

مواجهة الجريمة المعلوماتية في الجزائر

الدكتور رمزي حوحو ، أستاذ محاضر أ ، جامعة محمد خيضر - بسكرة
الباحثة منيرة بلورغني طالبة دكتوراه - جامعة محمد خيضر - بسكرة

الملخص:

أمام عصر السرعة والثورة المعلوماتية المعاصرة وإفرازاتها، ترتب على ذبوع المعارف التكنولوجية والثورة التقنية المعلوماتية التي أضافت الكثير من الجوانب الايجابية في حياتنا، إلا أنها في المقابل جلبت معها شكلا جديدا من الجرائم اصطلح على تسميتها بالجريمة المعلوماتية، ونسلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلومات، وتوسع دائرة المتضررين من الجرائم المعلوماتية. لذلك بذلت جهود جبارة سواء على المستوى الدولي سعيا منها لمواجهة هذا النوع الجديد من الجرائم حفاظا على أمن معلوماتها بالوقاية ومكافحة الجريمة المعلوماتية. والجزائر سعيا منها لمواكبة الركب الحضاري عملت هي الأخرى على مواجهة الجريمة المعلوماتية من خلال آليات تمثلت في اصدار نصوص تشريعية تجرم هذا النوع الجديد من الجرائم الذي هو الجريمة المعلوماتية.

مقدمة:

على الرغم من المزايا الهائلة التي تحققت وتحقق بفضل تقنية المعلومات على جميع الأصعدة وميادين الحياة المعاصرة، إذ أضافت المعلوماتية الكثير من الجوانب الايجابية في حياتنا، فإن هذه الأخيرة صاحبها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر، الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في البيئة الرقمية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت

هذه المخاطر تفاقما في ظل هذه البيئة التي تمثلها شبكة المعلومات، مما أفرز نوعا جديدا من الجرائم، لم يكن معهودا من قبل عُرِفَت بالجرائم المعلوماتية، ونوعا جديدا من المجرمين اصطاح على تسميتهم بمجرمي المعلوماتية. لذلك بذلت جهود سواء على المستوى الدولي أو الجزائري سعيا منها لمواجهة هذا النوع الجديد من الجرائم حفاظا على أمن معلوماتها. وأمام خطورة هذا النوع من الجرائم تتساءل عن كيفية مواجهة الجزائر لهذا النوع من الجرائم؟ والإجابة على هذه الاشكالية المطروحة تكون وفق مبحثين: المبحث الأول: الاطار المفاهيمي للجريمة المعلوماتية، المبحث الثاني: مكافحة الجزائر للجريمة المعلوماتية.

المبحث الأول: الاطار المفاهيمي للجريمة المعلوماتية

أمام عصر السرعة والثورة المعلوماتية المعاصرة وافرازاتها، لا يمكن انكار أهمية الانترنت أحد أهم دعائم تكنولوجيا الاتصال والمعلومات إلا أن هناك جانب له آثار سلبية من أهمها ظهور نوع جديد من الجرائم تدعى بجرائم المعلوماتية⁽¹⁾. ولحدثة هذا النوع من الجرائم وللإلام بالجريمة المعلوماتية نقسم هذا المبحث إلى المطالب التالية:

المطلب الأول: مفهوم الجريمة المعلوماتية وخصائصها

المطلب الثاني: أطراف الجريمة المعلوماتية

المطلب الثالث: الأسباب الدافعة لارتكاب الجريمة المعلوماتية

المطلب الأول: مفهوم الجريمة المعلوماتية وخصائصها

"تعتبر الجرائم المعلوماتية أحد ثمار التقدم السريع في شتى المجالات العلمية التي يتميز بها عصرنا الحاضر، فلقد صاحب التقدم الكبير في مجال العلوم والتقنية واستخداماتها لخير البشرية، تقدم آخر وموازي في مجال الجريمة. عصر الانترنت أو عصر السموات المفتوحة أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هاته الأوصاف انها تعبير عن مدى ضخامة القفزات العلمية التي تحققت ومدى تنوع الانجازات طرحت ثمارها بشكل ملحوظ في حياتنا في الفترة الأخيرة، ويبدو بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على تحصيلها والاستفادة منها، هذا الوجه المشرق لتقنية المعلومات يقابله من الجانب الآخر وجه مظلم الذي يتمثل في الإجرام المعلوماتي الذي وجد ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب

تتنوع وتتعير⁽²⁾. وبناء على ما تقدم أعلاه⁽³⁾ نتناول بالدراسة هذا المطلب في الفروع التالية:

الأول لتعريف الجريمة المعلوماتية، والثاني للطبيعة القانونية للجريمة المعلوماتية، والثالث لخصائص الجريمة المعلوماتية، والرابع لموضوع الجريمة المعلوماتية

الفرع الأول: تعريف الجريمة المعلوماتية

الجرائم الناشئة عن البيئة الرقمية جرائم حديثة ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطوراتها المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل الكتروني، وكذا بتكنولوجيا الاتصال وشبكات الربط. لكن التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية، خشية من حصر نطاقها داخل اطار تجريبي محدد قد يضر بها خاصة في ظل التطور المستمر لتقنية المعلوماتية، فما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى نتيجة تقنيات جديدة⁽⁴⁾. "وإذا كان التطور المتجدد والمستمر للمعلوماتية يمنع صور التجريم الحالية عن مواكبة ما يطرأ من صور اجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية تنظم اوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، وهذا ما يقع على عاتق الفقه بداية بوضع تعريف لهذه الظاهره الاجرامية، والذي قد يسهم في صياغة المشرع للنصوص القانونية ويساعد القضاء في تفسير هذه النصوص وتكييف الوقائع"⁽⁵⁾. وعليه فإنه:

أولاً: لم يتفق الفقه على ايراد تسمية موحدة للجريمة المعلوماتية، فهناك من يطلق عليها تسمية: الجرائم الالكترونية، جرائم المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، جرائم الكمبيوتر والانترنت، الجرائم المستحدثة⁽⁶⁾.

ثانياً: "أن مسألة وضع تعريف للجريمة المعلوماتية كانت محلاً لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووضعا تعريفاً مختلفة منها ما قد يتناول تعريفها من زاوية تقنية (فنية) أو من زاوية قانونية:

1- فالقائلون بالتعريف التقني يذهبون بالقول بان الجريمة المعلوماتية هي نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي المقصود، ويذهب أنصار هذا الاتجاه الفقهي إلى القول بأن تعريف جرائم الحاسب الآلي من الناحية القانونية وتصنيف صورها يتطلب تعريف

المفردات الضرورية المتعلقة المتعلقة بارتكاب جريمة الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات، الخدمات الحيوية.

2- وهناك جانب آخر من الفقه يذهب إلى تعريف جريمة الحاسب الآلي بأنها الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنت، ويرى أنصار هذا الجانب الفقهي أن من سمات هذه الجريمة أنها جريمة مستتره، وتتسم بالسرعة والتطور في وسائل ارتكابها، وهي أقل عنفا في التنفيذ من الجرائم التقليدية، وعابرة للحدود ويصعب اثباتها لعدم وجود أدلة مادية عليها، كما يسهل ائتلاف الأدلة الخاصة بها، ونقص الخبرة العلمية لدى الجهات القائمة على ضبطها، وعدم كفاية القوانين القائمة التي تعالجها. وعلى الرغم من وضوح وبساطة التعريف الذي أورده أنصار هذا الجانب إلا أن هناك من يأخذ عليه قصوره في عدم الاشارة إلى موضع الجريمة المعلوماتية على شبكة الانترنت كما في حالة تعطيل الشبكة عن العمل أو العمل على بطء سرعتها أو ائتلاف المواقع على هذه الشبكة.

3- وهناك اتجاه من الفقه يذهب إلى تعريف الجريمة المعلوماتية اعتمادا على وسيلة ارتكاب الجريمة لذلك الفقيه الألماني تاديمان بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي، وفي هذا الاتجاه عرفت بأنها الجرائم التي يكون وقع في مراحل ارتكابها بعض عمليات فعلية داخل الحاسوب، ويعبارة أخرى هي تلك الجرائم التي يكون الحاسوب فيها ايجابيا أكثر منه سلبيا. ويؤخذ على هذه التعريفات التي أوردها أنصار هذا الاتجاه اعتمادها على وسيلة ارتكاب الجريمة في تعريف الجريمة المعلوماتية، ذلك أن تعريف الجريمة المعلوماتية يقوم في الأساس على العمل الرئيسي المكون لها وليس فقط على الوسائل المستخدمة فيها، لأنه لا يمكن أن يطلق على جريمة ما أنها من جرائم الحاسب الآلي لمجرد أن الحاسب قد استخدم في ارتكابها.

4- ويذهب اتجاه آخر من الفقه إلى التركيز على الجانب الموضوعي في تعريف الجريمة المعلوماتية باعتبار أن هذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها فحسب بل تقع على الحاسب الآلي أو داخل نظامه. فعرفت الجريمة المعلوماتية من قبل أنصار هذا الاتجاه بأنها نشاط غير مشروع لنسخ أو تغيير أو حذف أو

الوصول إلى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه، وعرفت كذلك بأنها غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها.

5- وهناك اتجاه آخر لا يهتم بوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية والتقنية باستخدام الحاسب الآلي ولذلك عرفت هذه الجريمة بأنها أية جريمة يتطلب لاقتراها أن يتوفر لدى فاعلها معرفة بتقنية الحاسب، وفي ذلك الاتجاه عرفها الدكتور هشام فريد رستم بانها أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه.

6- كما عرفت الجريمة المعلوماتية بالقول هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها. ولم يسلم هذا التعريف من سهام النقد، إذ قيل أنه يوسع من نطاق هذه الجريمة ذلك أن التسوية بين السلوك غير المشروع قانونا والسلوك الذي يستحق اللوم أخلاقيا واستهجان الكافة يعارضه أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المؤثم معاقب عليه قانونا.

7- ويرى جانب من الفقه أن الجرائم التي ترتبط بالمعلوماتية ذاتها التي يطلق عليها الغش المعلوماتية ويقصد بها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية، ويعرفها الفقيه الفرنسي Masse بأنها الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح، أو هي كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها⁽⁷⁾.

ثالثا: "ولقد ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووضعوا تعريفات تتمايز وتختلف تبعا لموضع العلم المنتمية إليه، وتبعا لمعيار التعريف ذاته؛ فاختلقت بين أولئك الباحثين في الظاهره الاجرامية الناشئة عن تقنية المعلوماتية من الوجهة التقنية، وأولئك الباحثين في ذات الظاهره من الوجهة القانونية، وحتى من الوجهة القانونية تعددت التعريفات واختلفت بحسب الدراسة القانونية التي تتناولها. وفي سبيل ذلك فإن الفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية، ولعل جميع المحاولات التي بذلت من أجل تعريف الجريمة المعلوماتية لا تخرج عن احد الاتجاهين أولهما يضيق من مفهومها والثاني يوسسه"⁽⁸⁾ وفيما يلي تبيان هذين الاتجاهين:

أ- الاتجاه الذي يضيق مفهوم الجريمة المعلوماتية: "يذهب أنصار هذا الاتجاه إلى الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وأن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها

النصوص التقليدية للقوانين العقابية، وذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة فهي فقط التي تكون بحاجة إلى نصوص تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية، ومن التعريفات التي وضعها انصار هذا الاتجاه:

1 أن الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية وبملاحظته وتحقيقه من ناحية أخرى.

2 وفي هذا الاتجاه أيضاً عرفها الفقيه David Thomson (دافيد تومسون) أنها أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعليها معرفة بتقنية الحاسب، وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم من تكنولوجيا الحاسبات، هذا المفهوم قد أخذت بها وزارة العدل الأمريكية في تقريرها الصادر عام 1989 بعد تبنيها للدراسة وضعها معهد ستانفورد الدولي للأبحاث حينما عرّف الجرائم المعلوماتية بأنها أية جريمة لفاعليها معرفة فنية بالحاسبات تمكنه من ارتكابها.

3 وفي هذا الاتجاه أيضاً عرفها جانب من الفقه بالنظر إلى معيار الاعتداء، إذ يرى الأستاذ MASS أن الجريمة المعلوماتية هي تلك الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح، كما عرف الأستاذ PARKER الجريمة المعلوماتية بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارته تلحق المجني عليه أو كسب يحققه الفاعل.

4 وهناك اتجاه آخر أخذ في تعريفه للجريمة المعلوماتية بمعيار موضوع الجريمة وذلك ما ذهب إليه الفقيه (Rosenblatt) على أنها نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها⁽⁹⁾.

الملاحظ أن التعريفات المتقدمة تضيّق على نحو كبير من الجريمة المعلوماتية حتى أن البعض يرى أن الجريمة المعلوماتية في ظل هذا الاتجاه سوف تصبح أشبه بالخرافة فحصرها مثلاً في الحالات التي تتطلب أن يكون مقترف هذه الجريمة متمتعاً بقدر كبير من المعرفة التقنية لارتكابها، وهو إن تحقق في بعض الأحوال قد لا يتوفر في كثير منها، وقد يرتكب الفعل غير المشروع في البيئة الرقمية دون أن يكون فاعله بحاجة إلى هذا القدر من المعرفة، ورغم ذلك لا يمكن انكار أن هذه الأفعال تدخل في عداد الجرائم المعلوماتية. فالقيام بإتلاف البيانات المخزنة داخل نظام الكمبيوتر لا يتطلب من فاعله قدراً كبيراً من

العلم بتكنولوجيا الحاسبات الآلية، وعلى الرغم من ذلك فقد جرّمته الكثير من التشريعات العقابية. لذلك يؤخذ على هذه التعريفات السابقة أنها جاءت قاصرة عن الاحاطة بأوجه ظاهرة الإجرام المعلوماتي، فالبعض من فقهاء هذا الاتجاه ركز على معيار الجريمة والبعض الآخر ركز على وسيلة ارتكابها والبعض الآخر ركز على معيار النتيجة⁽¹⁰⁾.

II- الاتجاه الموسع لمفهوم الجريمة المعلوماتية، "ازاء الانتقادات التي وجهت للاتجاه الأول حاول بعض الفقه تعريف الجريمة المعلوماتية على نحو واسع لتفادي أوجه القصور التي شابت الاتجاه المضيق في التصدي لظاهرة الاجرام المعلوماتي. فعلى عكس من الاتجاه السابق فإن انصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة المعلوماتية باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الاجرامي يصبغ عليه وصف الجريمة المعلوماتية، وقد تباينت مواقف أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية بحسب المعايير التي اعتمد عليها كل فريق في تعريف الجريمة المعلوماتية، وتتباين مواقف الفقهاء انصار هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية، فيذهب:

1 فريق من الفقهاء إلى تعريف الجريمة المعلوماتية بأنها كل سلوك يتم بمساعدة الحاسب الآلي.

2 وفريق آخر يعتبرها كل جريمة تتم في محيط الحاسبات الآلية ومن هذه التعريفات ما جاء به الفقيه (MERWE) الذي يرى أن الجريمة المعلوماتية تتمثل في الفعل غير مشروع الذي يتورط في ارتكابه الحاسب الآلي.

3 كما ذهب البعض إلى القول بأن الجريمة المعلوماتية هي كل عمل أو امتناع يأتيه الانسان اضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لِحمايتها.

4 وفي ذات الاتجاه يرى كل من Michel et Credo أن الجريمة المعلوماتية تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالتلوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به.

5 وفي هذا الاتجاه أيضا عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا.

6 وهناك اتجاه فقهي آخر عرفها بالقول أن الجريمة المعلوماتية كل سلوك غير مشروع وغير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها.
7 كما عرفها الفقيهين (Richard totty) و(Anthony Hardcastle) على أنها الجرائم التي يكون للحاسب فيها دورا ايجابيا أكثر منه سلبيا⁽¹¹⁾.

"ولا شك أن الاتجاه المتقدم ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يؤخذ على هذا التوسع الذي من شأنه أن يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك مجرد مشاركة

الحاسب الآلي في النشاط الاجرامي، ولا يمكن بهذا التوجه فقد لا يعدو أن يكون الحاسب الآلي محلا تقليديا في بعض الجرائم كسرقة الحاسب الآلي ذاته أو الأقراص أو الأسطوانات المغنطة، فلا يمكن اعطاء وصف الجريمة المعلوماتية على سلوك الفاعل مجرد أن الحاسب أو احدى مكوناته المادية كانت محلا للاختلاس. ولم يسلم هذا الاتجاه من سهام النقد أيضا حين وسع من نطاق هذه الجريمة إلى درجة التسوية بين السلوك غير المشروع قانونا والسلوك الذي يستحق اللوم أخلاقيا واستهجان الكافة له في التعريف الذي أوردته منظمة التعاون الاقتصادي والتنمية OECD. ذلك أنه ليست بالضرورة أن يكون الانحراف في الأخلاق والسلوك المؤثم معاقب عليه قانونا⁽¹²⁾.

الفرع الثاني: الطبيعة القانونية للجريمة المعلوماتية

"تعد الجرائم المعلوماتية افرازا ونتاجا لتقنية المعلومات، فهي ترتبط وتقوم عليها، وهذا ما أكسبها لونا وطابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية. والسياسة الجنائية الحديثة تستدعي حصر الخصائص المميزة للجرائم المعلوماتية عن غيرها من الجرائم، وذلك من أجل محاولة وضع النصوص الملائمة لمكافحة هذا النوع من الجرائم المستحدثة والتي رافقت التطور التقني والمعرفي. فإذا كانت الجريمة بصفة عامة محل تطبيق القانون الجنائي فإنه وبالنظر إلى الطبيعة المتميزة للجريمة المعلوماتية فإنها تتعلق غالبا بما يسمى بالقانون الجنائي المعلوماتي. وقد أفضت هذه الحقيقة على هذا النوع من الجرائم طبيعة قانونية خاصة سواءا تعلقت بذاتية هذه الجريمة أو تعلقت بخصوصية المحل الذي يقع عليه الاعتداء في ارتكاب هذه الجرائم⁽¹³⁾. وقد أثير تساؤل حول الوضع القانوني للمعلومة؟ ومن أجل ذلك فقد انقسم الفقه إلى اتجاهين: الأول يرى

أن المعلومة لها طبيعة من نوع خاص، والثاني يرى أن المعلومة ما هي إلا مجموعة مستحدثة من القيم⁽¹⁴⁾، وفيما يلي شيء من التفصيل عن هذين الاتجاهين:

"أولاً: المعلومة لها طبيعة من نوع خاص: يرى هذا الاتجاه التقليدي بأن المعلومة لها طبيعة من نوع خاص وذلك انطلاقاً من حقيقة مسلم بها هي أن وصف القيمة يضي على الأشياء المادية وحدها، ويعنى آخر أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الاستحواذ عليها، وبمفهوم المخالفة وباعتبار أن المعلومة لها طبيعة معنوية فلا يمكن والحال اعتبار من قبيل القيم القابلة للاستحواذ عليها إلا في ضوء الحقوق والملكية الفكرية. وأياً كان الأمر فإن الأمر مستقر بصدد وجود خطأ عند الاستيلاء على معلومات الغير ولذلك فقد حاول هذا الاتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي لذلك يذهب الأستاذ Debois في وقت مبكر بأن الملكية العلمية سيتأتى يوماً ويعترف بها لصاحب فكره ثم يحصل على حق براءة اختراع باعتبار أن الفكرة السابقة مستبعدة في مجال الملكية الفكرية.

ثانياً: المعلومات مجموعة مستحدثة من القيم: يرى هذا الاتجاه الحديث أن المعلومات ما هي إلا مجموعة مستحدثة من القيم ويرجع الفضل في ذلك للأستاذين: Catala et Vivant ويذهب الأستاذ Catala إلى قابلية المعلومة للاستحواذ كقيمة واستقلالاً عن دعايتها المادية، على سند من القول أن المعلومة تقوم وفقاً لسعر السوق متى كانت غير محظورة تجارياً وأنها تنتج بصرف النظر عن دعائها المادية عن عمل من قدمها وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما، أي أن هذا الرأي يؤسس حجتين لإعطاء وصف القيمة على المعلومة: الأولى قيمة المعلومات الاقتصادية، والثانية وجود علاقة تبني تجمع بين مؤلفها. أما الأستاذ Vivant فيؤسس ذلك على حجتين أيضاً الأولى مستوحاة من بلانويل روريبيير وهي أن فكره الشيء أو القيمة لها صورة معنوية، وأن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي أن تكون جديره بحماية القانون، أما الحجة الثانية يتقدم الأستاذ Vivant بنضه حيث يرى أن كل الأشياء المملوكة ملكية معنوية، والتي يعترف بها القانون وترتكز على الاعتراف بأن للمعلومة قيمة، عندما يكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف، والإنسان الذي يقدم ويكشف ويطلع الجماعة على

شيء ما بصرف النظر عن الشكل أو الفكرة، فهو يقدم لهم معلومة بالمعنى الواسع ولكنها خاصة به. ويجب أن تعامل هذه الأخيرة بوصفها محلاً لحق فلا توجد ملكية معنوية بدون الاقرار بالقيمة المعلوماتية، ولذلك فهو يرى أن القيمة المعلوماتية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما. إذن اعتبار أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية، ولما كانت البرامج في جوهرها معلومات معالجة بطريقة آلية ولها قيمة اقتصادية فإنه يجب معاملتها معاملة المال⁽¹⁵⁾.

الضرع الثالث: خصائص الجريمة المعلوماتية

"لارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت اضفى عليها مجموعة من الخصائص والسمات المميزة التي ميزتها عن الجرائم التقليدية. ولعل أهمها ما يلي: الجرائم المعلوماتية:

1- ترتكب بواسطة الحاسب الآلي. 2- ترتكب عبر شبكة الانترنت.

3- متعددة الحدود أو جريمة عابرة للدول. 4- الجاني في الجرائم المعلوماتية.

5- صعوبة اكتشافها. 6- صعوبة اثباتها. 7- أعراض النخبة.

8- أسلوب ارتكابها. 9- خصوصية مجرمي المعلوماتية.

10- جريمة مستحدثة. 11- قلة الابلاغ عن الجريمة المعلوماتية.⁽¹⁶⁾

"وما يمكن قوله عن خصائص الجريمة المعلوماتية أنها جريمة العالم الافتراضي، الغير ملموس، وما يميزها أكثر الشخص الذي يقوم بهذه الجريمة الذي يختلف اختلافاً جذرياً عن المجرم التقليدي، فالمجرم المعلوماتي يتميز بذكائه وقدرته على التعامل مع جهاز الحاسوب والشبكة العنكبوتية، اللذان يساعده على ارتكاب جرائمه بدون أي جهد عضلي أي لا ضرب ولا كسر ولا سفك دماء. فالجريمة المعلوماتية تتم بتقنيات عالية، وكذلك هناك خاصية بارزة وهي عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم فهذه الجرائم هي صورة صادقة من صور العولمة⁽¹⁷⁾.

الضرع الرابع: موضوع الجريمة المعلوماتية

"يختلف موضوع الجريمة المعلوماتية بحسب اختلاف الزاوية التي ينظر فيها ازاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي فمن ناحية قد يكون هذا الأخير نفسه

موضوع الجريمة المعلوماتية، ومن ناجية قد يكون النظام المعلوماتي هو أداة الجريمة المعلوماتية ووسيلة تنفيذها. وبالتالي تنقسم هذه الجرائم إلى قسمين⁽¹⁸⁾.

أولاً: "القسم الأول: كون النظام المعلوماتي موضوعاً للجريمة المعلوماتية: فما يبدو في هذه الحالة أن الجرائم المعلوماتية بمعناها الفني تتفق مع الجرائم التقليدية البحتة، فمن ناحية نجد أن محل الجريمة

المعلوماتية في حالة ثمة اعتداء على المكونات المادية للنظام المعلوماتي (كالأجهزة والمعدات المعلوماتية وغيرها) يتمثل في جرائم سرقة أو اتلاف هذه المكونات والمتمثل في الحاسبات أو شاشاته أو شبكات الاتصال الخاصة أو حتى آلات الطباعة المرفقة بها. ومن ناحية أخرى إذا كان الاعتداء موجه إلى مكونات غير المادية للنظام المعلوماتي (كالبينات والبرامج) مثل جرائم الاعتداء على البيانات المخزنة في ذاكرة الحاسب الآلي أو البيانات المنقولة عبر شبكات الاتصال المختلفة والتي تتمثل في جرائم السرقة أو التقليد أو الاتلاف أو محو أو تعطيل هذه البيانات أو كان الاعتداء ذاته موجه إلى برامج الحاسب الآلي من خلال تزوير المستخرجات الالكترونية وإفشاء محتوياتها وما اصطلح على تسميته "بسرقة ساعات عمل الحاسوب الآلي"⁽¹⁹⁾.

ثانياً: "القسم الثاني: كون النظام المعلوماتي هو أداة الجريمة المعلوماتية: ففي هذه الحالة ليس هناك أدنى شك أننا بصدد جرائم تقليدية بحتة يكون فيها النظام المعلوماتي أو جهاز الحاسب الآلي هو أداة ارتكاب الجريمة المعلوماتية ووسيلة تنفيذها، ومن هذه الناحية نجد الجاني يمكن استخدام الحاسب الآلي لارتكاب السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات المعلوماتية وذلك عن طريق التلاعب في الحاسب الآلي وكذلك النظام المعلوماتي بصفة عامة"⁽²⁰⁾.

المطلب الثاني: أطراف الجريمة المعلوماتية

ترتب على ذبوع المعارف التكنولوجية نتيجة ثورة التقنية المعلوماتية التي أضافت الكثير من الجوانب الايجابية في حياتنا إلا أنها في المقابل جلبت معها:

- شكلاً جديداً من المجرمين اصطلح على تسميتهم بمجرمي المعلومات.

- توسع دائرة المتضررين من الجرائم المعلوماتية.

الضرع الأول: المجرم المعلوماتي

تقترب سمات المجرم المعلوماتي في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء⁽²¹⁾، حيث أن كل من هؤلاء المجرمين قد يكونوا من ذوي التخصصات

والكفاءات العالية ويتمتعون بالذكاء والقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه، بل أن بعضهم يتمتع باحترام وثقة عالية من الأشخاص المحيطين بهم في مجال العمل أم في المحيط الاجتماعي. وفيما يلي نتناول المجرم المعلوماتي من حيث سماته، ومن حيث فئاته.

أولاً: سمات المجرم المعلوماتي: "يتميز المجرم المعلوماتي بعدد من السمات والخصائص هي:

1 المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء.

2 المجرم المعلوماتي يبهر ارتكاب جريمته.

3 المجرم المعلوماتي انسان اجتماعي.

4 خوف المجرم المعلوماتي من كشف جريمته.

5 المجرم المعلوماتي يتمتع بالسلطة تجاه النظام المعلوماتي"⁽²²⁾.

ثانياً: فئات مجرمي المعلوماتية: "التسارع المذهل الذي شهده عالم المعلوماتية والتقنيات الرقمية الحديثة انعكس بدوره على الجرائم التي ترتكب في البيئة التقنية الالكترونية فأصبحت أمام جرائم مستحدثة سريعة

التطور، مرتكبوها ماهرون في ابتكار الأساليب الحديثة لخرق الحواجز الأمنية في هذا العالم الرقمي مستخدمين خبراتهم ومهاراتهم الذهنية والعقلية، وأمام هذا التطور والتغيير السريع في أنماط الجريمة المعلوماتية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي المعلوماتية، مع العلم أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر طائفة أو فئة"⁽²³⁾. وفيما يلي بعض هذه الفئات⁽²⁴⁾:

الفئة الأولى: صغار مجرمي المعلوماتية. الفئة الثانية: القراصنة.

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية.

الفئة الرابعة: مجرموا المعلوماتية أصحاب الآراء المتطرفة.

الفئة الرابعة: مجرموا المعلوماتية أصحاب الآراء المتطرفة.

الفئة الخامسة: مجرموا المعلوماتية في اطار الجريمة المنظمة.

الضرع الثاني: الضحية في الجريمة المعلوماتية

" لقد حدد الاعلان العالمي للمبادئ الأساسية لتوفير العدالة الرقمية وساءء استعمال السلطة الذي اعتمدهت الجمعية العامة للأمم المتحدة بقرارها رقم 401434 الصادر بتاريخ 1985/11/29 مصطلح الضحية والذي جاء شاملا لكل من المجني عليه والمتضرر من الجريمة. فوفقا لهذا الاعلان المشار إليه يقصد بالضحية الأشخاص اللذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني الفعلي أو المعانات النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات اهمال يشكل انتهاكا للقوانين الجنائية النافذة في الدول بما فيها القوانين التي تحرم الإساءة لاستعمال السلطة، كما يشمل المصطلح أيضا حسب الإقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين والأشخاص اللذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء.

يبنى على ذلك أن الضحية في الجريمة بصفة عامة كل شخص طبيعي أو معنوي أصيب بخسارته أو ضرر أو بعدوان نتيجة ارتكاب جريمة سواء بفعل أو بالامتناع عن فعل. أما المقصود بالضحية في الجريمة المعلوماتية هو كل شخص أصابه ضرر مادي أو معنوي نتيجة الإستخدام غير المشروع لتقنية المعلومات، وقد يكون شخصا عاما ممثلا في مؤسسات الدولة وهيئاتها وقد يكون خاصا ممثلا في الأشخاص الطبيعية أو المعنوية، وبحسب ذلك فإن الضحايا في الجريمة المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية من مجرد كمجرم أشخاصا عادية إلى مؤسسات مالية أو عسكرية أو قطاعات حكومية كان المجرم التقليدي لا يستطيع ارتكاب أي جرائم فيها أو في مواجهتها. فنظرا لطبيعة استخدام تقنية المعلومات في جميع المعاملات الاقتصادية والمالية الوطنية والدولية والإعتماد عليها في تسيير شؤون الحياة اليومية بالنسبة للأفراد والشؤون العامة بالنسبة للحكومات كان من شأن ذلك أن يضي أبعادا غير مسبوقه في توسع دائرة المتضررين من الجرائم المعلوماتية وتعدد فئاتهم. ويلاحظ أنه من الصعوبة بما كان تقدير حجم الجريمة المعلوماتية بتحديد ضحايا هذه الجريمة على وجه الدقة، وربما يرجع ذلك إلى مجموعة من العوامل منها ما يتعلق بالجريمة المعلوماتية ذاتها ومنها ما يتعلق بالضحايا أنفسهم، فأما العوامل المتعلقة بالجريمة المعلوماتية فإن أهمها هو عدم وجود تعريف يحظى بقبول عام للجريمة المعلوماتية وهو ما يقف عائقا أمام الدراسات الاحصائية التي

تهدف إلى بيان حجم الجريمة المعلوماتية، ذلك أن تحديد ما يعد جريمة معلوماتية يختلف من دولة إلى أخرى بالإضافة إلى أن الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية والتي يوفرها لها الحاسب الآلي بما يتمتع به من سرعة فائقة وقدره عالية على التخزين يجعل من اكتشافها أمرا في غاية الصعوبة فكثيرا من الجرائم المعلوماتية قد تم اكتشافها عن طريق الصدفة. وأما العوامل المتعلقة بالضحايا فيتمثل أهمها في إحجام المجني عليه عن الإبلاغ على الجريمة المعلوماتية خوفا من الفضيحة، والسبب في ذلك هو أن أكثر الجرائم المعلوماتية تقع داخل المؤسسات المالية وأكثر ما يحرص عليه القائمون على هذه المؤسسات هو السمعة المالية للمؤسسة ولذلك فهم يفضلون تحمل الخسائر التي قد تلحق بهم بسبب هذه الجرائم على ألا يعرف المتعاملون معهم بأن النظم المعلوماتية في المؤسسة قد تم التلاعب بها نتيجة لقصور ما⁽²⁵⁾.

"وعلى الرغم من عدم دقة الإحصائيات التي تتعلق بتحديد حجم الجريمة المعلوماتية إلا أنها تساعد في إعطاء مؤشر واضح عن مدى اتساع دائرة المتضررين منها وسوف نقوم بعرض أهم فئات المجني عليهم في مجال الجريمة المعلوماتية منهم: المؤسسات المالية والجهات الحكومية، الأشخاص الطبيعيون، مقدمي الخدمات الوسيطة في نطاق شبكة الانترنت"⁽²⁶⁾.

المطلب الثالث: الأسباب الدافعة لارتكاب الجريمة المعلوماتية

"الباعث أو الدافع هو: العامل المحرك للإرادة الذي يوجه السلوك الاجرامي كالحبة والشفقة والبغضاء والانتقام"⁽²⁷⁾. "والدوافع أو البواعث التي تدفع المجرم المعلوماتي لارتكاب جريمته تتنوع وأهم هذه الدوافع هي:

أولا: الرغبة في التعلم: الرغبة الشديدة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية ويشير الأستاذ (ليفي) مؤلف كتاب قرصنة الأنظمة إلى أخلاقيات هؤلاء القرصنة التي تتركز على مبدئين أساسيين:

- 1- أن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم.
- 2- أن عملية جمع المعلومات يجب أن يكون خاضعة للقيود.

وهناك من يرتكب جرائم الحاسوب؛ بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور، وهؤلاء الأشخاص يقومون بالبحث واكتشاف

الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكن من الاستمرار من التواجد داخل الأنظمة ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع المتنوعة والتقنيات الأمنية لأنظمة الحاسوب.

ثانياً: الدوافع المادية "الربح وكسب المال": الرغبة في تحقيق مكاسب مادية تكون هائلة أحياناً بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى اقدام مجرمي المعلوماتية على اعتراف جرائمهم من أجل تحقيق المكاسب المالية، إذ يتم اللجوء إلى ارتكاب الجريمة المعلوماتية إما عن طريق المساومة على البرامج أو المعلومات المحصلة عن طريق الاختلاس من جهاز الحاسوب أو عن طريق استعمال بطاقة سحب آلي مزور أو منتهية الصلاحية، وغير من ذلك الكثير وفي حالة نجاح المجرم في ارتكاب جريمته المعلوماتية فإن ذلك قد يدر عليه ارباحاً قد تكون هائلة في زمن قياسي⁽²⁸⁾.

ثالثاً: المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات: اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه⁽²⁹⁾، وعلى صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الالكترونية والتغلب عليها إذ يميل مرتكبوا هذه الجرائم إلى اظهار تفوقهم على وسائل التكنولوجيا الحديثة. فمجرموا المعلوماتية يمتلكهم شعور بالبحث عن القوّة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الاحساس بالدونية فزي بعض الأحيان وجد أن مجرد اظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي، وفي هذا الشأن نجد المحلل أو المبرج المعلوماتي هو مفتاح سر كل نظام قد ينتابه احساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته النفسية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية.

رابعا: الرغبة في الانتقام: الباعث على ارتكاب الجريمة المعلوماتية قد يكون الرغبة في الانتقام من شخص ما أو مؤسسة ما أو حتى بعض الأنظمة السياسية في الدول أو الانتقام من رب العمل^{(30) (31)}.

خامساً: دوافع أخرى: الدوافع السابقة ليست هي الوحيدة، بل هناك دوافع أخرى تدفع لارتكاب الجريمة المعلوماتية⁽³²⁾.

المبحث الثاني: مكافحة الجزائر للجريمة المعلوماتية

أبرزت المؤشرات والدراسات ازدياد حجم الخسائر والأضرار الناجمة عن الإجرام المعلوماتي خاصة في الدول التي تعتمد بشكل كبير على نظم التقنية المعلوماتية، الأمر الذي يشكل تحديا كبيرا في مواجهة هذه الجرائم ومكافحتها، أما في الجزائر فإن المحيط الكمي للإجرام المعلوماتي غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الإجرامي. وبناء عليه نتناول هذا المبحث من خلال: المطلب الأول: مواجهة الجريمة المعلوماتية في التشريع المقارن، المطلب الثاني: مواجهة الجريمة المعلوماتية في التشريع الجزائري

المطلب الأول: مواجهة الجريمة المعلوماتية في التشريع المقارن

لقد استدركت أغلب الدول بمختلف أنظمتها القانونية الفضل في ملاءمة القوانين النافذة الإستجابة للاعتداءات الحاصلة على النظم المعلوماتية⁽³³⁾، إذ "تختلف خطة التشريعات المقارنة في موضع النص على الحماية الجنائية وتتنوع إلى اتجاهين: الأول يرى إصدار قانون يعاقب فيه على جرائم الكمبيوتر بصورها المختلفة، وتقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة مثلا "السجلات والتوقيعات الإلكترونية" ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية. والاتجاه الثاني من التشريعات يذهب إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى إستيعابها الصور المستحدثة من الجرائم الإلكترونية، ثم تفرد هذه الخطة التشريعية قوانين خاصة ببعض الموضوعات مثل الاتصالات والتوقيع الإلكتروني والتي تتضمن نصوصا تتصل بتجريم الاعتداء على المستند الإلكتروني. ومن أمثلة التشريعات التي تبنت هذه الخطة الأخيرة القانون الألماني والفرنسي⁽³⁴⁾. ونبين ذلك وفق الفروع التالية:

الفرع الأول: مواجهة الجريمة المعلوماتية في التشريع الولايات المتحدة الأمريكية "يعتبر الشارع الأمريكي جرائم الكمبيوتر والجرائم الملحق بها من الجرائم الاتحادية، ويرجع ذلك إلى قانون سنة 1984 الذي أقره الكونجرس بشأن تجريم الاتصال غير المرخص به، والغش وإساءة إستعمال الكمبيوتر. ومنذ صدور هذا التشريع تزايدت نصوصه وتوسعت أحكامه حتى تتسنى مواجهة الصور المستحدثة من جرائم الكمبيوتر. وقد أدى الاتساع الضخم لشبكات المعلومات وعدم مركزية النشاط المتصل

بالكمبيوتر إلى وجود صعوبة بالغة في تنظيم هذا النشاط. ومع تزايد استخدام الكمبيوتر وتطور تقنياته ظهرت نماذج جديدة من السلوك الضار أدت إلى تطور التشريع على نحو مواز لها، وقد تمخض هذا التطور عن صدور عددٌ تعديلات منها قانون إساءة استعمال الكمبيوتر لسنة 1994 وبالإضافة إلى القوانين سائفة الذكر فقد أصدر الشارع الأمريكي في 30 يونيو سنة 2000 قانوناً اتحادياً للتوقيع الإلكتروني العالمي والتجارة الوطنية" أجاز بموجبه قبول واستخدام التوقيع والسجلات الإلكترونية في التعاملات التجارية الدولية وبين الولايات. وقد أبقى هذا القانون الإتحادي على كافة التشريعات الصادرة من الولايات للتوقيع والسجلات الإلكترونية، غير أنه في حال عدم صدور مثل هذه التشريعات فإن القانون الإتحادي للتوقيع الإلكتروني هو الذي يطبق. وهو ما يعني أن الغطاء التشريعي للمستندات الإلكترونية يمتد إلى كافة الولايات الأمريكية، حتى ولو لم تصدر قانوناً خاصاً به.

وقد سبق القانون الإتحادي للتوقيع الإلكتروني جهوداً تشريعية لإقرار التوقيع والسجلات الإلكترونية ومساواتها بالمستندات الكتابية، ومن هذه الجهود: القواعد الإتحادية للتوقيع والسجلات الإلكترونية الصادرة في 20 مارس سنة 1997 والتي وضعت لتطبيقها في مجال شركات الأجهزة. والقانون الإتحادي للغذاء والدواء ومستحضرات التجميل وقانون الخدمة الصحية العامة. وتعود الجهود التشريعية للتوقيع والسجلات الإلكترونية إلى ما طالب به ممثلو الصناعات الصيدلانية في سنة 1991 عن رغبتهم في استخدام البدائل الإلكترونية مثل تلك المحررة بخط اليد. وكان تبرير ذلك ما تحققه هذه الوسائل وخاصة في مجال حفظ السجلات من أهمية كبيرة لشركات التصنيع الصيدلاني. وقد أثمرت هذه الدعوة عن تشكيل مجموعة عمل تتحدد مهمتها في تنمية سياسة قبول التوقيع الإلكتروني من الهيئات.

وقد وضعت مجموعة العمل تقريراً في يولييه سنة 1992 إقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني؛ غير أنها في 31 أوت 1994 أصدرت تقريراً وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية. كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في 20 مارس سنة 1997 لتطبيق على شركات الأجهزة. كما صدر نموذج لقانون المعاملات الإلكترونية الموحد، وهو نموذج إختياري، وذلك بهدف توحيد القواعد التي تتصل بالمعاملات التجارية الإلكترونية بين تشريعات الولايات. وإلى جانب هذه التشريع فإن هناك بعض التشريعات التي يكفل الحماية الجنائية للبيانات المخزنة

إلكترونيا تضمنتها تشريعات إتحادية منها ما ينص عليه الفصل 119 من القسم الأول من تقنين الولايات المتحدة سالف الذكر. "والذي يحمل عنوان" إعتراض وسائل الاتصالات السلكية والإلكترونية والشفهية. أصدرت الكثير من الولايات الأمريكية تشريعات تتضمن وضع تنظيم للسجلات والتوقيع الإلكتروني .

ويعد أول تشريع يصدر في هذا الموضوع هو " قانون المعاملات الإلكترونية الموحد " الذي أصدرته ولاية كاليفورنيا في 16 سبتمبر سنة 1999 والذي دخل إلى حيز التنفيذ في أول يناير سنة 2000. وقانون المعاملات الإلكترونية الموحد الذي أصدرته ولاية نورث كارولينا والذي دخل حيز التنفيذ في الأول أكتوبر سنة 2000. وقد أصدرت ولاية نيويورك تشريعا في 28 سبتمبر سنة 1999 للسجلات والتوقيع الإلكتروني، وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات والتوقيع الإلكتروني.

وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات الإلكترونية وقبول التوقيع الإلكتروني في التعاملات التجارية. وقد كلف الشارع في ولاية نيويورك مكتب تقنيات الولاية بوضع تقرير يتضمن وضع تنظيم ودليل عمل لأفضل السبل لإنشاء واستخدام وتخزين والمحافظة على التوقيع والسجلات الإلكترونية (المادة الثالثة من الفصل الرابع من هذا القانون).وقد أصدرت ولاية كونتيكتكت قانونا للمعاملات الإلكترونية في فبراير سنة 2002 ودخل حيز التنفيذ في الأول من أكتوبر في ذات السنة .كما أصدرت ولاية بنسلفانيا قانونا مماثلا في 16 ديسمبر سنة 1999"⁽³⁵⁾.

الضلع الثاني: مواجهة الجريمة المعلوماتية في التشريع الفرنسي

"كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل عام 1985 عندما تقدم بمشروع قانون عقوبات جديد " Infractions أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان " الجرائم في المادة المعلوماتية تناول بالتجريم الموضوعات التالية:

- الإلتقاط العمدي للبرامج أو أي عنصر آخر من النظام المعلوماتي.

- استخدام برنامج أو معطيات أو أي عنصر من عناصر النظام المعلوماتي دون

موافقة من لهم الحق فيه.

- تخريب أو عرقلة أداء كل أو جزء من نظام المعالجة الآلية للمعلومات.

لكن هذا المشروع لم يكتب له النجاح، ولم يجد سبيله للتطبيق إلى أن تقدم النائب Jacques codfrain في 1986/08/05 ونواب آخرون في الجمعية الوطنية باقتراح مشروع قانون عن الغش المعلوماتي La fraude informatique حاول من خلاله تطوير بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف... وذلك لتشمل العدوان على المال المعلوماتي، وبعد المناقشات في البرلمان أسفرت عن قانون اختلف تماما عن ذلك المشروع الذي قدم لأول مرة بل تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل سنة 5198، فصدر بذلك القانون رقم 19 لسنة 1988 المتعلق بحماية نظم المعالجة الآلية للبيانات ثم تم ادراجه في قانون العقوبات لعام 1992 وطبق بعدها في 1991/03/01، وقد تضمن النص على مجموعة من الجرائم في المواد من 2/462 إلى 9/462 وهي: - الدخول أو البقاء غير المشروع في نظام معالجة آلية المعطيات أو في جزء منه.

- محو أو تعديل المعطيات الموجودة داخل النظام المعلوماتي.

- كل فعل عمدي من شأنه أن يعرقل أو يفسد أداء النظام لوظيفته.

- تزوير المستندات المعالجة آليا أيا كان شكلها واستعمال هذه المستندات.

أما المحطة التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004 عندما أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات⁽³⁶⁾. وبذلك يكون "قانون العقوبات الفرنسي قد تصدى للجرائم المعلوماتية من خلال أمرين:

أولا: تطبيق القواعد القانونية القائمة على الجرائم المعلوماتية.

ثانيا: فرض قواعد قانونية جديدة لمواجهة الجرائم المعلوماتية.⁽³⁷⁾

المطلب الثاني: مواجهة الجريمة المعلوماتية في التشريع الجزائري

"عرف نظام المعلوماتية تطورا بطيئا في الجزائر بالرغم من الامكانيات الاقتصادية والمالية

والبشرية التي تزخر بها مقارنة بالكثير من دول العالم الثالث، وبالأخص جيرانها من دول المغرب العربي، فالمشكل لم يكن يكمن في نقص العتاد المعلوماتي يقدر ما التخطيط العقلاني المسير للواقع إضافة إلى التأخر على صدور قوانين لتنظيم شبكة المعلوماتية، عكس شبكة الاتصالات التي وضعت لها قوانين واكبت التطور. فالجزائر لم تعرف قوانين

قبل سنة 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيا الاعلام والاتصال ما عدا شبكة الاتصال السلكية واللاسلكية ووسائل الإعلام السمعية والبصرية⁽³⁸⁾. وبناء عليه نبين ذلك في الضرع الموالية:

الضرع الأول: واقع المواجهة قبل سنة 2004

"في الواقع هناك العديد من التشريعات والاتفاقيات الدولية التي كانت تطبق في مجال المعلوماتية:

أولاً: التشريعات الوطنية: منها: الأمر رقم 66- 156 المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات المعدل والمتمم، والأمر رقم 66- 155 المؤرخ في 8 جوان 1966 والمتضمن قانون الاجراءات الجزائية، والأمر 75- 58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، وكذلك القانون 2000- 03 المؤرخ في 5 أوت 2000 الذي يتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، والأمر 03- 05 المؤرخ في 19 جوان 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة.

ثانياً: الاتفاقيات الدولية: هناك جملة من هذه الاتفاقيات التي صادقت عليها الجزائر وأصبحت تعتبر من النظام القانوني الجزائري، ومن أهمها نذكر: اتفاقية باريس لحماية الملكية الصناعية، والاتفاقية العالمية حول حق المؤلف لسنة 1952 والمراجعة في باريس 24 جوان 1971 وذلك تحت الأمر رقم 73- 26 المؤرخ في 5 جوان 1973، اتفاقية انشاء المنظمة العالمية للملكية الفكرية الموقعة بستوكهولم في 14 جوان 1967، واتفاقية بارن لحماية المصنفات الفكرية والأدبية وذلك تحت المرسوم الرئاسي رقم 97- 341 المؤرخ في 13 سبتمبر 1997،... بالإضافة إلى الانضمام إلى بعض التوصيات والبروتوكولات المتعلقة بتكنولوجيا الاعلام والاتصال. مع الاشارة إلى عدم انضمام الجزائر إلى الاتفاقية الدولية لمحاربة الجرائم الالكترونية ببودابست سنة 2001⁽³⁹⁾.

الضرع الثاني: واقع المواجهة بعد سنة 2004

"ولمسيره التطور التكنولوجي كان لا بد للجزائر على غرار الدول المتقدمة من ايجاد الاطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الاجرامية المستحدثة، فصدر القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، وتلاه القانون رقم 09- 04 المؤرخ في 5 أوت 2009⁽⁴⁰⁾. أولاً: المواجهة من خلال قانون العقوبات: "قام المشرع الجزائري بتعديل قانون العقوبات، هذا التعديل الذي

تمّ الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 156/66 المتضمن قانون العقوبات الجزائري بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من 394 مكرر إلى 394 مكرر⁽⁴¹⁾. وفيما يلي ملاحظات حول التعديل الذي مس قانون العقوبات المشار إليه⁽⁴²⁾؛ 1 "تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة ومتميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطلها وكذا من حيث مبنائها وطبيعتها ومحلها. ومن ثم لا يمكن إدراجها تحت أي نوع من الجرائم التقايدية"⁽⁴³⁾.

2 "كما أنه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطلها الجريمة فيما إذا كانت معلومات تتصل بمصالح اقتصادية أو مالية أو مسائل أمنية، وذلك سعياً من المشرع الجزائري إلى تعميم الحماية للمعلومات بكافة أنواعها ما عدى تشديد العقوبة إذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام"⁽⁴⁴⁾.

3 "فمن خلال استقراء نصوص هذه المواد يتبين أن المشرع الجزائري حاول حصر هذه الجرائم فيما يلي⁽⁴⁵⁾؛

¹ حول منظومة معلوماتية عن طريق الغش؛ وفرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة أو ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وبين ما إذا ترتب على ذلك تخريب لنظام اشتغال المنظومة.

² الاعتداء العمدي على المعطيات؛ فالمشرع لم ينص على الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات، وإنما نص على الاعتداء العمدي على المعطيات.
³ جرائم المعالجة الآلية للمعطيات الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.

⁴ جرائم الشخص المعنوي؛ تجدر الإشارة إلى أن مبدأ مسؤولية الشخص المعنوي لا ينفي مسؤولية الأشخاص الطبيعية في نفس الجريمة.

⁵ المشاركة في مجموعة أو اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم الماسة بأنظمة المعلوماتية؛ إن الحكمة من هذا التجريم هو توسيع نطاق العقوبة وذلك بإخضاع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي.

⁶ الشروع في الجريمة: أي أن المشرع جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة. كما نص المشرع في هذا القانون على العقوبات التكميلية⁽⁴⁶⁾.

4 "ومن خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين وجود تدرج داخل النظام العقابي، هذا التدرج يحدّد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات"⁽⁴⁷⁾.

ثانيا: المواجهة من القانون رقم 09-04⁽⁴⁸⁾: 1 أهداف وأهمية القانون 09-04: "جاء هذا القانون:

¹ بمجموعة من القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

² أخذًا بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك جاء عنوانه القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا.

³ كما أن التركيز على مجالي الاعلام والاتصال يوضح مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الاجرام والوقاية منه.

⁴ سد الفراغ الذي عرفه هذا المجال بصدور القانون رقم 04-15 الذي نص على حماية جزائية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف المعالجة الآلية للمعطيات.

⁵ أتى هذا القانون بتعزيز نفس القواعد من خلال وضع اطار قانوني أكثر ملاءمة.
⁶ تكمن أهمية هذا القانون في كونه يجمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين

القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف

على مرتكبها⁽⁴⁹⁾. 2 مضمون القانون 09-04: "جاء هذا القانون مقسما إلى ستة

فصول:

¹ نص الفصل الأول⁽⁵⁰⁾ على الأحكام العامة التي تبين الأهداف المتوخاه من القانون، وتحدد مفهوم مصطلح التقنية الواردة فيه، وكذا مجال تطبيق أحكامه. حيث عرّف الجرائم المرتكبة بتكنولوجيا الاعلام والاتصال، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية. كما عرّف المنظومة المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصل ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، أما المعطيات المعلوماتية فعرفها المشرع الجزائري على أنها أي عملية عرض وطرح للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها، وعرّف الاتصالات الالكترونية والتي في غالب الأحيان هي المعرضة الأولى للقرصنة على أنها أي تراسل أو إرسال أو استقبال أو اشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.

² أما الفصل الثاني⁽⁵¹⁾ فقد جاء بأحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، هذا كله لحماية النظام أو لمستلزمات التحريات والتحقيقات القضائية الجارية، وفيما يلي الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية:

^أ للوقاية من السلوكيات الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

^ب في حالة توافر معلومات على احتمال القيام باعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني.

^ج لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

^د في تنفيذ طلبات المساعدة القضائية الدولية المتبادلة. وقيد المشرع اجراء هذه العمليات إلا بإذن مكتوب من السلطات القضائية المختصة.

³ أما الفصل الثالث⁽⁵²⁾ فتضمن القواعد الإجرائية، وهذا بالنص على قواعد إجرائية خاصة بالتفتيش والجزز في مجال الجرائم المتصلة بتكنولوجيا الاعلام

والاتصال وفقا للمعايير العالمية المعمول بها في هذا الشأن، ومع مراعاة ما تضمنه قانون الاجراءات الجزائية من مبادئ عامة.

⁴ وتطرق الفصل الرابع⁽⁵³⁾ إلى الالتزامات المتعلقة بالمتعاملين في مجال الاتصالات الالكترونية، ولا سيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، وهذا بهدف اعطاء مقدمي الخدمات دورا ايجابيا في مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها.

⁵ أما الفصل الخامس⁽⁵⁴⁾ نص على انشاء هيئة وطنية تنسيقية في مجال الوقاية من الاجرام المتصل بتكنولوجيا الاعلام والاتصال ومكافحته، وقد تمت الاحالة على التنظيم لتحديد كفاءات سير هذه الهيئة. وحددت مهام هذه الهيئة فيما يلي:

أ¹ تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.
ب² مساعدة السلطات المختصة في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية.

ج³ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذا النوع من السلوك الاجرامي وتحديد مكان تواجدهم.

⁶ أما الفصل السادس⁽⁵⁵⁾ والأخير فنص على التعاون والمساعدة القضائية الدولية، واذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام. ففيما:

أ¹ يخص الاختصاص القضائي وفضلا عن قواعد الاختصاص العادية، فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الاستراتيجية للجزائر مستهدفة.

ب² يتعلق بالتعاون الدولي فهو يقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي لمكافحة هذا النوع من الجرائم خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل⁽⁵⁶⁾.

الخاتمة:

لقد ألفت الثورة المعلوماتية بضلالها على قوانين العقوبات لمختلف الدول بالتصدي للجانب السلبي منها مع ضرورة مراعاة تحقيق هدفين أساسيين هما: عدم تفويت الفرصة في الإستفادة من تطور التقنية المعلوماتية ومن ناحية أخرى ضرورة حماية الإقتصاد والأمن

الوطني وحقوق وحرريات الأفراد من جراء اللجوء إلى الاستخدام غير الشرعي لهذه التقنية، ولم يقف الأمر عند التشريعات الداخلية في مواجهة المعلوماتية، فخطورة هذه الجريمة وطبيعتها الدولية وعجز الدول فرادى عن التصدي لها جعل منها شأنًا دوليًا دفع بالمجتمع الدولي إلى توحيد جهوده وحشد قواه لمكافحة هذه الجرائم، فعقدت المؤتمرات وسنت الإتفاقيات⁽⁵⁷⁾

على هذا الأساس عنى المشرع الجزائري بمواجهة الجريمة المعلوماتية من خلال جملة من التشريعات أهمها تعديل قانون العقوبات بالقانون 04-15 واصداره للقانون 09-04. رغم ذلك لا بد من:

1 ضرورة وضع تشريع جزائري يتسق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم، وتنظيم الأحكام الإجرائية الخاصة بمواجهة هذه الجرائم.
2 إعداد برنامج أمن المعلومات من خلال إعداد خطط التدريب المختلفة مع تعيين المتخصصين في كل جهة
لنتولى مسؤولية الأمن المعلوماتي.

3 وضع ضوابط لمقاهي الانترنت وحصر المترددين عليها وعمل قاعدة بيانات لهم حتى يسهل متابعتهم.

4 منح سلطات التحقيق الصلاحية القانونية والتدريب العملي اللازم لاختراق نظام الحاسوب وضبط ما يحتويه من بيانات مخزنة.

5 ضرورة التعاون الدولي لمواجهة مشاكل صور السلوك المنحرف المتمثل في جرائم الكمبيوتر والانترنت، وذلك بعقد المزيد من الإتفاقيات الثنائية والجماعية⁽⁵⁸⁾.

الهوامش:

(1) سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير من جامعة باتنة، 2012-2013، ص 11.

(2) بن عقون حمزة، السلوك الاجرامي للمجرم المعلوماتي، مذكرة ماجستير من جامعة باتنة، 2011-2012، ص ص: 11، 12.

(3) تقديم هذا فيه ذكر لأهمية المعلومات التي تتعرض للإجرام الذي هو موضع الدراسة

(4) سعيداني نعيم، المرجع السابق، ص ص: 25، 26.

(5) نفس المرجع السابق، ص 26.

(6) عادل يوسف عبد النبي الشكري، (الجريمة المعلوماتية)، مجلة مركز دراسات الكوفة، مجلة تصدر عن جامعة الكوفة، عدد 07، (2008)، ص 112.

- (7) نفس المرجع السابق، ص ص: 112،....،114.
- (8) سعيداني نعيم، المرجع السابق، ص 26.
- (9) نفس المرجع السابق، ص ص: 26، 27.
- (10) نفس المرجع السابق، ص ص: 27، 28.
- (11) نفس المرجع السابق، ص ص: 28، 29.
- (12) نفس المرجع السابق، ص ص: 29، 30.
- (13) نفس المرجع السابق، ص 30.
- (14) محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديد للنشر، الاسكندرية، 2004، ص 49.
- (15) نفس المرجع السابق، ص ص: 49،....،51.
- (16) لأكثر تفصيل أنظر: رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة ماجستير من جامعة تلمسان، 2011-2012، ص ص: 42،....،48.
- (17) نفس المرجع السابق، ص 48.
- (18) محمد على العريان، المرجع السابق، ص 45.
- (19) نفس المرجع السابق، ص ص: 45، 46.
- (20) نفس المرجع السابق، ص 46.
- (21) "مصطلح المجرمين ذوي الباقات البيضاء مصطلح حديث نسبيا وأول من اطلقه عالم الاجتماع (Suther Land) حيث وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة وشمل أنواعا مختلفة من الجرائم كفسيل الأموال وتجاره الرقيق الأبيض وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم الفخمة" نقلا عن نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 76.
- (22) لأكثر تفصيل أنظر نهلا عبد القادر المومني، المرجع السابق، ص ص: 77،....، 81.
- (23) نفس المرجع السابق، ص 81.
- (24) نفس المرجع السابق، ص ص: 81،....،88.
- (25) سعيداني نعيم، المرجع السابق، ص ص: 63،....،65.
- (26) لأكثر تفصيل أنظر نفس المرجع السابق، ص ص: 65، 66.
- (27) نهلا عبد القادر المومني، المرجع السابق، ص 89.
- (28) ومثال ذلك "ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله: (لقد سرقت أكثر من نصف مليون دولار بفضل اجهزة الحاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكانني أن أكرر ذلك في أي وقت، لقد كان شيئا سهلا فأنا أعرف اسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفتني)، نقلا عن نفس المرجع السابق، ص 91.
- (29) "ويمكن توضيح هذا الأمر من خلال ما ذكره أحد قراصنة الحاسوب: (كانت الفرصة هي النداء الأخير الذي يبعثه دماغه فقد كنت أعود إلى البيت في آخر يوم في المدرسة وأدير تشغيل الحاسوب وأصبح عضوا في

نخبة قرصنة الأنظمة كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت اسجل اسمي في لوحة النشرات الخاصة حيث يقوم الأشخاص الآخرون للذين يفعلون مثلي بالتردد على هذا الموقع، ثم اتصفح اخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع انحاء البلاد وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحد بدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماما بينما أنتقل من جهاز حاسوب إلى آخر محاولا العثور على سبيل للوصول إلى هدي، لقد كان الأمر شبيه سرعة العمل في متهاة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات، وكان يرافقتي تزايد تدفق سرعة الأدرنالين الإنازة المحظور بفعال شئ غير قانوني وكل خطأ أخطوها كان يمكن أن تسقطني بيد السلطات كنت على حافة التكنولوجيا واكتشاف ما وراثها واكتشاف الكهوف الالكترونية التي لم

يكن من المفترض وجودي بها)، نقلا عن نفس المرجع السابق، ص ص: 91، 92.

(30) "فعلى سبيل المثال، دفع الانتقام بمحاسب شاب إلى أن يتلاعب بالبرامج المعلوماتية بحيث تختفي كل البيانات الحسابية الخاصة بديون هذه المنشأة بعد رحيله بعدة أشهر وقد تحقق هذا الأمر في التاريخ المحدد". نقلا عن نفس المرجع السابق، ص 92.

(31) نفس المرجع السابق، ص ص: 89،، 92.

(32) لأكثر تفصيل انظر نفس المرجع السابق، ص ص: 93، 94.

(33) وسوف نأخذ في هذا الصدد تجربة المشرع الفرنسي كنموذج قريب من المشرع الجزائري والمشرع الأمريكي ممثلا للنظام الأنجلوسكسوني.

(34) رصاع فتيحة، المرجع السابق، ص 91.

(35) نفس المرجع السابق، ص ص: 91،، 94.

(36) سعيداني نعيم، المرجع السابق، ص ص: 80، 81.

(37) أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2006، ص 124.

(38) بن عقون حمزة، المرجع السابق، ص 180.

(39) نفس المرجع السابق، ص ص: 180، 181.

(40) نفس المرجع السابق، ص 181.

(41) يوعناد فاطمة الزهره، (مكافحة الجريمة الالكترونية في التشريع الجزائري)، مجلة الندوة للدراسات القانونية، مجلة تصدر عن جامعة سيدي بلعباس، العدد الأول، 2013، ص 64.

(42) التعديل الذي مس قانون العقوبات المشار إليه هو بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الصادر في الجريدة الرسمية للجمهورية الجزائرية عدد 71 المؤرخة في 10 نوفمبر 2004.

(43) سعيداني نعيم، المرجع السابق، ص 79.

(44) نفس المرجع السابق، نفس الصفحة السابقة.

(45) لأكثر تفصيل أنظر المواد: 394 مكرر، 394 مكرر2، 394 مكرر3، 394 مكرر4، 394 مكرر6 من القانون رقم 04-15 السالف الذكر.

(46) يوعناد فاطمة الزهره، المرجع السابق، ص ص: 64، 65.

(47) نفس المرجع السابق، ص 65.

(48) القانون رقم 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا

الإعلام والاتصال ومكافحتها الصادر بالجريدة الرسمية للجمهورية الجزائرية عدد 47 المؤرخة في 16 أوت 2009.

(49) بن عقون حمز، المرجع السابق، ص ص: 187، 188.

(50) أنظر المواد: 1، 2، 3 من القانون 09-04 السابق الذكر.

(51) تضمن الفصل الثاني مادة واحدة فقط هي المادة الرابعة من نفس القانون.

(52) لأكثر تفصيل حول الفصل الثالث انظر المواد: 5، 6، 7، 8، 9 من نفس القانون.

(53) لأكثر توضيح أنظر المواد: 10، 11، 12 من نفس القانون.

(54) انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته تناولتها

المادة 13 أما المادة 14 فبيّنت مهام هذه الهيئة من نفس القانون.

(55) أحكام الفصل السادس تناولتها المواد: 15، 16، 17، 18، 19 من نفس القانون.

(56) بن عقون حمز، المرجع السابق، ص ص: 187، ...، 191.

(57) سعيداني نعيم، المرجع السابق، ص 78.

(58) بوعناد فاطمة الزهراء، المرجع السابق، ص ص: 72، 73.