي والعلمي في التعامل مع التكنولوجيا الحديثة بمختلف أنواعها، وتتعاظم المخاطر الناتجة عن الجرائم المعلوماتية لقدرتها الفائقة على التطور والانتشار وتخطيها للحدود الجغرافية مستغلة في ذلك ما أتاحته شبكة الإنترنت من انفتاح معلوماتي على العالم بأسره.

ومن بين هذه الجرائم نجد جرائم الإعتداء على المال المعلوماتي التي تعد من الجرائم المستحدثة الذي ارتبط وجودها بظهور ثورة تكنولوجيا المعلومات و الإتصالات، حيث صنفت من أخطر الجرائم كونها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية يقترفها أشخاص يتميزون بذكاء عالي ويمتلكون أدوات المعرفة التقنية مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية بشكل عام والمصالح ذات الطابع المالي المتعلقة بالمؤسسات المالية والمصرفية بشكل خاص.

ولقد شكلت هذه الجرائم الكثير من الصعوبات والإشكاليات القانونية نظرا لما يتمتع به المال المعلوماتي من طابع الخاص يختلف عن الجرم التقليدي سواء من ناحية طبيعة المال محل اعتداء أو من ناحية الصورة التي يتخذها الفعل الإجرامي الذي يعد بمثابة الركن المادي للجريمة، فالمال هنا شقين:

الأول: الشق مادي لا يثير أدنى مشكلة ولا يختلف مفهومه عن المفهوم التقليدي للمال بحيث يطبق عليه النص القانوني التقليدي.

الثاني: الشق المعنوي هنا يخرج المال من نطاق مفهومه التقليدي إلى مفهوم أخر غير ملموس أي معنوي من برامج ونظم وكيانات غير مادية.

وعليه كان من المنطقي أن تتجه السياسة التشريعية الجنائية في معظم دول العالم إلى إصدار بعض التشريعات التي تحد من هذه الظاهرة الاجرامية.

ومن بين الدول التي سارعت إلى سن وإصدار قوانين جديدة لمواجهة ومكافحة الجرائم المعلوماتية نجد الجزائر حيث قام المشرع الجزائري بتعديل بعض قوانينه القائمة كغيره من التشريعات الدولية الأخرى من أجل مسايرة هذا التطور الحاصل في ميدان التكنولوجيا، كالقانون رقم 04 -15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، الذي تم من خلاله استحداث نصوص خاصة متعلقة بالجرائم الماسه بأنظمة المعالجة الآلية للمعطيات، القانون رقم 04- 14، المؤرخ في 2004/11/10، المعدل والمتمم لقانون الإجراءات الجزائية الذي وضع قواعد وأحكام خاصة لسلطة التحري و المتابعة، والقانونرقم 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى استحداث مؤسسات أمنية وقضائية على غرار الأقطاب الجزائية المتخصصة .

إن أهمية الموضوع وأهدافه وعلى اتساع نطاقه كونه يجمع بين الجانب التقني لعالم المعلوماتية، و الجانب القانوني المتمثل في الجريمة المعلوماتية ذاتها، تبرر أسباب اختياره و تجعل منه موضوعا مستجدا ومستحدثا للدراسة والبحث بشكل دائم ومستمر بالنظر إلى نطاق المعلوماتية الذي لا ينفك يتوسع من يوم لآخر، إضافة إلى تطورها بشكل دائم ومستمر و عدم وجود عوائق تحد من هذا التطور و هو ما يجعل من أمر تطوير وتحديث النصوص القانونية أمرا واجبا في ظل التهديدات التي تشكلها الجريمة المعلوماتية.

بالنسبة لدوافع اختيار الموضوع فتعود على ضوء بعدين ذاتي وموضوعي، أما الأسباب الذاتية فترجع إلىالتزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية، خاصة فيما يتعلق بالمال المعلوماتي، وارتفاع درجة خطورته باعتباره من الأحداث اليومية الواقعة في العديد من المناطق داخل الدول، مما أصبح يشكل تهديد على الأمن العام، في ظل عجز سلطات عن رسم نموذج موحد لمكافحة هذه الجرائم، هذا من جهة ومن جهة أخرى الطموح العلمي الذي يدفع باتجاه تقصي الجديد في ميدان المال المعلوماتي والرغبة في المساهمة ولو بشكل محدود في إثراء النقاش القانوني في مثل هذه المواضيع، وهذا قد يرجع إلى وجود خلل في النظام الإجرائي السائد .

أما الأسباب الموضوعية فتمحورت حول الحداثة القانونية والتشريعية المنتهجة من قبل الدولة الجزائرية لمكافحة هذا النوع من النشاط الإجرامي، مما يدفع نحو البحث في مدى انسجام النصوص القانونية التقليدية لهذه المنظومة مع المستجدات الراهنة في مجال المعاملات الإلكترونية، فضلا عن وسائل الحماية الإجرائية المعتمدة من قبل المشرع لمواجهة الجرائم المعلوماتية.

وعن الدراسات السابقة المتعلقة بموضوع بحثنا، فإنه حظي بإهتمام عدد من الباحثين والفقهاء في العالم وفي الجزائر على وجه الخصوص على غـرار:

- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد تلمسان الجزائر، 2017-2018.

- سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق، جامعة بوبكر بلقايد تلمسان، الجزائر 2010.
- يوسف صغير، الجرائم المرتكبة عبر الإنترنيت، رسالة لنيل الماجيستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر،2013.

إن الهدف من هذه الدراسة يتمحور أساسا في تسليط الضوء على جرائم الإعتداء على المال المعلوماتي، مع توضيح مدى ملائمة النصوص التقليدية مع هذا النوع الجديد من الجرائم المستحدثة.

على غـرار أي بحث علمي قانوني، لا يخلو من العقبات فإن الوصول إلى وضع خطة متوازنة ومعالجة فعالة و دقيقة لموضوع البحث لم يكن بالسهولة المتوقعة بالنظر إلى طبيعة الموضوع من جهة ومن جهة أخرى لما يميزه من دقة المصطلحات والمفاهيم العلمية منها و القانونية، و التي يصعب التحكم فيها وتوظيفها بشكل متناسب و متلازم، في ظل قلة الدراسات السابقة في المجال المـال المعلوماتي حيث تمحورت أغلب الدرسات في الغالب حول معالجة الظاهرة الجريمة المعلوماتية بصفة عامة من ناحية السلوك الإجرامي التقليدي والعقوبات المقررة له، دون مواكبة التطور الحاصل في مجال الجرائم المعلوماتية التي تمتاز بالتجديد، بالإضافة إلى قلة المراجع الوطنية الحديثة المعالجة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

على ضوء ما سبق ذكره يثور تساؤل الرئيسي حول **الإطار القانوني الذي يحكم الجرائم المعلوماتية بصفة عامة وجرائم الاعتداء على المال المعلوماتي بصفة خاصة في ظل التشريع الجزائري؟ أو بصياغة اخرى ماهي الجرائم المعلوماتية التي تدخل ضمن قسم الجرائم الأموال في نظر المشرع الجزائري؟**

هاته الإشكالية العامة التي بدورها تتفرع عنها إشكاليات فرعية أو تساؤلات نذكر منها:

- ما هو مفهوم الجريمة المعلوماتية؟
- ماهي الطبيعة القانونية للمال المعلوماتي محل الإعتداء في التشريع الجزائري؟
- هل النصوص التقليدية كفيلة بحماية المال المعلوماتي؟
- ماهي الآليات و المكنيزمات الحديثة التي تبنتها الدولة الجزائرية لمجابهة هذه الظاهرة؟

وللإجابة على الإشكالية المطروحة تم الاعتماد في دراسة موضوع البحث على منهجين أولهما المنهج الوصفي الذي مس الجانب الفني من الدراسة والثاني المنهج التحليلي الذي تم الاستعانة به لتحليل مختلف القواعد والسنن القانونية المرتبطة بعناصر البحث.

من أجل الكشف عن مختلف خطايا الموضوع وكذا ايجاد أجوبة لكل التساؤلات المطروحة، تم تقسيم الدراسة إلى فصلين أولهما اهتم بدراسة الجوانب الفنية والإطار المفاهيمي للجريمة المعلوماتية تم تقسيمه بدوره إلى مبحثين اثنين أولهما تناول مفهوم الجريمة المعلوماتية حيث تم التطرق من خلال المطلب الأول إلى تعريف الجريمة المعلوماتية، فيما خصص المطلب الثاني لخصائص الجريمة المعلوماتية وتقسيماتها، في حين تناولنا في المبحث الثاني وفق مطلبين أطرافها ودوافع ارتكابها.

بالنسبة للفصل الثاني فتمحور حول الجرائم المعلوماتية الواقعة على الأموال وآليات مكافحتها في التشريع الجزائري، تم معالجته وفق مبحثين الأول تطرقنا من خلاله إلى دراسة المال المعلوماتي وفق مطلبين الأول تناولنا من خلاله الطبيعة القانونية للمال المعلوماتي والثاني عددنا من خلاله صور جرائم الاعتداء على المال المعلوماتي المستنبطة من التشريع الجزائري، أما المبحث الثاني فتركز على الجانب القانوني من خلال استعراض آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري، في مبحثين الأول تطرقنا من خلاله إلى الجانب التشريعي والثاني إلى الجانب المؤسساتي.

الفصل الأول

الإطار المفاهيمي

للجريمة المعلوماتية

تمهيد:

ظهر الحاسب الآلي كنتاج للتطور العلمي والتقدم التقني، الذي أدى إلى تدخل أنظمة المعالجة الآلية للمعلومات في كافة مجالات الحياة اليومية، نظراً لما تتمتع به من قدرة فائقة على تخزين أكبر قدر من البيانات والمعلومات، كما أوجدت الشبكات المعلوماتية وخاصة شبكة الإنترنت واستخدامها في نقل وتبادل المعلومات فجرا جديدا تمثل في بروز ما اصطلح على تسميته بالمجتمع المعلوماتي.

عرف رواج الإنترنت كوسيلة للاتصالات واستعمالاها في جل المعاملات اليومية ظهور سلبيات عديدة، خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أسفر على ظهور جرائم لم يكن يعرفها القانون من قبل أطلق عليها مصطلح الجريمة المعلوماتية.

انفرادت الجريمة المعلوماتية بسمات خاصة، استمدتها من الوسيلة التي ترتكب بها ألا وهي الشبكة العالمية للإنترنت، مما وضع المشرع في مختلف أنحاء المعمورة في موضع المتفرج رغم المحاولات التي جاء بها، فإذا كانت الجرائم التقليدية قد نالت جانبا من الاعتناء، وذلك بتحديد مختلف المفاهيم والتعاريف الخاصة بها، فإن الجريمة المعلوماتية مازالت قيد البحث من طرف الفقهاء والقانونيين.

ضف إلى ذلك أنها جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية بناء على ما سبق سنتناول في هذا الفصل مفهوم الجريمة المعلوماتية مع توضيح تقسيماتها وخصائصها التي تميزها عن باقي الجرائم في المبحث الأول، ثم نتطرق في المبحث الثاني إلى دراسة أطراف الجريمة المعلوماتية ودوافع ارتكابها.

المبحث الأول: مفهوم الجريمة المعلوماتية خصائصها و تقسيماتها.

لقد أضفى التطور الهائل لتقنية المعلومات واندماجها بتقنية الاتصالات فيما بعد طبيعة خاصة على جرائم كانت تقليدية قبل ظهورها، وأدى إلى ظهور أنماط مستحدثة من الأفعال الجرمية تباينت التعبيرات والاصطلاحات للدلالة على هذه الجرائم تباين رافق مسيرة ونشأة تلك التقنية، وأحاط بها الكثير من التساؤلات التي تتعلق بتحديد مفهومها باعتبارها جريمة مستحدثة ومتميزة عن باقي الجرائم التقليدية من خلال موضوعها وخصائصها، وكذلك تعدد المحاولات الرامية إلى تصنيفها وتحديد تقسيماتها، على هذا النحو سنحاول من خلال هذا المبحث التطرق لمختلف التعاريف من مختلف الزوايا في المطلب الأول ثم نعرج على الخصائص وتقسيمات في المطلب الثاني.

المطلب الأول: تعريف الجريمة المعلوماتية.

من الناحية القانونية لا يوجد مصطلح قانوني موحد فهناك من يطلق عليها وصف جريمة الغش المعلوماتي، وهناك من يطلق عليها وصف جريمة الاختلاس المعلوماتي، وهناك من يصفها بجرائم الاحتيال المعلوماتي، غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية[1]، و لقد تعددت التعارف الواردة بشأن الجريمة المعلوماتية بتعدد النظم والتشريعات، الاتجاهات الفقهية و القانونية.

الفرع الأول: التعريف الاصطلاحي:

عرفت منظمة التعاون الاقتصادي والتنمية سنة 1983 (OECD) الجريمة المعلوماتية بأنها " كل وفعل وعمل غير مشروع أو مخالف للأنظمة وغير مرخص يستهدف أنظمة المعالجة الآلية للمعلومات أو تبادلها أو نقلها "، وتشمل الجريمة المعلوماتية بهذا المفهوم كل الجرائم التي يمكن أن تقع أو تمس بشبكات الاتصال بصفة عامة، وشبكة الانترنت بصفة خاصة[2].

وقد ورد تعريف الجريمة المعلوماتية بحسب ما قدمه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد بفينا سنة 2000 بأنها " كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام الحاسوب" وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

---

[1]- تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته، رسالة مقدمة لأجل نيل شهادة الدكتورة، قسم العلوم الشرطية جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009، ص 15.

[2]-Myriam Quéméner- Yves Charpenel - La Cybercriminalité Edition Economica- Paris- France- 2010-p 08.

ومن التعاريف الذي تم التوسع فيها تعريف الخبير الأمريكي (باركر – Parker) الذي حاول إعطائها مفهوما واسعا يحيط بكل أشكال التعسف في مجال استخدام النظم المعلوماتية، هي من وجهة نظره " كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ينشأ خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[1].

إذن ما يمكن استنتاجه من جملة هذه التعاريف أن الجريمة المعلوماتية هي تلك الجريمة المرتبطة أساسا بمظاهر التقدم التكنولوجي، وهو ما يفسر اتجاه البعض لإطلاق مصطلح "جرائم التقنية الحديثة" على هذا النوع من الجرائم التي رشحها علماء الإجرام للتطور مستقبلا بالنظر إلى التقنيات الحديثة التي تظهر يوميا وبشكل دائم ومستمر.

الفـرع الثـاني: التعريف الفقهي

اختلف الفقهاء ورجال القانون على تعريف الجريمة المعلوماتية، حيث ان كل اتجاه اسس تعريفه بناء على الزاوية التي يرى فيها الجريمة (وسيلة ارتكابها – وهناك من يوسع في رؤيته للجريمة وهناك من يركز على جزء من الجريمة) وسنتطرق الى بعض التعاريف الفقهية وفقا لما يلي:

أولا: التعريف الفقهي الضيق للجريمة المعلوماتية:

كل اتجاه فقهي اعتمد وجهة نظر ضيقة في تعريفه للجريمة المعلوماتية، فمنهم من اعتمد على اداة الجريمة ومنهم من اعتمد على توافر المعرفة بتقنيات جهاز الحاسب الآلي، ومنهم من اعتمد على تعريفه بناء على موضوع الجريمة.

1- على اساس معيار أداة الجريمة:

تعرف الجريمة المعلوماتية وفقا لهذا المعيار على اساس اداة الجريمة فالجريمة تكون جريمة معلوماتية طالما ان الحاسوب او احدى الوسائل التقنية من وسائل ارتكابها كالهواتف الذكية مثلا.

عرفها الأستاذ MASS بأنها: " الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"

أما الفقيه الألماني TIEDMANN فعرفها كما يلي: " كل اشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بواسطة جهاز الحاسوب".

كما عرفها الفقيه MAWRE " الجريمة الإلكترونية هي الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه"[2].

---

[1]- تركي بن عبد الرحمان المويشر، مرجع سابق، ص15- 16.

[2] -غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، طبعة 2015، ص 23.

2- على أساس معيار توفر المعرفة بتقنية المعلومات:

اصحاب هذا الاتجاه لا يعتمدون على الحاسوب الآلي ، ولكن على الشخص الذي يستخدمه فبدون امتلاكه المعرفة بالتقنية لا يمكنه ان يستعمل الحاسوب ولا ان يرتكب جريمة اصلا فالأستاذ DAVID THOMSON عرفها بأنها "اي جريمة يكون متطلب لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب".

هنا المعيار الشخصي المتعلق بالجاني هو المعيار المعتمد، إذا تتم متابعة وملاحقة مقترف الفعل غير المشروع في حالة واحدة وهي علمه بتكنولوجيا الحاسبات الآلية.

3- على اساس معيار موضوع الجريمة:

يرى آخرون ان تعريف الجريمة الالكترونية انما يرجع الى موضوعها وغير متعلق بالوسيلة المستعملة او الفاعل ، حيث يرى هؤلاء ان الجريمة الالكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي دون النظر فيما اذا كان الحاسب هو الأداة المستعملة في ارتكابها[1].

ثانيا: التعريف الموسع للجريمة المعلوماتية:

من البديهيات ان الوسيلة التي ترتكب بها الجريمة التقليدية لا تدخل في تعريفها ولا حتى تمكن الجاني من التقنية، فقد لا يكون الجاني متمكنا ويرتكب الجريمة ولا موضوع الجريمة، وتفاديا للانتقادات التي وجهت للمفهوم الضيق ظهر المفهوم الواسع كما يلي:

عرفها PARKER بما يلي: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه ، أو كسب يحققه".

"كل استخدام في صورة فعل او امتناع من شانه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية او يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني"[2].

اما الفقيهان MIEL و CREDO، فعرفاها بانها " تشمل استخدام الحاسب كأداة الارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج كل المصرح به الحاسوب المجنى عليه أو بياناته".

---

[1] -غنية باطلي، المرجع نفسه، ص 17

[2] - دمان ذبيح عماد بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مجلة الحقوق والعلوم السياسية، العدد 13 جانفي 2020، ص 140.

واشمل تعريف للجريمة المعلوماتية الذي جاء به الدكتور عبد الفتاح بيومي حجازي جريمة تقنية تنشا في الخفاء، يقترفها مجرمون اذكياء يمتلكون أدوات المعرفة التقنية ، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات[1].

ثالثا: التعريف الفقهي المختلط او الجامع:

ان اعطاء تعريف موسع للجريمة المعلوماتية ادخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسب سواء وسيلة او موضوع أو مناسبة ارتكاب هذا ما ادى الى ظهور اتجاه ثالث وهو الاتجاه الجامع و يعتمد هذا الاتجاه في تعريف الجريمة المعلوماتية على معيار المصلحة المحمية.

وقد اعتمده M. ALTERMAN و H BLOCH " كل سلوك غير مشروع او يتعارض مع قواعد السلوك او غير مرخص والذي يخص المعالجة الآلية للمعطيات أو لنقل المعطيات".

وهو تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي والذي أوردته بلجيكا في تقريرها بان الجرائم المعلوماتية : هي كل فعل او امتناع من شانه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[2].

الفـرع الثـالث: التعريف القانوني.

تطرق المشرع الجزائري للجريمة المعلوماتية لأول مرة من خلال تعديله لقانون العقوبات بموجب القانون رقم 04-15[3]، وسماها بجرائم المساس بأنظمة المعالجة الآلية للمعطيات دون تعريفها، ثم أعاد تنظيمها بموجب القانون: 09-04[4]، وسماها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها في المادة الثانية بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

---

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي نموذجي الإسكندرية، دار الفكر العربي، القاهرة، 2009، ص 33.

[2]- خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع ، الجزائر، 2008، ص 25.

[3]- القانون رقم 04-15، المؤرخ في 10-11-2004، يعدل ويتمم قانون العقوبات، ج ر، عدد 71، المؤرخة في2004/11/10.

[4] - القانون رقم 09-04 مؤرخ في 05-08-2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 47، المؤرخ في2009/08/16.

و هو تعريف يجمع بين الجرائم المعلوماتية البحتة المرتبطة بالمنظومة المعلوماتية (جرائم المساس بأنظمة المعالجة الآلية للمعطيات)، وباقي الجرائم المرتكبة بوسيلة معلوماتية حصر المشرع وسيلة ارتكابها في المنظومة المعلوماتية، أو نظام للاتصالات الإلكترونية.

وأمام التطور المتلاحق للجرائم المعلوماتية، و ارتكابها باستعمال أحدث تقنيات تكنولوجيا الإعلام والاتصال، وتوظيفها لنشر الحملات العدائية ضد الوطن، أعاد المشرع تعريف هذه الجرائم بموجب الأمر 21-11، حيث نص في المادة 211 مكرر 22، الفقرة الأخيرة" يقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال: "أي جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية، أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال"[1].

و للوصول إلى المعنى المقصود فإنه يتعين تحديد معاني المصطلحات التي تضمنها هذا التعريف وهي:

أولا – النظم المعلوماتية: عرفت اتفاقية بودابيست لمكافحة الجرائم المعلوماتية في مادتها الأولى النظم المعلوماتية بأنها كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى، تنفيذا لبرنامج معين، بأداء معالجة آلية للبيانات المعلوماتية وتعني هذه الأخيرة كل تمثيل للوقائع، أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية، بما في ذلك برنامج معد من ذات الطبيعة يجعل الحاسوب يؤدي المهمة[2].

أما المشرع الجزائري فقد عرفها في المادة 02 من القانون 09-04 بأنها: "نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

فهي تعني بذلك مجموعة من الحواسيب المنفردة، أو المتصلة ببعضها البعض بواسطة شبكات اتصال داخلية أو خارجية، تعمل بصفة آلية وفق برامج مصممة خصيصا لتحقيق معالجة آلية للمعطيات.

[1] – الأمر رقم 21-11، المؤرخ في 2021/08/25، المعدل والمتمم للأمر 66-155، المتضمن قانون الإجراءات الجزائية. ج ر، العدد65، المؤرخ في 1966/06/08،

[2]– انبثقت اتفاقية بودابست عن اجتماع المجلس الأوروبي بتاريخ 23-11-2001، تحت رقم185، تحت عنوان" اتفاقية بودابست لمكافحة الجريمة المعلوماتية"، دخلت حيز التنفيذ بتاريخ: 2004/07/01 (للإشارة الجزائر لم تصادق على هذه الإتفاقية).

ثانيا: الاتصالات الإلكترونية: عرفها المشرع الجزائري بموجب المادة 02 من القانون رقم 09 04 بأنها: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

وقد عرفت المادة الأولى من القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها الوسيط الإلكتروني بأنه ارتباط بين أكثر من وسيلة لتقنية المعلومات الحديثة للحصول على البيانات والمعلومات الإلكترونية وتبادلها، ويقصد به شبكة الحاسب الآلي أو الأنترنيت، أو أية شبكة إلكترونية أخرى".[1]

فشبكة الاتصال هي أداة ربط بين حاسوبين أو أكثر، هذه الرابطة قد تكون مرتبطة تحت الأرض مثل الأسلاك أو الكابلات، كما يمكن أن تكون لا سلكية، أو بالأشعة تحت الحمراء، أو بالأقمار الصناعية، ويمكن أن تكون الشبكة محلية مقتصرة جغرافيا على منطقة صغيرة، أو تكون متسعة النطاق فهي تشكل مجموعة من الأنظمة المعلوماتية المتصلة.

ثالثا: تكنولوجيات الإعلام والاتصال: برزت تكنولوجيات الإعلام والاتصال كتكنولوجيا مستقلة بواسطة مزيج تكنولوجيا معالجة البيانات مع الاتصالات السلكية واللاسلكية فالأولى تعطي القدرة على معالجة وتخزين المعلومات، أما الثانية فهي الحامل لتوصيلها، هذا المزيج تم إحداثه بفضل المكونات الإلكترونية الدقيقة وتجهيزاتها المعقدة[2].

ورغم أن المشرع الجزائري لم يشر إلى تعريف مصطلح تكنولوجيات الإعلام والاتصال الذي يعد جديدا في نظر رجال القانون، فإنه يعني: "مجموعة التكنولوجيا المتقدمة التي أتاحتها الحاسبات الإلكترونية الدقيقة والاتصالات السلكية واللاسلكية المتطورة بواسطة الأقمار الصناعية وبعدها والاستثمار من بعد والمحطات الأرضية والبحرية للاتصالات اتاحتها الحاسبات الإلكترونية الدقيقة، والاتصالات السلكية واللاسلكية المتطورة بواسطة الأقمار الصناعية وبغيرها، والاستثمار من بعد والمحطات الأرضية والبحرية للاتصالات وشبكات بنوك المعلومات الإلكترونية، وما تستخدمه من وسائل اتصال متطورة مباشرة وغير مباشرة، وتعني أيضا:

[1]– علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط 1، منشورات زين الحقوقية والأدبية، سنة 2013، ص32

[2] – زرزار العياشي، غياد كريمة، استخدامات تكنولوجيا المعلومات والاتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية، ط 1، دار الصفاء للنشر والتوزيع، عمان، 2016، ص 29.

اكتساب ومعالجة وتخزين واسترجاع ونشر المعلومات عن طريق التكامل بين أجهزة الحاسبات الإلكترونية ونظم الاتصالات الحديثة"[1].

أو هو "مجموعة التقنيات المستخدمة في معالجة ونقل المعلومات خاصة الإعلام الآلي الانترنيت العمل التعاوني عن بعد الإدارة الإلكترونية للأنشطة، وغيرها من الدعائم الإلكترونية المساعدة في عمليات الاتصال"[2].

فتكنولوجيا المعلومات الحديثة هي التكنولوجيا التي أنتجها اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات، وهي تختلف عن تكنولوجيا المعلومات قبل الاندماج وبالتالي لا يجوز التدليل على الجرائم الناشئة عن إساءة استخدام وسائط هذه التكنولوجيا الحديثة باصطلاح يقتصر على تناول أحد أجنحتها دون الجناح الآخر، أو باصطلاح يتجاهل المفهوم الحالي لهذه التكنولوجيا، فالمصطلح لا بد أن يتسم بالمرونة وبعد النظر، بمعنى أنه لابد من وأن يراعى المستقبل، وما قد يفرزه لنا هذا التطور الهائل من الاختراعات الالكترونية من أجهزة غريبة تظهر كل يوم، ولا يصدق العقل بإمكانية اكتشافها[3].

يتبين من خلال ذلك بأن المشرع الجزائري وسع في تعريف الجرائم الإلكترونية بموجب الأمر 21-11، لتمتد إلى كل جريمة وقعت على النظم المعلوماتية أو ارتكبت باستعمال أي وسيلة ذات صلة بتكنولوجيات الإعلام والاتصال لتشمل بذلك كل الجرائم المرتكبة باستعمال التكنولوجيات القديمة والحديثة وعلى كل تقنية تظهر مستقبلا، وذلك بعدما كان يحصر وسيلة ارتكابها في المنظومة المعلوماتية أو نظام للاتصالات الإلكترونية.

ترتيبا على كل هذه التعاريف يمكننا تعريف الجريمة المعلوماتية بأنها " **كل سلوك غير مشروع يمس النظام المعلوماتي المادي أو المعنوي أو كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته و يمس بالأشخاص و الأموال أو امن الدولة بواسطة جهاز الحاسوب، أو باستخدام جهاز تكنولوجي".**

[1] – محمد الفاتح حمدي، استخدامات تكنولوجيا الإعلام والاتصال الحديثة وانعكاساتها على قيم الشباب الجامعي، مذكرة ماجستير، كلية العلوم الاجتماعية والعلوم الإسلامية، جامعة الحاج محمد الخضر، باتنة 2008-2009 ، ص 22.

[2] – فاروق عبده فلية، أحمد عبد الفتاح الزكي، معجم مصطلحات التربية لفظا واصطلاحا، دار الوفاء لدنيا الطباعة والنشر، الإسكندرية، 2004، ص ص 127-128.

[3] – علي عبود جعفر، مرجع سابق، ص 26.

المطلب الثاني: خصائص الجريمة المعلوماتية و تقسيماتها:

اختلف الفقه حول تقسيمات الجرائم المعلوماتية، حيث لم تراع أغلب التقسيمات خصائص الجرائم المعلوماتية وموضوعها، إذ نجد أهم ما يميز هذه الجرائم هو استهدافها البيانات المعنوية للحاسوب الآلي وترتكب بواسطة جهاز الإلكتروني، كما اختلف الفقهاء في تقسيم الجرائم الإلكترونية نتيجة ظهور جرائم جديدة من حين إلى أخر، أي أنها غير محصورة فلا يمكننا أن نجمل أصنفها وأشكالها وخصائصها فهي متغيرة ومتجددة، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الآلي ظهرت معها جريمة جديدة هذا من جهة ومن جهة أخرى كثرتها وسرعة تطورها، بناء على ما سبق سنتناول في هذا المطلب خصائص الجريمة المعلوماتية (فرع الأول) ثم نعرج إلى تقسيماتها من خلال الفرع الثاني.

الفـرع الأول: خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى التقليدية وهذا ما يشكل تحدي تشريعي أخر للمشرع، فلا يمكن لنا تصور وجود نصوص قانونية ناجعة على المستوى العملي التطبيقي دون ان تكون للمشرع نظرة على الخصائص التي تميز هذا النوع من الجرائم عن الجرائم التقليدية ومن خلال معرفته بخصائصها تمكنه من وضع اليات قانونية موضوعية واجرائية لمكافحتها ومن بين أهم هذه الخصائص ما يلى:

أولا: بيئة وقوع الجريمة المعلوماتية:

تقع الجرائم المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء عبارة عن نبضات الكترونية فنحن أمام ظاهرة إجرامية ذات طبيعة خاصة لها صلة بما يعرف بالقانون الجنائي المعلوماتي.

ووقوع هذه الجرائم في بيئة المعالجة الآلية للبيانات تستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي تتوافر فيه إمكانيات لتحديدها وتعديلها ومحوها وتخزينها واسترجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم[1].

[1] – نهلا عبد القادر المؤمني، الجرائم المعلوماتية، ط 02، دار الثقافة للنشر والتوزيع، ص51.

ثانيا: الجريمة المعلوماتية عابرة للحدود:

لقد أذابت شبكة الإنترنت الحدود الجغرافية بين دول العالم ولم تعد جريمة تخضع لنظام إقليمي محدود و إنما أصبحت تقع في بلد وتمر عبر بلد آخر، وتتحقق نتيجتها في بلد ثالث وكل ذلك في ثواني محدودة فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بإمكان ارتكاب جريمة عن طريق حاسوب موجود في دول معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، وهذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه. إضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، ولقد كانت القضية لمعروفة باسم مرض نقص المناعة المكتسبة من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية[1].

وتتلخص وقائع هذه القضية التي حدثت عام 1989 بقيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره الى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس حصان طروادة، إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس وفي 03 فيفري 1990 تم إلقاء القبض على المتهم جوزيف بوب في الولايات المتحدة الأمريكية وتقدمت بريطانيا بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة (بريطانيا) ووافق القضاء الأمريكي على تسليمه وكانت هذه هي المرة الأولى التي يسلم فيها متهم في الجريمة المعلوماتية[2].

ثالثا: صعوبة اكتشافها.

تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة فمن المفترض أن اكتشافها يتم عن طريق الفحص الدقيق أو عن طريق الشكوى التي يقدمها المجني عليه ويمكن رد الأسباب التي تقع وراء الصعوبة في ذلك إلى:

---

[1]–محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دون طبعة، دار النهضة العربية، القاهرة، ص 37.

[2] – نهلا عبد القادر المؤمني، المرجع السابق، ص 53.

- أنها جريمة هادئة لا عنف فيها.
- أنها جريمة فنية لا تترك أثرا كالآثار التي يتركها اقتحام مكان للسرقة مثلا.
- أنها جريمة تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسب الآلي.

وبالتالي فلا يستطيع القارئ العادي أن يعرف البيانات التي كانت مثبتة قبل تغييرها أو محوها فيكون من العسر اكتشافها، كما أن التغيير والمحو لا يتمان علنا وإنما بطريقة خفية لا تترك أثرا كتابيا يدل على السلوك الإجرامي الذي يتم بمجرد النبضات الالكترونية التي تقضي إلى نقل المعلومات، فلا شك بأنه كلما تقدم الإنسان في فهم تكنيك العمل في الحسابات الآلية كلما استطاع أن يرتكب جريمته دون أن يخلف أية آثار يمكن الاهتداء إليه من خلالها، سواء وقعت داخل الحدود أو امتدت إلى الخارج من خلال استخدام شبكات الاتصال لا تترك أية أدلة على حدوثها، لذلك يحجم رجال الأعمال عن الإبلاغ عنها خوفا على سمعتهم، بالإضافة إلى أنه يمكن تدمير المعلومات التي تستخدم كأدلة إثبات في بضعة أجزاء من الثانية[1].

رابعا: صعوبة إثباتها:

يصعب إثبات الجريمة المعلوماتية نظرا لكونها ترتكب بواسطة أو على الانترنت ومن قبل شخص ذي دراية فائقة بها، وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة و التخلص من آثارها وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها والقبض عليهم على غرار الجريمة التقليدية والى جانب الأسباب السابقة ، فانه تعود صعوبة إثبات الجرائم المعلوماتية إلى:

- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.
- أنها تعتمد على قمة الذكاء والمهارة في ارتكابها.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها فهؤلاء يعتمدون على التخفي عبر دروب الانترنت تحت قناع فني.
- يلعب البعد الزمني (اختلاف المواقيت بين الدول) والمكاني(إمكانية تنفيذ الجريمة عن بعد) والقانوني (القانون الواجب التطبيق) دورا مهما في تشتيت جهود التحري والتنسيق الدولي يتعقب مثل هذه الجرائم[2].

[1] – محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديد، الإسكندرية، 2001، ص ص97-98.

[2]– نبيلة هبة هروالة، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 40.

- عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثبات الجرائم المعلوماتية، ومن ثم يلزم البحث عن أدلة جديدة حديثة ناتجة عن ذات الحاسب ومن هنا تبدأ صعوبات البحث عن الدليل وجمع هذه الدليل[1].

خامسا: أسلوب ارتكاب الجريمة المعلوماتية:

لا تتطلب جرائم الانترنت عنفا لتنفيذها، بل تنفذ بأقل جهد ممكن وتعتمد على الخبرة في المجال المعلوماتي بشكل أساسي عكس الجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة، إذن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى عنف بل كل ما تحتاج هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير مشروعة.

سادسا: الجريمة المعلوماتية تتم بتعاون عدة أشخاص:

تتم عادة بتعاون أكثر من شخص، حيث تتميز الجريمة المعلوماتية أنها ترتكب من طرف شخصين أو أكثر، الأول يكون متخصص في تقنيات الحاسوب والانترنت يقوم بإخراج الجريمة إلى الواقع وحيز الوجود حيث يقوم بالجانب الفني من المشروع الإجرامي وشخص أخر يكون من المحيط لتغطية عملية التلاعب وتحويل المكاسب إليه والاشتراك في الجريمة الإلكترونية له صورتين أولهما اشتراكا سلبياً المتمثل على من يعلم بوقوع الجريمة في محاولة منه لتسهل إتمامها، أما الجانب الأخر فهو إيجابي يتمثل في المساعدة الفنية والمادية[2].

الفـرع الثـــاني: تقسيمات الجريمة المعلوماتية:

لا تخلو محاولات تحديد وتصنيف الجرائم المعلوماتية من الصعوبة، ويرجع ذلك بصفة أساسية إلى التطور التكنولوجي المستمر فالجريمة المعلوماتية تلاحق هذا التطور التكنولوجي في كل صوره للارتباط الوثيق بينهما، ولم تقف هذه الصعوبة حائلا دون المحاولة لتحديد الجرائم المعلوماتية وتقسيمها إلى طوائف مختلفة تتميز كل منها بسمات خاصة بها، ورغم تعدد التقسيمات واختلافها فيما بينها من حيث أشكال السلوك، إلا أنهيمكن حصر أنواع الجرائم المعلوماتية، فمنها من يستمد تجريمه من القانون العام ولكن الوسيلة المرتكبة تكون بواسطة تكنولوجيا المعلومات ومنها من يستمد تجريمه من القانون الخاص ولكن الوسيلة المرتكبة تكون بواسطة تكنولوجيا المعلومات ومنها من تكون الأنظمة المعلوماتية هي الهدف المعتدى عليه

[1]– محمد عبد الله أبو بكر سلامة، موسوعة الجرائم المعلوماتية، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006، ص97.

[2] – نهلا عبد القادر المؤمني، المرجع السابق، ص 58.

وكخلاصة يمكن أن يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الالكترونية ومن ناحية أخرى، قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها، وتقسم الجرائم المعلوماتية إلى:

أولا: الجرائم الواقعة بواسطة النظام المعلوماتي:

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها و يهدف الجاني من ورائها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاتها وبرامجه كوسيلة لتنفيذ الجريمة[1].

فجرائم القانون العام المرتكبة بواسطة تكنولوجيا المعلومات مثلا هي جرائم في الأصل يعاقب عليها القانون العام وبذلك تخضع هذه الجرائم في تعريفها وتحديد عناصرها وأركانها والعقوبة المقررة لها في التشريع الجزائري للقواعد العامة المنصوص عليها في قانون العقوبات، فهي في الحقيقة أعمال غير مشروعة ترتكب ضد الأشخاص أو الأموال أو كلاهما معا بواسطة وبمساعدة تكنولوجيا المعلوماتية مثل جرائم القذف و النصب و السب والإشادة بالأعمال الإرهابية، كما أن جرائم القانون الخاص المرتكبة ضمن تكنولوجيا المعلوماتية هي جرائم في الأصل تعاقب عليها بعض القوانين الخاصة وهي أفعال مرتبطة ارتباطا وثيقا بتكنولوجيا المعلومات وهي بذلك تكون مدرجة ضمن الحقل المعلوماتي مثل الجرائم الماسة بحقوق المؤلف والحقوق المجاورة كجرائم الاعتداء على أنظمة الإعلام الآلي ومواقع الانترنيت، الجرائم الماسة بالعلامات التجارية، الجرائم الماسة بتسميات المنشأ، الجرائم الماسة بالرسوم و النماذج الصناعية[2]، وتنقسم هذه الجرائم بدورها إلى:

01- الجرائم الواقعة على الأشخاص:

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول في المعلومات الخاصة للأشخاص عليه ظهرت عدة أنواع خاصة من الجرائم الإلكترونية الواقعة على الأشخاص كجريمة، خاصة عن طريق البريد الإلكتروني بإرسال رسالة التهديد والمضايقة الملاحقة و خاصة للترويع و التهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنيت كالفيسبوك، الفايبر و الواتساب[3].

---

[1] – سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق، جامعة بوبكر بلقايد تلمسان، الجزائر 2010، ص12.

[2] – ديش سورية، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص 241.

[3] –يوسف صغير، الجرائم المرتكبة عبر الإنترنيت، رسالة لنيل الماجيستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر، ص 50.

و كذلك جريمة القذف و السب و تشويه السمعة للمساس بشرف الغير و كرامتهم واعتبارهم عن طريق وسائل الاتصال المباشر أو الكتابة أو عن طريق المطبوعات أو المبادلات الإلكترونية (البريد الإلكتروني) صفحات الويب، غرف المحادثة.

كما تعتبر من أهم الجرائم الإلكترونية الواقعة على الأشخاص صناعة ونشر الإباحة و الجنس سواء للبالغين و الأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الإنترنيت بأشكال متعددة انطلاقا من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الإنترنيت[1].

يضاف إلى الجرائم الإلكترونية الشخصية جرائم انتحال الشخصية و التغرير و الاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان انتحال شخصية الفرد و انتحال شخصية الموقع[2].

02- الجرائم الواقعة على الأموال:

لقد صاحب تطور شبكة الإنترنيت تطور وسائل الدفع و الوفاء، و أضحت جزاً من المعاملات الإلكترونية و في خضم هذا التداول المال ي عبر الإنترنيت ظهرت عدة جرائم إلكترونية على الأموال مثل السطو، السرقة، التحويل الإلكتروني غير المشروع الأموال و قرصنة أرقام البطاقات الممغنطة حيث أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالطريقة الغير مشروعة ممكنة عبر قنوات شبكة الإنترنيت[3].

كما ظهرت جريمة القمار و غسيل أموال عبر الإنترنيت بظهور الكازينوهات الافتراضية أو أندية القمار الافتراضية التي أصبحت فيما بعد مسرحا كذلك لجريمة غسيل الأموال، حيث ساعدت الشبكة العنكبوتية في انتشارها و تطورها بنقل هذه الجريمة من دولة إلى دولة أخرى لاستثمارها في مجالات مشروعة[4].

---

[1]- عبد الرحمان بن عبد الله السيد، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي و شبكة المعلومات و الأنترنيت) دار الوراقين للنشر و التوزيع، بيروت، الطبعة الأولى، 2004 ، ص 312.

[2]- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الالي و الإنترنيت في مصر و الدول العربية، المكتب العربي الحديث، الإسكندرية، 2006، ص102.

[3]- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2010، ص ص، 76 -77.

[4] - صالحة العمري، جريمة غسل الأموال و طرق مكافحتها، مجلة الإجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، ص 179.

03- الجرائم الواقعة على أمن الدولة:

تعد هذه الجرائم من أخطر الجرائم المعلوماتية خاصة الإرهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث أتاحت الانترنيت للكثير من المنظمات الإرهابية الترويج لأفكارها ومعتقداتها وأدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الالكتروني على الدول بالاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام.

ثانيا: الجرائم الواقعة على النظام المعلوماتي:

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية تمس النظام المعلوماتي و تستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي[1].

و الجرائم الواقعة على الأنظمة المعلوماتية هي تلك الأفعال الغير مشروعة التي تجعل من الدعامة المادية للأنظمة المعلوماتية أو الأنظمة المعلوماتية هدفا لها مثل جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهذا من خلال عملية اختراقها باستعمال الفيروسات.

ويمكن أن تكون لهذه الأفعال الغير مشروعة التي تجعل من الدعامة المادية للأنظمة المعلوماتية أو الأنظمة المعلوماتية هدفا لها تجريم خاص ضمن بعض المجالات إذا ما ارتبطت بالتقليد كتقليد الاختراعات، أو التصاميم الشكلية للدوائر المتكاملة، أو برامج الحاسوب، والجرائم الواقعة على النظام المعلوماتي.

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات و الشرائط و الكابلات، و نتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها كأن تكون محل للسرقة و خيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة، و لقد حدث هذا النوع من الجرائم في فرنسا و أدى إلى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، و قدرت الخسائر ب 5 ملايين فرنك فرنسي[2].

[1]- سوير سفيان المرجع السابق، ص 39.

[2] - ديش سورية، المرجع السابق، ص247.

ثالثا: الجرائم الواقعة على البرامج الإلكترونية: تنقسم هذه الجرائم بدورها إلى:

01- الجرائم الواقعة على البرامج التطبيقية: تكون عن طريق تحديد البرنامج أولا ثم التلاعب به وتعديله، ومن أمثلتها قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick[1].

02- الجرائم الواقعة على برنامج التشغيل: هي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، و تقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثالها جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة و مثاله ما قامت به إحدى شركات التأمين الأمريكية في مدينة لوس أنجلس بواسطة مبرمجها تصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 460 بهدف تقاضي هذه الشركة لعمولات من اتحاد شركات التأمين.

رابعا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

تعد المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة إذ لم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية[2].

[1]- سوير سفيان، المرجع السابق، ص 39.

[2]- ديش سورية، المرجع السابق، ص 248.

المبحث الثاني: أطراف الجريمة المعلوماتية و دوافعها:

ينظر إلى شبكة الإنترنت دائما بوصفها أداة محايدة، وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته والذي غالبا ما يهيئ الفرصة المناسبة لاستغلال الوسيلة المعلوماتية التي أعدها سواء عن حسن نية أو لا فجوهر المشكلة مرتبط بذات الإنسان وشخصيته ودوافعه التي تحفزه للقيام بسلوك إجرامي عبر شبكة الإنترنت من أجل تحقيق نتيجة إجرامية، على حساب ضحاياه.

انطلاقا مما سبق سنقوم في هذا المبحث بدراسة طرفي الجريمة المعلوماتية من خلال (المطلب الأول) ثم نعرج على الدوافع التي تؤدي إلى ارتكاب هذه الجريمة (المطلب الثاني).

المطلب الأول: أطراف الجريمة المعلوماتية:

إن الجرائم المعلوماتية كغيرها من الجرائم تحتاج إلى أطراف، إلا إن أطراف الجريمة المعلوماتية يختلفون نوعا ما عن أطراف باقي الجرائم، ومما لاشك فيه أن الشخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية لإجراء الجريمة، وقد يكون عبارة عن مجموعة أشخاص تمثل شخصا معنويا و الشخص الطبيعي والمؤسسات العامة والبنوك وغيرها التي تحمل صفة الشخص المعنوي معرضون لاعتداءات عن طريق هذه الشبكة من المعلومات، ويمكن تحديد أطراف الجريمة المعلوماتية بالجاني أو المجرم المعلوماتي الذي سوف نتناوله في الفرع الأول، والمجني عليه أو الضحية الذي سوف نتطرق له في الفـرع الثـاني والشـاهد الـذي سنشير إليه في الفرع الثالث.

الفـرع الأول: الجاني في الجريمة المعلوماتية أو المجرم المعلوماتي:

في الجريمة المعلوماتية لا نكون بصدد مجرم عادي بل أمام مجرم ذي مهارات تقنية وذي علم بالتكنيك المستخدم في نظام الحاسبات الآلية، فشخصية المجرم المعلوماتي سواء أكان طبيعيا أو معنويا وآلية ارتكاب الجريمة تجعل منه شخصا يتسم بسمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي.

أولا: أصناف المجرم المعلوماتي:

أدى التطور في مجال استعمال الإنترنت إلى ظهور عدة أصناف من المجرمين يصعب حصرهم تحت طوائف محددة، فالمجرم المعلوماتي مجرم متخصص و محترف في تنفيذ جريمته المعلوماتية، حيث أن ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر، خلافا على المجرم العادي المجرم المعلوماتي لا يلجأ إلى العنف في تنفيذ جريمته، فهو في الغالب مجرم ذكي يتمتع بالمهارة و المعرفة و بدرجة عالية من الثقـافة[1].

[1]– رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر ،الجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس، لبنان، 24–25 مارس،2017، ص 101.

هناك عدة طوائف من المجرمين المعلوماتيين طائفة القراصنة (أولا)، طائفة مجرمو المعلومات أصحاب الآراء المتطرفة (ثانيا)، طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية (ثالثا)،طائفة مجرمو المعلومات في إطار الجريمة المنظمة (رابعا)، طائفة الحكومات الأجنبية (خامسا)، طائفة صغار السن (سادسا) سنتطرق إليهم بالتفصيل:

01- طائفة القراصنة: قراصنة المعلومات هم في الغالب مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى أنظمة المعلوماتية غير المسموح لهم بدخولها و كسر الحواجز الأمنية المحيطة بهذه الأنظمة، و يمكن تصنيفها إلى صنفين هما:[1]

أ- القراصنة الهواة Haekers: هذا القسم من القراصنة يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية و هذه الطائفة غالبا ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا أو مجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى[2].

ب- المحترفون Crackers: و هم ممن يحملون درجات جامعية عليا تخصص حاسب آلي و شبكات معلومات و يعملون محللي نظم و مبرمجين و يكونون على دراية ببرامج التشغيل[3].

02- طائفة مجرمو المعلومات أصحاب الآراء المتطرفة: هم فئة من المجرمون الذين يستخدمون الشبكات المعلوماتية و نشر أفكارهم الدينية والسياسية أو الاقتصادية المتطرفة، و يتميزون بكونهم لا يهدفون لتحقيق مكسب شخصي أو الحصول على نفع مادي ما، بل يعملون على تغيير المجتمع ليتماشى و يتوافق مع ما يعتقدون صحته من الأفكار والمعتقدات، و غالبا ما يتم ذلك عن طريق استخدامهم كافة المواقع الإلكترونية التي تسعى لتحقيق أغراض دعائية لصالحهم[4].

---

[1]- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، الجزائر، 2012، ص 38.

[2]- حمزة بن عقون، المرجع نفسه، ص39.

[3]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، مصر، 2008، ص 146.

[4]-رضية بركايل، التنظيم القانوني الجزائري للجريمة المعلوماتية في التشريع الجزائري، الملتقى الوطني حول الأمن المعلوماتي مهدداته وسبل حمايته، جامعة مولود معمري، تيزي وزو، الجزائر، 03-04 نوفمبر 2015، ص 224.

03- طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية: بحكم طبيعة عمل هؤلاء و نظرا لأن النظام المعلوماتي هم مجال عملهم الأساسي، و نظرا للمهارات و المعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، و أهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف و المجني عليه تجعل عملية ارتكاب الجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها[1].

04- طائفة الحكومات الأجنبية: مهمتهم استخباراتية تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها، سواء كانوا يعملون لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها، ومن مقتضيات عملهم ألا يتركوا دليلا عن عملهم، ويعرف الجاسوس "بأنه الشخص الذي يقوم بمجموعة من الأعمال المنجزة لصالح بلد أجنبي يهدف إلى إيقاع الضرر بسلامة بلد آخر و تكون غالبا معلومات سرية عن الجيوش أو أجهزة المخابرات و سواها، و ذلك بطرق ملتوية و مخالفة للقانون ما يعرضه لعقوبات قاسية"[2].

05- مجرمو المعلومات في إطار الجريمة المنظمة: وجدت هذه المنظمات في شبكة الانترنت وسيلة لا تضاهيها أخرى للقيام بعمليات تبييض الأموال على نطاق ومجال واسع، وكذلك لتدعيم تجارة الرقيق الأبيض، وتجارة الأعضاء البشرية.

كما تقوم هذه المنظمات الإجرامية المنظمة بتبني أصحاب الكفاءات والخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغرائهم بالمال لينظموا إلى صفوفها، ويمارس مجرمو المعلوماتية في نطاق هذه المنظمات نشاطات تدرّ على المنظمة أرباحا هائلة، فيقومون بتزوير البرامج وتقليدها، واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى[3].

06- طائفة صغار السن: يسميهم البعض صغار نوابغ المعلوماتية (Pranksters)، وتضم هذه الطائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح، دون أن تكون لديهم نية إحداث أي ضرر عليهم، وذلك عن طريق استخدام حاسبات آلية محمولة خاصة بهم أو حاسبات آلية خاصة بمدارسهم، ومن بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية، وعلى الرغم من صغر سنهم إلا أنهم قادرين على اقتحام أنواع الأنظمة البنكية و الشركات و المؤسسات المالية.

---

[1] -حمزة بن عقون، مرجع السابق، ص 43.

[2] -عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون كلية الحقوق و العلوم السياسية جامعة أبو بكر بلقايد تلمسان الجزائر، 2018، ص 108.

[3] - نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في القانون كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، الجزائر، 2013 ، ص 53.

ثانيا: سمات المجرم المعلوماتي:

يتميز المجرم في الجرائم المرتكبة عبر الإنترنت بسمات وخصائص تميزه عن المجرم في الجرائم التقليدية، فهو مجرم ذو كفاءة عالية في مجال التقنية، فإذا كان المجرم التقليدي يلجأ إلى استعمال العنف في غالب الأحيان، بالإضافة إلى عدم احتياجه إلى مستوى علمي من أجل القيام بأفعاله، فمجرم الإنترنت عكس ذلك، حيث أنه يحتاج فقط إلى جهاز حاسوب موصول بشبكة الإنترنت إلى جانب معرفة ودراية بمختلف الأنظمة المستعملة في هذا المجال، ويمكن حصر هذه السمات على النحو التالي:

01- المهارة: هي إتقان لغة ما أو حرفة ما يولد بها الإنسان أو يكتسبها في حياته، وهي التفنن والإبداع في إظهار شيء ما في أجمل صورة يتمتع مجرمي الانترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والانترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ جريمة الانترنت يتطلب قدرا من المهارة لدى الفاعل الذي قد يكتسبها عن طريق الدراسات المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات[1].

والمهارة هي أبرز خصائص مجرم تكنولوجيا المعلومات، فتنفيذ الجريمة التقنية يتطلب خصائص مجرم تكنولوجيا المعلومات، فتنفيذ الجريمة التقنية يتطلب قدرا من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات الحديثة أو مجرد التفاعل الاجتماعي مع الآخرين، غير أن هذا لا يعني بالضرورة أن يكون مرتكب جريمة تكنولوجيا المعلومات الحديثة على قدر كبير من العلم في هذا المجال أو تكون لديه خبرة كبيرة، بل إن الواقع العلمي قد أثبت أن بعض أنجح مجرمي تكنولوجيا المعلومات الحديثة لم يتلقوا المهارة سوى الحد الأدنى من المعرفة والمهارة لظهور الجريمة أو لإمكانية ظهورها.

قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في المجال التقني، كما أننا نرى عددا لا بأس به من صور جرائم المعلومات التي يتم ارتكابها عبر وسيلة تقنية أي عندما لا يكون نظام المعلومات الإلكترونية هو هدف الجريمة، لا يتطلب سوى الحد الأدنى من المعرفة والمهارة لظهور الجريمة أو لإمكانية ظهورها[2].

---

[1]- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دراسة مقارنة، دار النهضة العربية القاهرة، مصر، 2010، ص 51.

[2]- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر و التوزيع، الأردن، 2010، ص 71

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[1].

ويتمتع مجرمو الانترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب الانترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات ألياً، فتنفيذ جريمة الإنترنت يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا[2].

02- الذكـاء: تحفظ البعض من الفقه حيال رسم صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، وذلك على سند من القول أن بعض أنماط الجريمة المعلوماتية مثل إتلاف الحاسوب الآلي أو تدميره كليا أو جزئيا، أو سرقة المعلومات المخزنة داخل الحاسب الآلي، لا تحتاج في مرتكبها من يكون على قدر كبير من الذكاء، لذلك يتميز المجرم المعلوماتي غالبا بالذكاء ، حيث أن الجريمة المعلوماتية[3].

ويعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتي لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي الذي يميل إلى العف، فهذا المجرم لا يمكن أن ينتمي إلى طائفة المجرمين الأغبياء ، فمن يستعين بجهاز الحاسوب للاستيلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع من الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته.

كما تتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابه للجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحو يدمر هذه البيانات أو يعطل استخدام هذه البرامج.

---

[1]- خالد داودي، الجريمة المعلوماتية، ط 1، دار الإعصار العلمي للنشر والتوزيع، الأردن،2018 ، ص 33.

[2]- محمد الدايج الجريمة الإلكترونية في التشريع الجنائي الجزائري مذكرة لنيل شهادة الماستر مجامعة مستغانم 2016 ص34.

[3]- حمزة بن عقون المرجع السابق، ص 30.

و الذكاء من أهم صفات مرتكب الجرائم عبر الإنترنت، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الولوج إلى أنظمة الحاسب الآلي والقدرة على تعديل والتغيير في البرامج و ارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة من الذكاء لكي يتمكن من ارتكاب تلك الجرائم ، فمجرم الإنترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواء ذلك من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية و من ثم نيل مبتغاه[1].

ولقد أجرى الفقيه بارك الدراسة على مائة و سبعة وعشرون (127) شخصا من بينهم ثلاثة و ستون (63) طفلا بالولايات المتحدة الأمريكية، بمهارة مع صغار آخرين وجد أن هواة الكمبيوتر يعتبرون أشخاصا أذكياء لغاية و متحمسين و ساعين للإنجاز كما أفادت المتابعة لمدة خمسة أعوام على هؤلاء الأطفال أنهم تفوقوا دراسيا بالجامعة وبوظائف مرموقة[2].

03-امتلاك باعث متميز: الدافع أو الباعث أو الغرض أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا و قضائيا واسعا.

والباعث هو " العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام "، وهو إذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو يختلف من جريمة إلى أخرى، تبعا لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لأخر، وهو الهدف الفوري المباشر للسلوك الإجرامي ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات[3].

كذلك هو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة يضل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في غالب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى في الغالب تكون هي الباعث مثل الانتقام من رب العمل، وأيضا مجرد الرغبة قهر نظام الحاسب واختراق حاجزه الأمني[4].

---

[1]-غنام محمد غنام، الحماية الجنائية لبطاقة الإئتمان الممغنطة، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية دبي، الإمارات، 2003، ص 05

[2]- صنور عبد القادر، الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، جامعة مستغانم ، 2017 ، ص 37

[3]- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، 2007، الإسكندرية، ص 115

[4]- جزار منصورية، الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر، كلية الحقوق و العلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2016، ص36.

في دراسة قديمة لإحدى المجالات المتخصص في الأمن المعلوماتي تعرض لها الفقيه باركر Parker خلصت إلى أن 43% من حالات الاعتداء عادة نظم المعالجة الآلية المعلن عنها قد بوشرت بهدف اختلاس الأموال وأن 23%، من أجل سرقة المعلومات وأن 19 أفعال إتلاف و أن 15% سرقة وقت الآلة، أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[1].

أما فيما يتعلق بالرغبة في تحدي و قهر النظام فمن أشهر القضايا المتعلقة بهذه الحالة كان قد تعامل معها مكتب التحقيقات الفيدرالية، أطلق عليها اسم مجموعة الجحيم العالمي تتلخص وقائعها في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية وقد أدين اثنتين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة الأمريكية، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة[2].

04- اختيار الوسائل بعناية: الوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، وفيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسب الآلية هي في أغلب الحالات تتميز بالبساطة والسهولة في الحصول عليها، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج غليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي[3].

هذه الوسائل قد تكون في غالب الأحيان وسائل بسيطة و سهلة الحصول عليها خصوصا إذا كان النظام الذي يعمل به الكمبيوتر من الأنظمة الشائعة أما إذا كان النظام من الأنظمة غير المألوفة فتكون هذه الوسائل معقدة و على قدر من الصعوبة[4].

05- المجرم المعلوماتي متسلط: يقصد بالسلطة في هذا المجال ، جملة الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير منهم لديه سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وتتمثل عادة في امتلاك شفرة الدخول على النظام المعلوماتي وإجراء المعاملات، وقد تكون هذه السلطة أحيانا غير مشروعة في حال سرقة شفرة الدخول.

---

[1]- باركر هو فقيه وباحث اهتم بالجريمة المعلوماتية بشكل عام والمجرم المعلوماتي بشكل خاص.

[2]- بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 01، منشورات الحلبي الحقوقية بيروت، لبنان، 2012، ص 95.

[3]- فلاح عائشة، خصوصية الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق و العلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم 2016، ص 12.

[4]- جزار منصورية المرجع السابق، ص 37

وقد يستغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها فيدون بيانات وهمية وغير صحيحة ويطلب الحاسوب اعتمادها عند إجراء بعض العمليات و مثالها الموظف المشرف على الموظفين على مصالح المحاسبة وصرف الأجور الذي يمكن أن يدرج أسماء بعض الموظفين الوهميين ضمن قائمة الموظفين ثم يمرر عملية صرف الرواتب و يتولى إيداع رواتب الموظفين الوهميين في حسابه الخاص[1].

والسلطة بمفهوم أخر هي الحقوق والمزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة.

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي إجراء المعاملات، كما أن السلطة قد تكون شرعية من الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص أخر[2].

الفـــرع الثاني: الضحية المعلوماتي أو المجني عليه:

إن الضحية في الجريمة المعلوماتية بصفة عامة هو كل من أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع للمعلومات الرقمية[3].

إذ طالت الجرائم المعلوماتية مختلف شرائح المجتمع سواء كانت أشخاص طبيعية أو أشخاص معنوية، ويمكن تقسيم المجني عليهم في الجريمة المعلوماتية إلى الفئات التالية: المؤسسات المالية و الهيئات الحكومية (أولا) ، المؤسسات العسكرية (ثانيا)، الأشخاص الطبيعيون (ثالثا).

أولا: المؤسسات المالية و الهيئات الحكومية: تقع الجرائم المعلوماتية على الأشخاص المعنوية سواء كانت العامة والمتمثلة في مؤسسات الدولة حيث يتم اختراقها لأخذ مشاريعها و أسرارها، أو الخاصة المؤسسات المالية كالبنوك و الشركات المالية حيث ينجذب إليها مرتكبي الجرائم نظرا لما بها من أموال و من أهم هذه المؤسسات المالية هي البورصة لأن أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بين الأشخاص العاديين بل قد يصل الأمر إلى المعاملات المالية بين الدول[4].

---

[1]– الهاشمي كسراوي، الجريمة المعلوماتية، مجلة القضاء والتشريع، العدد 07، مركز الدراسات القضائية، تونس، ص17.

[2]– جزار منصورية، المرجع السابق، ص37.

[3]– مصطفى محمد موسى، المرجع السابق، ص 159.

[4]–خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009، ص 150.

وبالتالي فالهدف الرئيسي لهذه الجرائم يتمثل في النقود و تليها المعلومات باعتبارها الطريق إلى اقتصاد السوق[1].

ثانيا: المؤسسات الأمنية: لم تقتصر حدود ثورة المعلومات على القطاع المدني بل كان لها أكبر الأهمية في تطوير أنظمة الحرب الحديثة و أدت إلى ظهور ما يسمى بحرب المعلومات، حيث أضحت الدولة التي تملك المعلومات هي الدولة الأقوى، لذلك بدأ الاهتمام ينصب على الجاسوسية العسكرية و أصبح إطلاق الأقمار الصناعية من الجهات العسكرية هو المحور الذي يقوم عليه الاتجاه في تطوير الأجهزة والمعدات العسكرية، مما استتبع ظهور حروب جديدة تسمى بحرب المعلومات بين الدول[2].

وتعتمد آليات هذه الحرب على شبكات الحاسبات الآلية في نقل المعلومات عن طريق الشبكات و من خلال الأقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة و نظم المعلومات في أنظمة التسليح، نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها و عرضها بصورة مناسبة أمام القادة لاتخاذ القرار المناسب على أساس أهمية تلك المعلومات[3].

ثالثا: الأشخاص الطبيعيون: أصبح الأشخاص الطبيعيون يعتبرون أكثر ضحايا الجرائم المرتكبة عبر الانترنت، وذلك راجع إلى التزايد المستمر في أعداد المشاركين من خلال الشبكة العالمية للأنترنت، فلم تعد الجرائم المرتكبة عبر الانترنت مقتصرة على القطاعات المالية و العسكرية، و بالتالي فإن كثيرا من الأشخاص يتعرضون لجرائم النصب والسرقة والإتلاف و من الطبيعي أن تكون شبكة الانترنت المجال الخصب لارتكاب تلك الجرائم، حيث أصبحت ملايين الأسرار المتعلقة بالناس سواء كانوا أفرادا عاديين أو في مراكز معينة في متناول كل من يستطيع اختراق شبكة المعلومات التي تنطوي على كل هذه الأسرار[4].

تعتبر جرائم الإتلاف عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الإلكتروني الذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الأشخاص وتعتبر من أكثر الجرائم التي يتعرض لها الأشخاص أيضا سرقة أرقام بطاقات الائتمان[5].

---

[1]– فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكومبيوتر، منشورات الحلبي، لبنان 2003، ص 36.

[2]– خالد ممدوح إبراهيم، مرجع سابق، ص 151– 152.

[3]–يوسف صغير، المرجع السابق، ص 24.

[4]– محمد محمد شتا، المرجع السابق، ص 94.

[5]– يوسف صغير، المرجع السابق، ص 22.

الفــرع الثالث: الشاهد المعلوماتي:

هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسبة الإلكترونية والذي تكون لديه معلومات جوهرية أو مهمة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزاً له عن الشاهد التقليدي[1].

أولا: مفهوم الشاهد في الجريمة المعلوماتية: يعرف الشاهد في الجريمة المعلوماتية على انه هو الفني صاحب الخيرة والتخصص في تقنية الحاسب وشبكات الاتصال الذي تكون لديه معلومات جوهرية لولوج نظام المعالجة الآلية للمعطيات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله.

وتعد الشهادة وسيلة من الوسائل إثبات الجريمة الإلكترونية التي يمكن للمحقق أن يستعين بها والبحث عن الأدلة وتقديمها بين يدي القضاء وهو وسيلة من وسائل إظهار الحقيقة.

ثانيا: أنواع الشهادة المعلوماتية: تنقسم الشهادة في الجريمة الإلكترونية شأنها في ذلك شأن الشهادة في الجريمة التقليدية إلى ثلاثة أنواع الشهادة المباشرة والشهادة السماعية (الشهادة غير المباشرة) والشهادة بالتسامع[2].

01- الشهادة المباشرة: هي المعلومات التي يدلي بها الشخص، والتي وصلت إلى حواسه عن طريق مباشر ودون وساطة شخص كأن يكون هذا الشاهد قد رأى أو سمع أو شم.... الخ، أي أن يقوم الشاهد بالإدلاء بما شاهده من قيام مرتكب الجريمة بأية ترتيبات برمجية تتعلق بمرتكب الجريمة أو من خلال ما شاهده من قيام مرتكب الجريمة بعملية الاختراق لأي ملفات الكترونية أو القيام بأي من أنواع التزوير الالكتروني.

02- الشهادة السماعية أو غير المباشرة: الشاهد هنا لم يرى الجريمة ترتكب أو لم يسمع الجاني يتهدد ويتوعد المجني عليه، لكنه سمع عن طريق شخص آخر وهي تفترض رواية الشاهد عن غيره، فهو لم يعاين الواقعة بنفسه، وإنما سمع غيره بذكر معلومات بشأن ارتكاب جريمة معلوماتية مثل ارتكاب أي من الجرائم الإلكترونية المستحدثة أو جرائم الإنترنت.

---

[1] – هلالي عبد اللاه أحمد، التزام الشاهد في الجرائم المعلوماتية، دار النهضة العربية، مصر، 2000. ص23.

[2] – براهيمي صالح، الإثبات بشهادة الشهود في القانون الجزائري (دراسة مقارنة في المواد المدنية والجنائية)، رسالة الدكتورة في العلوم، كلية الحقوق جامعة تيزي وزو،2012، ص ص 20- 23.

ثالثا: فئات الشاهد المعلوماتي: تتعدد طوائف الشاهد في الجريمة المعلوماتية، وسنعرض لهذه الفئات فيما يأتي[1]:

01- القائم على تشغيل الحاسوب: وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به. ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج وهو يقوم بنقل البيانات من الوثائق إلى وسائط التخزين التي تجري معالجتها بواسطة الحاسوب. ويجب كذلك أن تكون لديه خبرة واسعة في الكتابة السريعة عن طريق لوحة المفاتيح.

02- المبرمجون: وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين مخططو برامج التطبيقات والثانية مخططو برامج النظم حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لإنجاز هذه المواصفات أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج أو الأجزاء[2].

03- المحللون: المحلل هو ذلك الشخص الذي يخلل الخطوات ويقوم بتجميع البيانات الخاصة بنظام معين. ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات. كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب[3].

04- مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به.

05- مدير والنظم: وهم الأشخاص الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية ويدخل ضمنها مدخل البيانات والمعلومات.

---

[1] - خالد ممدوح، المرجع السابق، ص 265.

[2] -على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) المكتب الجامعي الحديث الإسكندرية 2012، ص 62.

[3] - هلالي عب اللاه أحمد، المرجع السابق، ص 24.

06- مــزود و خدمات الإنترنت والاستضافة: يعد من قبيل الشهود على الجريمة المعلوماتية مزود و خدمات الإنترنت والاستضافة، فهذه الجهات حكم دورها الأساسي في ربط المستخدم بشبكة الإنترنت.

يمكن أن تقدم معلومات تساهم في الكشف عن مرتكب الجريمة. فإذا علم مدير الموقع بأن المحتوى موضوع النشر يتضمن جريمة يعاقب عليها القانون فإنه ينبغي عليه الامتناع عن نشره، وإخطار السلطات بذلك.

كما يتعين على مزودي خدمات الاستضافة إبلاغ السلطات بعناوين هؤلاء الأشخاص والبريد الإلكتروني والصفحة الشخصية[1].

وقد ألزم المشرع الجزائري في الفقرة الأولى المادة 10 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة تكنولوجيا المعلومات والاتصال مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية وإمدادهم بكل المعلومات المتعلقة بمحتوى الاتصالات.[2]

[1] -خالد حامد مصطفى، المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الإجتماعي مجلة رؤى استراتيجية، يصدرها مركز الإمارات للبحوث والدراسات الإستراتيجية، المجلد الأول، العدد 02، مارس 2013.

[2] - القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها.

المطلب الثاني: دوافع ارتكاب الجريمة المعلوماتية:

يعتبر الدافع الباعث، العرض أو الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص في الجريمة ، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، لأن القاعدة القضائية تقرر أن الباعث ليس عنصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب فإنها من حيث الدلالة تتمايز[1].

و للجريمة المعلوماتية عدة دوافع[2]، لارتكابها تتباين تبعا لطبيعة المجرم ومدى ثقافته وخبرته في مجال الحاسب الآلي، لأن المتهم يرتكب جريمته بناء على ما لديه من مهارة وخبرة[3]، فيرجع البعض دوافع ارتكاب الجريمة الالكترونية إلى دوافع شخصية والبعض الآخر إلى دوافع خارجية، وكل هذه الدوافع لها مصدر واحد هو الرغبة الإجرامية.

الفـرع الأول: الدوافع الشخصية:

يقصد بالدوافع الشخصية تلك عوامل اللصيقة بشخصية المجرم الإلكتروني والذي تدفعه لارتكاب الجريمة الالكترونية، ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم الالكترونية إلى دوافع مادية وأخرى ذهنية.

---

[1]– إن الدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كمحبة الانتقام، إذن هو قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، أما الغاية فهي الهدف البعيد الذي يرمي إليه جانب ارتكاب الجريمة كإشباع شهوة الانتقام أو مثلا كسلب مال المجني عليه في جريمة القتل.

أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، يتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه القانون (حمزة بن عقون، المرجع السابق ص 46–47).

[2]- يقول الدكتور Adam Graycar مدير المعهد الاسترالي لعلم الإجرام بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

* دافع معين لارتكاب العمل.
* هدف ضحية محاسبته.
* القرصنة المواتية.
*غياب عيون الأمن.

[3]– المتهم ذو خبرة في مجال البرمجة واستخدام شبكات الحاسب الآلي قد يكون هدفه مختلفا عن هدف المتهم الذي لا تتعدى خبرته مجرد تشغيل جهاز الحاسب الآلي.

أولا: الدوافع المادية: يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لارتكاب جريمته المعلوماتية، إلا أن الربح الكثير و الممكن تحقيقه من خلالها يدفع بالمجرم الالكتروني إلى تطوير نفسه حتى يواكب كل حديث يطرأ علي التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاختراق حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرا وراءه.

فالدافع الذي يدفع الجاني لارتكاب جرائمه ضد المؤسسات والشركات الاقتصادية هو الأضرار بهذه الشركات، والحصول على نفع مادي سواء بالمتاجرة بأسرارها الصناعية، أو الاعتداء على حقوقها في الإنتاج، أو الاعتداء على ذمتها المالية، وعليه يمكن القول بأن الدافع لارتكاب الجرائم الالكترونية هو النفع المادي سيحصل عليه الجاني من سيطرته على المعلومات.[1]

فحب المجرم الالكتروني للمال هو عصب الحياة يدفعه للقرصنة أو السرقة أو الاختلاس، عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير مكلف[2].

فالمكسب المادي لا يكون هدفا فقط لمن يتمتع بالكفاءة الفنية العالية و المهارة في مجال التكنولوجي بل المكسب يكون هدفا أيضا لمن هم أقل في المعرفة التقنية وقد يكونون غير مؤهلين على الإطلاق في مجال المعلوماتي، لذلك يكون أسلوبهم لارتكاب الجريمة مختلفان كون الجريمة تكون متعلقة بالحاسب الآلي أو المعلومات، ولكن دون الدخول على أنظمة تلك الحواسب ويكون أسلوب ارتكابهم للجرائم محدودا في مجال معين لا يحتاج إلى خبرة أو مهارة.[3]

ومند بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الانترنيت هو تحقيق الكسب المالي ففي دراسة قديمة للفقيه باركر الصادرة في إحدى المجلات المتخصصة (Sécurité Informatique) في موضوع الأمن المعلوماتي تبين أن: 43 %من حالات الغش المرتبط بالحاسوب من أجل اختلاس الأموال، 29 ترتكب من أجل سرقة المعلومات، 19% ترتكب من أجل الإتلاف و 15% ترتكب من أجل سرقة وقت الحاسوب لأغراض شخصية[4].

---

[1]– محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان 2005، ص 143.

[2] –نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعرف، الإسكندرية، مصر، ص 44.

[3]– أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، بدون دار النشر،2003، ص249.

[4] –ضياء أحمد علي نعمان، الظاهرة لإجرامية بين الفهم والتحليل، دار النهضة العربية، القاهرة، 2001، ص 11.

إذا انتقلنا للدراسات الحديثة كالدراسات المسحية والدراسات الإحصائية والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية N.F.I.C نجد أن هذا الدافع يسود على غيره من الدوافع، ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية.

وهناك فئة من مرتكبي الجرائم الالكترونية يرجع ارتكابهم لها للنجاة من غرق الديون المستحقة أو من المشاكل العائلية الراجعة إلى النقود أو من الخسائر الضخمة لألعاب القمار أو إدمان المخدرات وقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه المرحلة فالغاية تبرز الوسيلة[1].

وفي حالة نجاح المجرم الالكتروني في ارتكاب جريمته الالكترونية فإن ذلك يدر عليه أرباحا كبيرة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه لهذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول الجرائم المعلوماتية، أين أجريت هذه الدراسة، بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية و بنوك و مؤسسات مالية ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجرائم الالكترونية، فقد تبين أن 85% من المشاركين تعرضوا لاختراقات للأنظمة المعلوماتية و أن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات[2].

ثانيا: الدوافع الذهنية: تعتبر الدوافع الذهنية تلك العوامل النفسية اللصيقة بالمجرم الالكتروني تدفعه إلى ارتكاب الجريمة الالكترونية بهدف الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية، والرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية دون أن يكون له نوايا آثمة[3].

---

[1] –ضياء أحمد علي نعمان، المرجع السابق، ص 11.

[2] – وضاح محمود الحمود ونشأت مفطي المجالي، جرائم الانترنيت ، دار المنار للنشر، عمان، 2005، ص 31.

[3] – من أشهر القضايا التي وقعت قضية كان قد تعامل معها مكتب التحقيقات الفدرالية أطلق عليها اسم مجموعة والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية ، وقد أدين 2 من هذه المجموعة جراء تحقيقات التدمير أو النقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الجحيم العالمي Global Hell، تتلخص وقائعها في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض الجهات الداخلية في و. م أ وقد ظهر من هذه التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أو النقاط معلومات حساسة وقد أمضى المحققون ساعات طويلة في متابعة وملاحقة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة، أنظر: رشيدة بوكر، المرجع السابق، ص 97.

ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب الجرائم، وعليه فإن البعض يرى بأن الدافع إلى ارتكاب الجريمة الالكترونية يغلب عليه قهر النظام أكثر من شهوة الحصول على الربح، مع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها، إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا للجرائم الالكترونية من الرغبة في قهر النظام إلا أن الدافع الأخير، يتجسد في نسبة مرتفعة من الجرائم الالكترونية خاصة ما يعرف بأنشطة الـ (Hackers) المتطفلين على النظام والمتجسدة في جرائم التواصل مع أنظمة الحاسب، والاستخدام غير المصرح به النظام الحاسب، واختراق مواقع الانترنيت[1].

يميل مرتكبي هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها، وغالبا ما يجدون الوسيلة إلى تحطيمها أو التفوق عليها بمعنى أصح ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم الالكترونية الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات ، لإظهار تفوقهم على وسائل التقنية[2].

يعتبر هذا الدافع من أكثر الدوافع التي يجري استغلالها من قبل المنظمات الإجرامية (مجموعات الجريمة المنظمة) لجهة استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.

بالإضافة إلى الدوافع الشخصية اللصيقة بشخصية المجرم الالكتروني هناك دوافع أخرى خارجية خارجة عن نطاق المجرم الالكتروني تدفعه لارتكاب الجريمة الالكتروني.

الفـــرع الثاني: الدوافع الخارجية:

إن الإنسان يتأثر ويستسلم للمؤثرات والدوافع الخارجية بارتكابه بعض الجرائم الالكترونية، نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، وتتعدد المؤثرات التي تدفع المجرم الالكتروني إلى اقتراف مثل هذا السلوك من بينها دافع الانتقام والتواطؤ على الإضرار برب العمل ودافع المنشأة.

---

[1]– نسرين عبد الحميد نبيه المرجع السابق، ص 135

[2]– محمد محمود المكاوي، الجوانب الاخلاقية و الاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع، مصر، 2010، ص 52.

أولا: دافع الانتقام وإلحاق الضرر برب العمل:

هناك آثار سلبية في سوق العمل من جهة ، وفي البناء الوظيفي من جهة أخرى ، وقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معينة، وهذه العوامل قد تدفع إلى السرعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب الجرائم الالكترونية، باعثها الانتقام من المنشأة أو رب العمل وتحديدا جرائم إتلاف البيانات وربما تحتل أنشطة زرع الفيروسات وهناك عدة أمثلة، كان دافع الجناة فيها إشباع الرغبة في الانتقام، و التي تمثل الحقد على رب العمل الدافع المحرك لارتكاب الجريمة[1].

و بالتالي فإن دافع الانتقام يعد من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة وذلك إما لفصله من العمل أو تخطيه في الحوافز أو الترقية فيقوم هذا الشخص بالاستعداد مسبقا لمثل هذا الموقف كان يقوم مثلا بزرع برنامج يحمل تعليمات بمسح كافة البيانات في حالة عدم وجود اسمه في كشف الموظفين بالشركة ويقوم عند فصله منها بالانتقام عن طريق تشغيل هذا البرنامج[2]،وكذلك عن طريق احتفاظه بكلمة السر لكي يتمكن من الدخول على نظام الحاسب الآلي الخاص بالشركة وارتكاب أي من الجرائم أو إعطائها لشركة أخرى منافسة لكي تتمكن من الدخول إلى أنظمة تلك الشركة والتجسس على البيانات الخاصة بها.

و يمكن أن يصدر التصرف بغرض الانتقام من دولة معادية لدولة أخرى، وذلك عن طريق إما التجسس على المعلومات أو عن طريق زرع الفيروسات أو ارتكاب جرائم السرقة لأصول الأموال أو المحاولة تسوية صورة هذه الدولة باستخدام الشبكة الدولية للاتصالات[3].

ثانيا: الـدوافع الخاصة بالمنشأة:

يقصد بالدوافع الخاصة بالمنشأة تلك العوامل الخارجية التي تسهل للجاني ارتكاب الجريمة داخل المنشأة باستعماله التقنية المعلوماتية الخاصة بالمؤسسة إذ تكون وسائل ارتكاب الجريمة المعلوماتية في متناوله، إذ يعتقد بعض المتخصصين في تقنية الأنظمة المعلوماتية أن العاملين في منشاة معينة أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية استخدام الأنظمة المعلوماتية وبرامجها الأغراض شخصية

---

[1]– محمد محمود المكاوي، المرجع السابق، ص 51

[2]– كذلك من الأمثلة على ذلك القيام موظف يعمل لدى إحدى شركات التامين لكي يحتفظ بوظيفته التي سبق أن فصل منها بحجز وحدة التخزين المركزية الخاصة بالشركة كرهينة ووسيلة تهديد لرئيسه لإرجاعه للعمل وهو ما حدث بالفعل.

[3]–أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 250.

أو ممارسة بعض الهوايات الدائرة في مجال التقنية ومن شأن ذلك أن يؤدي إلى تمادي بعضهم إلى استخدام الأنظمة بصفة غير مشروعة تصل إلى ارتكاب جرائم خطيرة لمصلحته الخاصة[1].

لأن الشخص المسؤول عن المركز المعلوماتي هو بدون منازع في وضع يمكنه من استغلال نقاط الضعف، المتمثلة بمركز المعالجة وتعد العلاقة بينة وبين الأنشطة التي يزاولها ومركز الثقة الذي يحوزه أفضل أسلحة له لارتكاب جريمته المعلوماتية، ومن أمثلة ذلك قيام مستشار لدى احد البنوك الكبرى يسمى STANLEY RIFKIN، كان يتمتع بثقة مطلقة من جانب هذا البنك وقد سمحت اختصاصاته بالولوج والتحكم في مفتاحين الكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك إلى بنك آخر، وقد تمكن بفضل قدراته في مجال المعالجة الآلية للمعلومات وتالفة الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث واستطاع أن ينقل 100 مليون دولار إلى حساب بنكي فتح باسمه في سويسرا.

وفي الأخير نخلص إلى القول أن هذه هي أبرز دوافع ارتكاب الجريمة الالكترونية، لكنها ليست ثابتة ومعتمدة لدى الفقهاء والباحثين، لأن السلوك الإجرامي والدوافع لارتكاب الجريمة تتغير وتتحول بسرعة من حالة العبث أو محاولة التحدي والتغلب على الأنظمة إلى تدميرها أو على الأقل تقدير حيازتها للقيام بعمليات الابتزاز، أو استعمالها للحصول على الأموال، ولذلك فالدافع لارتكاب الجرائم الالكترونية قد لا يتوقف عند هذه الدوافع، وخير دليل على ذلك أننا نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد أن الجريمة الواحدة لها دوافع متخصصة خاصة إذا اشترك فيها أكثر من شخص وأكثر من جهة بحيث يسعى كل منهم لتحقيق مآربه الخاصة، فمثلا يكون الدافع لمن يسعى للحصول على المعلومات تمثل أسرار تجارية هو المنافسة التجارية، في حيث أن قسماً آخر يسعى في ممارسته لهذه الأنشطة تحقيق أهداف سياسية و إيديولوجية كتلك التي تمارس من قبل الدول[2].

[1]– أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، ط 2006، ص 91.

[2]– ضياء على أحمد نعمان، المرجع السابق، ص 18

خلاصة الفصل الأول

كحوصلة لما تم استعراضه أنفا، يتضح جليا أنمرونةالجرائمالمعلوماتية جعل من وضع تعريف موحد لهافي غاية الصعوبة، إذ اختلف الفقه من الجانب التقني والفني في تعريفها فالبعض استند إلى موضوع الجريمة والبعض الأخر إلى وسيلة الجريمة، غير انهم اتفقوا على وقوعها في بيئة إلكترونية.

أما بالنسبة للتعريف الذي جاء به المشرع الجزائري بعد عدة محاولات فكان بموجب الأمر 21-11 حيث نصت المادة 211 مكرر 22، الفقرة الأخيرة[1]: يقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال: "أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية، أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".

إن الطبيعة الخاصة لهذه الجريمة جعلتها تمتاز بسمات وخصائص تميزها عن باقي الجرائم التقليدية على غرار بيئة وقوعها، وقد تم تقسيمها حسب الفقة الجنائي إلى جرائم واقعة بواسطة النظام المعلوماتي وأخرى واقعة على النظام المعلوماتي.

ككل جريمة هناك ضحية ومجرم ودافع، وقد تعددت أصناف المجرمين والضحايا والدوافع ارتكاب هذه الجرائم بتعدد مجالاتها و تشعب ميادينها.

[1] -الأمر رقم 21-11، المؤرخ في 2021/08/25، ج ر، العدد65، المعدل والمتمم للأمر 66-155، المؤرخ في 1966/06/08، المتضمن قانون الإجراءات الجزائية.

الفصل الثـــــاني
الجرائم المعلوماتية الــواقعة على الأموال
وآليـــــات مكافحتها

تمهيد

لا يمكن إنكار فضل التكنولوجيا الحديثة ومدى مساهمتها في تطوير مجتمعاتنا، لكن في المقابل نجد العديد من الانعكاسات السلبية لهذه التقنيات الحديثة بسبب سوء استخدامها، مما يفتح المجال لارتكاب جرائم عدة من خلالها، على غرار جرائم الاعتداء على المال المعلوماتي.

وقد ساهم ظهور الأموال المعلوماتية بصورة كبيرة في تطور جرائم الاعتداء عليها والمساس بها و بالتالي أصبح المجتمع أمام مسؤولية جديدة تملي عليه معرفة أنواع وصور هذه الجرائم حتى يتسنى له مكافحتها كونها تتميز بسمات جديدة تميزها عما ألفناه في الجرائم التقليدية.

على إثر هذه التحديات الجديدة، وتماشيا مع زيادة معدلات هذا النوع من الجرائم في الجزائر يوما بعد يوم، تدخل المشرع الجزائري على غيره من التشريعات بسن إجراءات جديدة للتصدي لهذا البعد الجديد من الإجرام من خلال جانبين اساسيين وهما الجانب التشريعي الذي عرف تعديلات كثيرة على القوانين ذات الصلة بالمجال المعلوماتي والجانب المؤسساتي من خلال إنشاء مراكز ومصالح مختصة.

بناء لما سبق سوف نتطرق في هذا الفصل إلى دراسة الاموال المعلوماتية وآليات التي تبنها المشرع الجزائري للتصدي لهذه الظاهرة الإجرامية من خلال مبحثين، الأول خصصناه لدراسة المال المعلوماتي في مطلبين الأول تمحور حول طبيعة المال المعلوماتي والثاني حول صور الجرائم الوقعة على الأموال المعلوماتية وفق منظور المشرع الوطني، في حين تطرقنا في المبحث الثاني إلى الأليات و الميكنيزمات التي اقرها المشرع الجزائري لمجابهة هذه الجرائم من خلال مطلبين الأول طرقنا من خلاله للجانب القانوني و الثـاني للجانب المؤسساتي.

المبحث الأول: الطبيعة القانونية للمال لمعلوماتي وصوره في التشريع الجزائري:

إن النظام المعلوماتي يشمل أموال مادية و هي الحاسوب و الأجهزة الملحقة به والشبكات المعلوماتية و يشمل أيضا أموال معنوية و هي المعلومات بكل صورها، إذا انصب موضوع الاعتداء على الأموال في نطاق المعالجة الآلية للمعلومات على الحاسب الآلي ذاته و ما يرتبط به من ملحقات كالسرقة و الإتلاف فهذه الاعتداءات تقع على مكونات مادية للنظام المعلوماتي وبالتالي تخضع للحماية الجنائية بموجب النصوص التقليدية في قانون العقوبات، أما إذا انصب موضوع الاعتداء على الأموال المعنوية للنظام المعلوماتي المتمثلة في المعلومات أو برمجيات ونظم معلوماتية فقد يعتدى عليها عن طريق السرقة أو الإتلاف أو التزوير و العبث بها.

سنحاول من خلال هذا المبحث التطرق أولا للطبيعة القانونية للمال المعلوماتي، ثم نعدد صور الإعتداء على المال المعلوماتي وفق التشريع الجزائري.

المطلب الأول: الطبيعة القانونية للمال لمعلوماتي:

قبل الحديث عن الطبيعة القانونية للمال المعلوماتي وجب أولا تعريف المعلومات بشكل عام ثم تحديد الشروط الواجب توفرها فيها من أجل التمتع بالحماية:

الفرع الأول: تعريف المعلومات و الشروط الواجب توفرها فيها من اجل التمتع بالحماية:

أولا: تعريف المعلومات: عرف الأستاذ "باركر" المعلومات بأنها مجموعة من الرموز أو الحقائق أو المفاهيم او التعليمات التي تصلح لأن تكوم محلا للتبادل و الاتصال أو التفسير و التأويل أو المعالجة بواسطة الأفراد أو الأنظمة الإلكترونية و هي تتميز بالمرونة بحيث يمكن تغييرها و تجزئتها وجمعها او نقلها بوسائل وأشكال مختلفة[1].

كما عرفها البعض أنها " كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها أو تفسيرها على نحو يثري متخذي القرار و مساعدتهم على الحكم السديد على الظواهر و المشاهدات أو يساهم في تطوير المعارف النظرية أو التطبيقية"[2].

[1] – قورة نائلة، جرائم الحاسب الاقتصادية، النهضة العربية القاهرة، 2004، ص 93.

[2] – محمد محمد شتا، المرجع السابق، ص 62.

وتعرف البيانات أنها المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما"[1]، و تسمى العلاقة بين البيانات والمعلومات بالدورة الاسترجاعية للمعلومات إذ يتم تجميع وتشغيل مجموعة اضافية من البيانات و التي يتم تجميعها ومعالجتها مرة اخرى للحصول على معلومة إضافية يستند عليها في اصدار قرارات جديدة[2].

من خلال هذه التعريفات يتضح لنا و وفقا لما استقر عليه الفقه أن المعلومات هي من قبيل الأشياء المعنوية لا مادية و هو الأمر الذي كون عقبة في مجال تطبيق نصوص جريمة السرقة التقليدية على سرقة المعلومات.

ثانيا: الشروط الواجب توافرها في المعلومات للتمتع بالحماية:

كي تتمتع المعلومات بالحماية الجنائية لا بد أن تتوافر فيها مجموعة من الشروط و تتجلى هذه الشروط فيما يلي:

01- أن يكون في المعلومة التحديد والابتكار: إن المعلومة التي لا يتوافر فيها صفة التحديد لا يمكن أن تكون معلومة بالمعنى الحقيقي، فالمعلومة بوصفها مخصصة للتبليغ يجب أن تكون محددة كما أن المعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها من الأشخاص.

أما فيما يتعلق بالابتكار فانه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة فالمعلومة غير المبتكرة هي معلومة عامة شائعة و متاحة للجميع و يمكن للعامة الوصول اليها و لا يمكن نسبها على شخص محدد[3].

02- أن يتوافر في المعلومات السرية و الاستئثار: كلما اتصفت المعلومات بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومات محددا بمجموعة من الأشخاص، غير أن انعدام هذا التحديد يبعد الأفكار الخاصة بالسرقة والنصب، فالمعلومات غير السرية تكون صالحة للتداول و من ثمة تكون بمنأى عن أي حيازة، و هذا ما ينطبق على المعلومات التي تتعلق بحقيقة معينة كدرجة الحرارة في وقت معين أو المعلومات التي ترد على حوادث معينة كالبراكين و الفيضانات فهي قابلة للنقل والتداول بسهولة و ببساطة بين كل الأشخاص، والوصول الى المعلومات بسهولة يتعارض و الطابع السري لها.

---

[1]-محمد محمد شتا، المرجع نفسه، ص 61.

[2]- نهلا عبد القادر المومني، المرجع السابق، ص 102.

[3]- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسوب الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 2001، ص 155.

و قد تستمد المعلومات سريتها من طبيعتها كالاكتشاف في أحد المجالات التي تتميز بالسرية أو على إرادة الإنسان أو للسببين معا، كما هو الحال في الرقم السري لبطاقات الائتمان.

كما تعد خاصية الاستئثار (l'exclusivite) أمرا هاما في جميع الجرائم التي تنطوي على اعتداء قانوني على الأموال، فالفاعل الذي يستولي شيء يستأثر على ميزة تخص الغير، و في مجال المعلومات تتوافر صفة الاستئثار إذا على المعلومة (يستشعر الاستئثار عندما تكون المعلومة محلا لفكرة أو عمل ذهني، فصاحب هذه الفكرة أو هذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين و يمكن أن ينبع الاستئثار من سلطة شخص أو جهة ما العمل ينظر إليها بوصفها مملوكة له)[1].

الفرع الثاني: مدى انطباق وصف المال على المعلوماتية:

يقصد بالمال المعلومات الحاسوب بكل مكوناته وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب وهو يتكون من كيانين مادي ومعنوي و يضم الكيان المادي الأجهزة المادية المختلفة وهي أجهزة الإدخال و أجهزة الإخراج ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها، أما الكيان المعنوي فيشمل البرامج المختلفة التي تتحقق من خلالها قيام الحاسب بوظائفها المختلفة بالإضافة إلى المعلومات المطلوب معالجتها بالفعل[2].

إذا كانت الأجهزة المادية للحاسبات لا تحتاج إلى نصوص خاصة لحمايتها جزائيا إذ تشملها نصوص الجرائم التقليدية، فالأمر يختلف بصدد الكيان المعنوي لتلك الحاسبات لان جرائم الاعتداء على الأموال يشترط بشأنها عادة أن يكون موضوعها شيئا ماديا، وطبيعة الكيان المعنوي ليست كذلك وعليه فالسؤال يطرح حول مدى اعتبار الكيان المعنوي للحاسوب مالا[3].

المال هو كل ما يصلح أن يكون محلا للحق ذو القيمة المالية والشيء هو محل الحق، وتقسم الأشياء إلى أشياء مادية وأشياء غير مادية أو معنوية، علما بان الأموال من وجهة النظر التقليدية لا ترد إلا على أشياء مادية ولهذا كان تعريف المال بصدد جرائم الأموال بأنه "كل شيء مادي يصلح لان يكون محلا حق من الحقوق المالية" ولكن مع التطور ازدادت الأشياء المعنوية عددا وتفوق بعضها من حيث قيمتها على الأشياء المادية مما استدعى البحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي.

---

[1] – عبد الله حسين على محمود، المرجع السابق، ص156.

[2] – محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، القاهرة، سنة 1984، ص 217.

[3] – قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر، الجزائر، سنة 2006.

ومن هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي، هذه البرامج تكون عادة مثبتة على دعامة أو حامل، مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى أو أي مادة أخرى.

والبرنامج المستقل عن دعامته لا جدال في انه شيء معنوي وبالتالي لا يصدق عليه وصف المال طبقا للتحديد التقليدي للأموال الذي يشترط أن يكون محله شيئا ماديا، أما إذا سجل البرنامج أو نقش على دعامته فان تلك الدعامة بما عليها من برامج تصلح لان تكون محلا الجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرنامج تعتبر ضئيلة القيمة إذا ما قيست بقيمة البرنامج وعلى الرغم أيضا من أن الاعتداء عليها ليس في غاية في ذاته، وإنما الباعث على ذلك هو البرنامج نفسه لا دعامته ومع ذلك لا تأثير لهذه البواعث في القانون الجنائي[1].

ويعتبر الاعتداء على الدعامة في هذه الحالة قد وقع على شيء مادي مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط ، أما إذا وقع الاعتداء على البرنامج مستقلا عن دعامته، فان الأمر يختلف حيث يكون قد وقع على شيء معنوي، هذا الشيء المعنوي لابد وان تثبت له صفة المال أولا حتى يمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه، وقد انقسم الفقه في هذا الصدد إلى اتجاهين:

أولا: الفقه المؤيد لإضفاء وصف المال على البرنامج و المعلومات:

يرى جانب من الفقه أن المعلومات صالحة لان تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها ولا تتوقف عند نطاق المعلومات العامة ، وذلك على أساس أن هذه المعلومات صادرة عن صاحبها أي أنها ترتبط بشخصيته وهو الذي فكر فيه، أو هذا يعني أنها من الحقوق اللصيقة بشخصية صاحبها. وهذه المعلومات ذاتها هي موضوع هذا الحق ومن خصائصها القابلية للانتقال وهذا يعني أن هناك طرفا أخر يستقبل هذه المعلومات ، ومن هنا تنشأ علاقات إما بينها وبين صاحبها وأما بين صاحبها والغير، فالمعلومات باعتبارها نتاجا ذهنيا لمن يعطيها شكل المعلومة فهي تعد محور العلاقات مثل تلك التي تنشأ بين المالك وبين ما يملك فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها[2].

كل هذه التصرفات والحقوق هي التي دفعت جانبا من الفقه إلى القول بان المعلومات مال ليس فقط لوجود علاقة حق استئثار خاص عليها، وإنما أيضا لأنها تعتبر قيمة اقتصادية، فهي تطرح في السوق للتداول مثلها في ذلك مثل أي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادية.

---

[1]– عبد الله حسين على محمود، المرجع السابق، ص156.

[2] – محمد فتحي عبد الهادي، المرجع السابق، ص 217.

وإذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الاعتراف لها بصفة المال فان الفقه الحديث يرى على العكس أن المعيار في اعتبار الشيء مالا ، ليس على أساس ماله من كيان مادي وإنما على أساس قيمته الاقتصادية، وان القانون الذي يرفض إصباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع[1].

ومادامت البرامج في جوهرها معلومات معالجة بطريقة ما ولها قيمة اقتصادية فانه يجب معاملتها على أنها مال، كما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الفكرية ، ولولا أن المعلومات مالا ما كان المشرع ليستطيع التسليم لها بهذا الحق، وان كانت طبيعة هذه الملكية محل جدل فقهي، فإنها على كل حال نوع من الملكية أو الحق الذي لصاحبه في القليل الحق في احتكار استغلال هذا المال غير المادي أي المعلومات والتي منها برامج الحاسب الآلي.

ثانيا: الفقه المعارض لإضفاء وصف المال على البرنامج و المعلومات:

يرى جانب من الفقه بإبعاد المعلومات من مجال تطبيق السرقة، معتمدا في رأيه على فكرة مفادها أن الأموال الغير مادية هي الأموال الغير مجسدة و من ثمة فإن المعلومة وحدها لا تصلح أن تكون محلا للسرقة مادامت منفصلة عن سندها المادي "قرص ممغنط و رقة ..."[2]

حيث ذهب جانب من الفقه في فرنسا إلى أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والاستئثار وان تداولها والانتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلا للملكية الفكرية.[3]

ويفرق البعض الآخر بين المعلومات والبيانات التي تمت معالجتها الكترونيا فيرون أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها، لها طبيعة غير مادية ولا سبيل من ثم إلى اختلاسها أما البيانات التي تمت معالجتها الكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات ممغنطة يمكن تخزينها على وسائط معينة ونقلها واستغلالها وإعادة إنتاجها فضلا عن إمكانية تقديرها كميا وقياسها فهي إذن ليست شيئا معنويا كالحقوق والآراء والأفكار بل شيئا له في العالم الخارجي المحسوس وجود مادي وفقا لهذا الرأي فان المعلومات إذا لم تعالج أليا عن طريق الحاسب لا تعتبر من قبيل

---

[1]–عزيزة رابحي، المرجع السابق، ص 108.

[2]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، " الجرائم ضد الأشخاص و الجرائم ضد الأموال " الجزء الأول، الطبعة الثالثة، دار هومة، 2006، ص 259 .

[3] –هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، أسيوط، ط 1995، ص ص 256– 257.

الأموال الخاضعة للحماية الجنائية باعتبار أن هذه المعالجة تتم في صورة نبضات الكترونية ، مما يمكن القول معه بأنه لعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية، الأمر الذي يخضعها للنصوص التقليدية الجرائم الأموال، ويأخذ نفس حكمها البيانات المخزنة سواء في برامج الحاسب أو في ذاكرته وبالتالي تأخذ برامج وبيانات الحاسب وحكم الأموال عليه وبالتالي تتمتع بالحماية الجنائية المقررة لها[1].

إن اعتبار المعلومات مالا قابلا للتملك أو الاستغلال كما سبق أن وضحنا يزيل أمامنا عقبة كبيرة تسمح بتحول هذا النوع من الأموال إلى مجموعة الأموال التي يحميها القانون الجنائي والتي تتمثل في ضرورة أن يكون المال موضوع جرائم الاعتداء على الأموال شيئا منقولا مملوكا للغير فانه يمكن إسباغ حماية النصوص التقليدية عليه وذلك على أساس أن هذه النصوص جاءت عامة ولم يشترط أن تقع جرائم الأموال على منقول مادي وعليه يكون من المتصور أن تقع هذه الجرائم على محال غير مادي طالما اعترف لها بصفة المال وقابلية التملك، وقد سايرت هذا الاتجاه محكمة النقض الفرنسية في العديد من أحكامه[2].

ثالثا: موقف المشرع الجزائري من مسألة انطباق وصف المال على البرنامج و المعلومات من عدمه:

01- مدى اعتبار البرنامج مالا بصدد جريمة السرقة: طبقا للمادة 350 من قانون العقوبات فان "كل من اختلس شيئا غير مملوك له يعد سارقا " من خلال نص المادة يتبين أن المشرع لم يشترط صراحة ضرورة أن يكون المال موضوع الجريمة ماديا مما يجعل وقوع جريمة السرقة على مال معنوي أمرا لا يصطدم بمبدأ شرعية الجرائم والعقوبات، ولكن يبقى اعتبار البرنامج كمحل للسرقة غير قطعي[3].

02- مدى اعتبار البرنامج كمحل الجريمة النصب: طبقا لما نصت عليه المادة "372" من قانون العقوبات[4]، ليس كل شيء مادي ومنقول يصلح أن يكون محلا الجريمة النصب بل يجب أن يكون ضمن الأشياء التي عددتها المادة 372 على سبيل الحصر.

---

[1]- هشام فريد رستم، المرجع السابق، ص 258.

[2] - عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الالي، الدار الجامعية للطباعة والنشر، بيروت، سنة 1999، ص 23.

[3] - فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، ليبيا، أكتوبر 2009.

[4] - تنص المادة 372 من ق. ع. ج " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل بالفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج ".

تجدر الإشـارة إلى أن النص على المنقول ورد دون تحديد لطبيعته ودون أن يقيده المشرع بان يكون ماديا مما يسمح بتفسير هذا النص على نحو يسمح بدخول برامج الحاسب ضمن الأشياء التي تقع عليها جريمة النصب إلا انه حتى وان أخذنا بهذا التفسير، نصطدم بعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام ، وحتى على فرض أن التسليم قد تم ، فان المجني عليه لا يحرم من حيازة البرنامج والبيانات التي تبقى تحت سيطرته التامة[1].

03- مدى اعتبار البرنامج كمحل الجريمة خيانة الأمانة: حددت المادة 376 من قانون العقوبات[2]، الأشياء التي تصلح أن تكون محلا لجريمة خيانة الأمانة، بحث يستنتج أن الاختلاس يقع على مال منقول الذي سلم إلى الجاني بمقتضى عقد من عقود الأمانة، وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية، لهذا فان إخضاع الاعتداءات الواردة على المال المعلوماتي إلى نصوص خيانة الأمانة يثير بعض المشاكل القانونية نظرا للطبيعة غير المادية للقيم في حقل الجريمة المعلوماتية.

04- مدى اعتبار البرنامج كمحل الجريمة الإتلاف: طبقا للمادة 407 من قانون العقوبات " كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس ....".

كما تنص المادة 412 من نفس القانون" كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة وذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس ..."

بالرجوع إلى نص المادة 412 نجدها قد حددت الأشياء الخاضعة للإتلاف وبالتالي فإنها تشمل المكونات المادية للحاسوب سواء بوصفها أجهزة أو بضائع، كما أن الكيان المنطقي يمكن أن يخضع لهذا النص التجريمي باعتباره مالا بالنظر لما له من قيمة اقتصادية[3].

---

[1]- فشـار عطاء الله، المرجع السابق.

[2] - تنص المادة 376 من ق ع ج " كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير اجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها بعد مرتكبا الجريمة خيانة الأمانة يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 20.001 دج إلى 100.000 دج..... ".

[3] - فشـار عطاء الله، المرجع السابق.

بناء على ما سبق يمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه "**كل مال إلكتروني قابل للنقل و التملك أو بأنه المال الموجود على الحاسوب، سواء في صورة معلومات أو بيانات إلكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك و تكتسي الحماية القانونية**".[1]

يتميز عن غيره من الأموال بعدة ميزات نذكر منها:

- أنه مال غير قابل للنفاذ بمعنى أنه لا ينفذ بالاستعمال.
- أنه مال لا يفقد قيمته بالاستعمال ولكن يفقدها متى ما ظهرت معارف أو برامج جديدة،
- أنه مال يمكن استعماله في آن واحد بواسطة أطراف عديدة دون أن يفقد قيمته فقيمة المعلومات لا تتغير باتساع نطاق استخدامها.
- أن نفقات نقله من طرف إلى آخر لا تكاد تذكر لأنها ضئيلة للغاية أو لا يمكن مقارنتها بنفقة إنتاجها[2].

[1]– ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، سنة 2012، ص32.

[2]– محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2004، ص ص 162-163.

المطلب الثاني: صور جريمة الاعتداء على المال المعلوماتي:

تتعدد جرائم الإعتـداء على الأموال المعلوماتية وتختلف باختلاف الأسلوب، وتتطور من يوم إلى اخر بتطور الوسائل لهذا يصعب حصرها في صور محددة، على هذا الأساس سنحاول استعراض أهم صور الاعتداء على الأموال المعلوماتية المستنبطة من القوانين الوطنية من خلال الفروع التالية التي سنحصرها في جرائم التحويل غير الشرعي للأموال (الفرع الأول)، جرائم الاستخدام غير المشروع البطاقات الدفع الإلكتروني (الفرع الثاني)، جريمة الإتلاف المعلوماتي (الفرع الثالث)، وجرائم الاعتداء على المصنفات الرقمية (الفرع الـرابع).

الفـرع الأول: جرائم التحويل غير المشروع للأموال أو جرائم الاحتيال الإلكتروني:

يعرف النصب أو الاحتيال على أنه من جرائم الاعتداء على ملكية مال منقول يلجأ فيها الجاني بواسطة إحدى وسائل الاحتيال المعينة قانونا، إلى حمل المجني عليه على تسليم المال المنقول، و قد عرفها آخرون بأنها الاستيلاء على الحيازة الكاملة عمدا بطريق الحيلة أو الخداع على مال مملوك للغير[1].

وقد نص المشرع الجزائري على مفهوم جريمة النصب في نص المادة 372/ فقرة 1، من ق. ع .ج، بالقول " كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على أي منها أو شـرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثـروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث أمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقـوع شيء منها يعاقب بالحبس من سنة 01 على الأقل إلى خمس 05 سنوات وبغرامة من 100.000 إلى 500.000 دج".

إن هذا المفهوم للجريمة النصب يتعلق بذلك الصنف من الجرائم التي يقع على الأموال المادية، و لكن هل ينطبق ذلك على مستوى النظم المعلوماتية؟

أولا: الركن المادي لجريمة الاحتيال الإلكتروني:

يقوم الركن المادي لفعل الاحتيال على فعل التظاهر والإيحاء، الذي يكون صالحا للإيقاع بالمجني عليه في الغلط، بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي أي أن المجني عليه في جريمة الاحتيال هو من ينخدع بهذه المظاهر و يسلم ماله للغير.

والاحتيال لا يقع على الشخص الطبيعي فقط بل المعنوي أيضا، فالشركات والمؤسسات العامة و الخاصة هي من الأشخاص الاعتبارية في نظر القانون، حيث أن الحاسوب و شبكات الاتصال الداخلية

[1]–محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص 123.

و الخارجية تعــد من فروع ومكونات الشركة أو المؤسســة فإنها تكون صالحة لوقوع فعل الخداع و التحايـل عليها، و قد اعتبر الفقه ممارسة أفعال الاحتيال من خلال التلاعب بالبرامج و البيانات وما يترتب على ذلك من إيهام للمجني عليه بصحتها من أساليب الاحتيال، و حسب هذا الاتجاه فإن الحاسوب ليس سوى مجرد وسيلة للتحايل، أما الفقه الفرنسي فاعتبر أن غش الأنظمة المعلوماتية للاستيلاء على الأموال يحقق جريمة الاحتيال[1].

و تتعامل أغلب التشريعات مع جريمة التحايل المعلوماتي وفق ثلاث (03) اتجاهات رئيسة هي:

- تشريعات تستلزم لقيام جريمة الاحتيال أن يكون الضحية شخصا طبيعيا و من ثم لا يتصور قيام جريمة خداع الحاسوب بوصفه آلة.
- تشريعات ترى إمكانية تطبيق النصوص الخاصة بجريمة الاحتيال على النظم المعلوماتية وهي التشريعات الأنجلوساكسونية.
- تشريعات تطبق القواعد الخاصة بالغش والاحتيال في مجال البريد و التلغراف و البنوك على حالة الاحتيال والنصب المعلوماتي ومنها تشريع الولايات المتحدة الأمريكية.

ويشترط ليتحقق الركن المادي لجريمة الاحتيال تحقق الأفعال التالية:

أ: فعل النصب: أي تنفيذ فعل التلاعب بمدخلات النظام المعلوماتي أي تغذيته ببيانات غير صحيحة أو من خلال التلاعب ببرامجه، إضافة إلى فعل الإدخال والإتلاف و المحو و الطمس التي سبق و تفصيل معناها[2].

ب- استعمال الطرق الاحتيالية: تقوم هذه الطريقة على اعتماد مرتكبو جرائم الاحتيال المعلوماتي على شبكة الأنترنت أساسا، من خلال إرسال الرسائل الإلكترونية لضحاياهم، في شكل رسائل صادرة عن مؤسسات موثوق فيها، يطلب فيها من الضحايا المحتملين تقديم معلومات شخصية خاصة بهم، و هو ما يسمح لهؤلاء بتتبع ضحاياهم والعمل على الإيقاع بهم لأجل الاستيلاء على أموالهم، أو من خلال استعمال وسائل أكثر تطورا كتقنية (phishing)، أي إرسال عناوين مواقع إلكترونية للضحايا ودعوتهم لزيارتها، ويتسبب دخولهم لها في تسرب برامج تتبع لأجهزتهم الحاسوبية تسمح للمحتالين بالحصول على كافة المعلومات الخاصة بالضحية، و لعل الأسلوب الأحدث هو الاحتيال على الطريقة النيجيرية التي تعتمد على إرسال رسائل بريدية إلكترونية مفادها طلب المساعدة على تحويل العشرات من ملايين الدولارات من قبل الضحية، بدعوى

[1]- محمد أمين أحمد شوابكة، جرائم الكمبيوتر والانترنيت، دار الثقافة للنشر والتوزيع، عمان الأردن، ط01، 2004 ، ص 185.

[2]-هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية، مصر، 2008، ص 102.

أن المرسل يعاني من مشاكل سياسية في بلده الأصلي و أنه مستعد تقديم ما قيمته 10 إلى 15% من قيمة الأموال المحولة بشرط فتح حساب و تدعيمه بقيمة أولية لأجل إتمام العملية[1].

يكتمل الركن المادي لهذه الجرائم إذا ما سبب بصفة مباشرة للغير ضررا اقتصاديا أو ماديا، أي أن يكون الجاني قد نفذ الجريمة بغية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، و مصطلح الضرر الاقتصادي أو المادي واسع جدا بمفهومه فهو يشمل النقود و الأشياء المادية وغير المادية ذات القيمة الاقتصادية[2].

ثانيا: الركن المعنوي لجريمة الاحتيال الإلكتروني:

تعتبر جريمة النصب أو الاحتيال من الجرائم العمدية، التي يتخذ فيها الركن المعنوي صورة القصد الجنائي حسب ما أورده المشرع الجزائري في نص المادة 372 ق.ع. ج، وتبعا لذلك فإنه يستلزم أن يتوافر قصد جنائي خاص يتمثل في انصراف نية الجاني إلى تملك الشيء بطريق الاحتيال.

و القصد العام في هذه الجريمة هو نتاج اجتماع عنصري العلم و الإرادة معا، فعلم الجاني بأن فعله ينطوي على الاستيلاء على هذا المال، كما يجب أن تتحقق الجريمة بدون وجه حق و أن تتحقق المنفعة دون حق أيضا، و بالتالي فإن المعاملات التجارية الشرعية الإلكترونية التي تتم بهدف تحقيق منفعة اقتصادية لا يعد جريمة، كالأنشطة التجارية المتعلقة بالمنافسة والتي يمكن أن تسبب ضررا اقتصاديا لشخص، و تحمل المنفعة لآخر، و التي لا يتم ممارستها بنية الغش كاستعمال برامج جمع المعلومات الخاصة بالمنافسة التجارية على شبكة الأنترنت بواسطة صائد المعلومات"Bot"، وبالتالي تستبعد الجرائم التي بنيت على أساس الغلط أو المنافسة المشروعة[3].

وفي كل الأحوال فإن المجرم المعلوماتي يعتمد أسلوبين أساسيين لأجل تنفيذ جرائم الاحتيال المعلوماتي هما:

- العمل على نشر وتوزيع البرامج الخبيثة الفيروسات على أكبر و أوسع نطاق ممكن من خلال إخفائها على صفحات بعض المواقع الإلكترونية في شكل ومضات اشهارية أو مقاطع موسيقية أو فيديو معروضة للتحميل مجانا و بمجرد اطلاع المستخدم عليها يتسلل البرنامج الخبيث إلى حاسوبه و يبدأ مهمة جمع المعلومات وإرسالها إلى المجرم المعلوماتي.
- العمل على البقاء متخفيا لأطول مدة ممكنة من أجل جمع أكبر قدر من المعلومات، ويبقى أمر نجاح المحتال في مجال الاحتيال المعلوماتي مرهونا بمدى فطنة الضحية وقدرته على اكتشاف هذه البرامج الخبيثة.

---

[1]–Myriam Quéméner–Yves Charpenel – La cybercriminalité op cit–p 135

[2]– هلالي عبد اللاه أحمد، مرجع سابق، ص 103.

[3]– نفس المرجع، ص105

وقد قدم مكتب التحقيقات الفيدرالي الأمريكي (FBI) مجموعة من النصائح لمستعملي الأنترنت لأجل وقاية مستعمليه من الوقوع ضحايا جرائم الاحتيال المعلوماتي وهي:

- ❖ تجنب المشاركة في المزايدات على شبكة الأنترنت إلا بعد التأكد من صحتها و دور البائع و المزايد فيها.
- ❖ عدم تقديم أرقام الضمان الاجتماعي في مجال البيع بالمزايدة على الأنترنت.
- ❖ عدم تقديم أرقام بطاقات الائتمان إلا بعد التأكد من تأمين الموقع[1].

الفرع الثاني: جرائم الاستخدام غيـر المشروع لأدوات الدفع الإلكتروني:

تعتبر تقنية الدفع الإلكتروني للأموال من أهم التطبيقات الحديثة للمعلوماتية، فقد كسرت حاجز التعامل بالنقود وكذلك عوائق المبادلات المالية ، فأصبحت تتم بسهولة و سيولة كبيرة و لا تستغرق من الزمن سوى لحظات، غير انها و بقدر تطمينات المؤسسات المالية بمدى أمنها إلا أنها تبقى الهدف الأول لمجرمي المعلوماتية ، نظرا لما تدره من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة وما جاورها، فما هي طبيعة هذه التقنية وماهي الصور غير المشروعة لاستعمالاتها؟

أولا: وسائل الدفع الإلكتروني: عرفها المشرع الجزائري في المادة 06 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية على أنها" كل وسيلة دفع مرخص بها طبقاً للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد، عبر منظومة إلكترونية"[2].

ثانيا: أنواع بطاقات الدفع الإلكتروني: تتخذ البطاقات الخاصة بالدفع الإلكتروني أشكالا وانواعا عديدة، و ذلك كنتيجة لشيوع استعمالها ويمكن إيجاز ذلك فيما يلي:

01- بطاقات الوفاء: هي الأكثر شيوعا و يطلق عليها بطاقات الخصم الشهري و تستخدم في الوفاء بمقابل السلع و الخدمات التي يحصل عليها حاملها من التجار المعتمدين لدى المؤسسة المالية المصدرة لها.

02- بطاقات الائتمان: يستطيع حاملها أن يسدد بها مجموع التزاماته مباشرة حتى و لو لم يكن يمتلك حسابا أو رصيدا لدى البنك مصدر البطاقة، و لكنه يلتزم بتسديد ما عليه من ديون تجاه ابنك في أجل محدد بالاتفاق المسبق بينه و بين البنك، و كلما سدد ديونه في الأجل المحدد تجدد الاعتماد مرة أخرى، و أشهرها هي بطاقات Master card و Visa .

03- بطاقات الصرف الآلي: تعطي لحاملها إمكانية سحب مبالغ نقدية من حسابه الموجود لدى البنك مصدر البطاقة بحد أقصى متفق عليه.

---

[1] – ناير نبيل عمر، المرجع السابق، ص 84.

[2] – القانون رقم 18-05، المؤرخ في 2018/05/10، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، صادرة بتاريخ 2018/05/16.

04- بطاقات ضمان الشيكات: تتيح هذه البطاقة لحاملها تحرير شيكات للمستفيد، مع تولي البنك مصدر البطاقة الوفاء بقيمة الشيكات المحررة[1].

إن المزايا التي توفرها بطاقات الدفع الإلكتروني من تحويل للأموال، استقطبت اهتمام قراصنة المعلوماتية، حول إمكانية تخليق أرقام بطاقات بواسطة برامج تشغيل و كذلك التقاط البيانات المخزنة عليهما عبر قنوات الأنترنت و استخدامها بصفة غير مشروعة لأجل اقتناء السلع والخدمات مع خصم قيمتها من رصيد العملاء الشرعيين حاملي هذه البطاقة.

إذن فمجال التعدي على البطاقات لا يثار في حال سرقتها ماديا باعتبارها تخضع كجريمة لقواعد قانون العقوبات التقليدية، ولكن يثار الإشكال بخصوص الاعتداء الواقع على البيانات السرية المخزنة عليها سواء من قبل حاملها أو من قبل الغير.

ثالثا: صور الاستخدام غير المشروع البطاقات الدفع الإلكتروني: تعتبر جرائم الاستخدام التعسفي لبطاقات الدفع الإلكتروني، أشهر الجرائم التي تستهدف الأموال المتداولة عبر النظم المعلوماتية، وخصوصا مع تنامي التجارة الإلكترونية، وتتمثل صور هذا الاستعمال التعسفي الاستعمال غير الشرعي من قبل الغير، أي من غير حامل البطاقة، ويقصد بالجرائم المرتكبة من قبل الغير بأنها تلك الجرائم التي يرتكبها طائفة تهتم بمجال المعلوماتية، و تستهدف أمنها وأمن مرتاديها، فتركز جهودها على التقاط و قرصنة البيانات المالية الشخصية للأفراد أو المؤسسات البنكية من اجل إعادة استخدامها بدون وجه حق و لأجل اقتناء سلع و خدمات وتحميل الغير مسؤولية دفع مقابلها.

وتتكون بطاقة الدفع الإلكترونية من مكونين أساسيين هما:

- البطـاقة نفسها.
- البيانات السرية الخاصة بحاملها.

و قد يقع فعل الاعتداء إما على البطاقة نفسها أو على مكوناتها المعنوية في إحدى الأشكال التالية:

01- في حال سرقة البطاقة أو ضياعها نفسها: تتخذ البطاقة الخاصة بالدفع الإلكتروني شكلا خاصا مصنوعا من مادة البلاستيك، مطبوع عليها بعض المعلومات المتعلقة بحاملها، مع شريط ممغنط يحتوي على بيانات غير مقروءة تتعلق بالبنك و العميل، فإذا ما سرقت أو ضاعت هذه البطاقة من حاملها فعليه إبلاغ البنك الذي أصدرها فورا، لمنع استعمالها من قبـل الغير أو إلغائها، و هـو ما ينطبق أيضا على

[1]- محمد على قطب، الجريمة المعلوماتية و طرق مواجهتها، الجزء الثالث، وزارة الداخلية "أكاديمية الملكية للشرطة"، مملكة البحرين، أفريل2011، ص 08.

رقمها السري، وتصبح الجهة التي سحبت منها المبالغ بعد الإخطار هي المسؤولة و يتحمل الشخص الذي عثر أو سرق هذه البطاقة مسؤولية فعل سحب المبالغ من رصيدها[1].

02- في حالة سرقة أو ضياع بيانات البطاقة: جرت العادة أن لا يمنح البنك الرقم السري الخاص بالبطاقة إلا لحاملها، حتى لا يكون عرضة للسرقة أو الاحتيال من قبل الغير وبالتالي تنحصر مسؤولية الإدلاء بأرقام البطاقة البنكية عبر شبكة الأنترنت في حاملها، كما يمكن أن يتعرض إلى سرقة رقمه السري و بيانات بطاقته من خلال ملئه لنموذج الشراء الإلكتروني على شبكة الأنترنت[2].

كما يمكن أن يتعرض لسرقة بنياته السرية من خلال بعض الأساليب التي يعتمدها لصوص التجارة الإلكترونية و هي :

أ- إنشاء موقع إلكتروني وهمي على الشبكة مطابق لموقع بعض الشركات الكبرى واستعماله في الحصول على البيانات السرية للمتعاملين ثم إغلاقه.

ب-التسلل إلى مواقع الشركات التجارية والمالية و الحصول على معلومات عملائها.

ج- استعمال تقنية (Mail BomBing) أي إغراق الموقع المستهدف بالرسائل البريدية و بالتالي تحميله ما لا يستوعب من معلومات مما يؤدي إلى انفجاره عبر الشبكة، وبعثرة المعلومات المخزنة فيه ومنها البيانات السرية الخاصة بالعملاء[3].

03- حالة تزوير بيانات بطاقات الائتمان: يتم تزوير بطاقات الدفع الإلكتروني على نطاق شبكة الأنترنت من خلال تشكيل أرقام بطاقات خاصة ببنك معين، وذلك بعد تزويد الحاسوب بالرقم الخاص بالبنك مصدر البطاقة عن طريق برامج تشغيل خاصة و من ثم استخدام البطاقة المزورة التي لها مستخدم أصلي والقيام بعمليات الشراء بواسطتها مما يعرض العملاء الحقيقيين المشكلات مع البنوك بسبب استخدام بطاقاتهم، أو بطاقات مطابقة لبطاقاتهم، وهو ما يفسر اكتشاف البنوك لاعتراضات من حاملي بطاقات الدفع الإلكتروني، على عمليات لم يقوموا بها، لتبين التحريات بعدها أن هذه العمليات تم إجراؤها عن طريق شبكة الأنترنت من قبل لصوص المعلوماتية الذين يستعملون تقنيات خاصة تمكنهم من الحصول على أرقام البطاقات الخاصة بالعملاء واستخدامها في عمليات البيع و الشراء.[4]

---

[1]-خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب، دار النشر والتوزيع، عمان، ط 1، 2011، ص ص 134-135.

[2] -محمد أمين أحمد الشوابكة، مرجع سابق، ص 200.

[3] -محمد علي قطب، المرجع السابق، ص 12

[4]- عبد الله بن سعود بن محمد السراني، فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة مقدمة لنيل شهادة الدكتورة، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، ص 42.

الفــرع الثالث: جـريمة الإتلاف:

أولا: تعريف الإتلاف المعلوماتي: عرفه الفقه أنه" إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواء استيلاء على أموال أو اطلاع على معلومات و لكن إحداث الضرر بالنظام المعلوماتي و إعاقته عن أداء وظيفته من خلال تشويه المعلومات أو البرامج على نحو فيه إتلاف بها يجعلها غير صالحة للاستعمال"[1].

وقد يقع الإتلاف على يقع على المكونات المادية للنظام المعلوماتي، وقد يقع على المكونات المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي[2].

أما بالنسبة للمشرع الجزائري فلم يعرف الإتلاف المعلوماتي بل اكتفى بتجريمه في المادتين 407 و412 من القانون العقوبات[3].

ثانيا: صـور الإتلاف المعلوماتي: يتخذ الإتلاف المعلوماتي عدة صور على غرار:

- **إستبدال المعلومات:** تعتبر نوع من جرائم الغش أو التزوير المعلوماتي، ويعد من الأنماط السهلة للإجرام المعلوماتي كاستبدال رقم بأخر أو تاريخ[4].
- **محو المعلومات:** تتم من خلال شطب البرامج والمعلومات والبيانات المخزنة على الحاسوب ومحوها كليا و تدميرها الكترونيا.
- **تخريب البيانات:** نصت عليها المادة 407 من قانون العقوبات المذكورة سابقا، يقصد به تخريب البيانات والمعلومات و تغييرها وتعديلها بحيث يتم تشويهها وجعلها غير صالحة للاستعمال[5].

---

[1]– أيمن عبد الله فكرى، المرجع السابق، ص47.

[2] – نهلا عبد القادر المومني، المرجع السابق، ص 123.

[3] – تنص المادة 407 من قانون العقوبات الجزائري على انه " كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20.001 إلى 100.000 دج" و تنص المادة 412 من نفس القانون" كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة و ذلك بواسطة مواد من شانها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 20.001 إلى100.000 دج.

[4]– سوير سفيان، المرجع السابق، ص 39.

[5]– خالد عياد الحلبي، المرجع السابق، ص 69.

ثالثا: مظاهر الإتلاف المعلوماتي:للإتلاف المعلوماتي طرق وأساليب متعددة، فمنها ما يؤثر على ماديات النظام المعلوماتي، ومن ما يتعلق بالبرامج المعلوماتية ويؤثر على النظام المعلوماتي، ومنها ما يتصل بالمعلومات دون باقي عناصر النظام المعلوماتي ولعل أبرزها:

01- الإتـلاف عن طريق الإعاقة والاعتـداء: يتم من خلال (إعاقة سير العمل في نظام المعالجة الآلية للبيانات – الإعتداء على المعلومات المخزنة داخل النظام المعلوماتي – تضخيم البريد الإلكتروني – بث الفيروسات المعلوماتية عبر شبكة المعلومات لتعطيل الإتصالات)[1].

02- الإتلاف عن طريق الإضافة والتعديل في المعطيات: يتم من خلال (التدخل في المعطيات بإدخال معلومات وهمية أو مزورة – التدخل في الكيان المنطقي كتعديل البرامج من خلال التلاعب أو الاختلاس أو تغيير نظام التشغيل – خلق برامج جديدة على غرار خلق برنامج وهمي أو إعداد برامج ناقصة من الناحية الفنية).

03- الطرق الفنية للإتلاف المال المعلوماتي: تهدف لإلحاق الضرر لأنظمة الحاسب الآلي وتقوم بإتلافه، كما تقوم بتدميره الكترونيا وتشويهه أو تعديل طرق معالجته وذلك باستخدام الطرق الفنية والتقنية كالفيروسات وبرامج الدودة والقنابل المعلوماتية[2].

رابعا: محل جريمة الإتلاف المعلوماتي: ان محل جريمة الإتلاف هو مكونات الحاسوب المادية والمعنوية، ويكون محل المنقولات المادية المعلوماتية كأجهزة الحاسب الآلي وملحقاته المادية سواء كانت تحتوي بيانات أو برامج أو مجرد أوعية خالية بشرط أن يؤدي الإتلاف أو التخريب إلى الإقلال من قيمتها الاقتصادية.

أما المكونات الغير مادية ويطلق على هذه الحالة للإتلاف تدمير نظم المعلومات ويقصد به إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة الحـــاسب

---

[1]- محمد أمين الشوابكة، المرجع السابق، ص287.

[2]- **الفيروس المعلوماتي:** برنامج حاسب مثل أي برنامج تطبيقي آخر, ولكن يتم تصميمه بواسطة احد المجرمين بهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب. ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى, وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر, ويتوالد ذاتيا وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة (محمد أمين الشوابكة، المرجع السابق، ص288).

برنامج الدودة المعلوماتية: هي عبارة عن برنامج له القدرة على تعطيل أو إيقاف نظام الحاسب الآلي بصورة كاملة وهو يستنسخ نفسه عدة مرات، وينتشر من خلال الوصلات الإلكترونية يظهر معلومات غير صحيحة، تؤدي في النهاية إلى غلق النظام ومن ثم تلفه (محمد أمين الشوابكة، المرجع السابق، ص289).

القنبلة المعلوماتية: هو اصطلاح يطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف وتنقسم إلى قنابل منطقية و الزمنية (محمد أمين الشوابكة، المرجع السابق، ص290).

الآلي أيا كان شكلها، استيلاء على نقود أو اطلاع على معلومات، ولكن يبقى ببساطة إحداث الضرر بنظام المعلومات وإعاقته عن أداء وظيفته[1].

خامسا: الركن المعنوي لجريمة الإتلاف المعلوماتي: إن جريمة الإتلاف من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة فيتعين أن يعلم الجاني انه يعتدي على أموال معلوماتية مملوكة للغير وأن من شان فعله أن يتلف الشيء أو يعطله أو أن ينتقص من منفعته بشكل يجعله غير صالح للاستعمال بما يؤدي إلى إلحاق الضرر به[2].

الفـرع الرابع: جرائم الاعتداء على حقوق الملكية الفكرية:

صاحب الثورة المعلومات بروز مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية و هي تلك الملكية التي تنصب على برامج الحاسوب وبياناتها و المصنفات الرقمية المنشورة على شبكة الأنترنت التي بذل في إنتاجها وجمعها و إظهارها جهد فكري إبداعي جعل من الواجب حمايتها كحق ملكية فردية وجماعية صاحبها كمؤلف[3].

وتعد المصنفات الرقمية من قبيل الأموال المعلوماتية المشمولة بالحماية ضد صور التعدي باعتبارها ملكا لصاحبها ولا يحق لسواه استغلالها بهدف الانتفاع بها فما هي يا ترى هذه المصنفات و ما هي طبيعتها التي تشكل محلا للجريمة المعلوماتية وإلى أي مدى تحظى بالحماية الجنائية؟

أولا: تعريف المصنفات الرقمية: يعرف المصنف الرقمي بأنه "كل مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات" فبرنامج الحاسوب مصنف رقمي، وكذلك قاعدة البيانات و طبوغرافيا الدوائر المتكاملة باعتبارها نتائج تطور علم الحاسوب، بخلاف أسماء وعناوين الأنترنت و البريد الإلكتروني التي تعتبر من المصنفات التي ارتبط ظهورها بشبكة الأنترنت[4].

وتتصف المصنفات عموما بطابع الأصالة إما من حيث الإنشاء أو التعبير، أي أنه نتاج ذهني بطابع معين يبرز شخصية صاحبه سواء في مضمون و جوهر الفكرة أو في مجرد طريقة عرضها[5].

---

[1] –خالد عياد الحلبي، المرجع السابق، ص 71.

[2] – محمد أمين شوابكة، المرجع السابق، ص 221.

[3] – عبد الكريم عبد الله عبد الله، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة، سنة 2008، مصر، ص 249.

[4] – يوسف مسعودي، النظام القانوني لحماية المصنفات الرقمية، مقالة علمية، مجلة الدراسات القانونية، العدد 04، أوت 2009 مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية، الجزائر، ص 113.

[5] – محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2003، ص 216.

ثـانيا: أنواعها: يمكن حصرها في ما يلي:

01- برامج الحاسوب: يقصد بها برامج التشغيل مثال برنامج (Windows07) وكذلك البرامج التطبيقية كبرنامج معالجة النصوص الشهير (Windows Word) وقد أثارت البرامج الحاسوبية جدلا واسعا بين الفقهاء بين من نادى بإلحاقها بأنظمة الحماية الخاصة بحقوق المؤلف و بين من نادى بإلحاقها بمبادئ الحماية الخاصة ببراءات الإختـراع.

02- قواعد البيانات: هي تجميع مميز للبيانات والمعلومات يتوافر فيه عنصر الابتكار والترتيب عبر مجهود شخصي يكون مخزنا بواسطة الحاسوب و يمكن استرجاعه من ذاكرته أو من خلال شبكة الأنترنت.

03- التصاميم الشكلية للدوائر المتكاملة: هي عبارة عن رقائق إلكترونية صغيرة جدا تؤدي وظائف إلكترونية تدمج على الشرائح الإلكترونية للحاسوب لأجل تطوير أداءه.

04- عناوين الأنترنت: تعتبر مواقع الأنترنت أحد أهم المصنفات الرقمية الناشئة في بيئة الأنترنت وحتى الآن لا توجد تشريعات شاملة تنظم مسائل أسماء النطاقات، والإشكال يطرح عندما يكون الاسم مطابقا لاسم تجاري أو علامة تجارية.

05- محتوى مواقع الأنترنت: هي كل المحتويات المنظمة داخل موقع الأنترنت سواء مواد مكتوبة أو مرئية أو مسموعة[1].

وقد أشار المشرع الجزائري إلى مفهوم المصنفات الرقمية في الأمر 03-08 المؤرخ في 2003/07/19، في نصوص المواد 02-03-04-05، المتضمن قانون حماية الدوائر الشكلية والمتكاملة إضافة إلى نص المادة 03 والمادة 27 من الأمر 03-05 المؤرخ في 2003/07/19، المتضمن قانون حماية المصنفات وحقوق المؤلف، واشترط المشرع لا تكون هذه المصنفات محل حماية قانونية توفر شرطين هما:

- إفـراغ الإنتاج الذهني في صورة مادية.
- اصباغ صفة الابتكار على المصنف.

ثالثا: صور الجرائم المعلوماتية الواقعة على المصنفات الرقمية: اهتمت غالب التشريعات بوضع نصوص تجرم المساس بالحقوق المعنوية و الفكرية للغير، و بالتالي تضمن للمصنفات الحماية القانونية اللازمة، ومنها المصنفات الرقمية من كافة أنواع الاعتداءات، و هو ما تكلفت به وعلى نحو مفصل و دقيـق

[1]- يوسف مسعودي، مرجع سابق، ص 116.

اتفاقية بودابست لمكافحة الجريمة المعلوماتية في نص مادتها العاشرة(10)[1]، وهو ما دعمته المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010وهي الجهود التي توجها المشرع الجزائري بأحكام الأوامر 03-05 و 03-08 المتعلقة بحماية حقوق المؤلف والتصاميم الشكلية والدوائر المتكاملة الصادرين بتاريخ 19 جويلية 2003، إن كل هذه النصوص تجسد مفاهيم جرائم التعدي على المصنفات الرقمية التي يمكن حصر صورها فيما يلي:

01- الاعتداء على حقوق المؤلف من خلال جرائم التقليد(la contrefacon):

جرائم التقليد هي التي تعتمد على إعادة إنتاج أو عرض أو نشر بأية وسيلة كانت عملا فكريا من خلال التعدي على حقوق المؤلف[2].

إن إعادة إنتاج و بث أو نشر الأعمال المحمية عبر الأنترنت بدون موافقة حائز حق المؤلف هو أمر شائع للغاية والأعمال المحمية تشمل عموما الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية والجدير بالذكر أن السهولة التي يتم من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية و النطاق الذي بمقتضاه يتم إعادة إنتاجها وتوزيعها هي الشبكات الإلكترونية[3].

وهو ما قضت به المحكمة العليا الفرنسية بتاريخ 16 أكتوبر 2006 بمناسبة النظر في قضية إحدى الموظفات التي فصلت من قبل شركة تسيان أوروبا و التي بادرت بالانتقام من رئيس عملها من خلال نشر صور له مع صور سيارات نسيان على موقعها الإلكتروني الخاص، و هو الأمر الذي أدى تدخل الشركة المالكة لأجل حجب الموقع وسحب الصور باعتبارها صاحبة هذا العمل و أن نشر صور سياراتها هو تعدي على حقوقها الحصرية، وهو الطرح الذي أخذت به المحكمة و الذي اعتمدته في إدانة الموظفة السابقة بجنحة التقليد المتمثلة في إعادة إنتاج و نشر حقوق فكرية[4].

---

[1]- جاءت المادة العاشرة (10) من اتفاقية بودابست تحت الفصل الرابع الموسوم بالجرائم المتعلقة بالإنتهاكات الخاصة بحقوق المؤلف والحقوق المجاورة لها بالقول " تعتمد كل دولة طرف ما قد يلزم من التدابير التشريعية لتجريم الأفعال التالية في قانونها الوطني:انتهاك حقوق الملكية الفكرية - انتهاك الحقوق المجاورة.

وهو النص المطابق لما هو وارد في الاتفاقية العربية لمكافحة الجريمة المعلوماتية

[2]-Myriam Quéméner- wesCharpenel - La cybercriminalité op cit -p 145

[3]- هلالي عبد الله أحمد - مرجع سابق - ص 132.

[4]- Jean Michel Bruguière Le Droit de l'internet lois contrat et usage Edition Litec- Paris - France 2009-p 217.

فجـرائم المعلوماتية هي أكثر الجرائم مساسا بحق المؤلف و خصوصا جرائم التحميل غير المشروع عبر شبكة الانترنت، فمثلا المتصفحين لشبكة الانترنت اعتادوا على تحميل الأفلام والموسيقى دون شرائها من مصدرها الأساسي، مستغلين في ذلك برامج متخصصة في فك شفرات الحماية، وذلك إما بغرض استعمالها الشخصي أو بغرض إعادة نشرها و طرحها للغير على شبكة الانترنت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة.

وما يلفت الإنتباه تخلف أغلب التشريعات العربية عن الركب التقني الذي تبنته أغلب الدول المتقدمة في مجال محاربة الجريمة المعلوماتية الماسة بحقوق الملكية الفكرية فنجد أن عمليات النسخ و التحميل غير المشروع والمتعلقة بحقوق الغير الفكرية أمر جد شائع عند أفراد المجتمعات العربية و المجتمع الجزائري خصوصا كما تغيب بالمقابل ثقافة احترام حق الغير الفكري.

و يقوم الركن المعنوي في هذه الجرائم في حال ارتكابها عمدا و بدون وجه حق أي أنها جرائم تشترط التعمد لأجل قيام المسؤولية الجزائية، وعليه تستبعد أفعال الاستعمال المشروع لهذه الحقوق إذا تعلقت بحق الغير في الاستعمال و دون الإخلال بحقوق المؤلف كاستعمالها داخل إطار علمي داخل منشأة علمية أو نسخها بمعرفة مالكها لأجل حفظها من مخاطر التلف، أو دراستها بغرض نقدها وتطويرها، أو إذا استعملت من قبل هيئات الإذاعة المقروءة أو المسموعة أو المرئية[1].

[1]– محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، سنة 2003، ص ص 234– 235.

المبحث الثـــاني: أليات مكافحة جرائم المعلوماتية:

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة، لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة، وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم.

وتجسيدا لذلك، باشرت الدولة الجزائرية في إعداد برامج خاصة لمكافحة هذا الشكل الجديد من الجرائم واستحداث أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال، فضلا عن إجراء تعديلات على نصوص قانونية وسن نصوص جديدة تحدد ماهية هذا النوع من الإجرام ووسائله وكيفية تجريمه[1].

إذ اعتمدت من خلال هذه الاستراتيجية على مرتكزين أساسيين وهما الجانب التشريعي والجهاز المؤسساتي العملياتي وهو ما سنتطرق إليه في هذا المحور تباعا.

المطلب الأول: الجانب التشريعي:

في ظل التنامي المتسارع لاستعمال تقنية المعلوماتية في الجزائر، وما نتج عنها من تبعيات كفل الدستور الجزائري[2]، حماية الحقوق الأساسية والحريات الفردية، والسهر على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى، حذرت من المساس بهذه الحقوق[3].

على ضوء ما سبق سنتناول في هذا المطلب للقوانين العامة في الفرع الأول ثم نتطرق للقوانين الخاصة في الفرع الثاني.

---

[1]– سمير بارة، الأمن السيبراني Cyper Security في الجزائر، السياسات والمؤسسات المجلة الجزائرية للأمن الإنساني، جويلية 2017، ص264.

[2] – دستور الجمهورية الجزائرية الديمقراطية الشعبية، المعدل بموجب المرسوم الرئاسي 20–442، الجريدة الرسمية العدد 82، الصادرة بتاريخ 2020/12/30.

تنص المادة 35 من الدستور: " تضمن الدولة الحقوق الأساسية والحريات"، كما تنص المادة 47 فقرة 2 " لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت، في حين نصت كل من مواد 74،75 و76، على ضرورة حماية حرية الابتكار الفكري والفني والعلمي من كل أشكال الاعتداءات.

[3] – بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية – دراسة مقارنة، مذكرة لنيل شهادة ماستر في الحقوق تخصص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم سياسة بجاية، الجزائر، 2018 – 2017 ، ص 66.

الفـرع الأول: القــوانين العامة:

قامت الجزائر بسن مجموعة من القوانين العامة خاصة بمكافحة الجريمة المعلوماتية، وهي تعتبر متأخرة مقارنة ببعض الدول العربية، بالرغم من احتلالها المراتب الأولى عربيا وإفريقيا، ومن بين هذه القوانين نذكر:

أولا: قانون العقوبات الجـزائري: نتيجة لما أفرزته التطورات التكنولوجية الحديثة المتتابعة والمتسارعة من تعديات وسلوكيات سلبية وخطيرة طالت الأفراد والمؤسسات والدول، بدأ المشرع الجزائري بمواكبة ذلك التطور الرقمي على ضوء المعطيات الجديدة، أين قام بتعديل الأمر رقم 66-156، المتضمن قانون العقوبات بالقانون رقم 04 – 15 المؤرخ في 10 /11/ 2004، حيث تم إدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات (القسم السابع مكرر)، ضمن الموادمن 394إلى 394 مكرر8، تلاه التعديل الأخير القانون 24- 06[1]،الذي تم من خلاله إلى تشديد بعض العقوبات وهي كالآتي[2]:

01-جريمة الدخول أو البقاء في منظومة معلوماتية: تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط، وهو ما أشارت إليه المادة 394 مكرر/ فقرة1 من قانون العقوبات بنصها على:

"يعاقب بالحبس من ستة (06) اشهر إلى سنتين وبغرامة من 60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

كما أورد المشرع من خلال نفس المادة في الفقرتين 2 و3 ظرفين لتشدد عقوبة أولهما الدخول غير المشروع إلى المنظومات المعلوماتية أو حذف أو تغيير المعطيات، و الثاني في حالة ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، حيث تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج.

02- جـريمة التزوير المعلوماتي: ينحصر النشاط الإجرامي في هذه الجريمة في أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعهما معا حتى يتوافر النشاط الإجرامي فيها، إذ يتوفر الركن المادي للجريمة بمجرد القيام بفعل واحد على حدى، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[3].

---

[1]- القانون رقم 24-06، المؤرخ في 2024/04/28، المعدل والمتمم لقانون العقوبات.

[2]- القانون رقم 04 – 15، المؤرخ في 10 /11/ 2004، المعدل والمتمم لقانون العقوبات.

[3]- خثير مسعود الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات دار الهدى عين مليلة، الجزائر، سنة 2010، ص 123.

و لقد أكد المشرع على معاقبة هذه الجرائم في المادة 394 مكرر1 والتي تنص على ما يلي:" يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دجكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

03- جريمة الاستيلاء أو الاحتيال المعلوماتي على المعطيات: تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي، وهي ما تناولته المادة 394 مكرر 2 من الأمر رقم 26-06 والتي نصت على ما يلي: "يعاقب بالحبس من سنة (1) إلى ثلاث (5) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وبطريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.....القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

04- جريمة إتلاف وتدمير المعطيات: أشار إليها المشرع الجزائري في المادة 394 مكرر1 من قانون العقوبات والتي تنص على: " يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها"، وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات مثلا[1].

05- العقوبات التكميلية: إضافة إلى العقوبات الأصلية التي نصت عليها مواد القسم السابع من قانون العقوبات والقاضية بتوقيع عقوبتي الحبس والغرامة المالية لمرتكبي إحدى الجرائم المنصوص عليها في هذا القسم، نصت المادة 394 مكرر 6[2]، على توقيع عقوبة تكميلية تتمثل في غلق المواقع التي تكون محلاً للجريمة وغلق المكان المستغل لارتكابها شريطة أن يكون صاحبه على علم بذلك، فضلا عن مصادرة الأجهزة والوسائل التي تم استغلالها لارتكاب هذه الجريمة.

06- العقوبات المشددة: أوضح المشرع الجزائري الظروف التي تشدّد فيها العقوبة على الجرائم التي نص عليها القسم السابع مكرر من قانون العقوبات، والتي تكون في حالة إذا ما استهدفت هذه الجرائم جهاز الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام حيث تنص المادة 394 مكرر3 ما يلي:

---

[1]-عبد القادر دوحة، محمد بن حاج الطاهر، مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكترونية، الملتقى الوطني الأول النظام القانوني للمجتمع الإلكتروني، المركز الجامعي خميس مليانة، معهد العلوم القانونية، والإدارية، 09-10-11 مارس 2008، ص7.

[2] - قانون 24-06، المعدل والمتمم لقانون العقوبات.

"يعاقب بالحبس من سنتين (2) إلى عشر (10) سنوات وبغرامة من 700.000 دج إلى 2.000.000 دج،إذا استهدفت الجرائم المنصوص عليها في هذا القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات الأشد "[1].

07- تجريم الاشتراك في مجموعة أو اتفاق لغرض الإعداد الجريمة: نص المشرع على تجريم الاشتراك في مجموعة أو اتفاق لغرض الإعداد الجريمة على من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال الإشارة إليها في مادة المادة 394 مكرر 5 التي نصت على ما يلي:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"

08- الشخص المعنوي: بالنسبة للشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في القسم السابع من قانون العقوبات فقد نصت المادة 394 مكرر 4 على توقيع غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، كما اعتبرت المادة 394 مكرر 7 من نفس القانون أن الشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها.

ثانيا: قانون الإجراءات الجزائية: لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية[2]، لمواكبة التطور المعلوماتي الذي لحق بالجريمة المعلوماتية، محاولة منه تطوقها والقضاء عليها، أو على الأقل الحد من انتشارها، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة، الغرض منها هو مواجهتها وقد وردت هذه الأساليب في المادة 37 الفقرة الثانية من القانون 04-14، المتضمن قانون الإجراءات الجزائية[3].

ويمكن إجمال الترتيبات المتخذة من قبل المشرع الجزائري المتعلقة باستحداث أساليب التحري الخاصة في ما يلي[4]:

---

[1] – القانون 24-06، المعدل والمتمم لقانون العقوبات.

[2] – القانون رقم 04- 14، المؤرخ في 2004/11/10، المعدل والمتمم للأمر 66-155، المتضمن قانون الإجراءات الجزائية، ج ر العدد 71، بتاريخ 2004/11/10.

[3] – تنص المادة 37 الفقرة الثانية من القانون 04-14، المتضمن قانون الإجراءات الجزائية: " يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب وجرائم المتعلقة بالتشريع الخاص بالصرف"، وهو الأمر الذي ينطبق كذلك على قاضي التحقيق وضباط الشرطة القضائية.

[4] – مراد حسيني، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري، عملية التسرب الجزء الأول، الطبعة الأولى، قراءات في المادة الجنائية، دار النشر للمعرفة 2013 الجزائر، ص166.

- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: هي إجراءات تباشر بشكل خفي، تماشيا مع التقدم العلمي والتكنولوجي المعاصر، تتم من خلال اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وقد نص عليه المشرع في المواد 65 مكرر من5 إلى 10 من ق. إ .ج .ج.
- التسرب: يعتبر من أهم التقنيات التي استحدثها المشرع الجزائري حيث نص عليه في المواد من 65 مكرر 11 إلى 65 مكرر 18 من ق إ ج. ويسمح التسرب أو الاختراق كتقنية من تقنيات التحري الخاصة، لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية ويوهمهم على أنه شريك لهم.

وفي سبيل ذلك يمكن لضباط الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وذلك بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية بإخفاء الهوية الحقيقية[1].

الفـرع الثاني: القوانين الخاصة:

نطاق الجريمة الإلكترونية، التي أصبحت لا تقتصر على جريمة واحدة و إنما اتسعت إلى عدة جرائم وعلى أساس أن القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الإلكترونية الحديثة مما دفع بالمشرع الجزائري إلى استحداث قوانين خاصة لمواكبة هذا النوع المستحدث من الجرائم.

أولا: قانون 09-04 الخاص المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: تبرز أهميته هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أوفي حالة توفر معلومات عن احتمال الإعتداء على المنظومة المعلوماتية.

وقد تعرض الفصل الأول من هذا القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الإتصالات الإلكترونية، والفصل الرابع تعرض إلى القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والفصل الرابع تعرض إلى تحديد الإلتزامات التي تقع على المتعاملين في الإتصالات الإلكترونية، ثم الفصل الخامس نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السابع

[1]– الأمنة أمحمدي بوزينة إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية الأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة، 29 مارس 2017 ص71-72.

فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها بالمساعدة وتبادل المعلومات[1].

ثانيا: القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية:
أضاف هذا القانون جملة من الضوابط، من بينها إنشاء سلطة ضبط مستقلة للبريد والاتصالات الإلكترونية والتي من بين مهامها السهر على احترام متعاملي البريد والاتصالات الإلكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الإلكترونية والأمن السيبراني[2].

ويقصد بالاتصالات السلكية في مفهوم هذا القانون كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.

فيما أوضحت الفقرة الثانية من المادة 10 من نفس القانون المقصود بالأمن السيبراني وهو المجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة[3].

بموجب هذا القانون تم تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الإخبار بوجودها، وكذا تجريم محاولة فتح أو تخريب البريد أو المساعدة في هذه الجريمة، وقد وسن المشرع مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون[4].

---

[1]- قانون رقم 09-04 المؤرخ في 2009/8/16، هو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، صدر هذا القانون في الجريدة الرسمية رقم47، الصادرة بتاريخ 2009/08/16، يحتوي على ستة فصول تناولت التعريف بالجريمة، مراقبة الاتصالات الإلكترونية، القواعد الإجرائية، الهيئة الوطنية للوقاية من الجرائم المعلوماتية والاختصاص القضائي وهذا في19 مادة.

2 – مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، سنة 2021، ص 21.

[3] – القانون رقم 18-04، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر رقم 27، الصادرة بتاريخ 2018/05/13.

[4]– مهدي رضا، المرجع السابق، ص 21.

ثالثا: القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي: يقصد بمعالجة المعطيات ذات الطابع الشخصي في هذا القانون كل عملية أو مجموعة عمليات منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيئي وكذا الإغلاق أو التشفير أو المسح أو الإتلاف[1].

و قـد سن المشرع الجزائري مجموعة من الآليات والضوابط ذات الصلة بالمعالجة الآلية للمعطيات وحدد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وذلك في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم.

ومن أهم تلك الآليات استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي، تكلف بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة.[2]

كما جرم المشرع الجزائري بموجب هذا القانون في الفصل الثالث المتضمن الأحكام الجزائية من المادة 54 إلى المادة 74 الاعتداء على المعطيات ذات الطابع الشخصي بإقرار عقوبات مالية وأخرى سالبة للحرية مع إمكانية مصادرة محل الجريمة.

رابعا: القانون 08-01 المتعلق بالتأمينات الاجتماعية: تطرق هذا القانون إلى جانب من مكافحة الجريمة الإلكترونية في الشق المتعلق بهيئات الضمان الاجتماعي، وذلك من خلال نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلّم للمؤمن له اجتماعيا مجانا بسبب العلاج والتي تكون صالحة للاستعمال على كامل التراب الوطني[3].

كما تناول المشرع العقوبات المقررة في الحالات التالية:

- تسليم أو استلام بهدف الاستعمال غير المشروع
- القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية، إعداد أو تعديل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في

[1] – القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 بتاريخ 10 يونيو 2018.

[2] – سميحة بلقاسم، حميد بوشوشة، مجلة العلوم الانسانية لجامعة أم البواقي، المجلد 10، العدد 01، جوان 2023، ص546.

[3] – فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة ضمن أعمال المؤتمر الدولي الرابع عشر حول الجريمة الإلكترونية، طرابلس، مركز جيل للبحث العلمي، سنة 2017، ص ص 115- 136.

البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة، وهو ما أشارت إليه المادة 93 مكرر 2 والمادة 93 مكرر3من القانونرقم 08-01.[1]

خامسا: قانون رقم 18-05 المتعلق بالتجارة الإلكترونية: يحدد هذا القانون القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات فنجده يطبق في مجمل المعاملات التجارية الإلكترونية في حالة ما إذا كان أحد أطراف العقد الإلكتروني: متمتعا بالجنسية الجزائرية، أو مقيما إقامة شرعية في الجزائر، أو شخصا معنويا خاضعا للقانون الجزائري، أو كان العقد محل إبرام أو تنفيذ في الجزائر.

وقد أدرج المشرع عقوبات تقدر بغرامة من 200000 دج إلى 100000 دج كل من يعرض للبيع أو يبيع عن طريق الاتصال الإلكتروني، المنتجات أو الخدمات التالية : لعب القمار والرهان واليانصيب المشروبات الكحولية والتبغ، المنتجات الصيدلانية المنتجات التي تمس بحقوق الملكية الفكرية أو الصناعية أو التجارية، كل سلعة أو خدمة محظورة بموجب التشريع المعمول به، كل سلعة أو خدمة تستوجب إعداد عقد رسمي و يمكن القاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح من شهر إلى ستة أشهر.

كما اقر عقوبة غرامة من 500000 دج إلى 2000000 دج على كل معاملة عن طريق الاتصالات الإلكترونية تستهدف ما يلي: العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به وكذا كل المنتجات و الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي، و يمكن القاضي أن يأمر بغلق الموقع الإلكتروني والشطب من السجل التجاري.[2]

سادسا: القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني:
التصديق الإلكتروني هو شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني طبقا لسياسة التصديق الإلكتروني الموافق عليها.
- أن تمنح للموقع دون سواه.

[1]- القانون رقم 08-01، المتمم للقانون رقم 83-11، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية رقم 04 بتاريخ 27 يناير 2008.

[2] - قانون رقم 18-05، المؤرخ في 10 ماي سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28،صادرة بتاريخ 2018/05/16.

وقد يكون التوقيع الالكتروني أو شهادة التصديق الالكترونية محل جريمة الكترونية طالما أن استعمالها ومجال نشاطهم مرتبط بحالة التقنية و قد عاقب المشرع كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من مليون دينار 1.000.000 دج إلى خمسة ملاين دينار 5.000.000 دج أو بإحدى هاتين العقوبتين فقط [1].

سابعا: مكافحة الجريمة المرتكبة عبر الإنترنت من خلال قوانين الملكية الأدبية والفنية:إن التطور الملحوظ في مجال الاتصال رافقه تطور في وسائل نقل الإنتاج الفكري على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف كانت محل اهتمام ودراسة من قبل المختصين في مجال الملكية الفكرية، وقد كان من أهم هذه المصنفات، المصنفات الخاصة ببرامج الحاسوب، حيث إعترف المشرع الجزائري بحمايتها في المادة 04 من الأمر 03-05[2]، على أنها مصنفات أدبية سواء في صورتها الأصلية أو المشتقة وسواء كان البرنامج برنامج تطبيق أو تشغيل، بلغة المصدر أو بلغة الآلة.

و لقد شدد المشرع الجزائري العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، من خلال الباب السادس من الأمر 03-05، في فصلين الأول تمحور حول الدعوى العمومية والثاني تضمن الأحكام الجزائية.

و هنـاك العديد من القوانين التي تعنى بالملكية الفكرية ولها ارتباط وثيق بالجرائم المعلوماتية على غرار:

الأمر رقم 07-03، المؤرخ في 2003/07/19، يتعلق ببراءة الاختراع.
الأمر رقم 65-76، المؤرخ في 1976/07/16، يتعلق بتسميات المنشأ.
الأمر رقم 77-66، المؤرخ في 1966/04/28، المتعلق بالرسوم و النماذج.
الأمر رقم 08-03، المؤرخ في 2003/07/19، يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة.
الأمر رقم 06-03، المؤرخ في 2003/07/19، يتعلق بالعلامات.

[1] – القانون رقم 15-04، المؤرخ في 2015/02/01، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، صادرة بتاريخ 2015/02/10.

[2] – الأمر 03-05، المؤرخ في 2003/06/19، الصادرة بتاريخ 2003/06/23، ج ر، العدد 44، المعدل والمتمم للأمر 10-97، المتعلق بحقوق المؤلف والحقوق المجاورة.

المطلب الثاني: الجانب المؤسساتي:

إضافة للترسانة القانونية التي أقرها المشرع الجزائري في التعامل مع هذه الظاهرة، والتي تعتبر تدعيما نوعيا للمنظومة التشريعية في الجزائر، هناك جانب أخر هو الجانب المؤسساتي الداعم والتكميلي للجانب التشريعي في مجال محاربة الجريمة المعلوماتية، من خلال الهياكل الخاصة بكشف ومحاربة الجريمة المعلوماتية، وتتمثل في المراكز والوحدات والمصالح التي استحدثتها الدولة الجزائرية في إطار استراتيجيتها المكافحة الجريمة الإلكترونية والتصدي لها، والتي سنتطرق لها تباعا في النقاط التالية:

الفرع الأول: المؤسسات الأمنية:

على غرار الجانب القانوني الذي يكمله الجانب الأمني سارعت المؤسسات الامنية على اختلاف أنوعها إلى خلق فضاء جديد يتماشى وتطور الذي يشهده الإجرام المعلوماتي حيث عمدت إلى إنشاء مصالح متخصصة في مكافحة هذا لنوع من الإجرام على النحو الآتي:

أولا: المصلحة المركزية لمكافحة الجرائم السيبرانية التابعة للمديرية العامة للأمن الوطني:

في ظل التهديدات الأمنية الناجمة عن الجرائم الإلكترونية وأتساع رقعتها، سعت المديرية العامة للأمن الوطني لمجابهة هذا الإجرام، من خلال إنشاء المصلحة المركزية للجريمة المعلوماتية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، وقد كانت هذه المصلحة عبارة عن فصيلة شكلت النواة الأولى على مستوى المديرية العامة للأمن الوطني لمحاربة هذه الجريمة، حيث أنشأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني، حيث تم إدراجها ضمن للهيكل التنظيمي لمديرية الشرطة القضائية في يناير 2015.

وتتمثل مهام هذه المصلحة فيما يلي:

- مساعدة مصالح الشرطة القضائية في مجال التحريات التقنية.
- المشاركة في حماية الأنظمة المعلوماتية والفضاء السيبراني الوطني.
- التعاون والمشاركة في التحقيقات والتحريات ذات البعد الوطني والدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- اليقظة المعلوماتية والبحث عن الشبكات المفتوحة، عن كل محتوى غير شرعي يشكل في حد ذاته جريمة في قانون العقوبات أو يكون مخالف للنظام العام[1].

[1] - سميحة بلقاسم، حميد بوشوشة، المرجع السابق، ص548.

- المساهمة في التكوين المتخصص لعناصر الشرطة المتواجدين على مستوى فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات[1].

و ضمن مساعي المديرية العامة للأمن الوطني لمكافحة الجرائم المعلوماتية، قامت بإنشاء فرق متخصصة في مكافحة الجريمة المعلوماتية على مستوى 58 أمن الولايات تتمحور مهامها في ما يلي:

- ❖ استقبال شكاوى المواطنين في مجال الجرائم المتواجدة الفضاء السيبراني.
- ❖ البحث والتحري في الجرائم المعلوماتية تحت إشراف الجهات القضائية.
- ❖ توعية وتحسيس المواطنين بمخاطر الانترنت وخصوصا على الأطفال[2].

ولتعزيز مهام المديرية العامة للأمن الوطني بخصوص محاربة الجريمة الإلكترونية، وبالنظر للبعد الدولي الذي عادة ما يتخذه هذا النوع من الإجرام، فقد أكدت المديرية المعنية عضويتها الفعالة في المنظمة الدولية للشرطة الجنائيةINTERPOL حيث تتيح هذه الأخيرة مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، إضافة إلى مباشرة الإنابات القضائية الدولية ونشر أوامر بالقبض عن المبحوث عنهم دوليا[3].

ثانيا: نيابة مديرية الشرطة العلمية والتقنية التابعة للمديرية العامة للأمن الوطني: أسندت المديرية العامة للأمن الوطني مهمة مكافحة الجريمة المعلوماتية لنيابة مديرية الشرطة العلمية والتقنية، وتضع هذه الأخيرة لخدمة هذا الهدف مصالح علمية مختصة بذلك، تتولى أعمال البحث والتحري بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدات هي:

- المخبر المركزي للشرطة العلمية والكائن مقره بالجزائر العاصمة
- المخبر الجهوي للشرطة العلمية قسنطينة
- المخبر الجهوي للشرطة العلمية وهران.

يتولى كل مخبر سواء المركزي أو الجهوي مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم كل مخبر دائرتين هما:

1- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني، مجلة مصداقية، المجلد 1، العدد 1، سنة 2019، ص ص 100، 123.

2- إدريس عطية، المرجع السابق، ص 123.

3- فضيلة عاقلي، المرجع السابق، ص 133.

- **الدائرة العلمية:** وتتولى أعمال البحث والتحقيق وتحليل الأدلة المتصلة بالمجال البيولوجي والطب الشرعي والكيمياء والمخدرات وكذلك تلك المتعلقة بمجال التسميم والحريق و المتفجرات كل منها على مستوى مخبر خاص.
- **الدائرة التقنية:** وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى[1].

ومن جانب آخر، تؤدي الشرطة الجزائرية دورا هاما في مجابهة الإرهاب السيبراني، وذلك من خلال:

- ✓ الدوريات الالكترونية (خلايا اليقظة الإلكترونية لرصد أي تصرف مشبوه).
- ✓ محاولة تتبع الأثر الإلكتروني.
- ✓ التوعية والتحسيس عبر الفضاء السيبراني.
- ✓ العمل على تجفيف مصادر التمويل والتجنيد عبر الفضاء السيبراني.
- ✓ التعاون الدولي في مجال تبادل المعلومات و الخبرات[2].

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: أنشأ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 2004/06/26، ويعتبر مكسب مؤسساتي كبير للجزائر بفضل التقنيات الحديثة والمتطورة المستخدمة في مجال التحقيقات ومكافحة الجريمة وتبنيه نظام إدارة الجودة مما مكنه من الحصول على شهادة اعتماد على الصعيدين الوطني والدولي، ومن بين المهام المسندة للمعهد:

- إنجاز الخبرات والتحاليل بناء على طلبات القضاة المحققين والسلطات المؤهلة.
- الدعم التقني للوحدات أثناء التحقيقات المعقدة.
- تصميم بنوك معطيات وإنجازها وفقا للقانون.
- المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- المساهمة في تحديد سياسة جنائية مثلى لمكافحة الإجرام .
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحث التطبيقي وأساليب التحريات الفعالة في ميدان علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في تنظيم دورات تحسين المستوى والتكوين .

---

[1]– حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة الدكتورة في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، سنة 2015– 2016، ص177.

[2]– إدريس عطية، المرجع السابق، ص 123

كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام دورا فعالا في مجال مكافحة الجرائم السيبرانية إذ تكلف دائرة الإعلام الآلي والإلكتروني:

- ✓ معالجة وتحليل وتقديم كل دليل الكتروني لفائدة أجهزة العدالة.
- ✓ تقديم مساعدة تقنية للمحققين في التحقيقات المعقدة .
- ✓ السهر على تأمين اليقظة التكنولوجية من أجل تحيين المعارف والتقنيات والطرق المستعملة في الخبرات العلمية[1].

و تنقسم دائرة الإعلام الآلي والإلكتروني إلى (03) مخابر وكل مخبر مزود بفصيلة تسند لها مهمة اقتناء المعطيات من دعامات المعلومات وضمان نزاهة وشرعية الدليل الالكتروني وتتمثل هذه المخابر الثلاثة فيما يلي:

- مخبر الإعلام الآلي
- مخبر الفيديو
- مخبر الصوت لتحديد شرعية التسجيلات الصوتية مثلا[2].

وهكذا وبجمعه للكفاءات والمعدات والوسائل التكنولوجية المتطورة وفي محيط مكيف يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام أهم قلاع مكافحة الجريمة المعلوماتية وتتبعها على مستوى الوطني.

رابعا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني: أنشئ هذا المركز سنة 2008 ويهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق يتواجد مقره بالجزائر العاصمة يعكف هذا المركز على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها، سواء كانوا أشخاصا فرادى أو عصابات، وذلك من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك وحتى الأفراد[3].

ويعتبر هذا المركز نقطة اتصال وطني، يعمل على توفير المساعدة التقنية للمحققين ويتم فيه حفظ الأدلة ويوجه التحقيقات باستخدام التكنولوجيا الرقمية، إضافة إلى معاينة الجرائم ومراقبة البحث عن الجرائم وخصوصا على مستوى الإرهاب والقرصنة المعلوماتية[4].

---

[1]– أنظر الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz

[2]– أومدور نجاة خصوصية التحقيق في مواجهة الجرائم المعلوماتية. رسالة دكتوراه في القانون الخاص، كلية الحقوق جامعة محمد البشير الإبراهيمي، برج بوعريرج، سنة2021، ص101.

[3] – إدريس عطية، المرجع السابق، ص 112.

[4] – سفيان حديدان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الثامن، المجلد الثاني، 11 نوفمبر2017 ، ص ص 302-317.

كما يهدف مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، وقد تمكنت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وكذا من خلال الملتقيات ذات الطابع الوطني والدولي وتبادل الخبرات مع دول أخرى، أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي ورجال القانون، وذلك من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها[1].

ومن بين مهام هذا المركز كذلك ضمان المراقبة الدائمة والمستمرة على شبكة الانترنت القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية بالإضافة إلى المشاركة في عمليات التحري والتسرب عبر شبكة الانترنت لفائدة وحدات الدرك الوطني والسلطات القضائية،وكذا المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية، كما يضطلع هذا المركز بمساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة[2].

وتشير إحصائيات متعلقة بالجرائم الإلكترونية في الجزائر، إلى أن هذا النوع من الإجرام يعرف ارتفاعا رهيبا، ما جعل المصالح الأمنية تُحذر وتؤكد أن الجريمة انتقلت من العالم الحقيقي إلى الافتراضي العابر للحدود.

خامسا:مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة: استحدثت بتاريخ 11 جوان 2015 على مستوى دائرة الاستعمال و التحضير الأركان الجيش الشعبي، وأوكلت لها مهمة حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات اثناء استخدام التكنولوجيا، ضمان حماية منظومة الإعلام بالإضافة إلى اعتماد التكوين التقني والعلمي لنتاج الكفاءات والمهارات القادرة على خرق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية، دون ان ننسى الإعتماد المستمر على البحث العلمي لتطوير وسائل الدفاع استجابة للتطور في مجال التكنولوجيا، بإضافة إلى فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من هذا المجال.

[1] – سمير بارة، المرجع السابق، ص 280.

[2] – سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، العدد 01، صادرة بتاريخ 2021/06/09، ص ص 266 –282.

الفـرع الثـــاني: الهيئات المستحدثة:

أمام تنامي ظاهرة الإجرام المعلوماتي وسرعة انتشاره عمدت الجزائر إلى خلق مكنيزمات جديدة من شأنها مواكبة تطور هذه الظاهرة الإجرامية فعمدت إلى إنشاء هيئات واقطاب جزائية متخصصة والتي تمثلت في:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: نصت على إنشاء هذه الهيئة المادة 13 من القانون 09-04، المتضمن القواعد الخاصة للوقايةمن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقد خضعت لعدة تعديلات تماشيا والتطور الذي يشهده عالم الإعلام والإتصالات بداية بالمرسوم الرئاسي رقم 15-261، ثم المرسوم 19-172 والمرسوم 20-183 وأخير المرسوم الرئاسي 21- 439، المؤرخ في 2021/11/07[1]، الذي حدد تشكليه هذه الهيئة في المادة 05 التي نصت على ما يلي: "تتكون الهيئة من مجلس توجيه ومديرية عامة، توضعان تحت سلطة رئيس الجمهورية ويقدمان له عرضا عن نشاطاتهما".

أشارت المادة 04 من المرسوم الأخير إلى أن الهيئة تمارس المهام المنوطة بها تحت رقابة السلطة القضائية طبقا لأحكام قانون الإجراءات الجزائية والقانون 09-04[2]، وتكلف بما يأتي:

- تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية و التي تمس بأمن الدولة.

كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول.

- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

---

[1] – المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد86، الصادر في تاريخ 2021/11/11.

[2]- القانون 09-04، المرجع السابق.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وانجاز الخبرات القضائية.
- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبدل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، وفقا لأحكام المادتين 17 و 18 من القانون رقم 09-04.

ثانيا: المنظومة الوطنية لأمن الأنظمة المعلوماتية: نص عليها المرسوم الرئاسي رقم 20-05 حيث تعتبر أداة الدولة في مجال امن الانظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد استراتيجية وطنية لأمن الانظمة المعلوماتية وتنسيق تنفيذها، حيث تشتمل هذه المنظومة الموضوعة لدى وزارة الدفاع الوطني على مجلس وطني لأمن الأنظمة المعلوماتية بالإضافة إلى مجلس وطني لأمن الأنظمة المعلوماتية[1].

01- مجلس وطني لأمن الأنظمة المعلوماتية: يتولى في إطار إعداد الاستراتيجية الوطنية في مجل إعداد امن الأنظمة المعلوماتية على الخصوص وقد حددت المادة 04 من المرسوم 20-05، مهامه على غرار البث في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها دراسة مخطط عمل الوكالة و تقرير نشاطها والموافقة عليها، التنسيق مع الوكالة الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية وعلى تصنيف الأنظمة المعلوماتية، الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الالكتروني.

02- وكالة أمن الأنظمة المعلوماتية: هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية حيث نصت المادة 18 من المرسوم 20-05، على مهامها ومن ابرزها تحضير الإستراتيجية الوطنية، تنسيق وتنفيذ الإستراتيجية وضمان اليقظة التكنولوجية مع مرافقة الإدارات العامة، اعتماد منظومات إنشاء وفحص الإمضاء الالكتروني، التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية، تقوم زيادة عن ذلك بإبرام مشاريع شراكة في مجال أمن الأنظمة بعد موافقة المجلس وتقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال امن الأنظمة المعلوماتية[2].

---

[1]- المرسوم الرئاسي رقم 20-05، المؤرخ في 2020/01/20، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية العدد 04، الصادرة بتاريخ 2020/01/26.

[2]- المرسوم الرئاسي رقم 20-05، المؤرخ في 2020/01/20، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

ثالثا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تم إنشاء هذا القطب بموجب الأمر رقم 11-21 المؤرخ في 2021/08/25، المعدل والمتمم القانون الإجراءات الجزائية، وقد أوكلت لهذا القطب مهمتين أساسيتين تتمثلان في:

- المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال والجرائم المرتبطة بها.
- الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر رقم 11-21، إذا كانت تشكل جنحا.

وقد فصلت المادة 211 مكرر 24 في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها، والتي يتعين على وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب المختصين حصريا بالمتابعة والتحقيق والحكم فيها، إذ تتمثل هذه الجرائم في[1]:

- ✓ الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني،
- ✓ جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع،
- ✓ جرائم نشر وترويج أخبار مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،
- ✓ جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،
- ✓ جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- ✓ جرائم التمييز وخطاب الكراهية[2].

[1] – الأمر رقم 21-11، المعدل والمتمم للأمر 66-155، المتضمن قانون الإجراءات الجزائية.

[2] – الأمر رقم 21-11، المعدل والمتمم للأمر 66-155، المتضمن قانون الإجراءات الجزائية.

خلاصـة الفصـل الثــاني

نخلص من خلال ما سبق، أن النظام المعلوماتي يشمل أموال مادية واخرى معنوية هذه الأخيرة طرحت العديد من الإشكاليات القانونية كونها تشمل أشياء غير ملموسة أي غير مادية، ولقد تناول المشرع الجزائري صور الإعتداء على الأموال على النحو التقليدي في أربعة صور هي جرائم التحويل غير الشرعي للأموال جرائم الاستخدام غير المشروع البطاقات الدفع الإلكتروني، جريمة الإتلاف المعلوماتي و وجرائم الاعتداء على المصنفات الرقمية.

أمام تطور وخطورة هذا النوع من الإجرام وما أصبح يخلفه من تبعيات سلبية على الأفراد والمجتمع سارعت الدولة الجزائرية إلى تبني استراتيجية مزدوجة لتصدي له، الأولى تمثلت في الجانب القانوني من خلال اتباع خطوتين أساسيتين أولهما تعديل النصوص والقوانين السارية ذات العلاقة بهذا المجال، بحيث جعلها تواكب وتتكيف مع التحدي الرقمي الجديد على غرار قانون العقوبات وقانون الإجراءات الجزائية، وكخطوة جديدة قام بسن القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي يمكن اعتباره أنه أكثر تجاوبا مع خصوصية هذا النوع من الجرائم رغم النقائص التي يحتويها وعدم إلمامه بهذه الظاهرة الخطيرة من كل جوانبها.

أما من الجانب المؤسساتي، فتظهر جهود الدولة الجزائرية في مجال مكافحة الإجرام الإلكتروني وتحقيق الأمن السيبراني من خلال استحداث هيئات ومراكز جديدة تضطلع بأدوار جد هامة في مجابهة الجريمة المعلوماتية على غرار المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني، المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنظومة الوطنية لأمن الأنظمة المعلوماتية، ومؤخرا استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المختص في المتابعة والتحقيق والحكم في هذه الجرائم.

الخاتمة

يتجلى من خلال ما سبق استعراضه أن مجال تأمين الفضاء المعلوماتي ومكافحة الجرائم المستحدثة فيه على الصعيد التنفيذي على غرار تلك الجرائم الواقعة على الأموال المعلوماتية، يتطلب وضع سياسة شاملة وعامة من قبل الدولة ومؤسساتها وكذا توفير الوسائل المعلوماتية والمادية وتدابير الحماية التقنية والتنظيمية والتشغيلية وكيفية التصرف في مكافحة المخاطر السيبرانية والتبليغ عنها، وجب نشر هذه السياسة وتعميمها على مؤسسات الدولة والمنظمات ومختلف شرائح المجتمع المدني.

لقد اجتهد المشرع الجزائري للتصدي لهذا النوع من الجرائم من خلال تعديل الجوانب الموضوعية و الاجرائية للقوانين العامة والسعي لجعلها تواكب التطورات التكنولوجيا الحديثة كما قام باستحداث قوانين أخرى و هيئات خاصة أكثر تجاوبا مع طبيعة الجرائم الالكترونية، هذه الازدواجية في المعالجة ساهمت بشكل فعال في الحد من تفاقم ظاهرة الاجرام المعلوماتي في الدولة الجزائرية ورغم هذا فإن الواقع أثبت عدم كفايتها بالنظر إلى التطور السريع و المستمر لهذا النوع من الجرائم التي تتميز بطبيعة قانونية مغايرة تماما للجرائم التقليدية، **ومن بين النتائج المتوصل إليها:**

– المعلومة أصبحت تمثل قيمة اقتصادية فهي باستقلالها عن دعامتها تمثل قيمة قابلة للاستحواذ وذلك من شأنه أن يغير نظرة القانون إلى الأشياء المعنوية.

– عدم كفاية وملائمة نصوص الجرائم التقليدية لتحقيق الحماية الجنائية للمال المعلوماتي كونها تتعلق بوقائع مادية ولا تتناسب مع الوقائع المعنوية، باستثناء الإتلاف المعلوماتي الذي نص عليه المشرع صراحة في قانون العقوبات.

– رغم تدارك المشرع الجزائري للفراغ القانوني في مجال تجريم الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات غير انه تضمن سوى ثلاث انواع من الجرائم.

–عدم استحداث المشرع الجزائري نص خاص بالتزوير المعلوماتي والذي يعد من اخطر صور الغش عبر الحاسوب، حيث اكتفى بذكر التزوير الخاص بالمحررات في قانون العقوبات ولم يوسع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير.

– المجتمع الجزائري يشهد وتيرة متصاعدة لنسبة الإجرام المعلوماتي بدليل الإحصائيات المسجلة والمعالجة على مستوى مصالح الأمن، ما يفسره ضعف الوعي الاجتماعي بمخاطر الفضاء السيبراني من جهة و إستغلال المجرم المعلوماتي للتكنولوجيا الحديثة من جهة أخرى.

– افتقار الجزائر إلى استراتيجية واضحة ومتكاملة لمواجهة تحديات الذي تفرضها هذه الجرائم كون البيئة التنظيمية والتشريعية الخاصة بالأمن المعلوماتي في الجزائر، ما زالت في طور التشكل.

التوصيات:

- ضرورة إعطاء تعريف موسع للجريمة المعلوماتية مع التحديد الدقيق لصور السلوك الإجرامي المراد تجريمه.
- تطوير النصوص التقليدية المتعلقة بجرائم الأموال وتعديلها بما يتلائم وطبيعة المال المعلوماتي أو إصدار قانون خاص يتضمن الجرائم المال المعلوماتي.
- التوجه للاستفادة من احترافية الناشطين والباحثين في مجال الأنظمة المعلوماتية والهاكرز بصرف النظر عن سنهم أو جنسهم أو انتمائهم أو مستواهم التعليمي، بما يسمح بتطوير خبراتهم ومهارتهم وتوظيفها لابتكار البرامج المعلوماتية وأنظمة الحماية والأمن المعلوماتي، وهو ما يتأتى بتوفير فرص الدعم والحوافز لهم.
- محاولة الاستفادة من الإمكانيات و القدرات التي يمتلكها المجرم المعلوماتي و توظيفها في خدمة المجتمع وفقا للقانون 09_01 المتعلق بالعمل للنفع العام.
- تدريس مواد الأنظمة المعلوماتية و الجرائم التي قد تنشأ منها كجريمة الاعتداء على الأموال المعلوماتية في كليات الحقوق و المعاهد وكذا المدارس العليا للقضاء .
- تطوير نظم الحماية التقنية للنظم المعلوماتية.
- اتخاذ تدابير من شأنها الحفاظ على سرية المعلومات الخاصة بالحسابات البنكية وبطاقات الائتمان وغيرها من وسائل تبادل المعلومات.
- التحديث المستمر لبرامج حماية الحواسيب من الفيروسات.
- التدريب والتكوين المستمر للكوادر البشرية العاملة في مجال مكافحة الجرائم الالكترونية واستحداث شهادات عليا متخصصة في المجالات التقنية والقانونية المتعلقة بمكافحة الجرائم المعلوماتية، وحث الجامعات والمراكز البحثية على تسليط الضوء أكثر على مثل هذه الجرائم، من خلال تكثيف الندوات والملتقيات والأيام الدراسية حول هذا الموضوع.
- إنشاء أكاديميات قضائية لإعداد و تأهيل الخبراء القضائيين في كافة التخصصات العلمية و خاصة الجرائم المستحدثة وعلى رأسها جريمة سرقة المال المعلوماتي.
- تعزيز الترسانة القانونية من خلال إصدار نصوص قانونية جديدة تسد الفراغ القانوني الموجود في النصوص الحالية لمواجهة الصنوف المستحدثة للجريمة المعلوماتية والهجمات السيبرانية.
- بناء الاستراتيجية السيبرانية الوطنية من خلال تظافر جهود جميع الأطراف (القطاعين العام والخاص والمجتمع المدني- مختلف الجمعيات).

الملاحـــق

الملحق رقم 01:

إحصائيات الجرائم السيبرانية المسجلة على مستوى الوطني لمختلف المصالح الامنية:

سجلت المصالح الأمنية ارتفاعا قياسيا في الجرائم الإلكترونية أو ما يعرف بالجرائم السبيرانية، حيث ارتفعت من 12 ألف جريمة سجلت في 2022 إلى 14 ألف جريمة خلال سنة 2023.

وقصد مواجهة أشكال الإجرام الإلكتروني، سجلت مصالح الأمن الوطني المختصة في مكافحة الجرائم المعلوماتية وفرقها العملياتية التابعة لمصالح الشرطة القضائية، خلال الفترة الممتدة من الفاتح جانفي إلى غاية 31 أكتوبر من سنة 2023، (3325) قضية راح ضحيتها 2315 شخصا وتورط فيها 4138 مشتبها فيهم، تم تقديمهم أمام الجهات القضائية المختصة، بالمقابل سجلت مصالح الدرك الوطني ارتفاعا في عدد الجرائم الإلكترونية خلال سنة 2023، حيث تجاوز عدد القضايا التي عالجتها الفرق العملياتية للدرك الوطني المختصة في الإجرام الالكتروني 4500 قضية، فيما عالجت مصالح الأمن العسكري قرابة 4 آلاف قضية مصنفة في خانة السرية خلال سنة 2023.

وحسب التقارير المفصلة لمصالح الأمن المشتركة، فإن الرابط الوحيد بين هذه الجرائم هو سوء استخدام التكنولوجيا، سواء كانت برامج أو أجهزة رقمية، حيث شملت الجرائم المالية والاقتصادية، خاصة العابرة للحدود وتلك المستحدثة، إلى جانب الابتزاز، التهديد والتشهير السيبراني، اختراق مواقع مؤسسات وشركات عمومية وخاصة، وكذا المساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي.

كما شملت أيضا نشر المعلومات الزائفة والمضللة والقرصنة والتحرش الإلكتروني والنصب والاحتيال، إلى جانب بيع السلع غير المرخصة عبر الإنترنت، والاعتداء على حقوق الملكية الفكرية وجرائم أخرى.

و فقد أظهر تحليل معطيات الجرائم المسجلة أن القذف والسب والتشهير والتهديد عبر الفضاء الافتراضي هي أكثر الجرائم المسجلة، تليها جرائم بيع السلع غير المرخصة عبر الإنترنت والمصنفة ضمن خانة "الجرائم الجديدة"، ثم تأتي الجرائم ضد الأمن العمومي، والأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، ثم الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة، وبعدها اختراق مواقع المؤسسات والشركات العمومية والخاصة، كما أن 65% من الجرائم المرتكبة تمت عن طريق الفايسبوك وتعرض من خلالها عدد من الأشخاص من إطارات ومسؤولين في الدولة إلى ابتزاز وتهديد بنشر صور أغلبها مركب[1].

[1] – مقال منشور من قبل الصحفية نوار باشوش، عبر الجريدة الإلكترونية echoroukonline، بتاريخ 2024/02/18، تحت عنوان 60% من جرائم الابتزاز والتهديد والتشهير ارتكبت عبر مواقع التواصل، 14 ألف جريمة سيبرانية في 2023 والتسوق الإلكتروني في الصدارة، أطلع عليه بتاريخ 2024/05/30.

الملحق رقم 02:

إحصائيات الجرائم السيبرانية المسجلة على مستوى المديرية العامة للأمن الوطني خلال سنتي 2023/2022[1].

	عدد القضايا المسجلة		عدد الأشخاص المتورطين	
الجرائم	2022	2023	2022	2023
المساس بالأشخاص عبر شركة الأنترنت	1999	2046	1796	1905
المساس بأنظمة المعالجة الآلية للمعطيات	323	331	217	202
النصب والإحتيال عبر شركة الأنترنت	1130	801	1958	1318
المساس بالأطفال عبر شركة الأنترنت	113	56	124	78
نشر محتويات مخالفة للنظام عبر شركة الأنترنت	1066	1083	1332	1427
بيع السلع المحظورة عبر شركة الأنترنت	110	115	181	159
جرائم أخرى	395	286	538	476
المجموع	5136	4718	6146	5567

[1] – مجلة الشرطة، العدد 158، ماي 2024.

الملحق رقم 03:

مخرجات ملتقى وطني حول " الجرائم الإلكترونية بالجزائر وآليات مكافحتها وفق مقاربة متعدّدة التخصّصات" المنظم بــولاية الأغواط

نظّم مركز البحث في العلوم الإسلامية و الحضارة بالأغواط ملتقى وطني حول " الجرائم الإلكترونية بالجزائر وآليات مكافحتها وفق مقاربة متعدّدة التخصّصات"، يوم الاثنين13 شعبان 1444هـ الموافق لـ 06 مارس 2023م، تحت رئاسة الدكتور عمر بن عيشوش، شارك فيه عبر تقنية التحاضر عن بعد أزيد من مئة مشارك، بأزيد من سبعين مداخلة غطّت محاور الملتقى التي تناولت الاطار المفاهيمي (الجريمة الإلكترونية، الأمن السيبراني، مواقع التواصل الاجتماعي...)، وكذا أنواع الجرائم الإلكترونية الواقعة عبر مواقع التواصل الاجتماعي وخصائصها، بالإضافة إلى أدّلة الاثبات الجنائي في الجرائم الالكترونية، فضلا عن آليات مكافحة الجرائم الإلكترونية وفق مقاربات متعدّدة التخصّصات.

و قد سجلّت الجلسة الافتتاحية للملتقى مداخلة النقيب "عبد الرؤوف بن طراد" ممثّل قيادة الدرك الوطني الخبير القضائي في الإعلام الآلي والإلكتروني ورئيس مخبر الإعلام الآلي بملحقة معهد الأدّلة الجنائية وعلم الإجرام بورقلة، و الموسومة بـ: "أهمية الخبرة الرقمية في معالجة القضايا الإجرامية الإلكترونية"، و كذا مداخلة محافظ الشرطة السيد" بن حمزة عبد الحكيم"، ممثل المديرية العامة للأمن الوطني، و رئيس فرقة مكافحة الجرائم السيبرانية، و الموسومة بـ: " تجربة الشرطة الجزائرية في مكافحة الجرائم السيبرانية".

تتجلّى أهمية هذه الفعالية من خلال تفشي ظاهرة الإجرام والجريمة الإلكترونية المرتكبة عبر مواقع التواصل الاجتماعي على وجه الخصوص في المجتمع الجزائري و اهتمام الباحثين بها بشكل متزايد، لكونها أثارت عدة إشكالات فقهية وقانونية لم تثر من قبل؛ مما فتح مجالا جديد للبحث في خصائصها وآليات مكافحتها.

هذا و هدف الملتقى إلى السعي إلى معالجة موضوع الجرائم الإلكترونية في المجتمع الجزائري، وكذا فتح مجال واسع للباحثين لتقديم رؤاهم وانتقاداتهم البناءة، بالإضافة إلى العمل على إيجاد آليات عملية لمكافحة الجريمة الإلكترونية بصفة عامة والجرائم المرتكبة عبر وسائل التواصل الاجتماعي بصفة خاصة.
وقد خلص المشاركون إلى التوصيات التالية:

01- الدعوة إلى إنشاء مرصد وطني لمكافحة الجريمة الإلكترونية بشكل استباقي وتعزيز الأمن السيبراني للهيئات والمؤسسات العمومية، ومكافحة الإرهاب الإلكتروني.

02- توعية جميع أفراد المجتمع الجزائري بمختلف شرائحه عبر مختلف المنابر الإعلامية بخطورة الجرائم الإلكترونية، والهجمات السيبرانية ونشر الوعي الاجتماعي بمخاطرها وبالأخص تلك الماسة بالحياة الشخصية للمستخدمين، حتى لا يكونوا عرضة للاعتداءات، والحث على الاستخدام الأمثل لها، والتحذير من ظاهرة الإرهاب الإلكتروني، وضرورة توخيهم الحيطة والحذر من الإغراءات التي يمكن أن تقدّم إليهم بهدف إلتحاقهم بالجماعات الإرهابية، وحثهم على التبليغ الفوري لكل محاولة استدراج يتعرضون لها من قبل جهات معلومة أو مجهولة.

03- دعوة المشرع الجزائري إلى تعزيز الترسانة القانونية من خلال إصدار نصوص قانونية جديدة تسد الفراغ القانوني الموجود في النصوص الحالية لمواجهة الصنوف المستحدثة للجريمة الإلكترونية والهجمات السيبرانية.

04- تعزيز المرافقة الوالدية لأبنائهم أثناء استخدامهم للانترنيت والولوج للمواقع الإلكترونية ومواقع التواصل اجتماعي وقيامهم بخاصية الحظر أو الحدّ من ولوج أبنائهم لبعض التطبيقات أو المواقع، وتعزيز ثقافة أخلقة وسائط التواصل الاجتماعي وترشيد استخدامها.

05- ضرورة إيجاد حلول لحل مشكلات الاختصاص القانوني والقضائي التي تثيرها جرائم الاعتداء على المصنفات الإلكترونية في إطار تنسيق دولي متكامل من خلال إبرام اتفاقيات دولية تستمد منها التشريعات الجنائية الداخلية ضوابط نصوصها التجريمية بتحقيق تنظيم جنائي موضوعي وإجرائي شامل يتلاءم مع هذا الشكل الإجرامي المستحدث.

06- إشراك المجتمع المدني والمؤسسة المسجدية والتربوية والجامعية والجمعيات والنوادي العلمية والثقافية والرياضية في السياسة الوقائية من الجرائم الإلكترونية، عن طريق التوعية والتحسيس بخطورتها وإضرارها بمصالح المجتمع وأفراده، لاسيما بعد بروز وتفشي أنماط جديدة من الجرائم الواقعة عبر وسائل التواصل الاجتماعي كجرائم البث المباشر للمشاهد غير الأخلاقية.

07- دعوة المشرع الجزائري إلى تجريم فعل التنمر الالكتروني، وذلك من أجل تبني سياسة تشريعية واضحة المعالم تجاه هذه الجريمة، وفي حالة عدم صدور قانون خاص بهذه الجريمة، على المشرع إضافة نصوص قانونية خاصة بهذه الجريمة في قانون العقوبات، أو في القوانين ذات الصلة.

08- دعوة وزارة التربية الوطنية إلى إدراج محاور تتعلق بنشر ثقافة المواطنة الرقمية التي تبين الأساليب والمناهج الصحيحة لاستخدام تكنولوجيا الإعلام والاتصال في مقياس الإعلام الآلي في مرحلة التعليم المتوسط والثانوي.

09- دعوة وزارة التعليم العالي والبحث العلمي إلى إعادة النظر في المناهج المقررة في كلية الحقوق، وذلك بإضافة محاور لها علاقة بالتقنية الجديدة، مثل إدراج الجريمة الإلكترونية في مقياس قانون العقوبات، الإدارة الإلكترونية، القرار الإلكتروني التوقيع الإلكتروني في مقياس القانون الإداري، المحكمة الإلكترونية في مقياس قانون الإجراءات الجزائية.

10- ضرورة تفعيل التعاون الدولي والإقليمي لمجابهة الصنوف المستحدثة للجرائم الإلكترونية فلا مفر من التعاون الدولي في الجانب الإجرائي لكونها أضحت جريمة دولية تجاوزت جميع الحدود والأقاليم، كما يتوجب على الدول المتقدمة تقديم المساعدة التقنية للدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة، وذلك من خلال توفير التدريب والتكوين والوسائل اللازمة[1].

[1] – الملتقى الوطني حول " الجرائم الإلكترونية بالجزائر وآليات مكافحتها وفق مقاربة متعدّدة التخصّصات"، المنظم بولاية الأغواط من قبل مركز البحث في العلوم الإسلامية و الحضارة بتاريخ 06 مارس 2023.

قـــائمة المصـــادر و المـــــراجع

أولا: المصادر القانونية:

أ- الإتفاقيـات الدولية:

- اتفاقية بودابست لمكافحة الجرائم المعلوماتية والمنبثقة عن اجتماع المجلس الأوروبي بودابست، المجر، رقم 185، بتاريخ: 2001/11/21.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة مصر بتاريخ: 2010/12/21.

ب- الدستور:

- دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي 20-442، الجريدة الرسمية العدد 82، الصادرة بتاريخ 2020/12/30.

01- القــوانين:

- القانون رقم 04- 14، المؤرخ في 2004/11/10، المعدل والمتمم للأمر 66-155، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 71، الصادرة بتاريخ 2004/11/10.

- القانون رقم: 04-15، المؤرخ في 2004/11/10، المعدل والمتمم للأمر رقم 66- 156، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ 2004/11/10.

- القانون رقم 08-01، المتمم للقانون رقم 83-11، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية العدد 04، الصادرة بتاريخ 27 يناير 2008.

- القانون رقم 09-04 مؤرخ في 05-08-2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخة في2009/08/16.

- القانون رقم 15-04، المؤرخ في 2015/02/01،الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، الصادرة بتاريخ 2015/02/10.

- القانون رقم 18-04، المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، الجريدة الرسمية العدد 27، الصادرة بتاريخ 2018/05/13.

- القانون رقم 18-05، المؤرخ في 10 ماي سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28،الصادرة بتاريخ 2018/05/16.

- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34، الصادرة بتاريخ 10 يونيو 2018.

- قانون 24-06 المؤرخ في 2024/04/28، المعدل والمتمم للأمر رقم 66- 156، المتضمن قانون العقوبات، الجريدة الرسمية العدد رقم30، الصادرة بتاريخ 2024/04/30.

02-الأوامـــر:

- الأمر 66-155، المؤرخ في 1966/06/08، المتضمن قانون الإجراءات الجزائية.
- الامر رقم 66-156، المؤرخ في 08 /06/ 1966، المتضمن قانون العقوبات المعدل والمتمم
- الأمر 03-05، المؤرخ في 2003/06/19، الصادرة بتاريخ 2003/06/23، ج ر، العدد 44، المعدل والمتمم للأمر 10-97، المتعلق بحقوق المؤلف والحقوق المجاورة.
- الأمر رقم 21-11، المؤرخ في 2021/08/25، ج ر، العدد65، المعدل والمتمم للأمر 66-155، المؤرخ في 1966/06/08، المتضمن قانون الإجراءات الجزائية.

03-المراسيم الرئاسية:

- المرسوم الرئاسي رقم 20-05، المؤرخ في 2020/01/20، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية العدد 04، الصادرة بتاريخ 2020/01/26.
- المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد86، الصادر في تاريخ 2021/11/11.

ثانيا: المراجع الفقهية:

باللغة لعربية:

أ- الكتب العامة:

- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، " الجرائم ضد الأشخاص و الجرائم ضد الأموال " الجزء الأول، الطبعة الثالثة، دار هومة، 2006.

ب- الكتب متخصصة

- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، ط 2006.
- أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم إستخدام الحاسب الآلي، بدون دار النشر،2003.
- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

- بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 01، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.

-جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة دار الثقافة للنشر و التوزيع، الأردن، 2010.

- ديش سورية، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018.

- هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، القاهرة، ط 1995.

- هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، مصر، 2008.

- هلالي عبد اللاه أحمد، إلتزام الشاهد في الجرائم المعلوماتية، دار النهضة العربية، مصر، 2000.

- وضاح محمود الحمود ونشأت مفطي المجالي، جرائم الانترنيت، دار المنار للنشر، عمان، 2005.

- زرزار العياشي، غياد كريمة، استخدامات تكنولوجيا المعلومات والاتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية، ط 1، دار الصفاء للنشر والتوزيع، عمان، 2016.

- محمد أمين أحمد شوابكة، جرائم الكمبيوتر والانترنيت، دار الثقافة للنشر والتوزيع، عمان الأردن، ط01، 2004.

- محمد حماد مرهج الهبيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان 2005.

- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2003.

- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديد، الإسكندرية، 2001.

- محمد محمود المكاوي، الجوانب الاخلاقية و الاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع، مصر، 2010.

- محمد عبد الله أبو بكر سلامة، موسوعة الجرائم المعلوماتية، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006.

- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دون طبعة، دار النهضة العربية، القاهرة.

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

- محمد على قطب، الجريمة المعلوماتية و طرق مواجهتها، الجزء الثالث، وزارة الداخلية "أكاديمية الملكية للشرطة"، مملكة البحرين.

-محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، القاهرة، سنة 1984.

- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، مصر، 2008.
- مراد حسيني، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري، عملية التسرب الجزء الأول، الطبعة الأولى، قراءات في المادة الجنائية، دار النشر للمعرفة 2013 الجزائر.
- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، سنة 2012.
- نبيلة هبة هروالة، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
- نهلا عبد القادر المؤمني، الجرائم المعلوماتية، ط 02، دار الثقافة للنشر والتوزيع عمان، سنة 2008.
- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعرف، الإسكندرية، مصر.
- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسوبه الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 2001.
- عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الالي، الدار الجامعية للطباعة والنشر، بيروت، سنة 1999.
- عبد الكريم عبد الله عبد الله، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة، مصر، 2008.
- عبد الرحمان بن عبد الله السيد، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي و شبكة المعلوماتوالأنترنيت) دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004.
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي نموذجي الإسكندرية، دار الفكر العربي، القاهرة،2009.
- على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) المكتب الجامعي الحديث الإسكندرية 2012.
- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط 1، منشورات زين الحقوقية والأدبية، سنة 2013.
- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دراسة مقارنة، دار النهضة العربية القاهرة، مصر، 2010.
- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الالي و الإنترنيت في مصر و الدول العربية، المكتب العربي الحديث، الإسكندرية، 2006.
- فاروق عبده فلية، أحمد عبد الفتاح الزكي، معجم مصطلحات التربية لفظا واصطلاحا، دار الوفاء لدنيا الطباعة والنشر 127-128، مصر، 2004.

- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكومبيوتر، منشورات الحلبي، لبنان 2003.
- قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر، الجزائر، سنة 2006.
- قورة نائلة، جرائم الحاسب الاقتصادية، النهضة العربية، القاهرة، 2004.
- رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، كتاب أعمال المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس، لبنان، 24- 25 مارس،2017.
- خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع ، الجزائر، 2008.
- خالد ممدوح ابراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2010.
- خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب، دار النشر والتوزيع، عمان، ط 1، 2011.
- ضياء أحمد علي نعمان، الظاهرة لإجرامية بين الفهم والتحليل، دار النهضة العربية، القاهرة، 2001.
- غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، طبعة 2015.
- **باللغة الأجنبية:**

[1]-Myriam Quéméner- Yves Charpenel - La Cybercriminalité Edition Economica- Paris- France - 2010-p 08.

[2]- Jean Michel Bruguière Le Droit de l'internetloiscontrat et usage Edition Litec- Paris - France 2009-p 217.

ثالثا: الأطروحات والرسائل الجامعية:

أ- أطروحة الدكتورة:

- أومدور نجاة خصوصية التحقيق في مواجهة الجرائم المعلوماتية. رسالة دكتوراه في القانون الخاص، كلية الحقوق جامعة محمد البشير الإبراهيمي، برج بوعريرج، سنة2021.
- براهيمي صالح، الإثبات بشهادة الشهود في القانون الجزائري (دراسة مقارنة في المواد المدنية والجنائية)، رسالة الدكتورة في العلوم، كلية الحقوق جامعة تيزي وزو، 2012.
- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة الدكتورة في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، سنة 2015 -2016.

– عبد الله بن سعود بن محمد السراني، فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة مقدمة لنيل شهادة الدكتورة، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية.

– عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد تلمسان الجزائر، 2018.

– تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته، رسالة مقدمة لأجل نيل شهادة الدكتورة، قسم العلوم الشرطية جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009.

ب– رسائل الماجستير:

– حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، الجزائر، 2012 .

– محمد الفاتح حمدي، استخدامات تكنولوجيا الإعلام والاتصال الحديثة وانعكاساتها على قيم الشباب الجامعي، مذكرة ماجستير، كلية العلوم الاجتماعية والعلوم الإسلامية، جامعة الحاج محمد الخضر، باتنة 2008–2009.

– يوسف صغير، الجرائم المرتكبة عبر الإنترنيت، رسالة لنيل الماجيستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر،2013.

– سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق، جامعة بوبكر بلقايد تلمسان، الجزائر 2010.

ج– مذكرات ماستر:

– بوشعرة أمينة، موساوي سهام، الإطار القانوني للجريمة الإلكترونية – دراسة مقارنة، مذكرة لنيل شهادة ماستر في الحقوق تخصص قانون خاص وعلوم جنائية، كلية الحقوق والعلوم سياسة بجاية، الجزائر، 2018 – 2017 .

– جزار منصورية، الجريمة المعلوماتية، مذكرة لنيل شهادة الماستر، كلية الحقوق و العلوم السياسية جامعة عبد الحميد بن باديس مستغانم، 2016 .

– محمد الدايج الجريمة الإلكترونية في التشريع الجنائي الجزائري مذكرة لنيل شهادة الماستر مجامعة مستغانم 2016.

– فلاح عائشة، خصوصية الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر كلية الحقوق و العلوم السياسية جامعة عبد الحميد بن باديس، مستغانم 2016.

– صنور عبد القادر، الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، جامعة مستغانم، 2017.

رابعا: المقالات و المداخلات:

- الأمنة أمحمدي بوزينة إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية الأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة، 29 مارس 2017.
- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني، مجلة مصداقية، المجلد 1، العدد 1، سنة 2019.
- دمان ذبيح عماد بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مجلة الحقوق والعلوم السياسية، العدد 13 /01/ 2020.
- الهاشمي كسراوي، الجريمة المعلوماتية، مجلة القضاء والتشريع، العدد 07، مركز الدراسات القضائية، تونس.
- يوسف مسعودي، النظام القانوني لحماية المصنفات الرقمية، مقالة علمية، مجلة الدراسات القانونية، العدد 04، أوت 2009، مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية، الجزائر.
- مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، سنة 2021.
- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، الجزائر، 2013.
- سمير بارة، الأمن السيبراني Cyper Security في الجزائر، السياسات والمؤسسات المجلة الجزائرية للأمن الإنساني، جويلية 2017.
- سفيان حديدان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الثامن، المجلد الثاني، 11 نوفمبر 2017.
- سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، العدد 01، 09 جوان 2021.
- سميحة بلقاسم، حميد بوشوشة، مجلة العلوم الانسانية لجامعة أم البواقي، المجلد 10، العدد 01، جوان 2023.
- عبد القادر دوحة، محمد بن حاج الطاهر، مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكترونية، الملتقى الوطني الأول، النظام القانوني للمجتمع الإلكتروني، المركز الجامعي خميس مليانة، معهد العلوم القانونية، والإدارية، 09-10-11 مارس 2008.
- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، ليبيا، أكتوبر 2009.

– فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، ضمن أعمال المؤتمر الدولي الرابع عشر حول الجريمة الإلكترونية، طرابلس، مركز جيل للبحث العلمي، سنة 2017.

– صالحة العمري، جريمة غسل الأموال وطرق مكافحتها، مجلة الإجتهاد القضائي، العدد الخامس، مخبر اثر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة.

– رضية بركايل، التنظيم القانوني الجزائري للجريمة المعلوماتية في التشريع الجزائري، الملتقى الوطني حول الأمن المعلوماتي مهدداته وسبل حمايته، جامعة مولود معمري، تيزي وزو، الجزائر، 03-04 نوفمبر 2015.

– خثير مسعود الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات دار الهدى عين مليلة، الجزائر، سنة 2010.

– خالد حامد مصطفى المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الإجتماعي، مجلة رؤى إستراتيجية، يصدرها مركز الإمارات للبحوث والدراسات الإستراتيجية، المجلد الأول، العدد 02، مارس 2013.

– غنام محمد غنام، الحماية الجنائية لبطاقة الإئتمان الممغنطة، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية دبي، الإمارات، 2003.

خامسا: المواقع الإلكترونية:

الموقع الرسمي لوزارة الدفاع الوطني www.mdn.dz

الموقع الرسمي للشرطة الجزائرية www.algeriepolice.dz

فهـــرس الموضـــوعـــات

الفهـــــرس

ملخص:

ظهرت الجريمة المعلوماتية نتيجة تطور تكنولوجيا المعلومات والاتصال وما أفرزته الثورة الرقمية المعلوماتية، اذ انتقلت من مفهومها الضيق المتعلق بجرائم الحاسوب، إلى الجرائم المتعلقة بالمعالجة الآلية للمعطيات، وهذا باعتبار الحاسوب بيئة لارتكابها، أو وسيلة لتنفيذها، أو أن يكون هدفا لها في البيئة الافتراضية الالكترونية التي تمخض عنها جرائم مستحدثة القاسم المشترك بينها استعمال التقنية والمعلوماتية على غرار جرائم الاعتداء على المال المعلوماتي.

و مما لاشك فيه أن هذه الجرائم تختلف في مضمونها وجوهرها، فكل جريمة تعكس طابعها ووسائلها وأساليبها الخاصة، حيث تأخذ صورا عديدة تتفاوت وفق نوعها، نوع/ المستهدف – الجاني ومستوى تنفيذه.

وتتعد أنماط الإجرام المعلوماتي، وسمات المجرم والفعل الإجرامي، مبرزة بذلك فجوة التباين بين ملامح الواقع المادي للفعل الإجرامي التقليدي، والواقع الافتراضي للفعل الإجرامي الرقمي المستحدث.

و الجزائر كغيرها من دول العالم تشهد نموا متزايدا في نسب الإجرام المعلوماتي وهذا ما تبينه الإحصاءات المسجلة، والتي تعكس واقع الإجرام المعلوماتي وعلاقته بالفضاء الرقمي الذي يفرض بذاته أبعادا وتحديات جديدة ومتداخلة على مستويات عدة.

الكلمات المفتاحية: الجريمة المعلوماتية – المجرم المعلوماتي – المال المعلوماتي.

Summary:

Information crime emerged as a result of the development of information and communication technology and the digital information revolution. It evolved from the narrow concept related to computer crimes to crimes associated with the automated processing of data. This is considering that computers serve as an environment for committing these crimes, a means for executing them, or a target in the virtual electronic environment that gave rise to new crimes. The common denominator among these crimes is the use of technology and information, such as crimes involving the violation of informational property.

Undoubtedly, these crimes differ in their content and essence. Each crime reflects its own nature, methods, and unique approaches. They take on various forms depending on their type, the target, the perpetrator, and the level of execution.

The patterns of information crime, the characteristics of the criminal, and the criminal act itself vary, highlighting the gap between the features of the physical reality of traditional criminal acts and the virtual reality of newly developed digital criminal acts.

Algeria, like other countries around the world, is witnessing an increasing growth in the rates of information crime, as evidenced by recorded statistics. These statistics reflect the reality of information crime and its relationship with the digital space, which imposes new and intertwined dimensions and challenges at multiple levels.

Keywords: Cybercrime – Cybercriminal – Informational money.