

الجريمة الإلكترونية: دراسة في المفهوم والمظاهر

Cybercrime: a study of the concept and manifestations

1- وهيبة سالمي

جامعة الجلفة

hibasalmi63@gmail.com

الملخص باللغة العربية:

للنظام المعلوماتي أهمية كبيرة باعتباره تقنية حديثة في عالم تكنولوجيا المعلومات ، إلا أنه غالباً ما يكون مصدر خصب للجرائم التي تقع عليه و بواسطته، و بذلك تعد الجرائم الإلكترونية جرائم خطيرة و سريعة و متطورة و في تزايد مستمر تبعاً لازدياد استخدام تلك التقنية و هذا ما دفع بالعديد من الدول إلى مواكبة هذا التطور التكنولوجي بوضع النصوص الملزمة لمختلف استعمالات الإعلام الآلي .

الكلمات المفتاحية: الجريمة الإلكترونية، الأمن الإلكتروني، المجرم المعلوماتي، التهديدات السيبرانية؛ الجريمة السيبرانية

Abstract:

The information system is of great importance as a modern technology in the world of information technology, but it is often a fertile source for the crimes that occur on it and through it, and thus electronic crimes are serious, fast, sophisticated and constantly increasing according to the increased use of that technology and this is what prompted country. From countries to keep pace with this technological development by developing appropriate texts for various industries

Keywords: cyber crime, cyber security, cyber criminal, cyber threats; cyber crime

1. مقدمة:

نظرا للتطورات التكنولوجية التي شهدها العالم، واختراع الحاسوب، أصبح يستخدم في العديد من المجالات العملية والعملية التعليمية كالتحضير لبعض الدروس وتلقي المحاضرات والترفيه مروراً لاستخدامات متنوعة في مجالات أمنية ومالية، أصبح الحاسوب عرضة للتهديد والاختراق من أفراد وتنظيمات ودول في استعمالات غير قانونية تهدف للحصول على أموال أو معلومات أمنية حساسة بطرق غير قانونية وعلى قدر عال من الذكاء والتمرس والحنكة، وهنا ظهر ما يعرف بمفهوم الجرائم الإلكترونية فهي ظاهرة إجرامية مستجدة نسبياً تفرع في جنباتها أجراس الخطر لتنبه العصر الراهن لحجم المخاطر و هول الخسائر الناجمة عنها والتي تستهدف البيانات والمعلومات بطرق غير مشروعة الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال ونظراً لحدثة هذه الجريمة فقد اختلف الفقهاء في وضع تعريف موحد لها فهي تختلف عن الجريمة التقليدية من حيث خصائصها التي تميزها عن نظيرتها وطرق استعمالها ودوافعها كما أن المجرم الإلكتروني يختلف عن المجرم العادي وكذلك أنواعها، فهي تتعدد وتأخذ أنواعاً مختلفة كالجرائم ضد الأفراد والجرائم ضد الملكية بالاعتداء والتدمير لمختلف البرامج إضافة للجرائم ضد الدول والحكومات والتي تعمل على مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت وغالباً ما يكون هدفها سياسي بحت.

ولعل أهم أهداف الجريمة الإلكترونية هو الوصول إلى المعلومات والحصول على المال بهذه الطرق أسهل ومن دون بذل أي جهد.

وعلى هذا يثار التساؤل حول ماهية الجريمة الإلكترونية؟ وما هي مظاهرها؟

وللإجابة عن هذا الإشكالية نقترح الخطة التالية:

المبحث الأول: ماهية الجريمة الإلكترونية.

المبحث الثاني: مظاهر الجريمة الإلكترونية.

المبحث الأول: ماهية الجريمة الإلكترونية

الجريمة الإلكترونية حديثاً، لتحدث تغيراً ونقلة هائلة في سرعة تنفيذها فلقد عرفت تطوراً ملحوظاً باستخدام عرف العالم آخر ما توصلت إليه العلوم التقنية والتكنولوجية من اختراعات علمية هائلة كظهور الحاسوب الإلكتروني ووجود ما يعرف بالانترنت التي صارت الفضاء الأكثر استقطاباً لهذا النوع من الجرائم، ولكن الإحاطة بمفهوم الجريمة الإلكترونية الدقيق لا يزال محل خلاف فقهي، فهي ظاهرة إجرامية مستحدثة عن الجريمة التقليدية وتختلف عنها من حيث المفهوم والخصائص وعليه سيتم تقسيم هذا المبحث إلى مطلبين:

-المطلب الأول: مدلول الجريمة الإلكترونية

- المطلب الثاني: أركان الجريمة الإلكترونية

المطلب الأول: مدلول الجريمة الإلكترونية

إن مسألة وضع تعريف لأي مفهوم و ضبطه صار من الصعوبة لتعدد المدارس و المناهج و السياقات التي برزت فيها الظاهرة وهو ما يخص الجريمة الالكترونية و التي تحوي مقطعين هما الجريمة و الالكترونية، فإذا كانت الجريمة هي تلك السلوكيات و الأفعال الخارجة عن القانون فان المصطلح الثاني جاء لوصف فكرة إن يتم استعمالها من طرف الحاسب ولكن لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الالكترونية فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات و الاتصال، جرائم الكمبيوتر و الانترنت، الجرائم المستحدثة¹، الغش المعلوماتي، الجرائم السيبرانية فلقد انقسم الفقهاء إلى اتجاهين في تعريف الجريمة الالكترونية الاتجاه الضيق و الاتجاه الواسع كما أن لها أركان فالجريمة لا تقوم إلا بتوفرها وهذا ما سأتناوله في الفرعين المواليين

الفرع الأول: تعريف الجريمة الالكترونية :

لم يكن تحديد مفهوم للجريمة الالكترونية في متناول المختصين وهذا للاختلاف في وضع إطار موحد يضبط الظاهرة و يجد لها تفسيراً في ظل اختلاف المدارس و تنوع الخصوصيات، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق و البعض الآخر بنظر إليها بالمفهوم الواسع و سأحاول التطرق لذلك في البندين المواليين

البند الأول: الاتجاه الضيق من تعريف الجريمة الالكترونية :

عرف أنصار الاتجاه الضيق الجريمة الالكترونية بأنها "كل فعل غير مشروع، يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، لملاحقة تحقيقه من ناحية أخرى"² ومن بين التعريفات أيضاً تعريف الفقيه MERWE الجريمة المعلوماتية هي "الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية"³ فيما ذهب الفقيه ROSBLAT على أنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تغييرها أو حذفها أو التي تحولت عن طريقه"⁴ كما عرفها كل من A.HARD، TOTT، COSTER بأنها "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض العمليات الفعلية داخل الحاسوب" و بمعنى آخر هي "تلك الجرائم التي يكون للحاسب الآلي فيها دوراً ايجابياً أكثر من سلبية"⁵

إن التعريفات السابقة جاءت قاصرة على الإحاطة بأوجه ظاهرة الإجرام الالكتروني فبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة و البعض الآخر على وسيلة ارتكابها و آخرون على معيار النتيجة

¹ عادل يوسف عبد النبي شكري، بحث بعنوان الجريمة المعلوماتية و أزمة الشرعية الجزائية، جامعة الكوفة، 2008، ص 112

² حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، 2011_2012، ص 13

³ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الإسكندرية مصر، ص 153

⁴ طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 154

⁵ أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية مصر، ص 30

البند الثاني : الاتجاه الموسع من تعريف الجريمة الإلكترونية :

على عكس الاتجاه السابق يرى أنصار هذا الاتجاه ضرورة التوسيع من مفهوم الجريمة الإلكترونية ،فالبعض يرى إن هذه الجريمة هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب ،نظاما حاسوبيا أو أو شبكة حاسوبية للوصول إلى البيانات و البرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها و جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة⁶

أما البعض الآخر يغرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسب الآلي الرقمي و شبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف⁷ ، وفي تقرير الجرائم المتعلقة بالحاسوب اقر المجلس الأوروبي بقيام الجريمة في كل حالة يتم فيها تغير معطيات أو بيانات أو برامج أو محوها أو كتابتها أو أي تدخل آخر في مجال انجاز البيانات أو معالجتها و تبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر⁸

ومن خلال هذه التعاريف يتضح صعوبة الأخذ بهذا الاتجاه لان أنصاره يتجهون إلى أن الجرائم الإلكترونية هي تلك التي يكون محلها الحاسب الآلي فقد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب الآلي نفسه على سبيل المثال و من ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة كما انه يمكن أن ترتكب جريمة و يستعمل الحاسب الآلي ولا نكون أمام جريمة الكترونية كمن يقوم بالاتصال بواسطة الحاسب الآلي بشركائه في جريمة السطو على بنك

و بخصوص التعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و عرفها بموجب أحكام المادة 02 من القانون رقم 04-09 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"⁹ أي أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في تعديل قانون العقوبات بموجب قانون رقم 04-15 و المتمم للأمر 66-156 من المادة 394 مكرر إلى 394 مكرر 7 و ترك مجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو

⁶ كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 21-23 تشرين الأول ، بدون صفحة

⁷ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود

معمر يزي وزو، 06-03-2013، ص 09 نقلا عن كحلو علي ، جرائم الحاسوب وأساليب مواجهتها ، مجلة صادرة عن مديرية الأمن

الوطني، العدد 84، 2007، ص 51

⁸ مليكة عطوي ،...

⁹ القانون رقم 04-09 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و

مكافحتها الجريمة الرسمية العدد 47

نظام للاتصالات الإلكترونية مما يجعل هذا التعريف يشمل عدد هائل من الجرائم، ومن أمثلة عن الجريمة الإلكترونية في الجزائر تسرب أسئلة البكالوريا سنة 2016 ، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية¹⁰

الفرع الثاني : خصائص الجريمة المعلوماتية:

إن التقدم الكبير في مجال المعلوماتية يسر حياة الإنسان ووفر عليه جهد كبير و طبع شتى معاملاته بالسرعة الفائقة ولكن بالمقابل فقد ارتبط استعمال هذه الوسائل الحديثة بظهور جرائم جديدة وزيادة حدة بعض الجرائم فهذه التقنية أوجدت ألوانا جديدة من الجرائم وأسبغت عليها خصائص ميزتها عن الجرائم سواء تعلقت هذه الخصائص بالشخص الذي يقدم على هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت بالجريمة ذاتها وصعوبة اكتشافها أو ثباتها أو تعلق الأمر بالنطاق المكاني لهذه الجريمة

أولا : جريمة عابرة للحدود الوطنية

بعد ظهور شبكات المعلومات لم يعد هناك حدود تقف أمام نقل المعلومات فلقد أصبح من السهل إمكانية ربط عدد هائل لا حصر له من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر نقل كميات كبيرة من المعلومات و تبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية إذ غالبا ما يكون الجاني في بلد والمجني عليه في آخر كما قد يكون الضرر المتحصل في بلد آخر ثالث في الوقت نفسه

و عليه تتخذ جرائم الإلكترونية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية¹¹ ونتج عن هذه الخاصية العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة و كذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية¹² وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود الوطنية بشكل عام

ثانيا : صعوبة إثبات واكتشاف الجريمة الإلكترونية

من المفترض إن اكتشاف الجرائم يتم عن طريق الفحص والتدقيق أو عن طريق الشكاوى التي يقدمها المجني عليهم إلا إن إثبات الجريمة الإلكترونية يحيط بها الكثير من الصعوبات و التي تتمثل في إن جهات التحقيق لم تصل إلى المعرفة الواسعة والإحاطة الكاملة بهذه التكنولوجيا الحديثة و صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا فالجريمة الإلكترونية لا عنف فيها كالسرقة مثلا وإنما هي أرقام و بيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لديها أي اثر خارجي مرئي¹³ و أيضا الضحية في هذه الجرائم تمتنع في الغالب عن التبليغ عنها

¹⁰ جازيه سليمان، موقع العربي الجديد ، تاريخ الدخول 10-08-2020 الساعة 15:55

¹¹ أسامة احمد المناعة، جلال محمد الأزعي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار الثقافة للنشر والتوزيع ، 2014

ص93

¹² د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادي، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003، ص49

¹³ سيئاء عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية، الندوة الإقليمية حول

الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المملكة المغربية، 2007، ص52

لهذا لا نعجب إذا وجدنا إن أكثر هذه الجرائم لم تكتشف إلا بمحض الصدفة وهناك من يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته 01% فقط و ما تم الإبلاغ عنه إلى السلطات المختصة لم يتعدى 15% من النسبة السابقة و حتى ما طرح أمام القضاء من هذه الجرائم فان الأدلة فيه لم تكن كافية إلا في حدود الخمس¹⁴

ثالثا : خصوصية مرتكب الجرائم الإلكترونية

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يرتكب جرائم تقليدية ، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها فان الأمر يختلف بالنسبة للجرائم الإلكترونية فهي جرائم فنية تقنية في الغالب و الأشخاص الذين يقومون بارتكابها عادة يكونوا من ذوي الاختصاص في مجال تقنية المعلومات الإلكترونية

أوعلى الأقل شخص لديه حد أدنى من المعرفة القدرة على استعمال جهاز الحاسوب و التعامل مع شبكة الانترنت كما إن الباعث إلى ارتكاب المجرم لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي ، فقد يرتبط الدافع بحب التعلم و الاستكشاف، كما قد بالسياسة و الايدولوجيا.... إلى غير ذلك من الدوافع كما يتميز مجرم المعطيات بفئاته و أنماطه المختلفة و هو نوعين رئيسيين :

الأول هم الهواة المولعون بالمعلوماتية، و الثاني محترفو الجرائم الإلكترونية و أساس التمييز بين النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة ، بينما هو ساذج لدى النوع الأول لا يتعدى الرغبة في الاستطلاع و الاستكشاف، أما النوع الثاني فهو خبيث قد يكون دافع مالي أو سياسي أو غيره¹⁵

رابعا : الجرائم الإلكترونية فادحة الأضرار

إن الاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال في شتى المجالات ضاعف من الأضرار و الخسائر التي تخلفها الاعتداءات على معطيات هذا الحاسب، لا سيما إذا كانت تمثل قيما مالية، خاصة مع ازدياد اعتماد البنوك و المؤسسات المالية و مختلف الشركات على الحاسب الآلي في تسيرها و في هذا الخصوص تشير الدراسات إلى أن الأضرار الناجمة عن الجرائم الإلكترونية تفوق بكثير تلك الناجمة عن الجرائم التقليدية¹⁶ ففي الولايات المتحدة الأمريكية و حسب مكتب التحقيقات الفيدرالي (FBI) فالجريمة الإلكترونية تكلف خسائر تقدر بمائة و خمسين 150 ضعف ما تكلفه الجريمة العادية ، و ان الخسائر الناجمة عن 139 عملية غش معلوماتي وقع على البنوك بلغت ثمانمائة ألف دولار (\$800000) عام 1981 كما أن الغش المعلوماتي كان السبب في حدوث خمسين 50 حالة إفلاس في ثلاثمائة و أربعة و خمسين 354 بنكا بين شهري جانفي 1985 و جوان 1987

¹⁴ د.سعيد عبد الطيف حسن، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة

1999، ص95

¹⁵ د. عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الطبعة الثانية، القاهرة، 2002، ص36

¹⁶ Philip rose , la criminalité informatique edition dahlab imprimerie.alger pp 22-30

و في دراسة للمركز الوطني للجرائم الكمبيوتر والبيانات قدرت خسائر الجرائم المعلوماتية بين ثلاث (03) وخمس (05) مليارات دولار أمريكي وفي المملكة المتحدة أجرت لجنة المراجعة المحاسبية دراسة خلال عدة سنوات تبين منها أن خسائر 64 حالة عام 1984 قدرت ب 1133487 جنمها استراليا وفي الجزائر فقد سجلت فرق مكافحة الجرائم الالكترونية التابعة للمديرية العامة للأمن الوطني 4210 جريمة الالكترونية خلال سنة 2019 فلقد شهدت ارتفاع محسوس و ذلك بالتزامن مع بداية الحراك الشعبي في الجزائر¹⁷

خامسا : الجريمة الالكترونية جاذبة للمجرمين

إذا كانت بعض الجرائم التقنية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها فان الجرائم الالكترونية لا تحتاج إلى مثل تلك القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك و الجاني في سبيل تنفيذها لا يحتاج من الوقت سوى ثواني او دقائق و لا يحتاج من القوة العضلية غير تحريك الأنامل من على وسائل الإدخال و قد يتسبب بذلك في حصول خسائر فادحة رغم إن جريمته قد لا ترى بالعين

ونعومة هذه الجريمة وما تدره من أرباح و من إشباع للفضول عند البعض جعلها من الجرائم الجاذبة للمجرمين¹⁸.

المطلب الثاني : أركان الجريمة الالكترونية

لكي يكمن القول بوجود جريمة ما ، فان المشرع يتطلب كأصل عام ضرورة وجود أركان وبغير هذه الأركان لا يمكن القول بوجود جريمة و تتمثل هذه الأركان في الركن الشرعي الذي يتمثل في النصوص القانونية التي تجرم الفعل و الركن المادي و الذي يتمثل في السلوك الإجرامي و العلاقة السببية و كذلك النتيجة أما الركن الثالث فهو الركن المعنوي الذي يتجسد في القصد الجنائي للجريمة الالكترونية

الفرع الأول : الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع الفعل ، يبنى على ذلك عدم جواز ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم وعن فعل ارتكبه بعد إلغاء نص التجريم ، كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها و على القضاة التقيد بمدلول النص و الالتزام بمعانيته¹⁹

لذا ينتج عن مبدأ الشرعية قاعدة هامة وهي عدم رجعية القانون الجنائي و هذا عملا بما نصت عليه المادة 01 من قانون العقوبات و التي قضت "لا جريمة و لا عقوبة أو تدبير امني بغير قانون"²⁰ ، المشرع

¹⁷ منيرة ابتسام طرابلسي، تسجيل 4210 جريمة سيبرانية خلال 2019، موقع المحور اليومي ، 05-02-2020

¹⁸ أسامة احمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواشة، جرائم الحاسب الآلي و الانترنت ، دراسة تحليلية مقارنة، دار وائل

لنشر، عمان الأردن ، الطبعة الأولى، 2001، ص107

¹⁹ اسامة احمد المناعسة ، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار الثقافة للنشر و

التوزيع، عمان، 2014، ص93

²⁰ الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات ، جريدة الرسمية ، عدد 44

الجزائري استحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم البيانات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات²¹

الفرع الثاني : الركن المادي

الركن المادي هو ما يعرف بالسلوك الإجرامي الذي يستوجب القانون كمناط للعقاب على هذه الجريمة على أن يتحقق الضرر للسلوك الإجرامي كشرط لازم لتوقيع العقاب عليه من طرف المشرع و يستوجب وجود علاقة سببية بين هذا السلوك و النتيجة (الضرر)

أولا : السلوك الإجرامي

يتمثل السلوك الإجرامي للجريمة الإلكترونية في السلوك الخارجي الذي يقوم به المجرم الإلكتروني، وهو كل فعل مادي يسبب ضرر سواء اتجهت نيته إلى حصول هذا الضرر أم لم تكن ، وهذا السلوك المادي يجعل هذه الجريمة بواسطة الانترنت ذات ميزة و خاصية موحدة تباشر من حيث النشاط المادي فيها ، بحيث طور هذا السلوك عقلية الفاعل الذكية و التي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة²²

بالتالي فان ارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني بعدمه لا يستطيع الشخص حتى الاتصال بشبكة الانترنت ، و تظهر القيمة الموحدة في ضرورة النشاط التقني و إلا فقدت الجريمة أساسياتها

ثانيا : النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الذي قد يحدث أي التغير الذي يحصل في المحور الخارجي كنتيجة للسلوك الإجرامي الذي يقيم عليه المشرع أحكاما قانونية ، فالنتيجة الضارة لها مفهومان أولهما المفهوم المادي و ثانيهما المفهوم القانوني ، فالمدلول المادي يعني المخلفات التي أحدثتها الجريمة في المحور الخارجي و يوقع القانون على حدوثها عقوبة²³

و يجب أن يكون للجريمة طبيعة مادية ملموسة في المحيط الخارجي لتتم المعاقبة عليها ، و لكن توجد بعض الجرائم التي ليس لها نتيجة و تعرف بالجرائم السلبية

و من هذا المنبر بدت أهمية الاعتراف بالمدلول أو المعنى القانوني للنتيجة دون الأخذ بعين الاعتبار

حصول الضرر أولا . فمجرد الإخلال بهذه المصلحة ينتج قيام حصول الجريمة من الجهة القانونية

و يطرح موضوع النتيجة الجرمية في جرائم الانترنت مشاكل عديدة ، مثلا مكان و زمان تحقق النتيجة ،

فلو قام احد المجرمين في فرنسا باختراق جهاز خادم Server احد بنوك أمريكا، وهذا الخادم يتواجد في

إيطاليا ، فكيف يمكن العلم بوقت الجريمة

²¹ عاقل فيضيلة، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة أقيمت في أشغال المؤتمر الدولي حول الجرائم

الإلكترونية، الاتحاد العالمي للمؤسسات العلمية، طرابلس، لبنان، 24-25 مارس 2017، ص120

²² اسامة احمد المناعسة، جلال محمد الزعبي ، المرجع السابق ، ص53-55

²³ حنان ربحان مبارك المضحكي، الجرائم المعلوماتية ، دراسة مقارنة ، الطبعة الأولى، منشورات الحلبي الحقوقية ، بيروت، 2014، ص87 88

فهو هو توقيت بلد المجرم أم توقيت جهاز الخادم في إيطاليا ، و تطرح أيضا إشكاليات و صعوبات في القانون الواجب التطبيق في هذا الأمر لأن هناك أبعاد عالمية في هذا النطاق²⁴

ثالثا: العلاقة السببية

تتمثل العلاقة العلاقة السببية في الصلة التي تربط بين الفعل و النتيجة و تثبت إن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة و أهمية الرابطة السببية ترجع إلى إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة ولا بد من تواجد العلاقة أو الرابط السببية في كافة الجرائم العمدية و لكن يجدر الإشارة انه في بعض الأوضاع قد يحصل النشاط الإجرامي و لكن لا تتحقق النتيجة ، بالتالي نكون أمام حالة من حالات الشروع في السلوك الجرمي فقط لكن يواجهنا أشكال في الجانب السيبراني عند محاولة وصل النشاط الجرمي بالنتيجة الضارة التي حدثت بسببه 'نتيجة لصفة هذه الجرائم و طبيعتها المعقدة و الصعبة ، فمن أن تتولد عدة أضرار من نشاط جرمي واحد²⁵

الفرع الثالث : الركن المعنوي

لا يقتصر قيام المسؤولية الجنائية من الجهة القانونية أن يصدر من الشخص الجاني نشاط إجرامي ذو طابع مادي فقط وإنما يستلزم زيادة على ذلك توافر الركن المعنوي فهو يعتبر جوهر المسؤولية الجنائية عندما يعتبر الركن المادي مظهرها الخارجي

فيستلزم وجود رابطة أو علاقة سببية بين النشاط الإجرامي و إرادة الجاني المنطلقة إلى جعل النتيجة الغير المشروعة كبصمة للسلوك الإجرامي. و هو الخطأ العمدي فيتطلب أن يدرك المجرم انه يفعل نشاط غير مشروع. و أيضا أن تكون له الحرية المطلقة في الاختيار للقيام بهذا الفعل الإجرامي ، أما الإهمال و الرعونة فينتجان الخطأ الغير العمدي فهو لا يشترط من المجرم توافر الإرادة²⁶ بالتالي الركن المعنوي هو الاتجاه الذهني أو النفسي للجاني انه يمثل أساس القانون الجنائي ففي حيزه تتوافر كامل أساسيات المسؤولية الجنائية ، فالرابطة التي تصل بين شخصية الجاني و ماديات الجريمة هي محل الجرم في مفهوم استحقاق العقاب.

و تجدر الإشارة أن القصد الجنائي في الجرائم العمدية قد يكون قصدا عاما أو خاصا فالأول يقوم باتجاه إرادة المجرم للقيام بالسلوك الإجرامي مع توافر علمه بكامل عناصر الجريمة أما الثاني إلا و هو القصد الجنائي الخاص ، فيتحقق بالحالة أو الوضعية النفسية الشخصية المرتبطة بالنتيجة الضارة أو الدافع و ليست متعلقة بالسلوك المادي المكون للمجرم²⁷

هذا في الجرائم العمدية ، أما الغير عمدية فهي بغير قصد أو واقعة عن طريق الخطأ، سواء لم يكن في حسابان الفاعل نتيجة سلوكه أو عدم سلوكه ، وكان في مقدوره أو من واجبه حصولها و يكون الخطأ أما

²⁴ عماد مجدي عبد المالك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر 2001، ص 37

²⁵ حنان ربحان مبارك المضحكي، المرجع السابق ص 90

²⁶ المرجع نفسه ، ص 91

²⁷ محمد زكي ابو عامر، الإجراءات الجنائية ، الطبعة السابعة ، دار الجامعة الجديدة ، مصر 2002، ص 205

عاما أو خاصا ، ويقوم الأول بواقعة الإخلال بالقواعد العامة التي تكتسب من خبرة الإنسان العامة، أما الخطأ الخاص فهو الذي يحصل نتيجة لمخالفة القواعد المأخوذة من الشرائع و الأنظمة ، فيقوم هذا الخطأ بمخالفة قواعد قانونية ملزمة²⁸

و بخصوص الركن المعنوي في الجريمة الإلكترونية هو نفسه الركن المعنوي في جميع الجرائم التي تقتضي وجود قصد جنائي عام و خاص فالأول يكون موجودا أو محققا في جميع الجرائم التي الإلكترونية ، إلا أن القصد الخاص قد يتحقق في بعض الجرائم دون الأخرى ، لكن هذا لا يعني عدم وجوده في الجرائم الإلكترونية مثلا في جريمة تشويه السمعة عبر الانترنت ، فهذه الأخيرة تقتضي وجود قصد خاص . أما جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية ، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد العام و الخاص فالمجرم يعلم انه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير ، أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع²⁹

المبحث الثاني : مظاهر الجريمة الإلكترونية

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي اخطر الجرائم و إلى جنحة وهي متوسطة الخطورة ثم مخالفة وهي اقل خطورة و تصنف بحسب طبيعتها إلى جريمة عادية و جريمة سياسية ، عسكرية و أخرى إرهابية³⁰ ، علا خلاف هذه الجريمة فان الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها و أنواعها وذلك بسبب الاختلاف في تسميتها

فالبعض يصفها حسب الأسلوب المتبع في الجريمة و البعض الآخر يستند إلى دوافع ارتكابها ، إما بالنسبة للمشرع الجزائري فقد قسمها إلى جرائم مرتكبة بواسطة النظام المعلوماتي و نص عليها المشرع و لم يحددها وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام و الاتصال إما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات و عليه سيتم تقسيم هذا المبحث الى مطلبين :

المطلب الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

المطلب الثاني : الجرائم الواقعة على النظام المعلوماتي

المطلب الأول : الجرائم الواقعة بواسطة النظام المعلوماتي

يعد هنا النظام المعلوماتي هو أداة و وسيلة تنفيذ الجرائم ، فيعد الحاسب في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفة جسامتها و يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية وهي التي سوف نتطرق إليها في هذا المطلب

²⁸ حنان ربحان مبارك المضحكي، المرجع السابق ص 93-94-95

²⁹ احمد خليفة الملط ، مرجع سابق ، ص 120-121

³⁰ احسن بوسقيعة ، الوجيز في القانون الجزائري العام، الديوان الوطني للأشغال التربوية، 2002، الطبعة الأولى ص24

الجريمة الواقعة على الأشخاص (الفرع الأول) الجريمة الواقعة على الأموال (الفرع الثاني) الجريمة الواقعة على أمن الدولة (الفرع الثالث)

الفرع الأول : الجرائم الواقعة على الأشخاص

رغم تطور الحياة اليومية للأفراد و المجتمع بفضل استعمالهم للفضاء الافتراضي، إلا أنه أصبح سلاحاً فتاكاً في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص وعليه ظهرت عدة أنواع خاصة من الجرائم الإلكترونية الواقعة على الأشخاص و من بينها

أولاً : الجرائم الإلكترونية الواقعة على حرمة الحياة الخاصة للأشخاص

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للأشخاص و عدم الاعتداء على هذه الحرمة، و من بين هذه الجرائم

(1) جريمة التهديد : التهديد هو ذلك الفعل الذي يقوم به الشخص أو الذي ينذر آخر بخطر يريد إيقاعه بشخصه أو ماله أو هو الإعلان عن شريد إلقاءه بشخص معين و من شأن ذلك أن يسبب له ضرر أو قد يكون ذلك بمحرر موقع عليه أو بصور أو رموز أو شعارات و التهديد إما يكون مصحوباً بأمر أو شرط و قد يكون دون ذلك في بعض الأحيان و قد جرمه المشرع الجزائري في قانون العقوبات في المواد من 284 إلى 287 و من بين أنواعه التهديد و الابتزاز الإلكتروني و هو السعي من خلال وسائل التواصل الاجتماعي أو عن طريق البريد الإلكتروني بإرسال رسالة خاصة لترويع و التهديد³¹ أو للحصول على مكاسب مادية أو معنوية وذلك عن طريق تهديده بفضح أسرار أو معلوماته الخاصة مهما كانت وسيلة الحصول على هذه الأسرار و المعلومات ، ومهما كانت وسيلة التهديد و بغض النظر عن اثر التهديد في نفسية الضحية و بغض النظر عن سن الضحية ، ذكر أو أنثى و بغض النظر عن المطلوب من الضحية أكان القيام بعمل أو الامتناع عن عمل أو مال أو تكليف بأمر³².

(2) جريمة انتحال الشخصية

و المقصود بها استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته ، ولقد تميزت هذه الجريمة بسرعة الانتشار خاصة في الأوساط التجارية و تتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليبدل بمعلوماته الشخصية الكاملة كالاسم و العنوان الشخصي، رقم بطاقة الائتمان لتتمكن من الوصول لماله أو سمعته عن طريق الغش ، لقد نص قانون العقوبات الجزائري فيما يتعلق بجريمة انتحال صفة الغير و الاحتيال على الأشخاص في المادة 372 من قانون العقوبات

³¹ يوسف صغير، المرجع السابق، ص33

³² علاء رضوان، الجريمة و العقاب في واقع الابتزاز الإلكتروني، موقع اليوم السابع ، 10 فبراير 2020

كما يوجد جريمة انتحال شخصية احد المواقع ويتم ذلك عن طريق اختراق احد المواقع للسيطرة عليه ليقوم بتركيب برنامج خاص به هناك باسم الموقع المشهور³³.

(3) جرائم السب و القذف :

جرائم السب و القذف هي المساس بشرف الغير و سمعتهم و اعتبارهم و يكون ذلك كتابيا أو عن طريق المطبوعات أو الرسوم عبر البريد الإلكتروني أو الصوتي ، صفحات الويب بعبارات تمس الشرف ، فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية و قد يكون شخصا طبيعيا أو معنويا لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي شبكة الانترنت حيث جرمها المشرع الجزائري عندما أضاف المادة 144 مكرر في قانون العقوبات التي تجرم القذف و السبب المرتكبة بأية وسيلة معلوماتية أو إعلامية أو بأي وسيلة أخرى.

(4) المواقع الإباحية و الدعارة :

رغم الايجابيات التي قدمتها الانترنت للبشرية ، شكلت فرصة ملائمة لذوي النفوس الضعيفة و للمنظمات الإجرامية لتوظيفها في عمليات مختلفة ، ومن أهم الجرائم الإلكترونية الواقعة على الأشخاص صناعة و نشر الإباحة و الجنس سواء البالغين أو الأطفال خاصة بحيث إن أكبر صور الاستغلال الجنسي عبر شبكة الانترنت هي الاستغلال الجنسي للأطفال فهم يتعرضون لذلك بإشكال متعددة انطلاقا من الصور إلى التسجيلات المؤدية إلى للجرائم الجنسية العنيفة حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت³⁴ ، كما أن شبكة الانترنت توفر تسهيلا للدعارة عبر آلاف المواقع الإباحية و تسوق الدعارة و تستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

ثانيا : الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية :

يكون النظام المعلوماتي وسيلة الاعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات و تخزين و استخدام هذه المعلومات دون إذن صاحبها، لان استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع

و قد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية و هي الأمر رقم 03-05 الصادر في 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة، و الأمر 03-07 الصادر في 2003 المتعلق براءات الاختراع³⁵

³³ محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي ، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم

الأمنية ، الرياض، 2003، ص55

³⁴ كرسا سكولمان ، عن جرائم الانترنت طبيعتها و خصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19-20

يونيو 2007، ص40

³⁵ سوير سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الاجرام، كلية الحقوق، جامعة أبو بكر

بلقيد، تلمسان الجزائر، 2010، ص39

الفرع الثاني : الجرائم الواقعة على الأموال :

لقد صاحب تطور شبكة الانترنت تطور وسائل الدفع و الوفاء و أصبحت جزء لا يتجزأ من المعاملات الالكترونية و في خضم هذا التداول المالي عبر الانترنت ظهرت عدة جرائم الكترونية على الأموال كالسطو و السرقة و التحويل الالكتروني غير المشروع للأموال و قرصنة أرقام البطاقات الممغنطة، حيث أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالطريقة الغير مشروعة عبر قنوات شبكة الانترنت³⁶ وسوف نتطرق إلى أهم الجرائم الالكترونية الواقعة على الأموال كالآتي:

أولاً: السرقة الواقعة على البنوك:

يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات و المعلومات الشخصية للمجني عليهم و استخدام شخصية الضحية ليقوم بعملية السرقة المتخفية ما يؤدي بالبنك إلى التحويل البنكي للمال الالكتروني أو المادي إلى الجاني حيث يستخدم الجاني الحاسب الآلي لدخول إلى شبكة الانترنت و الوصول إلى المصارف و البنوك و تحويل الأموال الخاصة بالعملات إلى حسابات أخرى³⁷

ثانياً: تجارة المخدرات عبر الانترنت :

من أهم الجرائم الالكترونية على الأموال نذكر جريمة المخدرات عبر الانترنت حيث تتخذ المواقع الالكترونية للترويج للمخدرات و تسويقها للناشئ لاستخدامها، وتعليمه كيفية صناعتها بكافة أصنافها و أنواعها³⁸ ، كما يروجون سلعتهم عبر رسوم الغرافيتي المنتشرة على جدران الشوارع كي يلفتوا انتباه الزبائن إلى حساباتهم الالكترونية³⁹ ، وظهر نوع آخر من المخدرات فلم يعد استهلاكها يقتصر على ما كان يجري سابقاً بحقنها أو مضغها أو تدخينها وإنما تطور الفكر الإنساني ليحول نظم التعاطي إلى تعاطي الكتروني و يتمثل ذلك في جلوس تاجر المواد المخدرة أمام جهاز الحاسب الآلي ليتلقى طلبات شراء للمواد المخدرة عبر موقعه الالكتروني و هنا يكون التسليم عن طريق إجراء المشتري لعملية تحميل المخدر الذي يرغبه في شكل ملفات و هو ما يعرف بالمخدرات الرقمية

و المخدرات الرقمية هي عبارة عن ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية⁴⁰ .

ثالثاً: غسيل الأموال :

³⁶ د.خالد ممدوح إبراهيم، امن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2001، ص76

³⁷ عباس أبو شامة ، التعريف بالظواهر الإجرامية المستحدثة حجمها أبعادها و نشاطها في الدول العربية ، الندوة العلمية للظواهر الإجرامية

المستحدثة و سبل مواجهتها ، تونس 29-30 جوان 1999 ، ص20

³⁸ محمد صالح الألفي، أنماط جرائم الانترنت ، متوفر على موقع www.eastlaws.com

³⁹ أنتوني كاثريسون ، مجرمو الانترنت الخفي يبيعون المخدرات عبر تطبيقات شائعة و كومبيوترات مسيطرة عليها ، موقع Independent عربية

16مارس 2019.

⁴⁰ د. أبو سريع احمد عبد الرحمن، بحث حول استخدام الانترنت في تعاطي المخدرات. المخدرات الرقمية ، وزارة الداخلية ، قطاع الشؤون

الفنية، الإدارة العامة للمعلومات و التوثيق، ديسمبر 2010، ص05

إن جريمة غسيل الأموال عبر شبكة الانترنت تختلف عن نظيرتها التي تتم عبر الوسائل و الطرق التقليدية ، إذ تتم الأولى عبر وسائل و طرق حديثة و جد متطورة عما كان معمول بيه في السابق فلقد استفادوا مجرمو غسيل الأموال عبر الانترنت بتوفير السرعة و تفادي الحدود الجغرافية و القوانين المعيقة لغسيل الأموال و كذلك لتشفير عملياتهم و سهولة نقل الأموال و استثمارها لإعطائها الصيغة الشرعية⁴¹ ولقد نصت عليها جل التشريعات من بينها التشريع الجزائري كما أعطى من خلال قانون الإجراءات الجزائية المعدل و المتمم بالقانون 07-17 بعض الصلاحيات و المهام للسلطات القضائية و الخاصة للتحري و التحقيق في جرائم غسيل الأموال و الكشف عنها و عن مرتكبها و ملاحقتهم بتوقيع العقاب طبقا لنصوص قانون العقوبات المعدل و المتمم بأمر رقم 02-16

رابعا : الاستعمال الغير شرعي للبطاقات الائتمانية :

شاع في الآونة الأخيرة استعمال بطاقات الائتمان الالكترونية ، باعتبارها وسيلة من وسائل الدفع الحديثة، و أداة مصرفية تقوم مقام النقود في الوفاء بالالتزامات القانونية مقبولة على نطاق واسع لدى الأفراد و التجار وذلك من اجل التيسير على الأفراد في معاملاتهم و من بين أنواع جرائم تكنولوجيا المعلومات نجد عمليات السطو على بطاقات الائتمان الالكترونية، هذه الأخيرة التي تعد احدث أنماط السلوك الإجرامي باعتبارها نقطة تلاقي بين الجريمة المعلوماتية و بطاقة الائتمان الالكترونية و تكون عن الاستيلاء أو سرقة أرقام البطاقات ثم بيع المعلومات للآخرين ، ومن خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال، وذلك بإيهامه بحصول ربح ، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله⁴² أو إساءة استخدام الغير لبطاقات الائتمان، كان يقوم السارق باستعمال البطاقة للحصول على السلع و الخدمات او سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام البطاقات المزورة⁴³

خامسا : قرصنة البرمجيات :

هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات و بيعها للناس بسعر اقل ، و جريمة المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة نص عليها المشرع في الدستور المادة 44

الفرع الثالث : جرائم ضد أمن الدولة :

تعد هذه الجرائم من اخطر الجرائم الالكترونية خاصة الإرهاب المعلوماتي و الجريمة المنظمة و جريمة التجسس الالكتروني ، كما تعطي شبكة الانترنت فرصا للتأثير على المعتقدات الدينية و تقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة و المساس بأمنها الداخلي و بنظامها العام⁴⁴

⁴¹ صالحة العمري، جريمة غسيل الأموال و طرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة

التشريع محمد خيضر، بسكرة، ص 179

⁴² صغير يوسف، مرجع سابق، ص 45

⁴³ احمد خليفة الملط، مرجع سابق، ص 196

⁴⁴ سامي علي عياد حامد ، الجريمة المعلوماتية و إجرام الانترنت ، دار الفكر الجامعي، الإسكندرية، 2007، ص 77

وتقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني ونصت عليها المادة 394 مكرر 02 من الأمر 156-66 "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام"⁴⁵
أولاً: الإرهاب المعلوماتي :

الإرهاب الإلكتروني أو المعلوماتي هو هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونياً ،توجه من أجل الانتقام أو الابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبالتالي فلكي ينعى شخصاً بأنه إرهابي عبر الانترنت ، وليس فقط مخترقاً ، فلا بد وإن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات ، أو على الأقل تحدث أذى كافياً من أجل نشر الرعب والخوف

فالإرهاب الإلكتروني يعتمد على استعمال الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم⁴⁵
ولقد أصبحت تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية ، فهم يستخدمون الوسائل المتقدمة مثل الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتحويل بعض الأموال في سبيل تحقيق أهدافهم ، ويقوم الإرهابيون باستخدام الانترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية ، والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات ، وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية وسهولة الاستخدام⁴⁶

ومن أخطر التهديدات والهجمات التي تمس أمن الدولة التسلسل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالح جماعات إرهابية ، وكل ما يحتاجه الإرهابي ذو الخبرة الاحترافية في هذا المجال الحيوي والمعقد هو جهاز حاسب إلكتروني واتصال بشبكة الانترنت ومن ثم القيام بأعمال تخريبية وهو آمن في مقره ، بنقرات بسيطة على لوحة المفاتيح ، ودون أن يترك أثراً.

ثانياً : التجسس الإلكتروني :

التجسس الإلكتروني أو ما يعرف بالجاسوسية الرقمية التي ترصد وتراقب أي حاسب إلكتروني عن طريق التسلسل إلى أجهزتهم الحاسوبية أو محاولة اعتراض الإشارات وحزم المعلومات التي ترسل من قبل أجهزتهم عبر الانترنت، تعتبر الحواسيب أحد أهم وسائل التجسس على الخصوصيات الفردية لقدرة المختصين على تلقي معلومات منها دون علم أصحاب الأجهزة أنفسهم، يتم معظم هذا عن طريق شبكات الحاسب الآلي التي توصل بها معظم الحواسيب باستخدام ثغرات أمنية أو أمن الحاسوب Security cracking للحصول على وصول للمعلومات المخزنة على الحاسب

⁴⁵ د.حسين بن سعيد بن سيف الغافري، الإرهاب الإلكتروني، موقع وزارة عمان الرقمية

⁴⁶ سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها ، موقع المركز الديمقراطي العربي، 22 فبراير 2017

غالباً ما تتم عمليات تجسس دولية للحصول على معلومات سرية رسمية لدى الحكومات من قبل حكومات دول أخرى، أو قد يتم التجسس من قبل حكومة بلد على أفراد معينين من النشطاء السياسيين أو أفراد الجريمة المنظمة و العصابات الضخمة و المافيا ،يعتمد بعض المخترقين أحياناً لإدخال برامج تحول الأجهزة الحاسوبية لمكان مناسب للتجسس .⁴⁷

المطلب الثاني: الجرائم الواقعة على النظام المعلوماتي :

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية ويتمثل في الجرائم الواقعة على النظام المعلوماتي و الواقعة على المعلومات المدرجة بالنظام المعلوماتي و جرائم الاعتداء على البرامج النظام المعلوماتي وهذا ما سأطرق إليه في الفروع التالية

الفرع الأول : جرائم الاعتداء على المكونات المادية للنظام المعلوماتي :

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالاسطوانات و الشرائط و الكابلات ، و نتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية⁴⁸، كان تكون محلاً للسرقة أو خيانة الأمانة أو إتلاف أعمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد و العبث بمفاتيح التشغيل أو خربشة الشريط و إفساد اسطوانات التشغيل المغناطيسي بتعريضها إلى أي مجال مغناطيس متلف و يترتب على هذا الإتلاف خسائر كبيرة⁴⁹ ومن أمثلة ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة و توثيق المعلومات الحاسوبية إلى خسائر مالية معتبرة قدرت ب 5 ملايين فرنك فرنسي⁵⁰ ، و يرى البعض من الفقهاء انه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت الآلة ، فقد يلجأ العاملون بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه مالياً وليس على الأشياء المادية بمعنى الكلمة⁵¹ و تجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضالة قيمته ، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

الفرع الثاني: جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي :

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة ، وقد تقع هذه الجرائم إما على البرامج التطبيقية و إما على برامج التشغيل و سنتطرق لهاتين الصورتين فيما يأتي :

أولاً: الجرائم المعلوماتية الواقعة على البرامج التطبيقية :

⁴⁷ Is the U.S. turning into a surveillance society? American civil liberties union

⁴⁸ د.احمد خليفة الملط ، المرجع السابق، ص176

⁴⁹ د.زكي أمين حسونة ، جرائم الكمبيوتر والجرائم الأخرى التكتيك المعلوماتي ، المؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة

1993 25 إلى 28 أكتوبر 1993 ، تقرير مصر ، ص471

⁵⁰ Rose (Philippe).op-cit.P58-59

⁵¹ André Lucas. le droit de l'informatique. Paris.PUF 1987 p519,521

يقوم الجاني في هذه الصورة بتحديد البرامج أولاً ثم التلاعب فيه لتحقيق أكبر عدد من الاستفادة
المادية

(1) تعديل البرنامج :

الهدف الرئيسي من تعديل البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات⁵² ، و من أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick و حصل على اثر ذلك على مئات الدولارات كل شهر و كان من الممكن إن يستمر هذا العمل الإجرامي لولا أن البنك أراد تأسيس شركة جديدة للدعاية ان يكافئ أول و آخر عميل له ليكتشف عدم وجود ما يدعى⁵³ Zzwick

و هناك نظام آخر يسمى سلامي salami و يتم الاختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة على فترات زمنية طويلة و متباعدة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة و قد حقق بموجب هذا البرنامج احد المستخدمين الامركين بإحدى المنشآت التجارية يدعى Royce.E في خلال 6 سنوات ما يقرب من 2 مليون دولار⁵⁴

(2) التلاعب في البرنامج :

يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية و هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة و يتم وضعه في شبكة معلوماتية بهدف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع ، أو عن طريق قيام احد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي ، و يصعب اكتشاف لصغره و دقته و مثال على ذلك لقد قام مبرمج بأحد البنوك زرع برنامج فرعي بمنشأة بالكيانات المنطقية بإدارة الحسابات يتجاهل كل عمليات السحب التي تتم من قبله عن طريق شيكات حسابية إذ يتحمل البنك نتيجة لذلك نتيجة هذه الحسابات في باب ميزانية الإدارة .

ثانيا : الجرائم المعلوماتية الواقعة على برامج التشغيل

تعد برامج التشغيل تلك البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام ، و تقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي ، و يتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

⁵² د.احمد خليفة الملط، مرجع سابق، ص173

⁵³ Duleroy et rocco (A.M) , l'informatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel e Économist, octobre 1979

n 202

⁵⁴ د.احمد خليفة الملط، مرجع سابق، ص174

- (1) المصيدة : تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء و عيوب عمدا لا يكتشف بعضها عند استخدام البرنامج، اذ يترك المبرمج ممرات خيالية و فواصل و تفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية أو إحداث مخارج وسيطة للولوج داخل النظام المعلوماتي و الوصول إلى كل المعلومات التي تحويها الذاكرة، وهذه التقنية يمكن للمبرمج استخدام البرنامج في اي وقت وفق أهوائه ، وبذلك يصبح هو المهيمن على النظام و على صاحب العمل المعتدي عليه⁵⁵.
- (2) تصميم برنامج وهمي : و تقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة و مراقبة تنفيذها و من أمثلة على ذلك قيام إحدى شركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجها بتصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهمين بلغ عددهم 46000 بهدف تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها⁵⁶

الفرع الثالث: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة أليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي و لما لها من قيمة اقتصادية ، و بهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها او عن طريق إتلافها و هذا ما سنتناوله فيما يأتي :

أولا. التلاعب في المعلومات :

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطرق مباشرة أو غير مباشرة فاما التلاعب المباشر يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي و ياخذ هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لاسيما في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين و دائمي التغير بهدف الحصول على مرتباتهم ، (و من أمثلة على ذلك قام احد المسؤولين عن القسم المالي بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي و وضعه في حسابه الخاص و حساب شركائه باستعمال هذه الطريقة⁵⁷) أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طريق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك و تسجيلها و إعادة ترحيلها و إرسالها لحساب آخر في بنك بهدف اختلاس تلك النقود في حين التلاعب غير مباشر يتم عن طريق التدخل الغير المباشر لدى المعلومات المسلحة بالنظام المعلوماتي باستخدام احد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة و معرفة أرقام و شفرات الحسابات⁵⁸ ، ويتخذ عدة صور من بينها التلاعب في الشرائط الممغنطة و قد قام في هذا الصدد احد الموظفين بأحد فروع الشركة الفرنسية Isoverst gobain بإرسال شريط ممغنط يحتوي على

⁵⁵ د.محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات ، دار النهضة العربية، 1994، ص 67

⁵⁶ Equity fuding life insurance. L'informatique nouvelle , mai 1976

⁵⁷ Escroquerie aux Assedic de paris, jugement du 2fev 1982 TGI de paris 13ème ch.°39 ,avril 1982

⁵⁸ د.احمد خليفة الملط ، المرجع السابق، ص 179

139 إذن دفع و عند معالجته بالبنك بالقسم المعلوماتي تم رفض نسخه لعيب في طول الشريط ، و قد قال الخبراء انه لو نجحت هذه العملية لثم النصب على البنك بحوالي 21 مليون فرنك فرنسي⁵⁹ كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة و تكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة .

ثانيا: إتلاف المعلومات :

قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية بإتلاف المعلومات المخزنة بالنظام المعلوماتي ، و يتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو محو المعلومات ، و يشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة بمجرد استبدال رقم بأخر أو إحلال رقم مكان آخر⁶⁰ فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام المعلوماتي⁶¹ و قد استعمل شخص يدعى Vladimir Ioriblitt بإرسال طريقة تدعى ب bluff إذ كان يعمل بوزارة المالية و قام بإدخال فواتير وهمية لا حصر لها و تحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها

و إما محو المعلومات فهو من أسهل طرق الإتلاف كون انه من خصائص الجرائم المعلوماتية قدرة الجاني على محو آثار الجريمة في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفارة ، فمثلا قام شخصان باختلاس مبلغ يقدر ب 61.000 دولار مرسله من شركات التأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل⁶² .

و في الأخير نخلص إلى القول أن دراسة موضوع مكافحة القانونية للجرائم الماسة بالأمن الإلكتروني تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة بدأت في الظهور و الانتشار في معظم المجتمعات ، و نظرا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها.

ونرى بأن الجريمة الإلكترونية تتميز بعدة خصائص تميزها عن باقي الجرائم الأخرى أهمها طبيعتها المتعدية الحدود و طابعها التقني الذي يعقد من مسألة إثباتها، الشيء الذي يميز مرتكبها و يجعل دوافع ارتكابهم للجرائم المعلوماتية بمختلف أنواعها تختلف عن المجرمين العاديين .

59 Trip de paris. 12ème ch., corr. jugement du 13 janv. 1982, DALLOZ S 1982, p 502

⁶⁰ د، احمد خليفة الملط، مرجع سابق، ص 179

⁶¹ محمد سامي الشوا، المرجع السابق، ص 75

62 Le monde informatique , 21 fev 1983, sous le titre (la délinquance en cal blanc se parte lien)

كما أن للنظام المعلوماتي أهمية كبيرة باعتباره تقنية حديثة في عالم تكنولوجيا المعلومات ، إلا أنه غالبا ما يكون مصدر خصب للجرائم التي تقع عليه و بواسطته، و بذلك تعد الجرائم الالكترونية جرائم خطيرة وسريعة و متطورة و في تزايد مستمر تبعا لزيادة استخدام تلك التقنية و هذا ما دفع بالعديد من الدول إلى مواكبة هذا التطور التكنولوجي بوضع النصوص الملائمة لمختلف استعمالات الإعلام الآلي .