

خصائص الجريمة المعلوماتية وأسباب ارتكابها

أ/ بن مالك اسمهان، كلية الحقوق والعلوم السياسية بجامعة م برج بوعريبرج

ط.د/ كلية الحقوق والعلوم السياسية حمد لمين دباغين سطيف.

الملخص:

تعد الجريمة المعلوماتية من الجرائم المستحدثة في عصرنا الراهن، ترتكب باستخدام تقنية عالية لا حدود لها، وقد تزايدت معدلات هذه الجريمة في العقدين الأخيرين على وجه الخصوص، الأمر الذي أدى إلى بروز ظاهرة إجرامية تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني، ويستخدم مصطلح المعلوماتية لوصف فكرة أو جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون، والجرائم المعلوماتية هي الانتهاكات التي ترتكب ضد الأفراد أو مجموعة من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو إلى إحداث أذى مادي أو معنوي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات التي تمثل جوهر الجريمة المعلوماتية، وتعتبر الجريمة المعلوماتية ظاهرة اجتماعية حولت المجتمعات إلى مجتمع رقمي، حيث انتقل نشاط الناس من الواقع الفعلي إلى الواقع الافتراضي، وهي جريمة عابرة للحدود الوطنية سهل انتشارها سهولة الوصول إلى المستهدفين وانخفاض التكلفة وضعف الرقابة والسرعة في تنفيذها وتوظيف الاتصالات والتفاعلات في ارتكابها وهذا ما دفعنا لتناول هذا الموضوع وبيان أسباب ارتكاب هذه الجريمة وخصائصها في إطار القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي تحت عنوان خصائص الجريمة المعلوماتية وأسباب ارتكابها.

الكلمات المفتاحية: الجريمة المعلوماتية- الإجرام الإلكتروني- المجتمع الرقمي- الكسب غير

مشروع- الواقع الافتراضي.

Abstract

Cybercrime is considered a new crime nowadays; it is committed by a highly developed technics that has no limits. The rate of this crime has increased in the last two decades. This has led to the appearance of cybercrime as a criminal phenomenon. We use the term "informatics" to describe a special idea about the computer or information age while cybercrime is the acts and attitudes that violate the law. In other words, cybercrime is the crime that is done to individuals or group of people directly or indirectly in order to hurt them mentally or physically by using the

internet which is the core of this crime. Cybercrime is a social phenomenon that has turned societies into a single digital community where people activity transferred from actual world to virtual world. Moreover, this crime can be committed beyond national borders because of the lack of control and the use of telecommunication and reactions in its commission in addition to the speed in doing such crimes. All of these reasons and features of cybercrime are discussed in the first chapter of this conference entitled Law No. 18-07 on the the Protection of Natural Persons in the Field of Personalized Data Processing “The features of Informatics Crime and its Causes “

KEY WORDS: Informatics Crime -Cybercrime -digital community -illegal gains- virtual world

مقدمة:

يعد استخدام التكنولوجيا في تخزين المعلومات وتصنيفها واسترجاعها ونقلها، من الركائز الرئيسية التي تعتمد عليها غالبية المجتمعات في العصر الحديث نظرا للفوائد الكبيرة لتلك التكنولوجيا أبرزها ضمان سرعة نقل وتبادل المعلومات من مختلف أنحاء العالم والحصول عليها بسهولة وبأقل جهد ووقت وتكلفة، ونظرا لتلك المزايا فإنه يوما بعد يوم يتنامى الاعتماد على تكنولوجيا المعلومات في مختلف المجالات العلمية والعملية، ونتيجة لذلك أصبحت النظم المعلوماتية والحاسبات الآلية مستودعا لكم هائل وضخم من البيانات والمعلومات الشخصية، الاقتصادية، المالية والعسكرية، حيث أصبحت الشبكات الإلكترونية ممر لنقل كم هائل من تلك المعلومات من مركزها إلى مختلف أنحاء العالم، وعلى الرغم من الإيجابيات التي تقدمها تكنولوجيا المعلومة، إلا أن التهديدات والجرائم المرتكبة عن طريق هذا الفضاء أكبر وفي تطور وتزايد مستمر، لذلك لا بد من دراسة هذا الموضوع من جانب خصائص وأسباب ارتكاب الجريمة المعلوماتية وهو ما يدفعنا إلى طرح الإشكالية التالية:

ما هي خصائص الجريمة المعلوماتية؟ وما أسباب ارتكابها؟

وهذا من خلال مبحثين رئيسيين:

المبحث الأول: ماهية الجريمة المعلوماتية وصورها.

المبحث الثاني: خصائص وأسباب ارتكاب الجريمة المعلوماتية.

المبحث الأول: ماهية الجريمة المعلوماتية وصورها:

المطلب الأول: مفهوم الجريمة المعلوماتية:

اختلف الفقهاء والسراخ حول مفهوم الجريمة المعلوماتية، والسبب في ذلك إلى الطريقة التي تناول بها كل فقيه الجريمة المعلوماتية والمعيار الذي إعتمده في تعريفها، حيث ذهب البعض إلى تعريف الجريمة المعلوماتية بأنها نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه⁽¹⁾، يستند هذا التعريف إلى موضوع الجريمة وصور السلوك المادي المحرم، ويؤخذ عليه أنه يضيق من مفهوم الجريمة المعلوماتية حيث يخرج طائفة من الأفعال غير المشروعة يستخدم فيها الحاسوب كأداة لارتكابها كالاختيال المعلوماتي، فضلا على أن تعريف الجريمة المعلوماتية يقتصر على عدة صور للسلوك المادي للجريمة الذي قد يؤدي إلى خروج بعض الأفعال الأخرى التي لم يشملها التعريف من نطاق التجريم مثل الأفعال التي تستهدف الشبكات والمواقع الإلكترونية بقصد إعاقة الاتصال وانتقال المعلومات ومنع الوصول للمعلومات، والحرمان من الحزمة الإلكترونية بشكل عام.

فيما يستند البعض الآخر إلى الوسيلة حيث يعرف هذا الاتجاه الجريمة المعلوماتية استنادا إلى وسيلة ارتكابها وهو الحاسوب، بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية⁽²⁾.

وعرفت منظمة التعاون الإقتصادي والتنمية OECD (Organisation for Economic Co-operation and Development)

أن الجريمة المعلوماتية هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية⁽³⁾، كما تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقة المجرمين، والذي عقد في فينا سنة 2006 تعريفا للجريمة المعلوماتية أنها: «أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية»⁽⁴⁾.

المطلب الثاني: صور الجرائم المعلوماتية الماسة بالمعلومة الإلكترونية:

تعتبر حماية البيانات الشخصية والحق في الخصوصية من أكثر الأمور المتعلقة بحقوق الإنسان التي يسعى جاهدا لحمايتها من خلال سن نصوص قانونية تكفل تحقيق هذه الحماية، حيث سبق وأن نظم

المشروع الجزائري حماية البيانات والمعالجة الآلية لها في ثلاثة أنواع من الجناح في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات هي:

● جنحة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات.

● جنحة إدخال المعطيات عن غش في نظام المعالجة أو إزالة أو تعديل عن غش للمعطيات.

● جنحة القيام عمدا أو عن طريق الغش.

إلا أن هذه النصوص القانونية لم تحقق المواكبة اللازمة لحماية البيئة الشخصية في ظل التطور التكنولوجي فكان لزاما عليه أن يتدارك ذلك بوضع قانون يساير هذا التطور التكنولوجي من خلال القانون 07-18 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، فنظم المشروع الجزائري الحماية الجزائية لهذه المعطيات في ظل القانون 07-18⁽⁵⁾ في الفصل الثالث منه من المادة 54 إلى غاية 69، حيث تضمن هذا القانون عدة جرائم ماسة بالمعطيات الشخصية ترتكب إما أثناء عملية جمعها أو أثناء معالجتها أو أثناء استعمالها أو التصرف فيها وهي كالآتي:

- جريمة استعمال الأساليب غير المشروعة في جمع المعطيات الشخصية.

- جريمة جمع المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني.

- جريمة عدم استفاء الشروط المسبقة للمعالجة.

- جريمة خرق الالتزامات الواقعة على المسؤول عن المعالجة.

- جريمة استعمال المعالجة لأغراض غير تلك المصرح أو المرخص بها.

- جريمة الاحتفاظ بالمعطيات خارج المدة المحددة.

- جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية.

- جريمة إيصال المعطيات المعالجة أو المستلمة إلى غير المؤهلين بذلك.

وسيتم دراسة ثلاث جرائم في هذا التعديل وهي:

الفرع الأول: جريمة استعمال الأساليب غير المشروعة في جمع المعطيات الشخصية:

نصت على هذه الجريمة المادة 59 من القانون 07-18 على أنه:

«يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100000 دج إلى 300000 دج، كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة»⁽⁶⁾.

لهذه الجريمة ركنين أساسيين هما:

أولاً: الركن المادي.

ثانياً: الركن المعنوي.

ثالثاً: العقوبة المقررة.

أولاً: الركن المادي:

يقصد بعملية الجمع أن يقوم الجاني بالحصول على معطيات لشخص واحد أو عدة أشخاص وهي شكل من أشكال الاعتداء على المعطيات الشخصية، وتقوم الجريمة سواء تم الجمع يدوياً أي جمعها في ملفات أو سجلات ورقية مثلاً أو تم عن طريق ألي أي باستعمال الأجهزة المعلوماتية حسب المادة الرابعة من القانون 07-18 التي نصت على أن القانون يطبق على نوعي المعالجة آلية كانت أو غير آلية، لذلك يمكن أن يكون الجمع في جهاز معلومات أو عن طريق انتقاء المعطيات وإدراجها في سجلات أو ملفات رقمية، كما قد يتم جمعها من وثائق ورقية موجودة مسبقاً أو عن طريق مسألة في شكل استطلاع للشخص المعني مباشرة أو إعطاءه وثيقة أسئلة يجيب عنها كتابة.

من أجل أن تقوم هذه الجريمة يجب أن تكون المعطيات موضوع الجمع هي معطيات شخصية والتي جاء تعريفها في المادة (3) الثالثة من هذا القانون⁽⁷⁾، حيث تناول في هذه المادة بالتفصيل كل ما يتعلق

بالمفاهيم المستعملة في هذا القانون وذلك من أجل إزالة اللبس عن هذه المصطلحات المعلوماتية التي تعتبر حديثة الاستعمال في المجال القانوني، وقصد المشرع من المعطيات الشخصية:

«كل معلومة بغض النظر عن دعائها متعلقة بشخص معرف أو قابل للتعرف عليه، "الشخص المعني" بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية»⁽⁸⁾.

وبذلك فالمعطيات الشخصية هي تلك المعلومات المحصل عليها والتي تؤدي إلى التعرف إلى شخص ما بشكل مباشر أو غير مباشر كاللجوء إلى رقم التسجيل كرقم الهاتف أو رقم تسجيل السيارة أو رقم تسجيل الضمان الاجتماعي أو الضريبي، وهو دليل على إرادة المشرع في التوسع في مفهوم المعطيات الشخصية لإزالة الإشكال الذي يطرح حول التمييز بين المعطيات الشخصية والمعطيات الاسمية.

استوجب القانون لقيام جريمة الجمع غير المشروع للمعطيات أن تستعمل في ذلك طرق تدليسية أو غير نزيهة وهو السلوك الإجرامي الواجب توافره، إذ وردت هذه العبارات بنفس الشكل عند المشرع الفرنسي وهو ما سيأتي بيانه لاحقاً، إذ أن مصطلح "الطريقة غير مشروعة" يكفي وحده لضمان الوسائل التدليسية وغير النزيهة لجمع المعلومة، يضاف إليها كل أشكال الاختلاس من الوثائق أو السجلات الرقمية أو الحصول عليها عن طريق الدخول غير المشروع للأنظمة المعلوماتية أما الطريقة التدليسية فهي استعمال كل وسائل الخداع والاحتيال، كالكذب على الشخص المعني بالتأثير على إرادته إلى درجة أن يقتنع بصحة ما يدعيه الجاني، فيقدم معلومات ذات طابع شخصي يستغلها الجاني في جمعها.

أما الطريقة غير النزيهة تعني مخالفة الجاني لواجباته الأخلاقية سواء أثناء ممارسة مهنته أو وظيفته أو في تعامله مع الجمهور أثناء جمع المعطيات ذات الطابع الشخصي كاستغلال النفوذ أو تقديم الرشاوى من أجل الحصول على تلك المعطيات⁽⁹⁾.

ثانياً: الركن المعنوي:

من خلال العبارات المستعملة في هذه الجريمة يتضح أنها جريمة عمدية إذ استعمل المشرع عبارات: تدليسية أو غير نزيهة أو غير مشروعة من أجل الحصول على المعطيات الشخصية مع إرادة القيام بذلك.

ثالثا: العقوبة المقررة:

اعتبر المشرع هذه الجريمة جنحة عقوبتها الحبس من سنة إلى (3) ثلاث سنوات وغرامة من 100000 دج إلى 300000 دج⁽¹⁰⁾.

الفرع الثاني: جريمة جمع المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني:

نصت على هذه الجريمة المادة 68 من القانون 07-18 على أنه:

«يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60000 دج إلى 300000 دج، كل من قام، في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية، المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن»⁽¹¹⁾.

وعليه سيتم دراسة هذه الجريمة من خلال أركانها كالآتي:

أولا: الركن المادي.

ثانيا: الركن المعنوي.

ثالثا: العقوبة المقررة.

أولا: الركن المادي:

يقوم السلوك الإجرامي لهذه الجريمة بمجرد تحقق مرحلة الوضع أو الحفظ في الذاكرة الآلية حتى وإن كان الجاني لا يريد معالجتها، كما لا يكفي مجرد جمع المعطيات لقيامها أيضا إذا لم يتم بوضعها أو الاحتفاظ بها في تلك الذاكرة.

يقصد بالوضع هو إدراج المعطيات ذات الطابع الشخصي والمتعلقة بالماضي الجزائي للشخص المعني في سجلات معلوماتية مهما كانت طبيعتها بحيث لا يشترط القانون أن تكون معدة خصيصا لذلك بل قد يكون له رض آخر تم إدراج تلك السوابق فيه كما لو كان هذا السجل متعلقا بتيسير هيئة المستخدمين⁽¹²⁾.

أما الحفظ هو البقاء على هذا النوع من المعطيات داخل الذاكرة الآلية عن طريق تسجيلها، بحيث يمكن العودة إليها في أي وقت، لذلك يعد هذا النوع من الجرائم المستمرة لاستمرار عملية الحفظ لتلك المعطيات، حيث حصر المشرع الجزائري فعل الوضع أو الحفظ الذي يتم في الذاكرة الآلية فقط وبالتالي استبعاد الحفظ اليدوي من ذلك⁽¹³⁾.

يقصد بالمعطيات ذات الطابع الشخصي التي تكشف الماضي الجزائي للشخص المعني وفقا للمادة 68 السابقة الذكر من القانون 07-18 المتعلق بحماية المعطيات الشخصية، هي التي تختص جرائم أو إدانات أو تدابير أمن والواضح أن المشرع يقصد بها حصريا ذات الأصل الجزائي، فيقصد بعبارة الجرائم كل السلوكات المعاقب عليها جزائيا سواء في قانون العقوبات أو في القوانين المكملة مهما كانت درجتها مخالفة أو جنحة أو جناية⁽¹⁴⁾.

يقصد بالإدانات مجموعة الأحكام الجزائية الصادرة بالإدانة في حق الشخص المعني، والعقوبات التكميلية الملحقة بالعقوبات المحكوم بها وكذا العقوبات البديلة كالعقوبات للنفع العام، أما تدابير الأمن فهي تلك التي يتخذها القضاء الجزائري⁽¹⁵⁾ كتدابير تعليق رخصة السياقة الذي يمكن أن تتخذه لجنة التعليق المنصوص عليها في قوانين المرور.

ثانيا: الركن المعنوي:

اعتبر المشرع الجزائري هذه الجريمة ضمن الجرائم العمدية التي يتوافر فيها القصد الجنائي العام العلم والإرادة أي أن يعلم الجاني بأن عملية الوضع أو الحفظ في الذاكرة الآلية للمعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن وأن تتجه إرادة رغم ذلك إلى القيام بهذه الأفعال المجرمة قانونا.

ثالثا: العقوبة المقررة:

بالرجوع إلى المادة 68 السابقة الذكر فقد اعتبرها المشرع جنحة عقوبتها الحبس من ستة أشهر إلى ثلاث سنوات بالإضافة إلى عقوبة مالية تتمثل في الغرامة من 60000 دج إلى 300000 دج.

الفرع الثالث: جريمة عدم استفاء الشروط المسبقة للمعالجة:

اشترط المشرع في القانون 07-18 للقيام بمعالجة المعطيات ذات الطابع الشخصي ضرورة استيفاء بعض الشروط المسبقة والمتمثلة في الحصول على الموافقة الصريحة من الشخص المعني أو عدم صدور اعتراض منه، بالإضافة إلى القيام ببعض الإجراءات الشكلية أمام اللجنة الوطنية لحماية المعطيات والمتمثلة في التصريح والترخيص، ومخالفة هذه الشروط من شأنه أن يؤدي إلى قيام نوعين من الجرائم حسب المادة 55 و56 من ذات القانون.

أولاً: جريمة خرق أحكام المادة 7 من القانون 07-18:

نصت على هذه الجريمة المادة 55 من القانون 07-18 على أنه:

«يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100000 دج إلى 300000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقاً لأحكام المادة 7 من هذا القانون. و يعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة، لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيًا على أسباب شرعية»⁽¹⁶⁾.

الركن المادي:

يتمثل السلوك الاجرامي لهذه الجريمة في اختراق أحكام المادة 7 من هذا القانون والتي ألزمت الحصول على الموافقة الصريحة من طرف الشخص المعني للقيام بمعالجة المعطيات الشخصية⁽¹⁷⁾.

يقصد بحق الاعتراض أن يطلب الشخص المعني وقف أو رفض جمع أو معالجة المعطيات التي تخصه ولم يقيد المشرع الجزائري حق الاعتراض بنوع معين من المعالجة بل أجازته سواء في إطار المعالجة الآلية أو غير الآلية سواء كانت المعالجة من طرف هيئة عمومية أو خاصة.

كما يشمل حق الاعتراض ما نصت عليه المادة 36 من هذا القانون فيما يخص المعطيات المحصل عليها لدى الشخص المعني أو تلك المحصل عليها لدى الغير⁽¹⁸⁾.

كل المعطيات ذات الطابع الشخصي يجوز للشخص المعني بها الاعتراض على معالجتها بما في ذلك التي لا يلزم القانون في المادة 7 الحصول على موافقته باستثناء إذا كانت المعالجة تستجيب إلى التزام قانوني بحت لا يجوز الاعتراض فيها بصريح العبارة⁽¹⁹⁾.

كما يجب أن يؤسس حق الاعتراض على أسباب مشروعة وإن كان الغرض منه الإشهار التجاري، وقد استند البعض إلى حصر الأسباب المشروعة في حالة إثارة حماية الحق في الخصوصية، إلا أنه بالرجوع إلى أحكام القانون 07-18 يمكن الاستناد إلى المادة 2 من التي وضعت الإطار العام لحدود المعالجة ذات الطابع الشخصي، التي يجب أن تتم في ظل احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا يمس بحقوق الأشخاص وشرفهم وسمعتهم وهي ضوابط مشروعة يمكن الاحتجاج بها لممارسة حق الاعتراض.

الركن المعنوي:

تعتبر هذه الجريمة جريمة عمدية تقتضي لقيامها القصد الجنائي العام أي علم الجاني ان المعطيات التي أراد معالجتها تخضع للموافقة المسبقة للشخص المعني وكذا علمه بأن هذا الخير قد أصدر اعتراضا على ذلك مع توافر إرادة القيام بسلوك المعالجة بالمخالفة لأحكام القانون.

العقوبة المقررة:

اعتبر المشرع هذه الجريمة جنحة عقوبتها الحبس من سنة إلى ثلاث سنوات، بالإضافة إلى غرامة مالية مقدرة بـ 100000 دج إلى 300000 دج، سواء ما تعلق باختراق أحكام المادة 7 من ذات القانون أو كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني.

ثانيا: جريمة انجاز معالجة للمعطيات الشخصي غير مصرح بها أو غير المرخص بها (جريمة مخالفة المادة 12 من ذات القانون):

نصت على هذه الجريمة المادة 56 من القانون 07-18 على أنه:

«يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200000 دج إلى 500000

دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون.

و يعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له»⁽²⁰⁾.

سيتم دراسة هذه الجريمة من خلال الركن المادي والمعنوي والعقوبة المقررة لها.

الركن المادي:

تقع هذه الجريمة بالمخالفة لأحكام المادة 12 من القانون 07-18 التي أوجبت أن تخضع كل عملية معالجة للمعطيات ذات الطابع الشخصي لإجرائي التصريح أو الترخيص من طرف السلطة الوطنية لحماية المعطيات الشخصية ما لم يوجد نص قانوني آخر يستثني عملية معالجة معينة من ذلك⁽²¹⁾.

يقصد بالتصريح تقديم طلب يتضمن إخطار السلطة الوطنية بالالتزام بإنجاز عملية المعالجة للمعطيات الشخصية في إطار أحكام القانون السابق الذكر⁽²²⁾ ويسلم للمسؤول عن هذه المعالجة بموجب هذا التصريح وصل ايداع إما مباشرة أو يرسل إليه بالطريق الإلكتروني في أجل لا يتعدى 48 ساعة⁽²³⁾.

وقد ميز في القانون 07-18 بين ثلاث حالات للتصريح وهي:

التصريح العادي: الذي يشترط فيه أن تتوفر كل البيانات المذكورة في المادة 14 من نفس القانون وهي تسعة (9) بيانات تتضمن اسم وعنوان المسؤول عن المعالجة أو مثله، طبيعة المعالجة والغرض منها، صفة فئة أو فئات الأشخاص المعنيين والمعطيات وفئات المعطيات المتعلقة بهم، المرسل إليهم الذين قد تصلهم تلك المعطيات، طبيعة المعطيات المراد إرسالها إلى دولة أجنبية، مدة الحفظ، إبراز الجهة أو المصلحة التي يمكن للشخص المعني أن يمارس أمامها الحقوق المخولة له لحق التصحيح والإعلام والولوج والاعتراض، وصف عام يمكن من تقييم أولي متعلق بتدابير السرية وأمن المعالجة، الربط البيئي أو التقريب بين المعطيات وكذا التنازل عنها للغير أو معالجتها من الباطن.

التصريح البسيط: أجازته المشرع في أحكام المادة 15 من هذا القانون، عندما يظهر أن المعالجة لا تشكل أي خطر للإضرار بحقوق وحرريات الأشخاص المعنيين وخصوصياتهم، واشترط المشرع ضرورة توفر البيانات الستة (6) الأولى من المادة 14 من القانون 07-18 السابق ذكرها على أن تحدد السلطة الوطنية قائمة بأصناف المعالجات الآلية وغير الآلية الخاضعة للتصريح المبسط.

أما التغيير: هو إدراج معلومات جديدة غير تلك التي كانت موجودة، أي أنه يعتبر عملية أخرى لانحاز المعالجة وهذا ما قد يؤدي بعد الإخطار بها إلى قيام السلوك المعاقب عليه في المادة 56، وفي حالة التغيير لبعض المعلومات التي اشترطتها المادة 14 من القانون 07-18 في التصريح قد تقع تحت طائلة تجريم خاص.

أما الترخيص: فهو يختلف عن التصريح فهو قرار يصدر عن السلطة الوطنية المختصة بحماية المعطيات الشخصية يتضمن الموافقة على انجاز المعالجة للمعطيات ذات الطابع الشخصي، إلا أن المشرع في المادة 17 من القانون 07-18 استثنى بعض الحالات التي لا يكفي فيها تقديم تصريح لانجازها، وإنما يتوجب فضلا عن ذلك الحصول على ترخيص مسبق من طرف السلطة الوطنية⁽²⁴⁾.

الركن المعنوي:

اعتبر المشرع هذه الجريمة من الجرائم العمدية لا بد لقيامها توفر القصد الجنائي العام العلم والإرادة أي أن تتجه إرادة الجاني إلى انجاز المعطيات غير المصرح بها أو غير المرخص بها وأن يكون على علم بأن المشرع قد رتب على ذلك جزاء قانونيا.

العقوبة المقررة:

قرر المشرع لهذه الجريمة أو الجنحة عقوبة في المادة 56 مقدارها الحبس من سنتين(2) إلى خمس(5) سنوات وغرامة من 20000 دج إلى 500000 دج أما إذا تعلق الأمر بنقل معطيات ذات طابع شخصي نحو دولة أجنبية بدون ترخيص وفق ما نصت عليه المادة 44 بأن العقوبة المقررة هي الحبس من سنة إلى خمس سنوات وغرامة من 500000 دج إلى 1000000 دج.

المبحث الثاني: خصائص وأسباب ارتكاب الجريمة المعلوماتية:

المطلب الأول: خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بخصائص كثيرة أهمها أنها جريمة مستحدثة ومختلفة من حيث محلها ومخاطرها، ووسائل ارتكابها، والمشكلات الناتجة عنها، فهي تتميز بطبيعة خاصة، وتتمتع بعدة خصائص تميزها عن الجريمة التقليدية أهمها:

الفرع الأول: إستهداف المعلومة:

الجريمة المعلوماتية تستهدف المعنويات لا الماديات، فهي تستهدف المعلومات وهي أشياء معنوية غير محسوسة لأنها تقع في العالم الافتراضي⁽²⁵⁾.

الفرع الثاني: صعوبة الإثبات:

أهم الخصائص المميزة لهذه الجرائم أنها صعوبة الإثبات والاكتشاف مقارنة بالجرائم التقليدية، حيث يصفها البعض بأنها إجرام خفي يأتي الجاني جرمته في الخفاء، وبالتالي يصعب ضبطه، وإنما جريمة معقدة يتسم مرتكبها بالذكاء والاحتراف، لذا فالجريمة تكون أكثر تعقيدا الأمر الذي قد يصعب معرفة أو إكتشاف مرتكبها وهذا بسبب مجموعة من العناصر أهمها:

أولاً: إن جزءا كبيرا من الأدلة غير ملموس ويزول بسرعة، ويرجع ذلك إلى أن أنواع العناوين الإلكترونية والبيانات تخزن في ذاكرة النظام الحاسوبي لمدة قصيرة ولا تخزن بشكل دائم⁽²⁶⁾.

ثانياً: أنه إذا تم العثور على تلك الأدلة فإنه من السهولة إتلافها من قبل الجناة، فضلا عن أن غياب الاعتراف القانوني بطبيعة تلك الأدلة يعد من أهم عوائق الإثبات.

ثالثاً: لجوء مرتكبي الجرائم المعلوماتية إلى استخدام وسائل وأساليب متجددة تتميز بالطابع التقني والفني المعقد، والتي يصعب على أفراد الأجهزة الأمنية التعامل معها مثل جرائم الاعتداء بواسطة مجموعة حواسيب يزرع فيها برنامج يخضع لتحكم خارجي، ويطلق عليها جرائم الاعتداء بواسطة شبكة البوت نت، حيث يمكن لأحد القراصنة التحكم في مجموعة من الحواسيب المخترقة الموجودة على إحدى شبكات البوت نت قد تصل إلى آلاف أو ملايين الأجهزة⁽²⁷⁾.

رابعاً: صعوبة الوصول للدليل بفحص كميات هائلة من المعلومات.

خامساً: إحجام المخني عليه في بعض الحالات عن الإبلاغ عن وقوع تلك الجرائم خشية من زعزعة ثقة عملائهم (مثل الجرائم التي تستهدف البنوك أو الشركات)، إذ قد تكون الخسائر الكاملة أكبر من الخسائر الناجمة عن الهجوم الإلكتروني الذي تعرض له.

سادسا: التحديات والصعوبات القانونية التي تعرقل عملية متابعة الجناة التي تنجم عن مشاكل الحدود الأولويات القضائية وذلك نظرا لكون الجرائم المعلوماتية من طائفة الجرائم عابرة الحدود الوطنية.

الفرع الثالث: حجم الخسائر:

تتماز الجرائم المعلوماتية بخاصية حجم الخسائر الناجمة عنها والتي تفوق في معظم الأحيان تلك التي تترتب على الجرائم التقليدية، كمثال على ذلك ما قام به أحد مجرمي المعلومات وهو فلبي الجنسية بصنع فيروس يسمى "أحبك - I LOVE YOU" وقد انتشر الفيروس في مختلف دول العالم عن طريق البريد الإلكتروني، وقدرت كلفة الإجرام المعلوماتي في العالم خلال عامي 2007 و2008 بنحو ثمانية "8" مليارات دولار، وفيما يخص التجسس المعلوماتي على الشركات فقد بلغت قيمة ما استول عليه مرتكبي هذه الجرائم من ملكية فكرية لشركات تجارية "1 تريليون" دولار⁽²⁸⁾.

وحسب إحصاء قامت به شركة سيمانتك "Symantec" الأمريكية لحماية الشبكة الإلكترونية فإن المعدل السنوي لكلفة الجرائم الإلكترونية حول العالم يبلغ 114 مليار دولار، فقد أصدرت تقرير بعنوان "نورتون ساير كرم 2011" وهو أكبر تقرير من نوعه حول كلفة الجرائم الإلكترونية، خلصت فيه إلى أن 431 مليون بالغ حول العالم كانوا ضحية للتهديدات الإلكترونية عام 2010 أي ما معدله مليون ضحية يوميا و145 في الثانية.

وقالت الشركة أن كلفة الجرائم الإلكترونية عام 2010 بلغت 388 مليار دولار وهي قيمة الخسائر المالية وخسارة الوقت، أي أنهما تجاوزت قيمة السوق السوداء للماريجوانا والكوكايين والهروين التي تبلغ 288 مليار دولار⁽²⁹⁾، وتجدر الإشارة إلى أن هذه التقديرات قد لا تعكس حجم الخسائر الفعلي بسبب إحجام المجني عليهم في بعض الحالات عن الإبلاغ عن الجرائم التي يتعرضون لها خاصة الشركات والبنوك والمؤسسات المالية.

وبحسب تقرير صادر عن القمة العالمية للحكومات بعنوان «أسلوب عملي لتحديد الهجمات الإلكترونية»، بالتعاون مع شركة «بي دبليو سي»، تنبأت شركة الأبحاث الأمريكية «سايرسيكيوريتي فينتشرز» في عام 2016، بأن الجرائم الإلكترونية ستكلف العالم 6 تريليونات دولار أميركي سنوياً بحلول عام 2021، أي بزيادة الضعف عن كلفتها التي بلغت 3 تريليونات دولار أميركي عام 2015⁽³⁰⁾.

الفرع الرابع: جريمة عابرة للحدود:

تتميز الجريمة المعلوماتية أنها جريمة عابرة للحدود، فليس لها حدود، فهي متمردة على عنصر المكان والنطاق الجغرافي، حيث تدخل في طائفة الجرائم غير الوطنية، ويرجع ذلك إلى البيئة الإلكترونية التي تقع فيها تلك الجرائم والتي تقوم على الربط الإلكتروني بين الحواسيب، سواء داخل الدولة الواحدة أو بين عدة دول بواسطة شبكات إلكترونية مثل الانترنت والتي صممت في الأصل لتسهيل عملية نقل المعلومات والاتصالات فأصبحت تستخدم كوسيلة لارتكاب الجرائم، فقد ترتكب جريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية وتتحقق نتيجتها الإجرامية في دولة أخرى من العالم مروراً بمزود خدمة أو قنوات اتصال في إقليم دولة ثالثة، ويترتب على البعد الوطني للجريمة المعلوماتية عدة إشكاليات مشابهة لتلك المرتبطة بالجرائم ذات الطابع عبر الوطنية أهمها، إصدار إجراءات التحقيق وضبط المتهمين وملاحقتهم بمبدأ السيادة الوطنية للدولة وخاصة في الجرائم التي تتطلب إتخاذ إجراء من إجراءات التحقيق في إقليم دولة أجنبية، وكذلك إشكالية الاختصاص القضائي وإشكالية تحديد القانون واجب التطبيق، كما أنه من جهة أخرى تشكل الإجراءات الرسمية المعقدة والتي تستغرق وقتاً وليس بالقصير في حالات المساعدة القانونية أو القضائية بين الدول، والتي تتعارض مع طبيعة الجرائم المعلوماتية التي تتطلب سرعة في التحقيقات⁽³¹⁾.

حيث أن جزءاً كبيراً من الأدلة في الجرائم المعلوماتية كما سبق الإشارة غير ملموس ويزول بسرعة، وهو ما يتطلب أن تكون إجراءات التحقيق وجمع الأدلة بصورة سريعة وآنية.

المطلب الثاني: أسباب وطرق ارتكاب الجريمة المعلوماتية:

سنتناول في هذا المطلب أسباب ارتكاب الجريمة المعلوماتية وطرقها

الفرع الأول: أسباب ارتكاب الجريمة المعلوماتية:

أولاً: الدوافع أو الأسباب الذاتية:

أ: الرغبة الأكيدة في الانتقام:

الانتقام موجود داخل النفس البشرية، فكثيراً من الأفراد يفضلون تعسفياً أو بغير وجه حق من شركة أو منظمة حكومية، أو حتى مصرف، وهم يملكون المعلومات والتدريب اللازمين والمعرفة الكافية بخفايا هذه

الجهة، لذلك يرتكب الجاني الجريمة رغبة منه في الإنتقام لجعل الشركة او المؤسسة تتكبد الخسائر المالية الكبيرة.

ب: الطمع وحب الثراء السريع:

المال هو عصب الحياة، وهو ما يدفع الفرد للقرصنة أو السرقة أو الإختلاس عن طريق الحاسب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير المكلف.

ثانيا: الدوافع النفسية:

تتمثل في الرغبة في إثبات الذات والتفوق على تعقيد وسائل التقنية، فالصورة الذهنية لمرتكبي الجرائم الإلكترونية غالبا هي صورة البطل الذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبوا هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة فيحاولوا إيجاد الوسيلة إلى تحطيمها أو التفوق عليها.

ثالثا: دوافع عقائدية:

إن العقيدة من أقوى الدوافع والقوى المحركة للأشخاص، والتي يكون لدى الإنسان الاستعداد للتخلي عن الحياة بأسرها، فما هو الظن بما هو أيسر من ذلك، إذ أن كثيرا من الأشخاص يبررون محاولات اختراقهم لأجهزة الغير بتأويلات غريبة وأفكار سيئة، فمنهم من يحاول اختراق جهاز أو موقع بحجة أنه غير المذهب أو الطائفة الدينية أو بحجة تكفيره أو الإطلاع على أسرار له فضحه والتشهير به.

رابعا: دوافع عنصرية:

من الدوافع أيضا الدوافع العنصرية والتي تميز بين عنصر وآخر أو قبيلة أو عرق وبين آخرين، فبعض القبائل أو الأعراق لا يحبون القبيلة الأخرى أو العرق الآخر فتجد بعضهم يحاول عمل أعمال تخريبية من شأنها جر مشاكل على القبيلة أو العرق الآخر سواء باستخدام التدمير أو الإتلاف أو نشر الشائعات والأكاذيب أو غيره من طرق وأنواع الجرائم المعلوماتية.

خامسا: دوافع سياسية وإيديولوجية:

كثيرة هي المنظمات في عصرنا الحالي والتي تتبنى بعض الآراء والأفكار السياسية، الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها، ويتم ذلك بالتشهير بهم عن طريق شبكة المعلومات⁽³²⁾.

إذ أن هذا العصر الجديد للإرهاب تميز بالدور المركزي الذي تلعبه شبكة الأنترنت في تشكيلها ونقل الأفكار والخبرات عبرها، بين الجامعات والأفراد الذين يشكلونها، حيث أصبح الإرهاب وثيق الصلة بالتكنولوجيا لدرجة أنه يمكن معه القول أن بث الإرهاب عبر الأنترنت أصبح من سمات الألفية الثالثة، حيث يتميز الإرهاب الإلكتروني عن الإرهاب التقليدي بالطريقة العصرية المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات، ولذلك نجد أن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

فخطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية مما يجعلها هدفا سهلا للمال.

فبدلا من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الحيوية، ومثل أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية أو شل محطات إمداد الطاقة والماء، أو إختراق النظام المصرفي مما يضر بأعمال البنوك والأوراق المالية العالمية.

سادسا: دوافع إجتماعية:

يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة، فعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهظة التكاليف والتي تتطلب مهارات عالية أحيانا، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية (أو البيوت القصديرية)، وكنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته،

مما يجعلهم بعضهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية، حيث تتطلب رأس مال كبير والتحضر سبب رئيسي للجرائم الإلكترونية في بعض الدول كما يرى البعض.

وكذلك من الدوافع الاجتماعية البطالة: حيث الجريمة الإلكترونية شأنها شأن الجريمة التقليدية كالبطالة والظروف الاقتصادية الصعبة وتتركز البطالة بين قطاعات كبيرة من الشباب، ولذا فإن الشباب الذين يملكون المعرفة ويعانون من البطالة يستثمرون ذلك في النشاط الإجرامي الإلكتروني.

أيضا من الدوافع الاجتماعية الضغوط العامة: إذ تعد الضغوط التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة قطاع الشباب مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الاتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية.

سابعا: دوافع تتعلق بخصائص الجريمة المعلوماتية:

أ: الإزالة (Removable) الجريمة المعلوماتية لا تتطلب الإزالة فيمكن نسخها فقط.

ب: التوافر (Available) المعلومات في كل مكان جاهزة لتستهدف من الجريمة.

ج: القيمة (Valuable) معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم...قيمة.

د: المتعة (Enjoyable) كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.

هـ: الديمومة (Durable) المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

و: سرعة التنفيذ: لا يتطلب تنفيذ الجريمة المعلوماتية الوقت الكبير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنقل ملايين الدولارات من مكان إلى آخر، هذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

ي: التنفيذ عن بعد: لا تتطلب الجريمة المعلوماتية في أغلبها (ماعدات جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة

سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب.

ع: الجاذبية: خطر تمثله سوق المعلومات والحاسب والانترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات.

ي: عابرة للحدود الدولية: إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائية والانترنت جعل الانتشار الثقافي وعمولة الثقافة والجريمة أمرا ممكنا وشائعا لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان أصبحت ساحتها العالم اجمع.

الفرع الثاني: طرق الجريمة المعلوماتية:

وهي على سبيل المثال لا الحضر.

أولاً: تخريب المعلومات وإساءة إستخدامها: يشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية...

ثانياً: سرقة المعلومات: يشمل بيع المعلومات كالبحوث أو الدراسات الهامة او ذات العلاقة بالتطوير التقني، الصناعي، العسكري أو تخريبها أو تدميرها...

ثالثاً: تزوير المعلومات: يشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحويلها، مثل تغيير علامات الطلاب.

رابعاً: تزيف المعلومات: تشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

خامساً: انتهاك الخصوصية: يشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الالكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.

سادسا: التصنت: تشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

سابعا: التجسس: يشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

ثامنا: التشهير: يشمل استخدام المعلومات الخاصة أو ذات الصلة بالإنحراف أو الجريمة ونشرها بشكل القصد منه إغتيال شخصية الأفراد أو الإساءة.

تاسعا: السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

عاشرا: سرقة الاختراعات: خاصة في المجالات العلمية لاستخدامها أو بيعها.

إحدى عشر: الدخول غير القانوني: للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

إثنى عشر: قرصنة البرمجيات: يشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

ثلاثة عشر: قرصنة البيانات: والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحاسبات وكلمات الدخول وكلمات السر.

أربعة عشر: خلاعة الأطفال: تشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، والإناث بشكل عام، ونشر الجنس التحيلي على الشبكات.

خمسة عشر: القنابل البريدية: تشمل إرسال فيروسات لتدمير البيانات من خلال رسائل ملفوفة إلكترونية.

ستة عشر: إفشاء الأسرار: تشمل الحصول على معلومات خاصة جدا ونشرها.

سبعة عشر: الاحتيال المالي: بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسويق أو المالية أو الهاتف.

ثمانية عشر: الإرهاب الإلكتروني: يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الارهاب ومصادره، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

خاتمة:

نخلص مما تقدم أن الجريمة المعلوماتية أو الإلكترونية ليست جريمة تقليدية في ثوب جديد، وإنما هي بحق نوع مستحدث من الجرائم الذي يتطلب مكافحتها جهدا وتشريعا وتعاونا دوليا وبذلك نخرج ببعض المقترحات أو التوصيات وهي:

أ: ضرورة تبني فكرة العقوبات البديلة لبعض الفئات مبرمجوا المعلوماتية خاصة من الشباب والصغار الذين يكون لديهم دافع إجرامي أو نية الإضرار بالغير، أي تقل لديهم الخطورة الإجرامية، وإنما يقومون بذلك بدافع التسلية والمغامرة.

ب: نشر ثقافة التعامل الآمن والسليم مع تكنولوجيات المعلومات بين أفراد المجتمع من خلال التوعية بمخاطر استخدام وسائل تكنولوجيا المعلومات وشبكات الاتصال، وأساليب الاختراق وكيفية قيام قراصنة الانترنت مثلا باستهداف ضحاياهم لسرقة البيانات أو المعلومات الخاصة بهم واستخدامها لأغراض تخدم أهدافهم الإجرامية.

ج: التوعية بضرورة التبليغ السريع والفوري لحوادث الاعتداء التي يتعرضون لها من عمليات اختراق أو إتقاط المعلومات أو غيرها من الاعتداءات حتى تتمكن الجهات المختصة بمكافحة الجرائم.

د: ضرورة إحاطة المشتغلين بالقضاء بالحد الأدنى من المعرفة الفنية والتقنية التي تساعدهم على فهم الجريمة بشكل أعمق وأوضح.

هـ: حصر المواقع الإلكترونية المشبوهة المنتشرة على شبكة الأنترنت مثل المواقع التي قد تشكل في حد ذاتها جريمة كالمواقع التي قد تكون محرضة على ارتكاب الجرائم، أو قد تقدم المساعدة الفنية لمرتكبي هذه الجرائم من خلال الترويج لأفكار الاختراق أو تتيح لروادها استخدام برامج الاختراق.

و: التنسيق مع الجهات الدولية والإقليمية والدول الأخرى في مجال مكافحة الجرائم المعلوماتية وتبادل المساعدة الفورية من أجل إجراء التحقيقات المتعلقة بالجرائم المعلوماتية.

الهوامش:

- 1- تعريف الأستاذ "Rosenblatt" مشار إليه لدى: د/يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، ص. 213.
- 2- تعريف الأستاذ "E.Slie.D-Ball" مشار إليه لدى: يونس عرب، صور الجرائم الالكترونية واتجاهات ثبوتها، هيئة تنظيم الاتصالات مسقط، سلطنة عمان، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، 2- 4 نيسان 2006، ص 3 المتاح على الموقع الإلكتروني: [www. Itvarabic.org/coe/2006/E](http://www.Itvarabic.org/coe/2006/E)
- 3- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر 1990، ص 34.
- 4- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، دار الثقافة، عمان، الرذن، 2004، ص 10.
- 5- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية العدد 34.
- 6- المادة 59 من القانون 18-07 السابق الذكر.
- 7- المادة 3 من القانون 18-07 السابق الذكر.
- 8- المادة 3 من القانون 18-07 السابق الذكر.
- 9- القانون رقم 18-07 السابق الذكر.
- 10- المادة 59 من القانون 18-07 السابق الذكر.
- 11- المادة 68 من القانون 18-07 السابق الذكر.
- 12- الغرض من استحداث هذه الجريمة من أجل منع الخواص من إنشاء صحيفة السوابق العدلية خاصة، إذ أنها تقع بالمخالفة لأحكام المادة 10 من القانون 18-07 التي ذكرت على سبيل الحصر من هم المسؤولون عن المعالجة الذين يحق لهم معالجة أو جمع المعطيات الشخصية المتعلقة بالماضي الجزائي للشخص المعني.
- 13- المادة 68 من القانون 18-07 السابقة الذكر.
- 14- يستبعد من نطاق تطبيق المادة 68 الجرائم المدنية والتأديبية.
- 15- المادة 19 من قانون العقوبات الجزائري.
- 16- المادة 55 من القانون 18-07 السابق الذكر.
- 17- المادة 7 من القانون 18-07 على أنه: «لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني...».
- 18- المادة 36 من القانون 18-07 أنه: «يجوز للشخص المعني أن يعترض، لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي. وله الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية، ولا سيما التجارية منها، من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة...».
- 19- الفقرة 2 من المادة 36 من القانون 18-07 السابق الذكر.
- 20- المادة 56 من القانون 18-07 السابق الذكر.
- 21- المادة 12 من القانون 18-07 أنه: «ما لم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخيص منها طبقاً للأحكام المنصوص عليها في هذا القانون.
- 22- القانون 18-07 المتعلق بحماية المعطيات الشخصية.
- 23- المادة 13 من ذات القانون.
- 24- المادة 17 و 20 من القانون 18-07 المتعلق بحماية المعطيات الشخصية.

المادة 17: « تقرر السلطة الوطنية إخضاع المعالجة المعنية لنظام الترخيص المسبق عندما يتبين لها، عند دراسة التصريح المقدم لها، أن المعالجة المعتزم القيام بها تتضمن أخطاراً ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص...».

المادة 20: « يجب أن يتضمن طلب الترخيص المعلومات المذكورة في المادة 14 من هذا القانون. تتخذ السلطة الوطنية قرارها في أجل شهرين (2) من تاريخ إخطارها،... ».

25- يونس عرب، صور الجرائم الإلكترونية واتجاهات ثبوتها، منشأة المعارف الإسكندرية، 2008، ص4.

26- نسرین عبد الحمید نبیه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008، ص4.

27- شبكة البوت نت، تنشأ هذه الشبكة بزرع برنامج خبيث في الحاسوب المخترق والذي يسمى "بوت" ويتم توصيله أو إدراجه فيما بعد ضمن شبكة من الحواسيب المخترقة، ويقدر عدد الأجهزة الموجودة بكل شبكة متفرقة لأغراض مختلفة مثل قطع الخدمة وسرقة معلومات مهمة ونشر برامج خبيثة، حيث يمكن للمخترق التحكم في مجموعة كبيرة من الحواسيب المخترقة الموجودة على إحدى شبكات البوت نت.

28- محمد علي العرين، الجرائم المعلوماتية، كلية الحقوق، الإسكندرية، دار الجامعة الجديدة للنشر، 2011، ص18.

29- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، القاهرة، دار النهضة العربية، 2004، ص45.

30- وائل نعيم، دبي، مقال منشور بتاريخ 2018/03/02 في الموقع:

<https://www.albayan.ae/across-the-uae/accidents/2018-03-02-1.3200109>

31- أيمن عبد الله فكري، جرائم نظم المعلومات، الإسكندرية، دار الجامعة الجديدة للنشر، 2007، ص96.

32- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005، ص126.