المواجهة الجنائية لجرائم تقنية المعلومات وفقاً لأحكام القانون رقم ١٧٥ لسنة ٢٠١٨

"دراسة مقارنة"

د/ أحمد السيد الشوادفي علي النجار
مدرس القانون الجنائي- كلية الحقوق جامعة الزقازيق

ملخص البحث

من الإنصاف أن نعترف، أن أهم ما يميز العصر الحالي عن غيره من العصور هو ما نشهده اليوم من تطور هائل في المجالات التكنولوجية ٠الأمر الذي انعكس علي مجمل مجالات الحياة، بحيث يمكن القول بأنه لم يعد هناك شأن يتصل بالحياة الإنسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد٠

وعلي الرغم من الإيجابيات العديدة التي أحدثتها تقنية الإنترنت في تسهيل وتبادل المعلومات، إلا أن خشية متزايدة من تنامي الخروق والسلبيات والأعراض الجانبية لهذه الشبكة واستغلالها من قبل البعض لارتكاب أفعال إجرامية ٠

من أجل ذلك، كانت الحاجة ماسة إلي إصدار قانون بشأن مكافحة جرائم تقنية المعلومات، يهدف إلي تحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة علي المعلومات وكفالة سريتها وعدم إفشائها أو التصنت عليها إلا بأمر قضائي مسبب، وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها ٠

وموضوع هذا البحث؛ يهدف إلي تسليط الضوء علي المواجهة الجنائية لجرائم تقنية المعلومات وفقاً لأحكام القانون رقم ١٧٥ لسنة ٢٠١٨م ، وهو ما يستدعي الدراسة لبيان ما تضمنه من قواعد موضوعية وأحكام إجرائية بصدد تلك الجرائم٠

الكلمات المفتاحية: الجرائم المعلوماتية ـــ الجرائم الإلكترونية ـــــ جرائم الحاسب الآلي ـــــ الإجرام التقني الحديث ٠

(ISSN: 2356 - 9492)

Abstract of research

It is beyond doubt that technological breakthrough has distinguished the last few decades to an extent that affected almost each and every single field of human activity indicating that a new era was born.

Among the above-mentioned revolutionary technologies and probably the most important of them is the internet, which facilitated exchange and transformation of information , however the disadvantages of this technology have become increasingly a source of concern .

As a response it was necessary to enact a legislation prohibiting cybercrimes and preserving balance between determinants of protecting privacy on one side and the necessity to provide effective means to fight violations against cyber security .

Accordingly , this research aims at studying criminal law approach against cybercrimes according to provisions of law no.175 of 2018 focusing on both procedural and substantive content of that legislation .

Key words : cybercrimes , electronic crimes , technology crimes .

مقدمة

الحمد لله، والصلاة والسلام علي سيدنا محمد بن عبد الله وعلي آله وصحبه والتابعين وبعد:

[١] موضوع البحث:

الجريمة بذاتها لا تعد ظاهرة جديدة، وإنما هي ظاهرة قديمة قدم التاريخ إلا أن هذه الظاهرة بشكلها التقليدي أقل خطورة وتطوراً عما هو قائم بالنسبة للجريمة المستحدثة التي ترتكب عبر شبكة الإنترنت ( ) بشكل متلاحق وسريع ومتطور نتيجة ظهور أدوات تقنية المعلومات مثل الحاسب الآلي والهاتف المحمول وغيرها، الأمر الذي أدي إلي ظهور ما يسمي بالجريمة الإلكترونية أو المعلوماتية والتي تشكل خطراً شديداً علي الفرد وعلي المجتمع٠

الأمر الذي دفع الدول والمجتمعات إلي العمل ملياً للحد من هذه الجرائم من خلال التوعية والوسائل الوقائية الأمنية وغيرها ، بحيث بات لزاماً أن يواكب تطور الجريمة وأساليبها تطوراً في مجال السياسة التشريعية عموماً والسياسة الجنائية علي وجه الخصوص ، بعد أن أصبح واضحاً التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام الشبكة المعلوماتية، لهذا الاعتبار تكاتفت الجهود الدولية لمواجهة الأثار السلبية المترتبة علـــــــي إساءة استخدام تقنية الاتصالات والمعلومات ٠

ولقد حرص المشرع الدستوري في مصر علي تأكيد أهمية مكافحة الجرائم المعلوماتية، فقد نصت المادة (٣١) من دستور ٢٠١٤ (المعدل) علي أن: " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، علي النحو الذي ينظمه القانون" ٠

هذا، وقد أصدر المشرع الجنائي القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ونشر في الجريدة الرسمية ـــ العدد ٣٢ مكرر (ج) في ١٤ أغسطس ٢٠١٨ ٠ ويهدف هذا القانون إلي حماية البيانات والمعلومات الحكومية والأنظمة والشبكات المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة من الاعتراض أو الاختراق أو العبث بها أو إتلافها أو تعطيلها بأي صورة كانت ٠ كما يحمي البيانات والمعلومات الشخصية من استغلالها استغلالاً يسئ إلي أصحابها، وخاصة في ظل عدم كفاية النصوص التجريمية التقليدية بحماية

(ISSN: 2356 - 9492)

خصوصيات الأفراد وحرمة حياتهم الخاصة في مواجهة التحديات والمخاطر المستحدثة لاستخدام تقنية المعلومات ٠ وقد وضع هذا القانون قواعد إجرائية دقيقة تنظم إجراءات الضبط والتحقيق والمحاكمة المتعلقة بتلك الجرائم ٠

[٢] أهمية البحث:

ترجع أهمية البحث إلي التطور المستمر في نظم معالجة البيانات والمعلومات الآلية وتخزينها وتبادلها وتخليقها وتطويرها وتعدد المواقع والحسابات الخاصة والاتساع المضطرد في استخدام البريد الالكتروني والأجهزة والمعدات التقنية إلي جانب التطور المذهل في وسائل الاتصال المعلوماتي، كل ذلك كان له انعكاسات حتمية في تقنية المعلومات، إذ ترتكب جرائم بواسطة تلك الأنظمة والتقنيات باعتبارها من وسائلها وأدواتها، وهي ما يطلق عليها الأن تقنية المعلومات التي تكون المعلومات محلاً للجرائم أو أداة في ارتكابها ( ) ٠

من هذا المنطلق، كانت الحاجة ماسة إلي إصدار قانون بشأن مكافحة جرائم تقنية المعلومات، يهدف إلي تحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة علي المعلومات وكفالة سريتها وعدم إفشائها أو التصنت عليها إلا بأمر قضائي مسبب، وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها ٠

كما ترجع أهمية البحث إلي صدور القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، وهو ما يستدعي الدراسة لبيان ما تضمنه من قواعد موضوعية وأحكام إجرائية بصدد تلك الجرائم٠

[٣] منهج البحث:

تتبع هذه الدراسة " المنهج التأصيلي التحليلي المقارن " بين القانون المصري والقانون الفرنسي٠ ويركز البحث بمنهجه علي تحليل وتأصيل مجموعة القواعد والأحكام المنصوص عليها في القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ٠

[٤] خطة البحث:

بناء علي ما تقدم، ونظراً لما تمثله جرائم تقنية المعلومات من تأثير بالغ في الحياة العملية سأعالج ـــ بإذن الله تعالي ـــــ هذا الموضوع وفقاً للخطة الآتية:

المبحث الأول ـــــ ماهية الجريمة المعلوماتية ٠

[المطلب الأول] تعريف الجريمة المعلوماتية ٠

[المطلب الثاني] التطور التاريخي للجريمة المعلوماتية ٠

المبحث الثاني ـــــ الأحكام الموضوعية لجرائم تقنية المعلومات ٠

[المطلب الأول] جرائم الدخول غير المشروع، وتجاوز حدود الحق في الدخول، والاعتراض غير المشروع٠

[الفرع الأول] جريمة الدخول غير المشروع ٠

[الفرع الثاني] جريمة تجاوز حدود الحق في الدخول ٠

[الفرع الثالث] جريمة الاعتراض غير المشروع ٠

[المطلب الثاني] جرائم الاعتداء علي سلامة البيانات، والبريد الإلكتروني، وتصميم الموقع ٠

[الفرع الأول] جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية٠

[الفرع الثاني] جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة٠

[الفرع الثالث] جريمة الاعتداء علي تصميم موقع٠

[المطلب الثالث] جرائم الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة، وسلامة الشبكة المعلوماتية٠

[الفرع الأول] جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة ٠

[الفرع الثاني] جريمة الاعتداء علي سلامة الشبكة المعلوماتية ٠

(ISSN: 2356 - 9492)

المبحث الثالث ـــــ الأحكام الإجرائية لجرائم تقنية المعلومات ٠

[المطلب الأول] اجراءات الاستدلال الخاصة بجرائم تقنية المعلومات ٠

[الفرع الأول] مأموري الضبط القضائي في جرائم تقنية المعلومات ٠

[الفرع الثاني] إجراءات الاستدلال في جرائم تقنية المعلومات ٠

[المطلب الثاني] اجراءات التحقيق الخاصة بجرائم تقنية المعلومات ٠

[الفرع الأول] التحفظ علي البيانات والمعلومات ٠

[الفرع الثاني] التفتيش في النظم المعلوماتية٠

[الفرع الثالث] تسليم المعلومات ٠

[المطلب الثالث] اجراءات المحاكمة الخاصة بجرائم تقنية المعلومات ٠

[الفرع الأول] الاختصاص المكاني لجرائم تقنية المعلومات ٠

[الفرع الثاني] الاختصاص القضائي بنظر جرائم تقنية المعلومات ٠

* خاتمة ٠

* التوصيات ٠

* قائمة المراجع ٠

* الفهرس ٠

والله الموفق والمستعان ،،،

المبحث الأول

ماهية الجرائم المعلوماتية

تمهيد وتقسيم:

لقد عرف القرن العشرين تطوراً مذهلاً في مجال الاتصالات، وشكلت الشبكة المعلوماتية الدولية مثار هذا القرن التي امتدت عبر كامل انحاء المعمورة وربطت بين شعوبها، فأصبحت وسيلة للتعامل اليومي بين أفراد مختلف الطبقات والمجتمعات ٠

وأمام اختلاف العقليات والمستويات العلمية لمستعملي شبكة الإنترنت ظهرت ممارسات غير مشروعة، فأصبحت هذه الشبكة أداة ارتكابها أو محلاً لها حسب الحالة، مما أدي إلي ظهور طائفة جديدة من الجرائم العابرة للحدود، والمختلفة عن باقي الجرائم التقليدية، وقد سميت بالجرائم المعلوماتية أو الالكترونية أو جرائم الإنترنت ( ) ٠

وتأسيساً علي ما تقدم، سوف نتناول في المطلب الأول تعريف الجريمة المعلوماتية، بينما نتعرض في المطلب الثاني للتطور التاريخي لها ٠

[المطلب الأول] تعريف الجريمة المعلوماتية ٠

[المطلب الثاني] التطور التاريخي للجريمة المعلوماتية ٠

المطلب الأول

تعريف الجريمة المعلوماتية

علي الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات علي جميع الأصعدة، وفي شتي ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، والانحراف عن الاغراض المتوخاة منها، إذ تمثلت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة جرائم تقنية المعلومات أو ما يسمي بالجرائم الالكترونية، ليس هذا فحسب، بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية ( ) ٠

(ISSN: 2356 - 9492)

تبعاً لذلك اعتبرت الجرائم المعلوماتية أثراً من الأثار السلبية التي خلفتها التقنية العالية، كونها تطال في اعتداءاتها قيماً جوهرية تخص الأفراد والمؤسسات والدول في كافة النواحي الاقتصادية، والثقافية، والأمنية ٠ كما أن هذه الجرائم تركت في النفوس شعوراً بعدم الأمان، وغياب الثقة، الأمر الذي يؤدي إلي تهديد هذه التقنية لحياة الأفراد وأمنهم ٠

إنه نوع جديد من الإجرام، وجد في بيئة جديدة، بيئة افتراضية، مقوماتها معلومات وأرقام، أطلق عليها اسم الجريمة المعلوماتية ( ) ٠

والحقيقة الدقيقة أن المشرع المصري ـــــــ وكذلك الفرنسي ـــــــ لم يورد في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م تعريف معين للجريمة المعلوماتية ٠ لذلك جد الفقه واجتهد في وضع تعريف محدد ومنضبط لمفهوم الجريمة المعلوماتية، فذهب جانب من الفقه إلي أنها:" كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلي الاعتداء علي الأموال المادية أو المعنوية ( ) ٠ بينما ذهب جانب أخر إلي أنها:" كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلي المعلومات المخزنة داخل الحاسب الآلي، والتي تحول عن طريقه ( ) ٠ في حين ذهب جانب أخير إلي أنها: " كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به ، التي يحميها قانون العقوبات، ويفرض عليها عقاباً ( ) ٠

وتعرفها منظمة التعاون الاقتصادي والتنمية ـــــــ خلال مؤتمر عقد في باريس سنة ١٩٨٣م ـــــــ بأنها :" كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به، يرتبط بالمعالجة الالية للبيانات أو نقلها " ٠ ويعرفها أيضاً مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا عام ٢٠٠٠م بأنها:" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها فـــــــي البيئة الإلكترونية" ٠

وقد عرفها المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات بأنها:" كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون " ٠ كما عرفها المشرع السعودي في المرسوم الملكي رقم ١٧ لسنة ١٤٢٨ه بأنها: " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام" ٠ وكذلك عرفتها وزارة الداخلية الفرنسية بأنها:" الجرائم

التي ترتكب بواسطة الإنترنت أو باستخدام أنظمة الكمبيوتر وانتهاكها للبرامج مثل الاحتيال وخيانة الأمانة" ٠

ومن وجهة الباحث، فقد عرف الجريمة المعلوماتية بأنها: " كل سلوك غير مشروع، يتم باستخدام أي وسيط من الوسائط الإلكترونية ، ويتعلق بالمعالجة الإلكترونية للبيانات أو المعلومات " ٠

المطلب الثاني

التطور التاريخي للجريمة المعلوماتية

شهد العالم في السنوات القليلة الماضية عصراً جديداً من التقدم العلمي وما صاحبه من تطور ونهضة غير مسبوقة في كافة المجالات اليومية، وكان من أبرزها التقدم الحاصل في مجال تقنية المعلومات والاتصالات، وما ترتب عليه من إحداث ثورة تنموية بشرية على جميع المستويات والأصعدة المحلية والعالمية، فمن خلالها استطاع الإنسان أن يرصد ويتابع كل ما يدور ويجري حوله في جميع أنحاء العالم بالصوت والصورة منذ اللحظة الأولي، وأصبحت عملية تبادل المعلومات والمعارف تتم بسهولة ويسر، كما أدي الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة إلى تدفق المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية بحرية وسلاسة ٠ ( )

ولقد صاحب التطور التكنولوجي الهائل الذي أحدثته تقنية المعلومات ظهور بعض الفئات التي سعت إلي تحويل هذه التقنية إلي وسيلة إلي ارتكاب الجرائم، وأصبح يطلق عليها الجرائم الإلكترونية أو المعلوماتية ٠ ولقد حرص المجتمع الدولي علي مواجهة جرائم تقنية المعلومات كأمر واقع يستلزم وجود قواعد قانونية دولية متفق عليها لتنظيم مواجهتها ، ومن أبرز الصكوك الدولية والإقليمية التي اهتمت بهذه الجرائم، اتفاقية مجلس أوربا بشأن الجريمة السيبرانية لعام ٢٠٠١م ، والبروتوكول الإضافي للاتفاقية المعني بتجريم أفعال ذات طبيعة عنصرية أو كراهية الأجانب، المرتكبة بواسطة النظم الحاسوبية، وقراري الاتحاد الأوربي لعام ٢٠٠١م بشأن الاحتيال والتزوير في وسائط الدفع غير النقدية، ولعام ٢٠٠٥م بشأن الهجمات ضد نظم المعلومات٠ وقد اعتمد مجلس وزراء الاتحاد الأوروبي في ٢٧ نوفمبر ٢٠٠٨م ، استراتيجية المجلس التي تهدف إلى تعزيز مكافحة "الجرائم الإلكترونية" ( ) ٠ هذا بالإضافة إلي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ م، والقانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات لعام ٢٠٠٤م، ومشروع

(ISSN: 2356 - 9492)

اتفاقية الاتحاد الأفريقي بشأن إنشاء إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا لعام ٢٠١٢م ( ) ٠

وفي مصر، صدر القانون رقم ١٧٥ لسنة ٢٠١٨م ـــــ ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠م ـــــ بشأن مكافحة جرائم تقنية المعلومات، ولم يكن هو الخطوة الأولي في مجال التشريع المعلوماتي، بل سبقه العديد من الاجتهادات التشريعات التي تناولت بعض الصور لهذه الجرائم، ومن بين هذه التشريعات أو القوانين؛ قانون التوقيع الإلكتروني رقم [١٥] لسنة ٢٠٠٤م ، وقانون حماية الملكية الفكرية رقم [٨٢] لسنة ٢٠٠٢م ، وقانون الاتصالات رقم [١٠] لسنة ٢٠٠٠٣م، وقانون المحاكم الاقتصادية رقم [١٢٠] لسنة ٢٠٠٨م ٠

وفي فرنسا، فقد أدرج المشرع الجنائي نصوص مكافحة جرائم تقنية المعلومات في إطار مدونتها العقابية [المواد ٣٢٣-١إلي ٣٢٣-٧] من قانون العقوبات الفرنسي الجديد ، تحت عنوان " الاعتداءات علي نظام المعالجة الآلية للمعطيات" ٠ وقد كان قانون العقوبات الفرنسي من أوائل التشريعات التي عالجت هذه الجريمة حين صدر عام ١٩٩٢ وبدأ تطبيقه في عام ١٩٩٤م ونص عليها في المواد [٣٢٣-١إلي٣٢٣-٧] وهي ذاتها الجرائم التي كان منصوصاً عليها ضمن المواد [٤٦٢-٧ إلي ٤٦٢-٩] من قانون العقوبات المعدل في عام ١٩٨٨م، بالإضافة للتعديلات التي تمت في قانون العقوبات الجديد عام ١٩٩٤م٠

وفي ذات السياق، أصدرت دولة الكويت القانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات، ودولة الأمارات العربية المتحدة بإصدارها القانون الاتحادي رقم ٥ لسنة ٢٠١٢ وتعديلاته، والمملكة العربية السعودية في المرسوم الملكي رقم ١٧ لسنة ١٤٢٨ ٠ وتعد هذه الخطي التشريعية الحثيثة وبحق انعكاس صادق لعمق المشكلة التقنية والممارسات غير المشروعة لوسائل التقنية المعلوماتية بما تمثله من تهديد حقيقي لحقوق جديرة بالحماية القانونية ٠

المبحث الثاني

الأحكام الموضوعية لجرائم تقنية المعلومات

تقسيم:

لم تعد القواعد العامة في قانون العقوبات كافية لمواجهة التعاملات الإلكترونية وما قد ينجم عنها من جرائم إلكترونية، ومن ثم بدت الحاجة إلي تشريعات لمواجهة تلك الجرائم ٠ ونظراً لحداثة الجرائم الإلكترونية ، وظهور هذا النوع من الجرائم مع كل تقنية حديثة من تقنيات المعلومات٠ فقد سعي المشرع المصري لمواكبة هذا التطور الحاصل، وذلك من خلال استحداث نصوص وأحكام لمواجهة ومكافحة الجرائم الإلكترونية أو المعلوماتية ( ) ٠

وتأسيساً علي ما تقدم، سوف نتناول هذا المبحث من خلال المطالب الأتية:

[المطلب الأول] جرائم الدخول غير المشروع، وتجاوز حدود الحق في الدخول، والاعتراض غير المشروع

[المطلب الثاني] جرائم الاعتداء علي سلامة البيانات، والبريد الإلكتروني، وتصميم الموقع ٠

[المطلب الثالث] جرائم الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة، وسلامة الشبكة المعلوماتية ٠

المطلب الأول

جرائم الدخول غير المشروع، وتجاوز حدود الحق في الدخول، والاعتراض غير المشروع

تقسيم:

نص المشرع الجنائي علي عدد من الجرائم المتعلقة بالاعتداء علي سلامة شبكات وانظمة وتقنيات المعلومات ، في الفصل الأول من الباب الثاني من القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات٠ وعلي هدي مما تقدم، سوف نتناول هذا المطلب موزعاً علي الفروع الآتية:

(ISSN: 2356 - 9492)

[الفرع الأول] جريمة الدخول غير المشروع ٠

[الفرع الثاني] جريمة تجاوز حدود الحق في الدخول ٠

[الفرع الثالث] جريمة الاعتراض غير المشروع ٠

الفرع الأول

جريمة الدخول غير المشروع

نصت المادة [١٤] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة الدخول غير المشروع بقولها :" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، علي موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه ٠ فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة علي ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين" ٠

وفي فرنسا، نصت المادة [٣٢٣-١] من قانون العقوبات الفرنسي علي أنه:" يعاقب علي الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الألية للمعطيات بالحبس لمدة عامين وغرامة مقدارها ٦٠ ألف يورو ٠ وإذا ترتب علي ذلك حذف أو تغيير لمعطيات النظام أو إتلاف تشغيل النظام، تكون العقوبة الحبس ثلاث سنوات وغرامة قدرها ١٠٠.٠٠٠ ألف يورو ٠ وإذا ارتكبت الجرائم المشار إليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، فإن العقوبة تزيد إلي الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو " ( ) ٠

والعلة من تجريم هذا النص، هو الحفاظ علي الحسابات الخاصة والنظم المعلوماتية من الدخول غير المشروع فيها من قبل الغير٠ وقد استلزم المشرع الجنائي، لقيام جريمة الدخول غير المشروع قانوناً توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الدخول غير المشروع: بادئ ذي بدء، المطلع علي التشريعات الجنائية المختصة بمكافحة جرائم تقنية المعلومات، يجد جميعها تجرم الدخول غير المشروع للأنظمة المعلوماتية، وتبتدئ التجريم بهذه الجريمة؛ فلا يوجد تشريع خاص في الجرائم الإلكترونية يخلو من النص عليها، وهذا الأمر لم يكن عفوياً

وإنما يحمل دلالات فنية وقانونية علي أهمية هذه الجريمة؛ فمعظم الجرائم الإلكترونية يتطلب ارتكابها المرور بجريمة الدخول غير المشروع، فهي بوابة مرور إجباري لا مناص من عبورها لارتكاب غيرها من الجرائم؛ فهي ـــ بحق ـــ أم الجرائم الإلكترونية ( ) ٠ فقد أدي ربط الحاسبات الآلية بعضها بالبعض الآخر عن طريق شبكات المعلومات إلي سرعة انتقال المعلومات من جهة، وإلي سهولة التطفل عليها من جهة أخري عن طريق استخدام " المودم" حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يتواجدون فيها بالدخول أو الولوج إلي الحاسبات الآلية المستهدفة، ودون أي مساس مادي بحق ملكية الغير، أو ترك أي أثر يدل علي انتهاك المعلومات أو نسخها ٠ ( )

وتكمن أهمية هذه الجريمة؛ في عدم إمكانية تجريم مجرد الولوج للنظام المعلوماتي وفقاً للنصوص العقابية التقليدية، فالنظام المعلوماتي والمواقع الإلكترونية لا تعتبر أماكن خاصة أو مساكن حتي تتمتع بالحماية الجنائية المقررة لهذه الأماكن في حال دخولها دون وجه حق ٠ كما أن الدخول إلي النظام المعلوماتي والوصول إلي البيانات والمعلومات، كون هذه الأخيرة ضعيفة داخل النظام، بحيث يمكن الاعتداء عليها بسهولة، وتتميز كذلك بالضخامة والتنوع في ذات الوقت، هذه الاعتبارات دعت التشريعات إلي توفير حماية جنائية للنظام المعلوماتي من الدخول غير المشروع ( ) ٠

ومن الجدير بالإشارة، أن الدخول غير المشروع للأنظمة المعلوماتية يهدد العديد من المصالح المحمية، حكومية وفردية وتجارية، إذ أن أغلب أنظمة الحواسيب تمتلكها الحكومة، والعديد من الحكومات تعتمد في إدارتها لمرافقها علي نظام الحكومة الإلكترونية٠ كما يهدد الدخول غير المشروع بعض الأنظمة المعلوماتية، أمن الدولة الوطني، كالاطلاع علي معلومات تمس أمن الدولة أو الوصول إلي أنظمة التحكم في المفاعلات النووية٠ بالإضافة إلي الأنظمة المعلوماتية قد تحتوي علي معلومات تتصل بالحياة الخاصة للأفراد، ويشكل الوصول إليها عن طريق الدخول غير المشروع انتهاكاً للحق في الخصوصية، وفي جريمة الدخول غير المشروع اعتداء علي المصالح التجارية من خلال الاطلاع علي الأسرار التجارية والاعتداء علي حقوق الملكية الفكرية، وزعزعة الثقة في المعاملات التجارية الالكترونية ( ) ٠

ومحل هذه الجريمة ، وفقاً لما جاء بنص المادة (١٤) من قانون جرائم تقنية المعلومات السالف ذكرها، إما أن يكون موقعاً إلكتروني ، أو حساب خاص ، أو نظام معلوماتي ٠ وقد بين المشرع الجنائي ماهية كل مصطلح من هذه المصطلحات ، في

(ISSN: 2356 - 9492)

المادة الأولي (تعريفات) من الباب الأول من القانون سالف الذكر، وذلك علي النحو التالي:

[أولاً] الموقع الإلكتروني: مجال أو مكان افتراضي له عنوان محدد علي شبكة معلوماتية، يهدف إلي إتاحة البيانات والمعلومات للعامة أو الخاصة ٠

[ثانياً] الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول علي الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي ٠

[ثالثاً] النظام المعلوماتي: مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية ٠

ويشترط في محل الجريمة أن يكون محظوراً الدخول في هذه المواقع أو الحسابات الخاصة أو النظم المعلوماتية ٠

[ثانياً] الركن المادي لجريمة الدخول غير المشروع: يقصد بمصطلح " الدخول غير المشروع إلي النظام المعلوماتي" في مجال تقنية المعلومات ( ) كافة الأفعال التي تسمح بالدخول إلي نظام معلوماتي والإحاطة أو السيطرة علي المعطيات التي يتكون منها أو الخدمات التي يقدمها ( ) ٠ ويتحقق الركن المادي لهذه الجريمة؛ بأي فعل إيجابي من شأنه الولوج إلي موقع الكتروني أو حساب شخصي أو نظام معلوماتي، ومن ثم يتطلب ـــــ بداءة ـــــ لدخول المواقع أو الحسابات الخاصة أو الأنظمة المعلوماتية، وجود حاسب آلي أو أي جهاز تقني أو وسيلة تقنية معلومات يستخدمها الجاني، وكذلك توافر خدمة الانترنت بما يسمح للجاني بالوصول إلـــــــــي المواقع الالكترونية أو الحسابات الخاصة الموجودة علي مواقع الانترنت ( ) ٠ ويستوي أن يكون الدخول غير المشروع علي الموقع أو الحساب الخاص أو النظام المعلوماتي بأي طريقة كانت، مثل استخدام كلمة السر الحقيقية متي كان الجاني غير مسموح له باستخدامها، أو عن طريق أي من البرامج التي تمكن من الدخول إلي المواقع أو نظم المعلومات أو الحسابات الخاصة، أو باستخدام صفحة أو رقم خاص بشخص آخر مصرح له بالدخول، كما يستوي أن يكون الدخول عن طريق حاسب آلي متصل بالإنترنت أو بهاتف من الهواتف الذكية التي تتصل بالإنترنت أو بأي وسيلة أخـري ( ) ٠

كما يتحقق فعل الدخول غير المشروع متي كان الجاني قد دخل إلي النظام كلية أو جزء منه كالدخول إلي طرفيه الحاسب أو شبكية الاتصال أو البرامج، وكذلك يتحقق الدخول غير المشروع متي كان مسموحاً للجاني بالدخول لجزء معين في

البرامج حيث تجاوزه إلي جزء آخر غير مسموح له بالدخول فيه ٠ ومن ثم يخرج من نطاق هذه الجريمة قيام الجاني بالدخول إلي برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كذلك لا تقوم الجريمة متي اقتصر دور الجاني علي مجرد قراءة الشاشة إذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع إلي النظام المعلوماتي ، إذ لابد أن يكون الجاني قد اتخذ سلوكاً إيجابياً في كسر الحماية الفنية ـــــ في حالة وجودها ـــــ للدخول إلي نظام المعلومات محل الجريمة ( ) ٠

كما يشمل الركن المادي لهذه الجريمة أيضا، الدخول عن طريق الخطأ، إذا اقترن هذا الدخول بالبقاء بالموقع أو الحساب الخاص أو النظام المعلوماتي٠ وقد نصت المادة [١٤] من قانون مكافحة جرائم تقنية المعلومات علي ذلك بقولها: " كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، علي موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه" ٠ فالبقاء بعد الدخول خطأ؛ يعني أن الجاني لم تنصرف نيته منذ البداية إلي دخول الحساب أو الموقع أو النظام المعلوماتي ولكنه دخله مصادفة أو قام موقع آخر مثلاً بتحويله إليه وهو ليس له حق الدخول عليه، ولكنه لم ينصرف حالاً أي لم يخرج من النظام وانصرفت إراداته إلي البقاء فيه، فهنا يعد بقاؤه في الموقع أو الحساب أو النظام المعلوماتي غير مشروع ( ) ٠ وينصرف الحكم السابق كذلك إلي حالة الشخص المسموح له بالدخول إلي جزء في النظام المعلوماتي ثم يدخل إلي مكان آخر غير مصرح له به أو يبقي مدة أكثر من تلك المدة المسوح له البقاء فيها داخل النظام ٠ ويري البعض أن هذه الجريمة تقوم بسلوك سلبي؛ فرغم دخول الجاني بإرادته ورغم علمه بأن ذلك غير مشروع، فهو يرفض الخروج من النظام فهو سلوك سلبي تقوم به الجريمة ٠

ومن ثم يمكن تعريف البقاء غير المصرح به بأنه :" تواجد الشخص داخل النظام المعلوماتي، دون تصريح من صاحب الإذن في التواجد في النظام في الحالات التي يكون فيها الدخول مشروع، أو لكون الدخول غير مجرم ، ويتصور ذلك في حالتين ـــــ [الأولي] أن يكون الدخول مشروط بالبقاء بفترة زمنية محددة [والثانية] أن يدخل الشخص إلي النظام المعلوماتي بطريق الخطأ ٠ ويستمر في التواجد في النظام علي الرغم من اكتشافه لذلك ( ) ٠

ومن الجدير بالإشارة، أنه لا يشترط لقيام الجريمة، أن ينجح الجاني في الوصول إلي أي من البرامج أو المعلومات كي يتم النشاط الإجرامي لها ، بل يكفي مجرد الدخول غير المشروع إلي الحاسب الآلي ، فإذا كانت العلة من وراء تجريم الدخول غير المشروع إلي النظام المعلوماتي، هي حماية البرامج والمعلومات من

(ISSN: 2356 - 9492)

الوصول إليها والتلاعب بها وسرقتها ( ) إلا أن هذه الجريمة هي من الجرائم التي تمثل تعدياً محتملاً علي الحق، وليست من الجرائم التي تتمثل في تحقق الاعتداء علي الحق الذي يحميه القانون ( ) وعليه تعتبر جريمة الدخول غير المشروع إلي النظام المعلوماتي من الجرائم الشكلية التي لا يستلزم لقيامها تحقق نتيجة معينة ( ) ٠ وهو ما أخذ به المشرع المصري ـــــ وكذلك الفرنسي ـــــ باعتبار أن فعل الدخول غير المشروع إلي نظام الحاسب الآلي يستوجب العقاب بمجرد حدوث هذا الدخول، وبعبارة أخري فإن الدخول المجرد في ذاته معاقب عليه، حتي ولو لم يترتب علي الدخول أي ضرر أو فائدة للجاني( ) ٠

كما لا يشترط كذلك لقيام الجريمة، استلزام صفة معينة في شخص الجاني، فقد يكون محترفاً أم غير محترف، عاملاً في الجهة التي حدث فيها الدخول غير المشروع أو من غير العاملين لديها ( ) ٠ كذلك لا يشترط في الدخول غير المشروع، أن يتم علي قواعد البيانات كلها أو جزء من نظام التشغيل ( ) ٠ ويري البعض في هذا الصدد بأن الدخول له مدلول معنوي، حيث أن الدخول إلي النظام المعلوماتي أو النظام الالكتروني يشبه الدخول إلي ذاكرة الإنسان، كما أن له مدلول مادي يتمثل في ان الشخص قد حاول الدخول أو دخل بالفعل إلي النظام المعلوماتي ٠

والحقيقة الدقيقة، أن المشرع الجنائي قد استلزم لقيام الجريمة قانوناً أن يكون الدخول إلي النظام المعلوماتي أو البقاء فيه، بدون وجه حق؛ أي أن يكون الجاني غير مصرح له بالدخول علي النظام أو محظور عليه ذلك، فيعد الدخول إلي المواقع الإلكترونية أو الأنظمة المعلوماتية أو الحسابات الخاصة، غير مشروع إذا كان بدون رضاء صاحبه، أو بدون إذن الشخص المسئول عن النظام، أو أن يكون الجاني غير مخولاً بالبقاء فيه، أو أن يتجاوز المدة الزمنية المسموح له للبقاء فيه، علي الموقع أو الحساب الخاص أو النظام المعلوماتي ( ) ٠

وغني عن البيان، أن الدخول يعد غير مشروع متي كان مخالفاً لإرادة صاحب النظام أو من له حق السيطرة عليه ( ) ٠ وعليه فلا يكون هناك تجريم في حالة ما إذا كان الدخول إلي النظام بالمجان ومتاحاً للجمهور، ففي مثل هذه الحالة يصبح الدخول إلي النظام حقاً من الحقوق ( ) ٠ والذي نود التأكيد عليه، أن جريمة الدخول غير المشروع إلي النظام المعلوماتي هي من الجرائم الوقتية، أما جريمة البقاء غير المشروع فهي جريمة مستمرة، لاستغراقها مدة من الزمن قد تطول أو تقصر ٠ ومن أمثلة هذه الجريمة، قيام الجاني باستخدام برامج اختراق لأجهزة الحسابات، ليتمكن من خلالها اختراق الحاسب الآلي للمجني عليها، وتشغيل الميكروفون والكاميرا الخاصة به للتجسس عليها وعلي أسرتها والتقاط صور لها أثناء

تواجدها بمنزلها دون علمها٠ وفي قضية أخري ، قام أحد الأشخاص الفرنسيين بالدخول عن طريق الانترنت بطريق الغش إلي نظام المعالجة الآلية الخاصة بأحد المستشفيات، والمحجوز بها زوجته، وقيامه بتغيير المعلومات الطبية الخاصة بها مما أدي إلي وفاتها ( ) ٠

وقضي في هذا الخصوص من محكمة جنح مستأنف في فرنسا بإدانة أحد مندوبي شركة فرنسا للاتصالات والذي كان مكلفاً بالرقابة والإشراف علي سنترال تليفوني بتهمة الدخول بطريق غير مشروع إلي نظام المعالجة الآلية للمعلومات، لأنه قام بتوصيل جهاز المنيتل بخط التجارب وظل متصلاً بشكل مستمر(طوال النهار) بأحد مقدمي الالعاب التليماتيه والذي كان يمنح جوائز علي شكل بونات شراء تتناسب مع مدة التوصيل أي أن الجوائز تزداد تبعاً لزمن الاستعمال أو الاتصال ٠ وكانت تتم إزالة هذا الاستخدام غير القانوني بطريقة فنية خاصة ٠ وقد أحيل المتهم إلي المحكمة بتهمة السرقة إلا أن المحكمة لم تأخذ بهذا التكييف لأن محكمة النقض سبق أن قضت بأن الاتصالات التليفونية هي نوع من الخدمات لا يمكن حيازتها ٠ وانتهت المحكمة إلي إدانة المتهم الذي الحق إضراراً بشركة فرانس تيلكوم تقدر بمبلغ ٧٥٠٠٠٠ فرنك عن جريمة الدخول بطريق غير مشروع إلي نظام المعالجة الآلية للمعلومات والتي يكفي لقيامها ثبوت علم المتهم بأنه ليس له الحق في الدخول إلي النظام ( ) ٠ كما قضت محكمة جنح paris بإدانة متهم عن جريمة الدخول بدون وجه حق إلي نظام المعالجة الآلية للمعلومات في واقعة غريبة من نوعها حيث كان هذا المتهم يقدم نفسه علي أنه مندوب المجموعة الفيدرالية FBI لكي يحصل من الشركات علي توريد خدمات تليفونية نظير مبلغ ٢٥٠٠٠٠ دولار ٠

والذي نود التأكيد عليه، أن مشرعنا الجنائي لم يشترط لقيام الجريمة أن يكون النظام محمي بحظر الدخول عليه ٠ كما لم يشترط المشرع الفرنسي أيضاً أن يكون النظام المعلوماتي محمي بأحد صور الحماية، بل جعل التجريم يشمل المواقع المحمية وغير المحمية ٠ وفي السياق ذاته، رأت الجمعية الوطنية الفرنسية أنه من غير المناسب التمسك بهذا الشرط، لأنه سوف يترتب عليه قصر الحماية الجنائية علي الأنظمة المحمية بواسطة أجهزة الأمن، ومن ثم يستبعد من مجال التطبيق النص علي أفعال الولوج التي ترتكب ضد الأنظمة العامة المفتوحة للعامة ٠

وخلاصة القول، لكي يتحقق الركن المادي في هذه الجريمة، فلابد أن يتحقق فعل الدخول غير المشروع أو البقاء غير المشروع أو يتحقق الأثنين معاً ٠

(ISSN: 2356 - 9492)

[ثالثاً] الركن المعنوي لجريمة الدخول غير المشروع: هذه الجريم عمدية، يتمثل الركن المعنوي لها في القصد الجنائي العام بعنصريه العلم والإرادة، فيتعين أن يكون الجاني عالماً بأنه ليس من حقه دخول الموقع أو الحساب الخاص أو النظام المعلوماتي ، أو أنه دخل بطريق الخطأ ولكنه رفض الخروج، فمن يرفض الخروج بعد دخوله خطأ يتحقق في جانبه القصد الجنائي العام الذي تقوم به الجريمة ، كما يتعين أن تتجه إرادة الجاني إلي الدخول أو البقاء بعد الدخول الخاطئ٠ ومن ثم لا يقوم القصد الجنائي إذا وقع الجاني في خطأ يتعلق بحقه في الدخول أو حقه في البقاء بعد الدخول الخاطئ أو كان يعتقد خطأ أنه مسموح له بالدخول أو البقاء، وتلك مسألة تخضع لتقدير قاضي الموضوع ( ) ٠ وقد قضي بتوافر الركن المادي في جريمة البقاء وكذلك علي توافر القصد الجنائي في هذه الجريمة في الحالة التي يقوم فيها مستخدمو الشركات باستعمال الكمبيوتر الخاص بعملهم في ممارسة العاب التسلية الإلكترونية، الأمر الذي يكلف شركاتهم مبالغ كبيرة نظير استعمال الخط التليفوني ( ) ٠

والذي نود لفت الانتباه إليه في هذا المقام ، أن القصد الجنائي يعد متوافراً سواء في الدخول أو البقاء، بغض النظر عن الباعث فإذا كان قصد المتهم من الدخول إلي نظام معين هو أن يثبت للمسئولين أن هناك ثغرات في أنظمتهم المطبقة ، فإن ذلك يعتبر من قبيل البواعث التي لا تنفي القصد الجنائي، وتطبيقاً لذلك فقد قضي بوقوع الجريمة من مهندس للكمبيوتر أراد أن يثبت لأحد البنوك قدرته الفنية علي اختراق أنظمة البنك حتي يفوز بعقد تدريب كوادر البنك، فقام باختراق أنظمة هذا البنك علي الرغم من تعدد وسائل الحماية التي وضعها البنك ضد الاختراق ٠ لذا قضي بوقوع الجريمة من هذا المهندس ولو كان الجهاز الإلكتروني الذي قام المتهم بتفكيكه كان قد استغني عنه البنك صاحب الجهاز واستطاع المتهم الحصول عليه من تاجر آخر لديه هذا الجهاز وتمكن بفضل ذلك من التعرف علي بيانات مسجلة في هذا الجهاز واستعملها في اختراق نظام البنك ( ) ٠

[رابعاً] عقوبة جريمة الدخول غير المشروع: ميز المشرع الجنائي في العقوبة بين حالتين:

(الحالة الأولي) في حالة القيام بالفعل دون ترتب نتيجة: عاقب القانون في هذه الحالة، أي علي الدخول أو البقاء غير المشروع ـــ دون حدوث ضرر ـــ بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين٠

(الحالة الثانية) في حالة القيام بالفعل مع ترتب نتيجة، من جراء الدخول غير المشروع أو البقاء دون وجه حق: عاقب القانون علي الدخول أو البقاء غير المشروع إلي النظام المعلوماتي بعقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، إذا نتج عن الدخول أو البقاء غير المشروع ضرر يتمثل في إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة علي ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي٠

وعليه، فقد اعتبر مشرعنا الجنائي الإضرار بالنظام المعلوماتي أو الحساب الخاص أو الموقع الإلكتروني، ظرفاً مشدداً للعقاب، وذلك في الحالات الأتية:

[١] الاتلاف: ويقصد به تدمير أو محو تعليمات البرامج ذاتها وجعلها غير صالحة للعمل، ويجب لقيام الجريمة أن يقع علي العناصر غير المادية التي يتكون منها الحاسب الآلي، كالمعلومات والبيانات والبرامج علي اختلاف أنواعها ووظائفها ٠ ومثال ذلك تسريب فيروس معلوماتي للنظام ليدمره أو علي الأقل ليبطئ من أدائه، أو ليشوه هذا الأداء أو لإيقافه عن العمل أو عدم استجابة النظام المعلوماتي للأوامر ٠

[٢] المحو: ويقصد به إزالة جزء من المعطيات المسجلة أو المخزنة في نظام معالجة البيانات خاصة ذاكرة الحاسب الآلي أو علي دعامة موجودة داخل النظام، ويستوي أن يكون المحو كلياً أو جزئياً ٠

[٣] التغيير: ويعني استبدال المعلومات أو المعطيات الموجودة داخل النظام أو الموقع أو الحساب الخاص بمعطيات أو معلومات أو بيانات أخري عن طريق التلاعب في البرامج، وذلك بالإمداد بمعطيات مغايرة أو بيانات أو معلومات عن تلك التي صمم البرنامج لأجلها ٠

[٤] النسخ: ويعني الحصول علي نسخة من معلومات أو بيانات الموقع أو الحساب الخاص أو النظام المعلوماتي ٠ وتتمثل هذه العملية بقيام الجاني بتخزين ما يحتويه النظام المعلوماتي علي أداة معينة، دون أن يترك وراءه أثر علي النظام المعلوماتي، فلا يحذف أو يضيف بل يأخذ نسخة فقط، فهذه الصورة تتميز بعدم التعرض لأصل البيانات والمعلومات المحفوظة علي النظام المعلوماتي ( ) ٠

[٥] إعادة النشر: وتعني إذاعة ما حصل عليه الجاني من معلومات أو بيانات من الموقع أو الحساب الخاص أو النظام المعلوماتي ( ) ٠

(ISSN: 2356 - 9492)

وفي فرنسا، فقد نص المشرع الجنائي في المادة [٣٢٣-١] سالفة الذكر، علي عقوبة الحبس لمدة عامين وغرامة مقدارها ٦٠ ألف يورو في جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الألية للمعطيات ٠ فإذا ترتب علي ذلك حذف أو تغيير لمعطيات النظام أو تخريب لنظام تشغيل النظام، تكون العقوبة الحبس ثلاث سنوات وغرامة قدرها ١٠٠.٠٠٠ ألف يورو ٠ وإذا ارتكبت الجرائم المشار إليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، فإن العقوبة تزيد إلي الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو " ٠ ويستهدف هذا النص في المقام الأول حماية الولوج إلي نظم المعلومات لا حماية حق الملكية ذاته، ومن جهة أخري استجاب لرغبة ملاك الأنظمة المعلوماتية ٠

ويتحقق الركن المادي لهذه الجريمة بمجرد شروع أي شخص ـــ ليس له الحق ـــ في الدخول ، أو تدخل بالفعل في نظام مبرمج للبيانات ٠ كما يتحقق التواجد غير المشروع بمجرد علم الشخص بأنه تدخل بمحض الصدفة أوعن طريق الخطأ ـــ وعلي نحو غير مشروع ـــ في نظام مبرمج للبيانات، ويستمر في حالة اتصال به بدلاً من الانفصال عنه في الحال ( ) ٠ وهذه جريمة من جرائم الامتناع التي يصعب تقديم دليل اثبات فيها، حيث يزعم المتهم دائماً حال القبض عليه أنه كان علي وشك الانفصال عن النظام المعتدي عليه ٠ والجدير بالتنويه، أنه يستوي أن يكون الدخول أو الولوج إلي النظام المعلوماتي المعتدي عليه كلياً أو جزئياً، حيث يستطيع المعتدي في حالة التدخل المقترن بالغش أن يدعي بسهولة بأن تجوله كان محدوداً بجزء ضيق جداً مـــــن النظام ٠ ولا يمكن التحقق من مثل هذا الادعاء مـــن الناحيـــة العمليـــــة ٠ وبالنسبة للركن المعنوي، يجب أن يتوافر لدي الفاعل قصد خاص علاوة علي القصد العام والذي يتمثل في نية الغش ٠ ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وبسوء نية وبغرض خداع الغير ٠ ويتمثل قصد الغش في معرفة المتهم بأنه قد ولج أو تواجد في نظام البيانات المبرمج ضد رغبة صاحب النظام وأياً كان الدافع إلي ذلك ( ) ٠

الفرع الثاني

جريمة تجاوز حدود الحق في الدخول

نصت المادة [١٥] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة تجاوز حدود الحق في الدخول بقولها: " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين

ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلي موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدي حدود هذا الحق من حيث الزمان أو مستوي الدخول" ٠ والعلة من التجريم؛ هي حظر عمليات الدخول غير المشروع إلي المواقع الإلكترونية أو الحسابات الخاصة أو النظم المعلوماتية، من خلال تجاوز حدود استعمال الحق في الدخول، سواء من حيث الزمان أو مستوي الدخول ٠ وقد اشترط مشرعنا الجنائي، لقيام هذه الجريمة قانوناً، توافر الأركان التالية:

[أولاً] ركن المحل لجريمة تجاوز حدود الحق في الدخول: استلزم مشرعنا الجنائي لقيام جريمة تجاوز حدود الحق في الدخول، أن تقع علي موقع أو حساب خاص أو نظام معلوماتي، وقد سبق لنا بيان ماهية كل مصطلح من هذه المصطلحات، ومن ثم نحيل إليها منعاً للتكرار ٠

[ثانياً] الركن المادي لجريمة تجاوز حدود الحق في الدخول: يتمثل الركن المادي في هذه الجريمة في الدخول المشروع، أو كما أطلق عليه المشرع " الدخول باستخدام حق مخولا له " ٠ لكن مع تعدي حدود هذا الحق من حيث الزمان أو مستوي الدخول٠ والمقصود بتعدي حدود الحق في الدخول من حيث الزمان أو مستوي الدخول، هو مجاوزة الحد المصرح فيه بالدخول، فقد يكون الجاني أحد المصرح لهم بالدخول إلي الموقع أو إلي الحساب الخاص لمدة ساعة أو ساعتين ، لكنه يتجاوز هذه المدة الزمنية بدون مبرر، أو كان مسموحاً له بجزء معين في البرامج ولكنه تعدي هذا الجزء ( ) ٠

ولا يشترط المشرع وسيلة معينة للدخول إلي المواقع الإلكترونية أو الحسابات الخاصة أو الانظمة المعلوماتية، فيستوي أن يتم عن طريق استعمال كلمة سر حقيقة يعلمها الجاني أو رمز أو كود سري أو بأي طريقة أخري٠ كما لم يشترط أن يكون الجاني في هذه الجريمة من المحترفين في أنظمة الحاسب الآلي والأنظمة المعلوماتية عموماً أو لا يحترف مثل هذه الأمور، وكذلك لا يشترط أن يكون التصريح للجاني بالدخول إلي الموقع الالكتروني أو الحساب الخاص أو النظام المعلوماتي بسبب وظيفته أم غير ذلك ( ) ٠ ومن تطبيقات القضاء الفرنسي في هذا الصدد، في دعوي تتلخص وقائعها في قيام بعض العاملين في شركة الخطوط التليفونية باستعمال تلك الخطوط ـــ دون دفع المقابل المالي ـــ للقيام بألعاب " الفيديو جيم" للحصول علي جوائز مقررة لمن يستمر في اللعب مدة معينة ٠ وقد اعمل هذا القضاء وصف البقاء في النظام بطريق الغش، وليس وصف الدخول في النظام، حيث إن هؤلاء العاملين

(ISSN: 2356 - 9492)

كان من حقهم الدخول في النظام أصلاً لمراقبته والإشراف عليه وإصلاح اعطاله ( ) ٠

وغني عن البيان، أنه يخرج من وصف الجريمة ما كان مأذوناً فيه للشخص من الاطلاع عليه من البيانات أو المعلومات مثل الموظف الذي يعمل في حدود صلاحياته الوظيفية، أو ممن يعملون ضمن شبكة معلومات واحدة لا تمنع أصحابها من الاطلاع علي بعضهم علي بعض ، وتثور الجريمة متي تعدي هذا الموظف حدود التصريح أو الصلاحية الممنوحة له ( ) ٠

[ثالثاً] الركن المعنوي لجريمة تجاوز حدود الحق في الدخول: هذه الجريم عمدية، يتمثل الركن المعنوي لها في القصد الجنائي العام بعنصريه العلم والإرادة، فيتعين أن يكون الجاني عالماً بأن من حقه الدخول إلي الموقع أو الحساب الخاص أو النظام المعلوماتي، لكن خلال فترة زمنية محددة أو في جزء معين من الموقع أو الحساب أو النظام، ثم تتجه إرادته إلي تجاوز حدود هذا الحق من حيث الزمان أو من حيث مستوي الدخول٠

[رابعاً] عقوبة جريمة تجاوز حدود الحق في الدخول: نص مشرعنا الجنائي في الماد [١٥] سالفة الإشارة علي عقوبة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، في حالة تجاوز حدود الحق في الدخول إلي المواقع الإلكترونية أو الحسابات الخاصة أو الأنظمة المعلوماتية، سواء من حيث الزمان أو من حيث مستوي الدخول ٠

الفرع الثالث

جريمة الاعتراض غير المشروع

نصت المادة [١٦] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات علي جريمة الاعتراض غير المشروع بقولها:" يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحسب الآلي وما في حكمها " ٠ وتتمثل علة التجريم، في توفير الحماية القانونية للبيانات والمعلومات المتداولة من الاطلاع عليها بدون مسوغ قانوني؛ فالأصل أن البيانات المعروضة علي شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي تتمتع بالسرية، ومن ثم لا يجوز لأحد الاطلاع عليها إلا بمسوغ قانوني مشروع، فإذا قام شخص بالاعتداء

علي هذه الحرمة وانتهاك تلك السرية، فإنه يكون مرتكباً لجريمة الاعتراض غير المشروع ٠

وقد استلزم المشرع لقيام تلك الجريمة توافر الأركان الآتية:

[أولاً] ركن المحل لجريمة الاعتراض غير المشروع: عرف المشرع الجنائي الاعتراض ـــــ في المادة الأولي من قانون جرائم التقنية المعلومات ـــــ بأنه : " مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوي أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق "٠ ويتضح من هذا التعريف أن المقصود باعتراض المعلومات أو البيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، هو معرفة محتوي أو مضمون هذه المعلومات أو البيانات أو ما هو متداول علي الشبكة المعلوماتية أو الحاسب الالي وذلك بالتقاطها باستخدام وسائل فنية وتقنية، تمكن من هذا الاعتراض بدون وجه حق ( ) ٠ ومن أمثلة ذلك، اعتراض الجاني لرسالة شركة ما تتضمن عطاء في أحد المناقصات لمعرفة السعر المقدم منها عن طريق الوسائط الالكترونية، ليقدم سعراً يجعله يفوز بالمناقصة ٠

بيد أنه ينبغي ملاحظة، أن الاعتراض غير المشروع يختلف عن جريمة الدخول غير المشروع عمداً أو الدخول خطأ والبقاء في الموقع، فالحالة الأخيرة لا تتم إلا من خلال قيام الجاني بتشغيل الحاسب الآلي المتصل بالموقع والذي هو محل الدخول غير المشروع للدخول إلي نظامه، أما في حالة الاعتراض؛ فإن الحاسب الآلي يكون مشغلاً بمعرفة صاحب الموقع أو غيره، ويقتصر دور الجاني في هذه الحالة علي مجرد اعتراض المعلومات أو البيانات أو رسائل البريد الإلكتروني، ومن هنا كان الاختلاف بين الجريمتين بوضع نموذج قانوني لكل منها يختلف عن الأخرى، مـــــــــن قبل المشرع المصري ( ) ٠

وقد استلزم المشرع الجنائي، لقيام جريمة الاعتراض غير المشروع قانوناً، أن تقع علي المعلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحسب الآلي وما في حكمها ٠ وقد عرف المشرع البيانات والمعلومات الإلكترونية ـــــ في المادة الأولي من قانون مكافحة جرائم تقنية المعلومات سالف الذكر ـــــ بأنها: " كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف

(ISSN: 2356 - 9492)

والرموز والإشارات والصور والأصوات، وما في حكمها " ٠ كما عرف الشبكة المعلوماتية بأنها: " مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها التبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها" ٠ وعرف الحاسب كذلك بأنه: " كل جهاز أو معدة تقنية تكون قادرة علي التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها او تبادلها أو تحليلها أو للاتصالات " ٠

[ثانياً] الركن المادي لجريمة الاعتراض غير المشروع: يتمثل الركن المادي في هذه الجريمة في الاعتراض، ويتحقق الاعتراض بأي فعل من شأنه الاطلاع علي البيانات أو المعلومات والحصول عليها بدون مسوغ قانوني٠ ويتم هذا الاعتراض باستخدام وسائل فنية، يتمكن الجاني من خلالها بالتجسس المعلوماتي، وذلك بمشاهدة البيانات أو المعلومات أو أي محتوي، بغرض التصنت أو التسجيل أو تغيير المحتوي أو مراقبة كل ما هو متداول، من خلال الولوج إلي داخل النظام المعلوماتي واستخدامه، أو بشكل مباشر عن طريق أجهزة تصنت، ويحدث هذا بتسجيل الأحاديث أو نسخها أو تسجيلها عن طريق خط التليفون العادي أو المحمول، لأنه الوسيلة الوحيدة للاتصال بشبكة الإنترنت٠ فالبيانات والمعلومات الموجودة علي الشبكات في عالم الانترنت، هي عبارة عن معلومات يمكن اعتراضها ببرامج تلتقط كل ما يمر علي الشبكة من بيانات بل وإمكانية التعديل فيها أو نسخها أو تخزينها أو إعادة توجيهها وكذلك إساءة استخدامها، فأي نشاط مادي يقوم به الجاني للتسلل إلي أي اجهزة حاسب آلي وما في حكمها أو أي شبكة معلوماتية لتعطيل أو تخزين أو نسخ أو تسجيل أو تغيير المحتوي أو لإساءة الاستخدام أو تعديل المسار لأية معلومات أو بيانات أو لكل ما هو متداول علي شبكة معلوماتية، والتي ترسل من قبل هذه الأجهزة أو الشبكة المعلوماتية عبر الانترنت، يقوم به الركن المادي لهذه الجريمة ( ) ٠

وحقيقة الحال، فإن الاطلاع أو الحصول علي البيانات أو المعلومات، قد يقع من الجاني نفسه أو من الغير، ولا يشترط أن يشاهد الجاني هذه البيانات بعينه، فيتوافر الاعتراض إذا شاهد الغير هذه البيانات حتي ولو لم يشاهدها الذي أظهرها فعلاً، كما لا يشترط أن يحصل الجاني علي هذه البيانات لنفسه أو بنفسه، وإنما يتحقق الاعتراض إذا تحصل الغير علي هذه البيانات، ولو لم يتحصل الفاعل نفسه عليها، فإذا لم يشاهدها أو يحصل عليها ، فإن الاعتراض لا يكون موجوداً ٠ ولا يشترط

تحميل أو تصوير أو تسجيل هذه البيانات، فالاعتراض يتوافر بمجرد مشاهدتها أو سماعها أو معرفتها أو الحصول عليها، حتي ولو لم يتم تحميلها أو تصويرها ( ) ٠

ويستوي لدي المشرع أن يكون الاطلاع أو المشاهدة قد تمت بشكل متعمد، أي أن الجاني يعلم أماكنها، فدخل عليها وفتح صفحتها لمشاهدتها، أو أنها قد جاءت بشكل عرضي، كأن تكون هناك بيانات مفتوحة علي شاشة الحاسب الالي بمعرفة شخص مخول بفتحها، ويأتي شخص أخر لمشاهدة هذه البيانات علي الرغم من أنه غير مصرح له بمشاهدتها، ولا يشترط لوقوع الجريمة أن يكون الجاني هو الذي قام بإعداد أجهزة معينة لبث هذه البيانات من أجل أن يشاهدها، وإنما يكفي أن تتم المشاهدة حتي ولو لم يكن الجاني له أي دور في إظهار هذه البيانات، ويكفي أن تكون البيانات صالحة للمشاهدة وقت ارتكاب الجريمة حتي ولو أصابها بعد ذلك عطب أو عطل يجعلها غير صالحة للمشاهدة، أو تم حذف هذه البيانات بعد ذلك من الشبكة المعلوماتية أو المكان الذي كانت منشورة به٠

وجدير بالإشارة أنه يشترط في الجاني أن يكون قادراً علي المشاهدة بعينه وقت ارتكاب جريمته، فإن ثبت أنه كان كفيفاً أو كان بصره ضعيفاً جداً وقت وقوع الجريمة، ولا يقدر علي مشاهدة البيانات، فإن الجريمة تنتفي، إما إذا ثبت أنه وقت الجريمة كان قادراً علي المشاهدة بعينه الطبيعية أو باستخدام نظارة طبية أو أداة تمكنه من المشاهدة بوضوح ، فإن الجريمة تتحقق بشأنه، حتي ولو أصبح بعد ذلك كفيفاً ولا يستطيع الابصار٠ كما تتحقق الجريمة أيضاً بمجرد الحصول عليها، سواء تم هذا الحصول بنسخ البيانات علي ذات جهاز الحاسب الآلي أو علي اسطوانات أو كتابتها يدوياً بواسطة أوراق وأقلام أو قد تم طبعها علي أجهزة الطباعة المختلفة ( ) ٠

وغني عن البيان، أنه يجب لقيام الجريمة قانوناً أن يكون الاعتراض بدون مسوغ قانوني مشروع، وعليه فلا قيام للجريمة إذا كان الذي يشاهد البيانات أو يتحصل عليها له صفة قانونية تبيح له مشاهدتها أو الاطلاع عليها ٠

[ثالثاً] الركن المعنوي لجريمة الاعتراض غير المشروع: هذه الجريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة، علم الجاني بأنه يعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أي من أجهزة الحاسب الالي ، فإذا كان المتهم يعتقد أن ما يشاهده أو يتحصل عليه لا يمثل جريمة التقاط، إذ ظن أن تلك البيانات أو المعلومات

(ISSN: 2356 - 9492)

يمكن لأي شخص مشاهدتها والاطلاع عليها دون أي شروط أو متطلبات معينة في شخصية المشاهد أو القائم بالحصول عليها، فلا قيام للجريمة في حقه ٠ كما يجب أن تتجه إرادة الجاني إلي المضي قدماً من أجل المشاهدة أو الاطلاع علي البيانات أو المعلومات، وعليه فلا قيام للجريمة قانوناً إذا كان المتهم لا يريد المشاهدة أو الحصول علي البيانات كمن يريد تحميل برنامج أو موضوع معين، ثم يكتشف أنه قد قام بتحميل هذه البيانات عن طريق الخطأ ٠

[رابعاً] عقوبة جريمة الاعتراض غير المشروع: حدد المشرع الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين

المطلب الثاني

جرائم الاعتداء علي سلامة البيانات، والبريد الإلكتروني، وتصميم الموقع

تقسيم:

نتناول دراسة هذا المطلب من خلال الفروع الثلاثة الآتية:

[الفرع الأول] جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية٠

[الفرع الثاني] جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة٠

[الفرع الثالث] جريمة الاعتداء علي تصميم موقع٠

الفرع الأول

جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية

نصت المادة [١٧] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات علي جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية بقولها:" يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغي كلياً أو جزئياً متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة علي أي نظام معلوماتي وما في حكمه، أياً كانت الوسيلة التي استخدمت في الجريمة " ٠

وفي فرنسا، نصت المادة [٣٢٣-٢] من قانون العقوبات الفرنسي علي أنه: " يعاقب علي تعطيل أو إفساد نظام المعالجة الآلية للمعطيات بعقوبة الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو٠ وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة ، فإن العقوبة تزيد إلي الحبس لمدة سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو" ( )٠ بينما نصت المادة [٣٢٣-٣] من القانون ذاته بأنه:" يعاقب علي الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها بعقوبة الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو٠ وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة ، فإن العقوبة تزيد إلي الحبس لمدة سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو" ( ) ٠

والعلة من التجريم، تتمثل في توفير الحماية الجنائية لسلامة البرامج والنظم المعلوماتية ومحتواها من البيانات والمعلومات من أفعال الاتلاف المادي أو المعنوي، سواء أتخذ ذلك صور التخريب أو الاتلاف أو التعطيل ٠ ويشترط المشرع الجنائي، لقيام جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية ، توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية: استلزم مشرعنا الجنائي لقيام جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية، أن تقع علي البرامج والبيانات أو المعلومات ٠ وقد أشرنا سلفاً إلي معني كل من البيانات والمعلومات الإلكترونية، فنحيل إليه منعاً للتكرار ٠ أما البرنامج المعلوماتي، فيقصد به :" مجموعة الأوامر والتعليمات المعبر عنها بأي لغة أو رمز أو إشارة والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي " (المادة الأولي من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات) ٠

[ثانياً] الركن المادي لجريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية: تعالج هذه المادة عملية تدمير البيانات أو المعلومات أو البرامج عن طريق برامج المعلوماتية، ذلك أن السلوك الإجرامي الذي يقصده المشرع في هذه الجريمة، هو ذلك السلوك الذي لا يتم بطريقة مادية، ولكن عن طريق برامج معلوماتية منها برامج الفيروس المعلوماتي ( ) لأنه لا يتأتى أن يتم التدخل في

(ISSN: 2356 - 9492)

المعلوماتية أو البرامج المعلوماتية عن طريق تقنية المعلومات، ومنها الشبكة المعلوماتية إلا عن طريق برنامج معلوماتي وليس وسيلة مادية ( ) ٠ ويكفي لتوافر الركن المادي لهذه الجريمة إتيان الجاني لأي صورة من هذه الصور التي وردت في المادة [١٧] من القانون سالف الذكر، حيث تؤدي إلي صورة إلي العبث بالمعلومات التي يتضمنها النظام المعلوماتي، وهي:

[١] الاتلاف: ويعني تدمير المعلومات أو البيانات والبرامج أو نظم المعلومات الكترونياً عن طريق المحو تماماً أو المحو جزئياً علي نحو يجعلها غير صالحة لأداء مهامها والغرض المعدة له، أو عن طريق إخفاء المعلومات أو تشويهها بحيث لا يمكن الوصول إليها دون أن يترتب علـــــــــــــــي ذلك محوها تماماً أو بأي طريقة تؤدي إلي فقد منفعتها وعدم صلاحيتها للاستعمال، كما يتم الاتلاف بتدمير الوسائط التي تحتوي علي المعلومات أو البيانات أو البرامج، كما يتم بتشفير هذه المعلومات والاحتفاظ بمفتــاح الشفـــــــــرة ٠

والحقيقة الدقيقة، إن الاتلاف قد يقع علي العناصر أو المكونات المادية للنظام المعلوماتي كأجهزة الحاسب الآلي، وقد يقع علي العناصر غير المادية التي يتكون منها نظام الحاسب الآلي كالمعلومات أو البينات والبرامج علي اختلاف أنواعها ووظائفها ، ومن ثم إذا كان الاتلاف قد وقع علي المكونات المادية المتصلة بالحاسب الآلي وملحقاته كالشاشة أو لوحة المفاتيح أو الفارة أو الأشرطة أو الأقراص الممغنطة وغيرها مما له علاقة بهذا المجال، فلا نكون بصدد الركن المادي لهذه الجريمة، وإنما بصدد جريمة إتلاف مادية معاقباً عليها بموجب قانون العقوبات، فمحل الاتلاف هنا مال منقول مملوك للغير، وهذا الاتلاف المادي يخرج عن نطاق الجريمة المعلوماتية ( ) ٠

ومن الجدير بالذكر، أن الإتلاف المعلوماتي المنصب علي المعدات والأجهزة له أساليب متعددة يجري استخدام أكثرها من قبل العاملين بالجهة المجني عليها، وأبرز هذه الأساليب لصق ورق صنفرة علي بعض أجزاء من البطاقات المثقبة لتخريب الأجهزة القارئة لها، إدخال قطع أو اسطوانات حديدية صغيرة أو شرائح من الألومنيوم أو قصاصات ورق في فتحات أجهزة الحاسب لتعطيله، صب بعض المشروبات كالقهوة، أو بعض السوائل كمحلول الملح أو سوائل التنظيف في جهاز التحكم في تشغيل الحاسب، إدخال غازات تسبب تأكلاً في الأسلاك والأجهزة، وضع حامض الهيدروكلوريك في مقدمة مروحة الشفط الخاصة بجهاز التكييف، تسخين بعض أجزاء حساسة من الحاسب بوضع سجائر مشتعلة عليها، القاء رماد السجائر المشتعلة علي الاسطوانات الممغنطة أو القيام بحكها، قطع الكابلات الموصلة

للأجهزة، وضع بعض القوارض، كالفئران وغيرها، حيث توجد توصيلات أسلاك الحاسب لقرضها ( ) ٠

وحقيقة الحال، فإن بواعث الإتلاف عديدة ومتنوعة ويأتي في مقدمتها؛ عدم رضاء المستخدمين عن أرباب أعمالهم، والذين يعبرون عنه في شكل إتلاف المعدات المادية المعلوماتية بهدف إحراجهم أو الضغط عليهم، وهذا ما حدث في مدينة Oppdal النرويجية ، حيث تم إتلاف ثلاث حاسبات آلية لشركة صناعية باستخدام مواد حارقة وذلك عقب فصل عشرين مستخدماً كانوا يعملون بها ٠ وفي فرنسا، فقد أعلنت لجنة CIODO مسئوليتها عن أفعال التعدي ضد الشركات الرئيسية المشيدة للمعدات المادية المعلوماتية خاصة في إقليم تولوز، وترتب علي ذلك خسائر قدرت بحوالي عشرات الملايين من الفرنكات الفرنسية ( ) ٠

[٢] التعطيل: ويقصد به توقف الشيء عن القيام بوظيفته لفترة مؤقتة، ويتحقق بأي فعل من شأنه إيقاف عمل النظام المعلوماتي ٠ وقد عرف القانون العربي النموذجي تعطيل النظام بأنه: " تعطل في النظام يتطلب فنياً إصلاح الامكانات المادية للحاسب أو ضبط نظام التشغيل فيه" ٠ ولم يشترط المشرع الجنائي وسيلة معينة لتعطيل أو لإعاقة النظام، فقد يتم بطريقة مادية أو معنوية، فمن الطرق المادية أعمال العنف التي تقع علي أجهزة الحاسب الالي وشبكة الاتصال عن طريق تخريبها بكسرها أو سكب السائل عليها أو أي مادة أخري أو منع العاملين في النظام من العمل ، وقد يتم التعطيل بوسيلة معنوية كما لو قام الجاني بإدخال فيروس علي البرامج أو عدل كلمة السر او كيفية أداء النظام لوظيفته بوسيلة تؤدي إلي توقف أو تعطيل في أداء وظيفة داخل النظام المعلوماتي ٠ ومن أمثلة التعطيل أو التوقيف للنظام المعلوماتي، ما حدث في فرنسا حين تم إتلاف ماكينة فرز الشيكات لدي أحد البنوك الكبيرة مما أدي إلي خسائر تقدر بنحو خمسة ملايين فرنك ٠

[٣] تعديل المسار: ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخري، كذلك فقد يتم التلاعب في المعطيات عن طريق استبدال هذه المعطيات، أو عن طريق التلاعب في البرامج، وذلك بإمداده بمعطيات مغايرة عن تلك التي صمم البرنامج لأجلها ( ) ومن ثم تغيير مسارات تشغيلها باستخدام إحدى وظائف الحاسب الآلي، وهو ما يتحقق باستخدام برمجيات متخصصة في ذلك ٠ ومن الفيروسات التي تساهم في تعديل النظام فيروس حصان طروادة ، ومنها كذلك فيروس الدودة والذي هو عبارة عن برنامج معلوماتي يتسم بقدرته العالية علي تعطيل وإيقاف الحاسب الآلي كاملاً ٠

(ISSN: 2356 - 9492)

[٤] الإلغاء: ويقصد به إزالة البيانات أو المعلومات الموجودة داخل البرنامج أو النظام المعلوماتي ويستوي لدي المشرع أن يكون الالغاء كلياً أو جزئياً ٠ ولم يشترط المشرع أن تكون هناك حماية تقنية لنظم البيانات والمعلومات من قبل صاحب النظام، بل تقع الجريمة حتي ولو حصل الاتلاف أو التعطيل أو الالغاء ، والنظم غير محمية، ولم يكلف الجاني العناء الكثير في إتلافها ( ) ٠

وفي فرنسا، فقد نصت المادة [٣٢٣-٢] من قانون العقوبات الفرنسي علي أنه:" يعاقب علي تعطيل أو إفساد نظام المعالجة الآلية للمعطيات٠٠" ٠ وتعالج تلك المادة، جريمة إعاقة سير عمل النظام المعلوماتي، وتُعرف بأنها كل فعل يتسبب في تباطؤ أو إرباك عمل نظام المعالجة الالية للبيانات، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام ٠ ويستوي لدي المشرع أن يكون من شأن نشاط الجاني إعاقة أو إفساد نظام التشغيل أو الإرسال، كما يستوي أن يؤدي نشاط الجاني إلي توقف نظام العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شأنها أن تعوق سير النظام، كالاعتداء المادي علي النظام أو نشر فيروسات بالنظام المعلوماتي ( ) ٠

وقد قضي في هذا الخصوص، بإدانة شخص قام بإدخال فيروس علي أحد أنظمة المعالجة الآلية للمعلومات عن طريق وضع فيروسات علي اسطوانات إعلانية تحتوي علي ملخص لبرامج دعائية، وقد قام الجاني بزراعة هذا الفيروس علي هذه الاسطوانات مع إعداد جريدة متخصصة في مجال المعلوماتية وباستخدام هذه الاسطوانات تم نقل الفيروس إلي نظام التشغيل فأتلف المعلومات ( ) ٠ كما قضي بأنه يقع تحت طائلة هذا النص الجناة الذين قاموا بتوصيل العديد مـــــــــن أجهزة الميناتل بالمراكز الخدمية المعنية، وأخذوا يرسلون بشكل آلي رسائل كثيرة مما ترتب عليه من إرباك لأنظمة المعالجة الالية للمعلومات ( ) ٠ وكذلك قضي بتوافر جريمة الإخلال بالنظام المعلوماتي من المتهم الذي قام بإرسال رسائل كثيرة إلي أحد الأجهزة الخاص بإحدى الشركات المنافسة موهماً هذا الجهاز أن الرسائل تصل إليه من أجهزة متعددة، وتتضمن طلابيات شراء من الشركة، وقد كانت تلك الطلبات غير جدية وكان هدف المتهم منها أن يملي الأجهزة الخاصة بهذه الشركة حتي تكون عاجزة عن تلقي طلبات جديدة وبالتالي يضر بها في النهاية ، لذا قضي بتوافر هذه الجريمة في تلك الحال ( ) ٠

وعلي جانب آخر، نصت المادة [٣٢٣-٣] من القانون العقوبات الفرنسي بأنه :" يعاقب علي الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها٠٠" ٠ ومفاد تلك المادة أن المشرع

الفرنسي قد جرم أي نشاط يترتب عليه إتلاف المعلومات المخزنة بالنظام المعلوماتي، وعاقب علي إدخال بيانات في نظام المعالجة الالية للمعلومات أو إلغاء أو تعديل البيانات المخزنة في النظام المعلوماتي، وبالتالي فقد ظهر واضحاً من خلال هذا النص أن المشرع الفرنسي لا يحمي النظام المعلوماتي فقط بل يحمي المعلومات المخزنة فيه ، وذلك ضد أي اعتداء يترتب عليه اتلاف المعلومات المخزنة ( )وعلي ذلك فهذا النص يعاقب علي إتلاف المعلومات المخزنة في ذاكرة الحاسب أو علي وسيط التخزين المعلوماتي ( ) حيث يؤدي إدخال البيانات إلي شغل ذاكرة النظام المعلوماتي بالكامل فيعجز عن التعامل مع هذه المعطيات بمعالجتها أو باستخراجها مطبوعة علي أوراق، ونفسي الشي بالنسبة لمحو المعلومات أو تعديلها ٠

وقد قضي في هذا الخصوص بإدانة متهم قام بإدخال فيروس في أحد أنظمة المعالجة الآلية للمعلومات، عن طريق وضع هذا الفيروس علي اسطوانات اعلانية تحتوي علي ملخص لبرنامج يراد الترويج له، ثم وزع هذه الاسطوانات مع اعداد جريدة متخصصة في مجال المعلوماتية ٠ وباستخدام هذه الاسطوانات تم نقل الفيروس إلي نظام التشغيل فأتلف المعلومات ( ) ٠ كما قضي كذلك بتوافر الجريمة من العاملة التي قامت بتعديل الفيشات الورقية الخاصة بالشركة التي تعمل بها، ثم قامت بإدخالها في جهاز الكمبيوتر بالشركة ( ) ٠

والحقيقة الدقيقة أن تدمير نظم البيانات والمعلومات يفوق في الضرر الذي يترتب عليه ، ذلك الضرر المترتب علي إتلاف المعدات المادية الخاصة بنظم المعلومات، وذلك لأن البيانات والمعلومات أصبحت ذا قيمة اقتصادية ومالية كبيرة، حيث يعكف علي إعداد البرامج خبراء متخصصون يتقاضون مرتبات مرتفعة ويستغرق عملهم بضع سنوات، وكذلك بالنسبة للبيانات وبنوك المعلومات المنتشرة في مجال الإدارة والصناعة، والتي ترتبط بها العديد من المنشآت وأبرز ما يمزيها سمة التركيز الواردة فيها، فيما كانت تتضمنه السجلات الضخمة أصبحت الآن مخزنة علي وسيط ممغنط F.D أو علي قرص مبرمج C.D أو علي وسيط الكتروني يسمي F.M 0 ( ) وقد طبقت محكمة النقض الفرنسية المادة [٣٢٣-٣] من قانون العقوبات، علي قيام أحد الأشخاص بتعديل وإلغاء لمعلومات تتعلق باللوائح المطبقة بإحدى الشركات بطريق العمد، وقد أقرت المحكمة بأنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات تم ارتكابها بواسطة شخص ليس له حق الدخول في النظام، ولا يشترط أن يتوافر لدي الجاني نية الإضرار، وبناء علي ذلك أيدت حكم محكمة الاستئناف الذي أدان المتهم عن هذه الجريمة بعدما استخلصت اركانها من قيام الشخص بتعديل

(ISSN: 2356 - 9492)

البيانات والتي سبق وأن قام بتسجيلها بطريقة نهائية علي نظام آلي للمحاسبة كان يقوم بالإشراف عليه ( ) ٠

ويتضح من خطة المشرع الفرنسي في مواجهة الاتلاف المعلوماتي أنها قد ميزت بين أمرين [الأول] حماية النظام المعلوماتي من الاتلاف المعلوماتي بالمادة [٣٢٣-٢] عقوبات فرنسي ٠ [والثاني] حماية المعلومات من الاتلاف المعلوماتي بالمادة [٣٢٣-٣] عقوبات فرنسي ٠

[ثالثاً] الركن المعنوي لجريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية: هذه الجريم عمدية، يتمثل الركن المعنوي لها في القصد الجنائي العام بعنصريه العلم والإرادة، فيتعين أن يكون الجاني عالماً بأن فعله يشكل اعتداء علي سلامة الأنظمة المعلوماتية، وأن تتجه إرادته إلي تحقيق ذلك ٠ وفي فرنسا ، تعد تلك الجريمة كذلك عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة ( ) ويتوافر العلم لدي الجاني من خلال قيامه بأحد الافعال التي جرمها النص القانوني من الاتلاف أو إعاقة النظام المعلوماتي عن أداء وظائفه، وان تتجه إرادته إلي ارتكاب الفعل وتحقيق نتيجته ( ) ٠ وقد قضي في هذا الصدد بأن ما قمت به المتهمة التي كانت تعمل في إحدى الشركات، وذلك قبل تركها العمل في تلك الشركة من إدخال بيانات غير صحيحة تتعلق بمعدل احتساب الضريبة علي القيم المنقولة ٠ وقد أدي ذلك إلي إرباك العمل بما كانت تزمع الشركة القيام به من أعمال المحاسبة داخل الشركة ٠ ومن الواضح أن قصد المتهمة كان منصرفاً إلي تحقيق تلك الغاية ( ) ٠

كما قضي في قضية تتلخص وقائعها في أن متخصصين في علم الكمبيوتر باعوا مجلة ملحق بها C.D محمل بفيروس مما أدي إلي تدمير بيانات في أنظمة الغير ٠ قضت محكمة الاستئناف ببراءتهم علي سند من عدم ثبوت توافر العلم لدى هؤلاء المتهمين بوجود هذه الفيروسات ٠ دفع المدعون بالحق المدني بتوافر العلم استناداً إلي هؤلاء المتهمين متخصصون في علم الكمبيوتر ولابد أنهم يعلمون بوجود مثل هذه الفيروسات، فلم تتعرض محكمة الاستئناف لهذا الوجه من أوجه الدفاع إيراداً ورداً مما أدي إلي نقض الحكم لإخلاله بالحق في الدفاع ( ) ٠

[رابعاً] عقوبة جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية: حدد مشرعنا الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين ٠ بينما حدد المشرع الفرنسي لجريمة المادة [٣٢٣-٢] عقوبات فرنسي ـــ والخاصة

بحماية النظام المعلوماتي ـــ عقوبة الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو٠ وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة ، فإن العقوبة تزيد إلي الحبس لمدة سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو" ٠ وقد حدد كذلك لجريمة المادة [٣٢٣-٣] عقوبات فرنسي ـــ والخاصة حماية المعلومات من الاتلاف المعلوماتي ـــ عقوبة الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو٠ وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة ، فإن العقوبة تزيد إلي الحبس لمدة سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو " ٠

الفرع الثاني

جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة

نصت المادة [١٨] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة بقولها:" يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً الكترونياً أو موقعاً أو حساباً خاصاً بآحاد الناس ٠ فإذا وقعت الجريمة علي بريد الكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين" ٠

وتتمثل علة التجريم في توفير الحماية الجنائية لخصوصية الأفراد مستخدمي الشبكة المعلوماتية ووسائل الاتصالات والمعلومات، من خلال تجريم الاعتداء علي حساباتهم الخاصة أياً كانت صورتها، سواء أكانت بريداً الكترونياً أو موقعاً خاصاً أو حساباً خاصاً ٠ فمن الملاحظ في الآونة الأخيرة كثرة الانتهاكات والاعتداءات الموجهة لوسائل التواصل الاجتماعي بما فيها البريد الالكتروني والمواقع والحسابات الخاصة الشخصية، وتعريضها لمحاولات التعدي عن طريق سرقتها أو اختراقها وكشف سريتها، وسرقة محتواها، وقد يصل الأمر نتيجة هذه الانتهاكات إلي ابتزاز مالكيها وتهديدهم ٠ لذلك جرم المشرع المصري في المادة سالفة الذكر، كل فعل ينطوي علي انتهاك لخصوصية البريد الالكتروني أو المواقع أو الحسابات الخاصة (٠)

(ISSN: 2356 - 9492)

ويشترط المشرع الجنائي، لقيام جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة: ، توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة: استلزم مشرعنا الجنائي لقيام جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة ، أن تقع علي البريد الإلكتروني أو الموقع أو الحساب الخاص ٠ وقد أشرنا سلفاً إلي معني كل من الموقع والحساب الخاص، فنحيل إليه منعاً للتكرار ٠ أما البريد الإلكتروني ، فيقصد به:" وسيلة لتبادل رسائل إلكترونية علي عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها" (المادة الأولي من القانون رقم ١٧٥ لسنة ٢٠١٨م) ٠

وخدمة البريد الإلكتروني (e-Mail Electronic Mail) هي عبارة عن خط مفتوح علي كل انحاء العالم يستطيع الفرد من خلاله إرسال واستقبال كل ما يريده من رسائل سواء (بالصوت أو الصورة أو الكتابة) إلي أي من الاصدقاء أو غيرهم، سواء كانوا يسكنون في الشارع المجاور أو علي الطرف الآخر من الكرة الأرضية٠ وإذا كان المرسل إليه نائماً أو مشغولاً يمكن لجهاز الحاسب الآلي أن يحتفظ له بالرسالة في صندوق البريد ليجد إشارة في انتظاره فور تشغيل الجهاز تخبره أن له رسالة أو أكثر في البريد٠ والأكثر من ذلك أنه إذا كان المرسل إليه في رحلة عمل خارج مكتبه أو منزله فإن الحاسب الآلي يرسل له رسالة صوتيه علي تليفونه المحمول بأن له رسالة مهمة في صندوق البريد ٠ والجدير بالذكر أن خدمة البريد الإلكتروني تتيح للمستخدم كتابة الرسالة المراد بثها علي الحاسب الآلي بنفس الطريقة التقليدية المستخدمة لكتابة الرسائل والتقارير ٠ وبعد ذلك يكتب المرسل العنوان الخاص بالمرسل إليه، وهو العنوان الالكتروني علي الشبكة، حيث يوجد لكل مستخدم عنوانه البريدي الخاص به ٠ وبعد ذلك يتم الضغط علي مفتاح الارسال لكي تنطلق الرسالة إلي العنوان المطلوب في أي مكان في العالم من خلال الشبكة ٠ مع ملاحظة أنه هذه الخدمة تحافظ علي سرية الرسائل، حيث يوجد لكل مستخدم كلمة سر للتعامل مع البريد الالكتروني، بحيث لا يعمل النظام إلا بعد إدخالها ( ) ٠

[ثانياً] الركن المادي لجريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة: يتمثل الركن المادي في هذه الجريمة في كل سلوك مادي يحصل به اعتداء علي البريد الإلكتروني أو موقع أو حساب خاص، يؤدي إلي اتلاف أو تعطيل أو إبطاء أو اختراق له، أياً كانت الوسيلة التكنولوجية المستخدمة في ذلك ٠ وبيان ذلك، فيما يلي:

[١] الاتلاف: ويتحقق بأي فعل من شأنه جعل البريد الإلكتروني أو الموقع أو الحساب الخاص غير صالح للاستخدام، كما لو قام الجاني بتغيير المحتوي المعلوماتي له أو حذف البيانات من عليه، بما يعيق صاحبه من استخدامه أو استعماله مرة أخري، والاتلاف قد يكون كلياً أو جزئياً ٠

[٢] التعطيل: ويقصد به توقف الشيء عن القيام بوظيفته فترة مؤقتة ٠ وهذا التعطيل عن طريق شغل عنوان البريد الإلكتروني أو الموقع أو الحساب الخاص بحيث يبدو ظاهراً لأي مستخدم يريد الدخول أن الموقع مشغول من كثرة الزائرين، علي حين أن الحقيقة هي أنه ليس مشغولاً، وذلك لمنع الغير من الوصول إليه ٠

[٣] الإبطاء: ويتحقق بأي فعل من شأنه تقليل كفاءة وسرعة استخدام البريد الالكتروني أو الموقع أو الحساب الخاص للمجني عليه ٠

[٤] الاختراق: ويعني الدخول غير المصرح به، ويتحقق بأي صورة من صور التعدي وبأي وسيلة تقنية مثال ذلك عن طريق كلمة السر الحقيقة والتي لم يكن مصرحاً للجاني استعمالها، أو باستخدام برامج أو شفرة خاصة تمكن من اختراق البريد الالكتروني أو الحساب أو الموقع، أو عن طريق رقم لشخص آخر مصرخاً له بالدخول ٠ كما يتحقق الاختراق متي كان صاحب البريد الالكتروني أو الحساب أو الموقع قد وضع قيوداً للدخول مثل سداد رسوم اشتراك أو تسجيل بياناته كاملة ولم يلتزم بها الجاني ( ) ٠

[ثالثاً] الركن المعنوي لجريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة: هذه الجريمة من الجرائم العمدية التي يتمثل ركنها المعنوي في القصد الجنائي العام بعنصريه العلم والإرادة فيلزم أن يكون الجاني عالماً بأنه يقوم بالإتلاف أو تعطيل أو إبطاء موقع أو حساب خاص أو بريد الكتروني أو أنه يتسلل إليه مخترقاً له بدون وجه حق ، وان هذا الحساب أو الموقع أو البريد الالكتروني خاص بشخص طبيعي أو شخص اعتباري خاص كالشركات، ثم تتجه إرادته بالرغم من تحقق هذا العلم لديه إلـــــــي ارتكاب فعل الاتلاف أو التعطيل أو الابطاء أو الاختراق للحساب أو الموقع أو البريد الالكتروني ( ) ٠

[رابعاً] عقوبة جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة:: حدد مشرعنا الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، وذلك حال كون المجني عليه من آحاد الناس ٠ بينما حدد مشرعنا عقوبة

(ISSN: 2356 - 9492)

الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، إذا كان المجني عليه من الأشخاص الاعتبارية الخاصة كالشركات التجارية والمؤسسات الخاصة والجمعيات الخاصة ٠

الفرع الثالث

جريمة الاعتداء علي تصميم موقع

نصت المادة [١٩] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة الاعتداء علي تصميم موقع بقولها:" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو أخفي أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بدون وجه حق " ٠

وتتمثل علة التجريم في حماية المواقع الإلكترونية من أفعال التعدي عليها من قبل الجناة الذين يرغبون في تغيير قيم هذه المواقع، أو محاولة إتلافها أو محاولة تعديلها أو إعاقتها عن العمل ( ) ٠ ويستلزم المشرع الجنائي، لقيام جريمة الاعتداء علي تصميم موقع ، توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الاعتداء علي تصميم موقع: استلزم مشرعنا الجنائي لقيام جريمة الاعتداء علي تصميم موقع أن تقع علي موقع الكتروني، وقد عرفت المادة الأولي من قانون جرائم تقنية المعلومات الموقع بأنه: " مجال أو مكان افتراضي له عنوان محدد علي شبكة معلوماتية، يهدف إلي إتاحة البيانات والمعلومات للعامة أو الخاصة " ٠ فالمواقع الإلكترونية، هي مجموعة من الصفحات المتصلة علي الشبكة العالمية، والتي تعتبر كياناً واحداً يمتلكه عادة شخص واحد أو منظمة واحدة، ويكرس لموضوع واحد أو لعدة مواضيع وثيقة الصلة، ومن خلال هذه المواقع يمكن لأصحابها بث المادة التي يريدونها فهي مكان للاطلاع علي الكتب والأبحاث وهي مكان للتسوق ومكان للحوار ٠٠٠ إلخ " ٠ وهناك أنواع عديدة للمواقع الإلكترونية، سواء كانت مواقع تجارية ، أو مواقع تعليمية أو مواقع ترفيه أو مواقع حكومية أو مواقع إخبارية أو عسكرية ، ومواقع أخري شخصية ٠

والواقع من الأمر، أن للشخص الحق في إنشاء موقع الكتروني أو بالأحرى مكان افتراضي له عنوان محدد علي شبكة معلوماتية بهدف إتاحة البيانات والمعلومات الالكترونية للعامة والخاصة، إذ يلجأ الشخص عند إنشاء الموقع إلي ابتكار ووضع تصميم له يعبر عن ذاته ومهنته وعمله وشخصيته وهويته٠ إلا أنه في

كثير من الأحيان يتعرض هذا الحق للانتهاك متي تم الاعتداء علي تصميم الموقع أو إبطائه أو إتلافه أو تشويه أو إخفائه ٠ وقد بات إنشاء المواقع وخلقها بسيطاً للغاية من خلال الدخول لموقع جوجل وبالتحديد لصفحة إنشاء موقع جديد باستخدام الكمبيوتر ثم الضغط علي خيار إنشاء الموجودة أسفل الصفحة ثم إضافة محتويات الموقع الجديد، والضغط علي خيار " نشر وتوزيع" عند الانتهاء من إضافة المكونات ( ) ٠

ـــــ ماهية تصميم موقع: ويقصد به عملية تخطيط وتنفيذ محتويات متعددة الوسائط عبر شبكة الإنترنت بواسطة أنظمة التقنيات كلغات التوصيف المناسبة للعرض علي متصفحات الانترنت أو بقية واجهات المستخدم المبينة في الانترنت، أي إنشاء مجموعة من الملفات الموضوعة جنباً إلي جنب علي خادم انترنت أو أكثر مما يسمح بعرض المحتوي، ويشمل المحتويات والواجهات التفاعلية للمستخدم علي شكل صفحة إنترنت عند طلبها، والتي تحتوي علي عدة عناصر مثل النصوص والنماذج البريدية والصور، وبمعني آخر، هي عملية استخدام بعض التقنيات واللغات التي تعرف بلغات التوصيف والترميز والتي يتم ترتيبها وفق سياق معين لتكوين خطوط أو نصوص أو رسوم نقطية "وسائط" تكون في النهاية الواجهة التفاعلية والمحتوي الداخلي للموقع، ولغات التوصيف والترميز هي عبارة عن لغة صممت خصيصاً لإعطاء أوامر لجهاز الحاسب الآلي ( ) ٠

[ثانياً] الركن المادي لجريمة الاعتداء علي تصميم موقع: يتمثل الركن المادي في هذه الجريمة في كل نشاط مادي يحصل به اعتداء علي الموقع الإلكتروني ، يؤدي إلي إتلاف أو تعطيل أو إبطاء أو تشويه أو إخفاء أو تغيير تصاميم الموقع الالكتروني، سواء كان موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي ٠ وبيان ذلك، فيما يلي:

[١] الإتلاف: وهو كل فعل من شأنه جعل الموقع غير صالح للأستخدام٠ ويلاحظ أن إتلاف الموقع قد يكون كلياً أو جزئياً ٠

[٢] التعطيل: وهو ما يتحقق بكل فعل من شأنه إيقاف عمل الموقع٠

[٣] الإبطاء: وهو من صور تعطيل الموقع الالكتروني، ويقصد به كل من شأنه الإقلال من كفاءة وسرعة الموقع٠

[٤] التشويه: ويقصد به العبث بالواجهة الخارجية للموقع لتبدو بصورة غير متناسقة ومخالفة لما ارتضاه

(ISSN: 2356 - 9492)

لها صاحب الموقع أن تكون عليه، سواء الواجهة المكونة للصفحة الرئيسية أم للصفحات الداخلية للموقع التي تحوي كل منها محتوي معين من المعلومات، كما يعني التشويه العبث في الجزء البرمجي أي الجزء الداخلي الغير ظاهر للمستخدمين علي نحو يجعل الموقع لا يستجيب للأوامر التي تحرك واجهة الموقع الخارجية ( ) ٠

وما يجب لفت الانتباه إليه، أنه يستوي في الأفعال السابقة أن الجاني يكون قد اقترفها عن طريق الشبكة المعلوماتية الدولية أو عن طريق شبكة محلية أو كان ذلك بطريقة أو وسيلة أخري من وسائل تقنية المعلومات، وهي كثيرة ومتعددة وقابلة للزيادة في المستقبل في ضوء ثورة المعلومات التي تشهدها البشرية في الوقت الحالي ٠ والجدير بالإشارة، أن هذه الجريمة من المفترض أن يسأل عنها كذلك مسئولية مدنية شركات تقنية المعلومات المنوط بها تأمين وحماية المواقع علي الشبكة الدولية للمعلومات، طالما لم يثبت تورطهم عمداً في التعدي علي الموقع، وذلك لأنهم ملزمون ـــ وهو التزام بتحقيق نتيجة ـــ بمنع مثل هذه الاعتداءات، والتي يكون هدفها حجب الموقع عن الآخرين ومنع الدخول إليه، الأمر الذي يسبب ارتباكاً لدي الجهات ذات العلاقة بمثل هذه المواقع، لاسيما لو كانت من المواقع الخدمية، ذات الارتباط المباشر بمصالح الجماهير والتي تؤدي بشكل إلكتروني ( ) ٠

وغني عن البيان، أنه يشترط قانوناً لقيام الجريمة المذكورة، أن يكون التغيير بغير وجه حق، بأن يكون التعديل أو التغيير قد تم من شخص غير مصرح له قانوناً بالدخول أو تعديل البيانات أو تغييرها، فمناط عدم المشروعية هو انعدام سلطة الجاني في الدخول إلي الموقع مع علمه بذلك ٠ وتبرز الإشارة إلي أن الاعتداء علي تصاميم المواقع الالكترونية يفترض ارتكاب الجاني لفعل الدخول غير المشروع للموقع الالكتروني حتي يتسنى له تغيير تصاميم الموقع، وهو ما يتحقق من خلال اتخاذ الموقع لشكل آخر غير الذي كان عليه قبل الدخول إليه، أو أن يقوم الجاني بمحو بعض بيانات الموقع أو برامجه

ويضع محلها بيانات أخري ( ) ٠

[ثالثاً] الركن المعنوي لجريمة الاعتداء علي تصميم موقع: هذه الجريمة من الجرائم العمدية التي يتمثل ركنها المعنوي في القصد الجنائي العام بعنصريه العلم والإرادة ، فيلزم أن يكون الجاني عالماً بأن فعله يمثل دخولاً علي موقع خاص بشركة أو مؤسسة أو شخص طبيعي، وأن من شأن فعله أن يؤدي إلي إتلاف أو تعطيل أو إبطاء أو تشويه أو إخفاء أو تغيير تصاميم الموقع الالكتروني، سواء كان موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي ٠

[رابعاً] عقوبة جريمة الاعتداء علي تصميم موقع: حدد مشرعنا الجنائي لهذه الجريمة عقوبة بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين ٠

المطلب الثالث

جرائم الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة، وسلامة الشبكة المعلوماتية

تقسيم:

نتناول دراسة هذا المطلب من خلال الفرعين التاليين:

[الفرع الأول] جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة ٠

[الفرع الثاني] جريمة الاعتداء علي سلامة الشبكة المعلوماتية ٠

الفرع الأول

جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة

نصت المادة [٢٠] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة بقولها:" يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوي الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها ٠ فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق علي بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ٠ وفي جميع الأحوال، إذا ترتب علي أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه " ٠

(ISSN: 2356 - 9492)

وتتمثل حكمة التجريم، في مواجهة حالات الاعتداء علي الأنظمة المعلوماتية والمواقع الإلكترونية والحسابات المملوكة للدولة أو أحد الأشخاص الاعتبارية العامة، وتوفير الحماية القانونية لتأمين هذه المواقع أو الحسابات ٠ علاوة علي أن المواقع الحكومية هي المواقع الأكثر رسمية وتمثيلاً لسيادة الدولة علي الفضاء الالكتروني، وأن العدوان عليها يؤثر بشكل كبير في هيبة الدولة وفي نفوس المواطنين ٠ ويشترط المشرع الجنائي، لقيام جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة ، توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة: استلزم مشرعنا الجنائي لقيام جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة، أن يكون محلها موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكاً لها، أو يخصها ٠ ومن ثم يخرج من نطاق التجريم، المواقع والحسابات الشخصية المملوكة للأفراد أو لأشخاص القانون الخاص، والتي يخضع الاعتداء عليها للمواد ١٥،١٦ من قانون مكافحة جرائم تقنية المعلومات ٠ وقد أشرنا فيما سبق إلي معني كل من الموقع ، البريد الالكتروني، الحساب الخاص، النظام المعلوماتي فنحيل إليه منعاً للتكرار، وتجدر الإشارة هنا إلي أن المواقع الحكومية هي المواقع التابعة للنطاق الالكتروني الخاص بالدولة، وغالباً ما ينتهي بـ [gov] تمييزاً لها عن غيرها ٠

ويذهب البعض إلي أن العدوان علي الصفحات الرسمية الحكومية علي مواقع التواصل الاجتماعي يبقي خارج نطاق التجريم، إذ أن هذه الصفحات وإن كانت حكومية إلا أنها منشأة علي مواقع الكترونية غير حكومية، بالنظر إلي أن مواقع التواصل الاجتماعي هي مواقع خاصة مملوكة لشركات خاصة، ولا يمكن أن ينسحب وصف المواقع الالكترونية الحكومية علي تلك الصفحات٠ ومع وجاهة الرأي السابق، إلا أن البعض الأخر قد ذهب إلي أن النص القانوني الوارد بالمادة [٢٠] من قانون مكافحة جرائم تقنية المعلومات يتسع ليشمل الحسابات الخاصة للدولة علي مواقع التواصل الاجتماعي، فنص المادة سالف الذكر يشير إلي أن تقرير الحماية الجنائية لأي موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة الدولة أو لحسابها أو أحد الاشخاص الاعتبارية العامة أو مملوك لها أو يخصها، علاوة علي أن العبرة في إسباغ الحماية الجنائية المقررة للمواقع الالكترونية أو الحسابات الخاصة أو البريد الالكتروني يكون بنعتها بصفة الرسمية عليها، وهو ما لا يتحقق إلا بوجود رابطة بيها وبين الدولة، وهذه الرابطة هي أن الموقع أو الحساب الخاص يدار بمعرفة الدولة أو أحد الاشخاص الاعتبارية العامة أو لحساب الدولة أو أحد أشخاصها

الاعتبارية، أو كان مملوكاً للدولة أو أحد أشخاصها الاعتبارية أو يخصمها، ومن ثم يكون الحساب أو الموقع رسمياً إذا كان خاضعاً لإدارة الدولة أو مملوكاً لها ( ) ٠

[ثانياً] الركن المادي لجريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة: يتمثل الركن المادي في هذه الجريمة في كل من الصور الآتية:

[١] الدخول غير المشروع: أصبحت الشبكات الإلكترونية الحكومية تتضمن الكثير من المواقع والخدمات والمعاملات الحكومية، وبالتالي تعد مسرحاً لجريمة الدخول غير المشروع ( ) ويتمثل هذا الأخير في النشاط المتمثل بالاتصال بنظام الكمبيوتر بأي طريقة كانت وعادة ما يقصد الفاعل بذلك الاطلاع علي المعلومات التي يحتويها هذا النظام ( ) ٠ والدخول إلي النظام يتم بأي وسيلة تقنية، سواء كان ذلك عن طريق استعمال كلمة السر الحقيقة متي كان الجاني غير مخول في استخدامها أو عن طريق استخدام برامج أو شفرة خاصة أو عن طريق استخدام الرقم الكودي لشخص أخر في الدخول من خلال شخص مسموح له بالدخول، سواء عن طريق شبكات الاتصال التليفونية أو لطرفيات محلية أو عالمية ٠ وتقع الجريمة من أي شخص أياً كانت صفته، سواء كان يعمل في مجال الأنظمة أم لا علاقة له بنظم الحاسب الالي، سواء كان يستطيع الاستفادة من النظام أم لا ، إنما فقط يكفي ألا يكون من أولئك الذين لهم حق الدخول إلي هذا النظام ٠ ويتحقق الدخول غير المشروع متي كان الدخول يمثل مخالفة لإرادة صاحب النظام أو من له حق السيطرة عليه، كتلك الأنظمة التي تتعلق بأسرار الدولة أو الدفاع عنه ٠

[٢] البقاء بدون وجه حق في النظام المعلوماتي: ويتمثل في بقاء المتهم داخل نظام الكمبيوتر بعد دخوله إليه عرضاً وبطريق الخطأ ٠ فمجرد الدخول الخاطئ لا يعاقب عليه القانون، لانتفاء القصد الجنائي، حيث أن الجريمة عمدية، ولكن يعاقب علي البقاء في هذا النظام بعد أن تبين المتهم حقيقة الأمر ٠ وهناك فرض آخر، فقد يدخل المتهم النظام بطريق مشروع، ولكنه يستمر بعد الوقت المحدد لبقائه فيه، وكثيراً ما يحدث ذلك إذا كان استعمال النظام محدداً بوقت معين نظير أجر مالي، فيتخطى المتهم هذا الوقت ( ) ٠

[٣] تجاوز حدود الحق في الدخول: والمقصود بتعدي حدود الحق في الدخول من حيث الزمان أو مستوي الدخول، هو مجاوزة الحد المصرح فيه بالدخول، فقد يكون الجاني أحد المصرح لهم بالدخول إلي الموقع أو إلي الحساب الخاص لمدة ساعة أو

(ISSN: 2356 - 9492)

ساعتين ، لكنه يتجاوز هذه المدة الزمنية بدون مبرر، أو كان مسموحاً له بجزء معين في البرامج ولكنه تعدي هذا الجزء ٠

[٤] الاختراق: عرف المشرع الجنائي الاختراق في المادة الأولي من قانون مكافحة جرائم تقنية المعلومات بأنه:" الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلي نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها " ٠ والاختراق بمعني الدخول غير المصرح به؛ يتحقق بأي صورة من صور التعدي وبأي وسيلة تقنية، فقد يكون عن طريق كلمة السر الحقيقة والتي لم يكن مصرحاً للجاني باستعمالها، أو باستخدام برامج متخصصة في فك كلمة السر أو من خلال شفرة خاصة تمكن من الاختراق، كما يتحقق الاختراق عن طريق ملفات التجسس التي يزرعها الجاني في الحاسوب الشخصي للمجني عليه وتمكنه من معرفة بياناته وأسراره ٠ كما يتحقق الاختراق كذلك متي كانت الدولة أو الشخص الاعتباري العام صاحب البريد الإلكتروني أو الحساب الخاص أو الموقع أو النظام المعلوماتي قد وضع قيوداً للدخول مثل سداد رسوم اشتراك أو تسجيل بيانات المستخدم كاملة ولكنه لم يلتزم بذلك ٠

ومن الجدير بالإشارة أن الاختراق يؤدي إلي إبطاء حركة المتصفح أو انقطاع الاتصال ، وقد يعطل الدخول إلي البيانات وكذلك الاطلاع علي المعلومات الشخصية لصاحب الموقع أو البريد الالكتروني أو الحساب الخاص ٠

[ثالثاً] الركن المعنوي لجريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة: هذه الجريمة عمدية، يتمثل ركنها المعنوي في القصد الجنائي العام بعنصريه العلم والإرادة، فيتعين أن يكون الجاني عالما بأنه ليس من حقه دخول الموقع أو الحساب الخاص أو البريد الالكتروني أو النظام المعلوماتي وأنه خاص بالدولة أو شخص معنوي عام، أو يعلم أنه دخل بطريق الخطأ ثم رفض الخروج ، فمن يرفض الخروج بعد دخوله خطأ يتحقق في جانبه القصد الجنائي العام الذي تقوم به الجريمة، ثم يتعين أن تتجه إرادة الجاني إلي الدخول أو البقاء بعد الدخول الخاطئ٠ وأن يعلم كذلك أن هذا الحساب الخاص أو الموقع أو النظام المعلوماتي تديره الدولة أو شخص اعتباري عام سواء بنفسه أو يدار لحسابه، وأنه يعترض أياً منها وأن حصوله علي البيانات الحكومية يتم بدون وجه حق ، وأن من شأن هذا الدخول أو الاختراق أو الاعتراض أن يحدث إتلاف للبيانات أو المعلومات أو الحساب الخاص أو النظام المعلوماتي أو البريد الالكتروني، أو من شأنه أن يدمرها أو يشوهها أو يغيرها أو يغير تصاميمها أو يؤدي إلي نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً او جزئياً ٠ كما يلزم كذلك ان تتجه إرادته إلي الدخول عمداً أو البقاء في الموقع أو

النظام المعلوماتي أو الحساب الخاص أو البريد الالكتروني الخاص بالدولة او بشخص معنوي بعد دخوله إليها بطريق الخطأ متجاوزاً الحدود المخولة له من حيث الزمان ومستوي الدخول، وتتجه كذلك إلي اختراقها أو اعتراضها متوقعاً أن ينتج عن سلوكه المادي العبث بها إتلافاً او تشويهاً علي نحو ما ورد بالفقرة الثالثة من المادة سالفة الذكر ( ) ٠

[رابعاً] عقوبة جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة: حدد مشرعنا الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين ٠ فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق علي بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ٠

وفي جميع الأحوال، إذا ترتب علي أي من الأفعال السابقة ـــــ الواردة بالمادة ٢٠ سالفة الذكر ـــــ إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه ٠

الفرع الثاني

جريمة الاعتداء علي سلامة الشبكة المعلوماتية

نصت المادة [٢١] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي جريمة الاعتداء علي سلامة الشبكة المعلوماتية بقولها:" يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعترض عملها أو أجري بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها ٠ ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين الف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين ٠

(ISSN: 2356 - 9492)

فإذا وقعت الجريمة علي شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة الف جنيه ولا تجاوز مليون جنيه" ٠

وعلة التجريم، تتمثل في المحافظة علي سلامة الشبكة المعلوماتية، ضد محاولات العبث بها، وحرصاً علي أن تؤدي وظيفتها علي أفضل وجه مكمن في ضوء ما تحمله من بيانات ومعلومات يمكن أن تفيد المجتمع وأعضاؤه، علاوة علي أضفاء الحماية للشبكة المعلوماتية التي تخص الدولة أو أحد الأشخاص الاعتبارية العامة ٠ ويشترط المشرع الجنائي، لقيام جريمة الاعتداء علي سلامة الشبكة المعلوماتية ، توافر الأركان الأتية:

[أولاً] ركن المحل لجريمة الاعتداء علي سلامة الشبكة المعلوماتية: استلزم مشرعنا الجنائي لقيام جريمة الاعتداء علي سلامة الشبكة المعلوماتية ، أن يكون محلها الشبكة المعلوماتية ٠ وقد بين مشرعنا الجنائي ماهية تلك الشبكة بقوله: " مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها ، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها" ٠ [م١ من قانون مكافحة جرائم تقنية المعلومات] ٠ ويتضح من التعريف السابق، أن الشبكة المعلوماتية تشتمل علي مكونين ـــ [الأول] مادي، ويضم أجهزة الحاسب الآلي والأجهزة المادية والمعدات وخطوط الربط التي تتكون منها الشبكات ٠ [والثاني] البرامج والبيانات والمعلومات ونظم تشغيل الشبكات التي تشكل المكون المعنوي أو المنطقي للشبكة ٠ ومن أبرز الشبكات المعلوماتية شبكة المعلومات الدولية " الانترنت" والتي تسمي بشبكة الشبكات، وهي شبكة حواسيب ضخمة متصلة مع بعضها البعض، وتخدم شبكة الإنترنت ما يقرب من ثلاثة ونصف مليار مستخدم، وتنمو بشكل سريع للغاية بنسبة ١٠٠% ومن أبرز استخدامات شبكة الإنترنت المتعددة، خدمات البريد الالكتروني، ومحركات البحث، ومواقع الويب، وعقد الاجتماعات والمؤتمرات، ومواقع أو شبكات التواصل الاجتماعي ومن أشهرها موقع التواصل الاجتماعي فيس بوك الذي تأسس عام ٢٠٠٤ ويضم في الوقت الحالي أكثر من مليار مستخدم حول العالم ( ) ٠

[ثانياً] الركن المادي لجريمة الاعتداء علي سلامة الشبكة المعلوماتية: يتمثل الركن المادي لهذه الجريمة في كل نشاط مادي يقوم به الجاني يؤدي إلي أمرين: [أولهما] إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها ٠ وبيان ذلك، في الآتي:

[١] إيقاف شبكة معلوماتية عن العمل: ويقصد به توقف برامج أو أجهزة تشغيل الشبكة عن العمل ، وإن كان ذلك يتم عن طريق اجهزة الشبكة نفسها، وهذا التوقف قد يكون بشكل دائم أو جزئي ٠

[٢] تعطيل الشبكة المعلوماتية: ويقصد به إعاقة سير عمل الشبكة المعلوماتية أو النظام المعلوماتي المشغل لها ٠

[٣] الحد من كفاءة عمل الشبكة المعلوماتية: ويقصد به التقليل من كفاءة عمل الشبكة أو تشغيلها وذلك عن طريق استخدام برامج ضارة لإبطاء عمل الشبكة ٠

[٤] التشويش علي الشبكة المعلوماتية : ويقصد به أي عائق يحول دون قدرة الشبكة المعلوماتية علي الإرسال أو الاستقبال ٠

[٥] اعتراض الشبكة المعلوماتية: ويقصد به مشاهدة البيانات أو المعلومات الخاصة بالشبكة المعلوماتية أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوي أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق٠

[وثانيهما] أجري بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها : وقد عرف مشرعنا الجنائي المعالجة الإلكترونية بأنها:" أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الالكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخري " ٠ [م١ من قانون مكافحة جرائم تقنية المعلومات] وعليه تتحقق هذه الصورة بقيام الجاني بإجراء تعديل علي البيانات الخاصة بالشبكة، ومن ثم تغيير النظام المعلوماتي أو البرامج التي تنظم عمل هذه الشبكة، بالشكل الذي يؤدي إلي تعطيلها أو إيقاف العمل بها٠ وقد استلزم المشرع أن تكون هذه المعالجة قد تمت بدون وجه وحق، ويتحقق ذلك إذا كان الدخول للشبكة قد تم من شخص غير مصرح له بالدخول أو البقاء داخل الشبكة أو النظام المعلوماتي أو كان الدخول من شخص مخول له ذلك، ولكنه تجاوز حدود الدخول أو البقاء علـــي الشبكة ( ) ٠

[ثالثاً] الركن المعنوي لجريمة الاعتداء علي سلامة الشبكة المعلوماتية: هذه الجريمة عمدية، يتمثل ركنها المعنوي في القصد الجنائي العام بعنصريه العلم والإرادة، فيتعين

(ISSN: 2356 - 9492)

أن يكون الجاني عالماً بأن من شأن ما يقوم به ينصب علي شبكة معلوماتية، وأن من شأن فعله إيقاف الشبكة المعلوماتية عن العمل أو تعطليها أو يحد من كفاءة عملها أو يقوم بالتشويش عليها أو يعيق عملها ويعترضها ٠ كما يلزم كذلك أن تتجه إرادته إلي إتيان الفعل وإحداث النتيجة الإجرامية المتمثلة في إيقاف الشبكة المعلوماتية أو تعطيلها عن العمل ٠

[رابعاً] عقوبة جريمة الاعتداء علي سلامة الشبكة المعلوماتية: حدد مشرعنا الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين ، وذلك في حالة توافر القصد الجنائي، أي ارتكبها الجاني في صورة العمد ٠ أما في حالة الخطأ غير العمدي، فقد حدد مشرعنا الجنائي لهذه الجريمة عقوبة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين الف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين ٠ وإذا وقعت الجريمة علي شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة الف جنيه ولا تجاوز مليون جنيه" ٠

المبحث الثالث

الأحكام الإجرائية لجرائم تقنية المعلومات

تقسيم:

لم تعد القواعد العامة في قانون الإجراءات الجنائية كافية بذاتها لمواجهة التعاملات الإلكترونية، وما قد ينجم عنها من جرائم إلكترونية، ومن ثم بدت الحاجة إلي إجراءات خاصة بالإضافة للأحكام الإجرائية الواردة بقانون الإجراءات الجنائية لمواجهة تلك الجرائم ٠ وعليه فقد اشتمل قانون مكافحة جرائم تقنية المعلومات علي عدد من الأحكام الإجرائية التي تستهدف إنشاء تنظيم إجرائي دقيق ينظم إجراءات الضبط والتحقيق والمحاكمة المتعلقة بتلك الجرائم ٠ ومن ثم سوف نتناول هذا المبحث من خلال المطالب الثلاثة الاتية:

[المطلب الأول] اجراءات الاستدلال الخاصة بجرائم تقنية المعلومات ٠

[المطلب الثاني] اجراءات التحقيق الخاصة بجرائم تقنية المعلومات ٠

[المطلب الثالث] اجراءات المحاكمة الخاصة بجرائم تقنية المعلومات ٠

المطلب الأول

اجراءات الاستدلال الخاصة بجرائم تقنية المعلومات

تقسيم:

إجراءات الاستدلال هي إجراءات تحضيرية وتمهيدية للدعوي الجنائية، وهي تهدف إلي جمع التحريات والمعلومات عن الجريمة واكتشاف مرتكبها وهذه الإجراءات ليست من إجراءات الدعوي الجنائية، فهي سابقة عليها ولا يترتب علي اتخاذ إجراء منها تجريك الدعوي الجنائية ( ) ٠

والحقيقة أن دراسة الاستدلال في الجرائم المتعلقة بتقنية المعلومات تقتضي بحث أمرين [الأول] بيان الأشخاص المنوط بهم قانوناً جمع الاستدلالات في جرائم تقنية المعلومات وأهمية الدور الذي يلعبونه في هذا الخصوص٠ وهؤلاء يعرفون بـ " مأموري الضبط القضائي " ٠ [والثاني] إجراءات الاستدلال التي يملك مأموري الضبط القضائي اتخاذها بصدد جرائم تقنية المعلومات ٠ ومن ثم سوف نتناول هذا المطلب من خلال الفرعين التاليين:

(ISSN: 2356 - 9492)

[الفرع الأول] مأموري الضبط القضائي في جرائم تقنية المعلومات ٠

[الفرع الثاني] إجراءات الاستدلال في جرائم تقنية المعلومات ٠

الفرع الأول

مأموري الضبط القضائي في جرائم تقنية المعلومات

نصت المادة [٥] من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، علي أنه: " يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلي الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم " ٠ ويتضح من تلك المادة، أن المشرع الجنائي قد منح صفة الضبطية القضائية ـــ بموجب قرار من وزير العدل بالاتفاق مع الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات ـــ للعاملين بالجهاز القومي لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومي ( ) بالنسبة إلـــي الجرائـــم التي تقع بالمخالفـــة لأحكام هذا القانون، والمتعلقـــة بأعمال وظائفهم٠

وتكون هذه الطائفة من مأموري الضبط القضائي ذات الاختصاص النوعي المحدد بنوع معين من الجرائم ـــ جرائم تقنية المعلومات ـــ ويكون اختصاصها شاملاً إقليم الجمهورية كله أو مقصوراً علي دائرة واحدة، كما هو الحال بالنسبة لمفتشي التموين والصحة ورجال الجمارك وغيرهم ٠ وتقضي القواعد العامة في الاختصاص بأن وجود مأمور ضبط قضائي متخصص (ذي اختصاص نوعي محدد) لا يحول دون قيام مأمور ضبط ذي اختصاص نوعي عام بإجراء يدخل في اختصاص مأمور ذي اختصاص نوعي محدد ( ) ٠ وبتطبيق ذلك علي مأموري الضبط القضائي ذوي الاختصاص النوعي المحدد ممن نص عليهم في المادة (٥) من قانون جرائم تقنية المعلومات لسنة ٢٠١٨ يؤدي إلي القول بأن قيام مأمور ضبط من رجال المباحث بعمله لا يترتب عليه البطلان ( ) ٠ وقد قضي في هذا الخصوص بأن:" إضفاء صفة الضبط القضائي علي موظف ما في صدد جرائم معينة لا يعني مطلقاً سلب تلك الصفة في شأن هذه الجرائم عينها من مأموري الضبط القضائي ذوى الاختصاص العام " ( ) ٠

ومن الجدير بالتنويه، أن المادة الخامسة سالفة الذكر قد نصت علي أنه: " يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلي

الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم" ٠ ويقصد بالجهاز وفقاً للمادة الأولـــــي مـــــن القانـــون الجهاز القومي لتنظيم الاتصالات ٠

الفرع الثاني

إجراءات الاستدلال في جرائم تقنية المعلومات

أناط الشارع الإجرائي بمأموري الضبط القضائي اختصاصا أصيلاً في جمع الاستدلالات والتحريات عن الجرائم ومرتكبيها والتي تلزم للتحقيق في الدعوي ٠ والمكنة المخولة قانوناً لمأموري الضبط القضائي في الاستدلال والبحث والتحري عن الجرائم التي وقعت بالفعل تنطوي علي صلاحيتهم في القيام ببعض الإجراءات التي توصلهم إلي مبتغاهم في الكشف عن حقيقة الجريمة المرتكبة وأشخاص مرتكبيها وقبل أن نتناول ما يدخل في عداد إجراءات الاستدلال، يجب التنويه إلي أن هذه الإجراءات ـــ أياً كان مسماها ـــ يجمعها قاسم مشترك ألا وهو أنها لا تنال ـــ بحسب طبيعتها ـــ من حريات الأفراد أو تمس حرمة مساكنهم علي خلاف إجراءات التحقيق٠ ويعتبر من إجراءات الاستدلال:

[أولاً] تلقي التبليغات والشكاوي عن الجرائم: أوجبت المادة [٢٤] من قانون الإجراءات الجنائية علي مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوي التي ترد إليهم بشأن الجرائم٠ والإبلاغ عن الجريمة معناه الإخبار عنها إلى رجل الضبط القضائي، وهو حق عام لجميع الأفراد أن يمارسوه حتي ولو لم يكونا مجنياً عليهم أو مضرورين من الجريمة ٠ والإبلاغ عن الجريمة الإلكترونية له أهمية من ناحيتين ـــ [الأولي] من الناحية الإحصائية [والثانية] من الناحية القانونية، فمن الناحية الإحصائية تظهر أهمية البلاغ في بيان حجم الظاهرة الإجرامية وامكانية عمل بيان احصائي بعدد الجرائم المرتكبة والمبلغ عنها وبالتالي تلاشي ظهور الرقم الأسود الذي تتسم به تلك الجرائم المستحدثة ٠ أما من الناحية القانونية، فهو بمثابة أداة اتصال علم السلطات المختصة بوقوع الجريمة ٠ ومن جهة أخري فإن أهمية البلاغ في الجريمة الإلكترونية تظهر في مساعدة المحقق علي تحديد ما إذا كان السلوك محل البلاغ يعد سلوكاً إجرامياً يقع ضمن الجرائم الإلكترونية أم لا ، وكذلك وضع تصور مبدئي عن مسرح الجريمة الإلكترونية وخطة التحقيق المناسبة واختيار فريق التحقيق المناسب لنوع الجريمة ٠

(ISSN: 2356 - 9492)

ويتخذ البلاغ في الجريمة الإلكترونية صور عديدة فقد يتم كتابياً أو شفوياً بمعرفة المجني عليه أو غيره ممن شاهدوا وقوع الجريمة أو وصل إليهم خبر وقوعها شأنه في ذلك شأن البلاغ في الجرائم التقليدية، وقد يتم عن طريق الانترنت أي ما يسمي " بالإبلاغ الرقمي" وذلك أما عن طريق ارسال رسالة إلكترونية إلي عنوان البريد الالكتروني للجهات المختصة بالتحقيق والتحري، كعنوان البريد الالكتروني للدرك الوطني الفرنسي باعتباره الجهة المختصة بالتحقيق والتحري عن الجرائم الالكترونية في فرنسا أو عن طريق ملئ استمارات رقمية متواجدة في المواقع المتخصصة لتلقي البلاغات والشكاوي، كموقع إدارة مكافحة جرائم الحاسبات وشبكات المعلومات في جمهورية مصر العربية علي العنوان ٠ ومن الجدير بالذكر، أنه يجب لمليء تلك الاستمارة التوضيح والتدقيق في المعلومات بشأن الجريمة المبلغ عنها وذلك لتسهيل عملية التأكد منها من قبل سلطات التحقيق والبحث والتحري ٠

وعلي الرغم من أن لكل جريمة من الجرائم معلوماتها الخاصة التي تحرص جهة تلقي البلاغات والشكاوي استيفائها، إلا أن هناك معلومات تكاد تكون مشتركة بين معظم هذه الجرائم أي الجرائم الالكترونية، ويمكن الحصول عليها عن طريق طرح أسئلة تتناول جوانب محددة يجيب عنها المبلغ أو يقوم هذا الأخير بمليء بيانات الاستمارة الخاصة بالبلاغ والمتاحة علي مواقع الجهات المختصة بتلقي البلاغات والشكاوي ، ومن تلك الأسئلة ما يلي: تاريخ ووقت تلقي البلاغ، المعلومات الخاصة بالمبلغ، المعلومات الخاصة بمتلقي البلاغ ، ونوع الجريمة الالكترونية محل البلاغ، الأسئلة الستة المشهورة والمتعلقة بالجريمة ماذا؟ وأين؟ ومتي؟ وكيف؟ ومن؟ ولماذا؟ وكذلك استيفاء المعلومات ذات العلاقة بالأنظمة الحاسوبية مثل طبيعة العتاد ونوعية البرمجيات والمسئولين عن الأنظمة وطريقة الاتصال بهم وغيرها ، وهل الجهاز المستخدم فـــــــــــــي ارتكاب الجريمة ضمن شبكة أجهزة، وهل هناك أجهزة طرفية أم لا ( ) ٠

[ثانياً] المعاينة: عرف الفقه المعاينة بأنها:" إجراء بمقتضاه ينتقل المحقق إلي مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك الأشياء الأخرى التي تفيد فـــــــــــي كشف الحقيقة ( ) ٠ وتعد المعاينة إجراء استدلالياً إذا ما باشرها مأمور الضبط القضائي وفقاً للمادة ١/٢٤ إجراءات جنائية التي توجب علي مأموري الضبط ومرؤوسيهم القيام ببعض الإجراءات من بينها المعاينة عندما يبلغون بجريمة أو يعلمون بها بوسيلة مشروعة ويقوم بها أيضاً مأموري الضبط القضائي في حالة التلبس (م١/٣١ إجراءات جنائية) ٠ وقد تكون المعاينة إجراء من إجراءات التحقيق الابتدائي إذا ما باشرتها النيابة العامة بوصفها

سلطة تحقيق مع التزامها بالشروط الشكلية لإجراءات التحقيق كاستصحاب كاتب التحقيق وغيرها من الشروط الشكلية وإلا عدت من إجراءات الاستدلال ( ) ٠ وتقتضي المعاينة سرعة الانتقال إلي مكان الجريمة حتي لا يتطرق الشك إلي الدليل المستفاد منها وذلك إذا ما انقضت فترة بين وقوع الجريمة وإجراء المعاينة تسمح بأن يتمكن الجاني من إزالة بعض الآثار المادية التي تفيد في كشف الحقيقة ( ) ٠

والحقيقة الدقيقة أن هناك بعض المعوقات التي تواجه المحقق عند إجراء المعاينة وتتمثل في أمرين: [الأول] أن الجرائم التي تقع علي نظم المعلومات والشبكات قلما يخلف عن ارتكابها أثاراً مادية [والثاني] أن عدداً كبيراً من الأشخاص قد يترددون علي المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يفسح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أز زوال بعضها، وهو ما يلقي ظلالاً من الشك علي الدليل المستمد من المعاينة ( ) ٠ لذلك لا تلعب المعاينة في مجال الكشف عن جرائم تقنية المعلومات، بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ( ) ٠

ومن الجدير بالذكر، أن هناك بعض الخطوات الفنية التي يجب علي مأموري الضبط القضائي مراعاتها عند إجراء المعاينة وتتمثل في:

[١] تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بوجه خاص علي تصوير الأجزاء الخلفية للحاسب وملحقاته ٠ ويراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة ٠

[٢] العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام ٠

[٣] ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتي يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد علي المحكمة ٠

[٤] عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أية مجالات لقوي مغناطيسية (ممرات مغناطيسية) يمكن أن تتسبب في محو البيانات المسجلة ٠

[٥] التحفظ علي محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة ٠

(ISSN: 2356 - 9492)

[٦] التحفظ علي مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات ٠

[٧] قصر مباشرة المعاينة علي الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات ، وتلقوا تدريباً كافياً علي التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجريمة المعلوماتية ( ) ٠

[٨] فصل الكهرباء عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير علي أثار الجريمة ٠

[٩] إبعاد الموظفين عن أجهزة الحاسب الآلي، وكذلك عن الأماكن الأخرى التي توجد بها أجهزة الحاسب الالي ( ) ٠

[١٠] رفض أي عرض للمساعدة من أي شخص غير مصرح بذلك ٠

وأمام ذلك فإن علي المحقق الجنائي عند معاينة مسرح الجريمة الإلكترونية أن يضع في الحسبان أنه أمام مسرحين هما: [الأول] مسرح تقليدي: ويقع خارج بيئة الحاسب الآلي والانترنت ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلي مسرح أية جريمة تقليدية ، قد يترك الجاني أثار عدة كبصمات أصابعه علي لوحه المفاتيح أو الفارة أو علي المكونات المادية للحاسب وبما قد يتركه الجاني من متعلقات شخصية أو وسائط تخزين رقمية أو غيرها من الأدلة المادية التي يتعامل معها أعضاء فريق التحقيق كل بحسب تخصصه ٠ [والثاني] مسرح سيبراني " افتراضي" ويقع داخل أورقة الحاسب وشبكات الانترنت ويتكون من البيانات الرقيمة التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكاته وفي ذاكرته وفي الأقراص الصلبة بداخله ٠ وهنا يأتي دور فريق التحقيق والذي يتكون من خبراء متخصصين مع المحقق الجنائي في التعامل مع الأدلة الرقمية ( ) ٠

[ثالثا] سماع الشهود: عرف الفقه الشهادة بأنها: " ما يقر به شخص أمام جهة قضائية عما يكون قد رآه أو سمعه أو أدركه بحاسه من حواسه متعلقاً بالجريمة ( ) ٠ وتعد الشهادة إحدى طرق الإثبات الهامة في المواد الجنائية، بل هي اقدمها وأهمها؛ حيث تعد عماد الإثبات فـــــي تلك المواد والوسيلة التي لا غني عنها ( ) ٠ ويجوز لمأموري الضبط القضائي سماع الشهود دون تحليفهم اليمين القانونية ، لأن سماع الشهادة بيمين هو من إجراءات التحقيق التي لا يملكها مأموري الضبط القضائي، بحسب الأصل، مالم تقم ضرورة تبرر ذلك ٠

ويقصد بالشاهد في الجرائم المعلوماتية الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب، والذي تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله٠ والشاهد المعلوماتي ـــــ وذلك تمييزاً له عن الشاهد التقليدي ـــــ بهذا المفهوم يشمل عدة طوائف من أهمها :

[١] مشغلو الحاسب: وهو الأشخاص المسئولون عن تشغيل الحاسب الآلي والمعدات المتصلة به ٠

[٢] خبراء البرمجة: وهو الأشخاص المتخصصون في كتابة أوامر البرامج٠ ويمكن تقسيمهم إلي فئتين هي مخططو برامج التطبيقات، والفئة الثانية هي مخططو برامج النظم ٠

[٣] المحللون: وهم الأشخاص الذي يعهد إليهم بتحليل الخطوات ويقومون بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلي وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الواحدت٠

[٤] مهندسو الصيانة والاتصالات: وهو المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به٠

[٥] مديرو النظم: وهو الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية ( ) ٠

[٦] مقدم الخدمة: أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات ٠

[٧] المستخدم: كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنيات المعلومات أو يستفيد منها بأي صورة كانت ٠

ومن الجدير بالذكر، أن الشاهد عندما يقدم المعلومات التي لديه لابد وأن يقدمها بأسلوب سهل ومفهوم حتي يكون بمقدور سلطات التحري والتحقيق فهم وإدراك تلك المعلومات ، كما يتعين عليه أن يتوخى التحديد والدقة في المعلومات التي يقدمها أو يبلغها لسلطات التحقيق والتحري، وذلك بأن يقدم وصفاً أو بياناً دقيقاً ومحدداً للشيء محل الواقعة دون زيادة أو نقصان، فالإعلام الناقص إعلام مبتور لا يحقق الغاية المرجوة من ورائه وكذلك الإعلام المبالغ فيه٠ هذا بالإضافة إلي تحريه الصدق والأمانة في المعلومات التي يقدمها، فلا يقدم معلومات كاذبة أو مستندات مزورة أو

(ISSN: 2356 - 9492)

يباشر عملاً غير أمين في أجهزة الحاسب الآلي من شأنه خداع أو تضليل رجال السلطة العامة ( ) ٠

والسؤال المطروح الآن: هل يلتزم الشاهد في جرائم الكمبيوتر بأن يتعاون مع سلطة التحقيق كأن يقوم مثلاً بعمليات معينة علي الجهاز إذا كان من المتخصصين في هذا المجال لكي يساعد العدالة؟ للإجابة علي هذا التساؤل أهميتها حيث أن الخبير المنتدب من الجهة القضائية قد لا يمكنه معرفة الأساليب النية التي يمكن اتباعها للكشف عن أدلة تفيد في كشف الحقيقة ، وقد لا يعلمها إلا هذا الشاهد مثل كلمة المرور والبرامج المستخدمة والتي استعان بها المتهم في ارتكاب الجريمة المعلوماتية ٠ والحقيقة أنه وفقاً للقواعد العامة في الشهادة لا يلتزم الشاهد إلا بذكر ما يعلمه ولا يجوز إجباره علي القيام بسلوك معين ( ) ٠ وهذا يؤكد أهمية وجود قواعد خاصة تضعها نصوص خاصة في هذا المجال لكي تفرض واجب التعاون مع الجهة القضائية في أثناء التحقيقات والمحاكمة علي الشاهد ( ) ٠

ومن الجدير بالذكر، أن كثيرا من التشريعات تلزم الشاهد بتقديم ما يعرفه عن الجريمة وليس القيام بعمل معين ٠ مثال ما نصت عليه المادة (٢٨٤) من قانون الإجراءات الجنائية المصري بقولها :" إذا امتنع الشاهد عن أداء اليمين أو عن الإجابة في غير الأحوال التي يجيز له القانون فيها ذلك، حكم عليه ٠٠ " ٠ ومعني ذلك أن الشاهد يلتزم بالإجابة عن أسئلة توجهها المحكمة وليس للمحكمة أن تلزمه بالقيام بعمل معين ٠ وبالمثل فن المادة (٣٣١) من قانون الإجراءات الجنائية الفرنسي تحدد واجبات الشاهد في الشهادة بخصوص الوقائع المسندة إلي المتهم أو بخصوص شخصية الأخير أو أخلاقياته ٠ وعلي العكس من ذلك ، تفرض بعض التشريعات المقارنة واجب التعاون علي الشاهد، ومن ثم يصبح الشاهد ملتزماً بأن يساعد الجهة القضائية بان يقدم الدليل أو يسهل الدخول إلي المواقع التي تفيد في كشف الحقيقة ٠

[رابعاً] ندب الخبراء: لمأموري الضبط القضائي أن يندب الخبراء المختصين لفحص الاثار والأدلة التي وجدت علي مسرح الجريمة ويبدون آرائهم في المسائل الفنية البحتة، ومن ذلك الاستعانة بخبراء البصمات ٠ ولا يجوز لمأمور الضبط القضائي تحليف الخبراء المنتدبون اليمين، سواء قبل أدائهم المهام المكلفين بها أو عند سماع أقوالهم في المحضر الذي يجريه بعد انتهائهم من مهمتهم، إلا إذا خيف ألا يستطاع ذلك فيما بعد (م ٢/٢٩ إجراءات جنائية) ٠ ولم يغفل المشرع في القانون ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، الحديث عن أحكام الخبرة في هذا القانون، فنص في المادة (٥) منه علي: " أن ينشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنين

من غير العاملين به ٠ وتطبق علي الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصـــــة بقواعد تنظيم الخبرة أمام جهات القضاء" ٠ واستثناء من تلك القواعد، تسري علي الخبراء المقيدين بالسجل الثاني القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وجد ٠ وتحدد اللائحة التنفيذية ( ) لهذا القانون قواعد وشروط وإجراءات القيد في كل من السجلين " ٠

والحقيقة الدقيقة، أن من أصعب الأمور التي قد تواجه الخبير هي عملية تجميع الأدلة الإلكترونية ولذلك يمكن تحديد الخطوات التي يمكن اتباعها من أجل اشتقاق هذا النوع الأدلة وتتمثل هذه الخطوات في المراحل الآتية:

[١] خطوات ما قبل التشغيل والفحص:

ـــــ التحقق من مطابقة محتويات الأحراز لما هو مدون عليها ٠

ـــــ التحقق من صلاحية وحات النظام للتشغيل ٠

ـــــ تدوين بيانات وحدات المكونان المضبوطة كالنوع والأحراز ٠

[٢] خطوات التشغيل والفحص:

ـــــ القيام بتسجيل باقي بيانات الوحدة ٠

ـــــ إعداد نسخة من كل وسائط التخزين المضبوطة وذلك لحماية الأصل من أي تلف أو تدمير الناتج عن سوء الاستخدام أو وجود فيروسات ٠

ـــــ تحديد أنواع وأسماء المجموعات البرامجية كبرامج التشغيل وبرامج التطبيقات ٠

ـــــ إظهار الملفات المخبأة والنصوص المخفية داخل الصور ٠

ـــــ استعادة الملفات التي تم طمسها من الأصل وذلك باستخدام أحد برامج استعادة المعلومات ٠

ـــــ تخزين الملفات او المعطيات وعمل نسخ طبق الأصل من الأسطوانة والقرص المرتبطة بالجريمة ٠

(ISSN: 2356 - 9492)

ـــــ يقوم الخبير بتجريد قائمة تتضمن جميع الأدلة التقنية التي تم الحصول عليها في الديسك الخاص مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في حاسب آخر وهذا للتأكد من سلامة القائمة ٠

[٣] تحديد مدي ارتباط الدليل المادي بالدليل التقني:

في هذه المرحلة تتم الربط بين الدليل المادي والدليل التقني ، وهذا بعد القيام بفحصها، الأمر الذي يكسب هذه الأدلة التقنية الموثوقية ٠

[٤] مرحلة تدوين النتائج وإعداد التقرير:

في هذه المرحلة يتم إعداد تقرير يتضمن جميع مراحل البحث، مرفقة بملاحق إيضاحية مصورة أو مسجلة ٠

وجملة القول، فإن إجراءات الاستدلال التي يجوز لمأمور الضبط القضائي ان يباشرها وه في سبيل أداء مهمته الأساسية في الكشف عن الجرائم والتوصل إلي معاقبة مرتكبيها لا تقع تحت حصر، فكل إجراء يقوم به في هذا السبيل يعتبر صحيحاً ومنتجاً لأثره، طالما أنه لم يمس حقاً شخصياً لأحد الأفراد ولم ينتهك حرمه المساكن ولم يتدخل بفعله في خلق الجريمة أو التحريض علي مقارفتها ( ) ٠

ـــ إثبات إجراءات الاستدلال في محضر: أوجب القانون علي مأموري الضبط القضائي أن يثبتوا جميع الإجراءات الاستدلالية التي يتخذونها في سبيل الكشف عن الجرائم والتوصل إلي مرتكبها في محاضر موقع عليها منهم، يوضح فيها تاريخ وساعة مباشرة الإجراءات والمكان الذي بوشرت فيه والنتيجة التي أسفرت عنها ومضمون ما أبداه الشهود والخبراء الذين سمعوا من أقوال وآراء مزيلة بتوقيعاتهم، وإرسال هذه المحاضر إلي النيابة العامة مع الأوراق والأشياء المضبوطة (م٢/٢٤ إجراءات جنائية) ٠

المطلب الثاني

اجراءات التحقيق الخاصة بجرائم تقنية المعلومات

نصت المادة [٦] من القانون ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات علي أنه: " لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد علي ثلاثين يوماً قابلة للتجديد لمرة واحدة، متي كان لذلك فائدة في ظهور الحقيقة علي ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي:

١- ضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه ٠ ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، علي ألا يؤثر ذلك علي استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ٠

٢- البحث والتفتيش والدخول والنفاذ إلي برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط ٠

٣- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته، وحركة الاتصالات التي تمت علي ذلك النظام أو النظام التقني ٠

وفي كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسبباً ٠ ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة، في المواعيد ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية " ٠

ومفاد هذا النص، أن المشرع الجنائي قد منح جهات التحقيق المختصة ، أن تصدر أمراً مسبباً لمأموري الضبط القضائي للقيام بإجراء أو أكثر من الإجراءات المنصوص عليها فيها وهي: [الأول] الأمر بالتحفظ علي البيانات والمعلومات وضبطها [والثاني] التفتيش في النظم المعلوماتية [الثالث] الأمر بتسليم المعلومات ، وعليه سوف نتناول هذا المطلب موزعاً علي الفروع الأتية:

[الفرع الأول] التحفظ علي البيانات والمعلومات ٠

[الفرع الثاني] التفتيش في النظم المعلوماتية ٠

[الفرع الثالث] تسليم المعلومات ٠

الفرع الأول

التحفظ علي البيانات والمعلومات

أجازت المادة السادسة من القانون لجهة التحقيق المختصة أن تأمر ضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه ٠ ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، علي ألا يؤثر ذلك علي استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ٠ ولا شك أن الإجراءات المنصوص عليها في

(ISSN: 2356 - 9492)

المادة السابقة، تتماشي مع الطبيعة المعنوية الخاصة للبيانات والمعلومات، والتي تتطلب إجراءات خاصة للتعامل معها بغرض ضبطها، وتسهيل إجراءات الحصول عليها من جانب السلطات العامة، وأجهزة إنفاذ القانون، ولا شك كذلك أن هذه الإجراءات مستحدثة وغير مألوفة بالنسبة للقواعد الإجرائية التقليدية المعروفة في جمع الأدلة ٠ ولبيان ماهية هذه الإجراءات، يجب علينا توضيح المقصود بكل منها، علي النحو التالي:

[أولاً] ضبط البيانات أو المعلومات: وهو إجراء الهدف منه ضبط الأدلة الرقمية بهدف الاستفادة منها في كشف الحقيقة في جرائم تقنية المعلومات ( ) ، وهو إجراء مشابه لإجراء ضبط الأشياء المعروف في قانون الإجراءات الجنائية ٠ والحقيقة الدقيقة أن إجراءات الضبط في مجال جرائم تقنية المعلومات تتميز ببعض الأوجه الخاصة التي تنفرد بها عن إجراءات الضبط في الجرائم الأخرى٠ من ذلك ما نصت عليه المادة (٥٦) إجراءات فرنسي (المعدلة بالقانون رقم ٥٧٥ لسنة ٢٠٠٤ الصادر في ٢١ يونيه سنة ٢٠٠٤م) من أنه يجوز عند القيام بضبط بيانات معلوماتية ضرورية للكشف عن الحقيقة أن يرد الضبط علي الدعامة المادية التي سُجلت عليها تلك البيانات أو أن يتم عن طريق نسخ البيانات علي دعامة مستقلة ٠ ويتم هذا النسخ في حضور الأشخاص الذين يساعدون في عملية الضبط٠ ومن الأوجه التي تميز عملية ضبط المعلومات المبرمجة أيضاً ما تنص عليه المادة السابقة من جواز أن يقوم القائم بالضبط بمسح المعلومات بعد أخذ نسخة منها ٠ كما أجازت المادة ذاتها لرجل الضبط أن يقوم بحجز الأشخاص الموجودين عند تفتيش أجهزة ومعدات معالجة وتخزين البيانات الوقت اللازم لإتمام عملية التفتيش والضبط ( ) ٠ ومن ناحية أخرى ، تم تحديد الملفات المضبوطة وجردها ، وأن نسخة من هذا الوسيط أو المحتوي يتم تسليمها إلـــــــــــى المختبر الجنائي المختص حتى يتمكن من معرفة طبيعة البيانات ( ) ٠

[ثانياً] سحب البيانات أو المعلومات: ويقصد به استخراج البيانات أو المعلومات من الحاسب الآلي أو من النظام المعلوماتي بغرض ضبطها، ومؤدي ذلك وجود البيانات والمعلومات داخل نظام معلوماتي ما وتكليف الجهة المسئولة عن هذا النظام باستخلاص البيانات والمعلومات التي تراها جهة التحقيق علي صلة بجريمة ما ٠

[ثالثاً] التحفظ علي البيانات أو المعلومات: وهو من الإجراءات الممهدة لجمع الأدلة، ويتولى القيام بها مقدمو خدمات الانترنت بتكليف من السلطات القضائية المختصة باعتبارها إجراءات لازمة وضرورية لتسهيل مهمة التحقيق في كشف جرائم تقنية المعلومات والبحث عن أدلتها وضبطها ٠ وترجع أهمية التحفظ علي البيانات بالنظر

إلي الطابع المتواتر والتدفق المستمر للكم الهائل من المعلومات والبيانات التي يتم تبادلها بين الأفراد من خلال شبكات الاتصالات والمعلومات، وعليه يتجه مزودي خدمة الانترنت إلي تخزين هذه البيانات لفترة زمنية مناسبة ـــــ بهدف معالجة هذه البيانات ـــــ بالنظر لما يتطلب تخزين هذه البيانات من موارد وأموال طائلة، ونظراً لمتطلبات التحقيق في جرائم تقنية المعلومات، والتي تشترط ضرورة الحفاظ علي أدلة الجريمة ٠

هذا بالإضافة إلي ما قد تتضمنه الإجراءات القضائية من طلبات للتعاون القضائي الدولي التي تستغرق فترات زمنية طويلة، فقد نصت العديد من المواثيق الدولية علي مواد تهدف إلي تأسيس آليات لتحقيق جرائم تقنية المعلومات الغرض منها منع حذف البيانات، من خلال تقرير سلطة أوامر للأشخاص المتحكمين في البيانات من مقدمي الإنترنت والاتصالات الالكترونية وخدمات استضافة المواقع الالكترونية، بالحفاظ وصون سلامة البيانات لفترة زمنية محددة ٠

ومن الإنصاف أن نعترف، أن المشرع الجنائي في تنظيمه لتلك المسألة قد وازن بين حق الأفراد في احترام خصوصياتهم وبين المصلحة العامة ومقتضيات حسن سير التحقيق في هذه الجرائم، من خلال التزام مقدمي الخدمة بعدد من الالتزامات، والتي من أبرزها، الالتزام بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة زمنية محددة هي ١٨٠ يوماً متصلة ( ) ٠ كما أوجب عليه المحافظة علي سرية البيانات التي تم حفظها وتخزينها وعدم إفشائها بغير إذن مسبب من إحدى الجهات القضائية، وهذا الالتزام عاقب المشرع الجنائي، مقدم الخدمة علي مخالفته بموجب المادة (٣١) من قانون جرائم التقنية ( ) علاوة علي التزامه بتأمين البيانات، بما يحافظ علي سريتها وعدم اعتراضها أو اختراقها أو تلفها ٠

وفي فرنسا، فقد نص قانون الأمن اليومي الفرنسي رقم [٢٠٠١-١٠٦٢] المؤرخ في ١٥ نوفمبر ٢٠٠١ علي أنه في حالة الضرورة ولكشف الجرائم ولأغراض التحقيق وبهدف تقديم معلومات إلي السلطة القضائية، يتم احتفاظ مقدمي الخدمة بالمعلومات والبيانات الفنية لمدة عام واحد كحد أقصي مشترطاً أن تنحصر تلك البيانات في معلومات عن الأشخاص المقدم لهم الخدمة وكذلك أنواع الخدمات المقدمة من قبل مزود الخدمة، ولا يجوز بأي حال من الأحوال الاحتفاظ بمحتوي المراسلات المتبادلة ولا أي معلومات تتعلق بموضوع هذه المراسلات ( ) ٠ وقد نصت التوصية رقم ١٣/٩٥ الصادرة عن المجلس الأوربي علي أنه :" يتعين أن يفرض التزام علي مزودي الخدمات الذين يقومون خدمات الاتصالات اللاسلكية للجمهور، إما من خلال

(ISSN: 2356 - 9492)

شبكة عامة أو من خلال شبكة خاصة ، أن يقدموا لسلطة التحقيق المعلومات اللازمة لتحديد هوية مستعمل الشبكة" ٠

[رابعاً] تتبع البيانات أو المعلومات: ويقصد به ملاحقة ومتابعة تحركاتها، ومن ثم يفترض هذا الأمر تكليف مقدمي الخدمة بمتابعة تحركات البيانات والمعلومات وتتبع مصادرها لأغراض الضبط ( ) ٠

الفرع الثاني

التفتيش في النظم المعلوماتية

نصت المادة [٦] من القانون ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات علي أنه: " لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد علي ثلاثين يوماً قابلة للتجديد لمرة واحدة، متي كان لذلك فائدة في ظهور الحقيقة علي ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي: ٠٠

٢- البحث والتفتيش والدخول والنفاذ إلي برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط ٠

ـــــ شروط صحة التفتيش:

إن الهدف الرئيسي من التفتيش هو البحث عن الدليل الجنائي في الجرائم المرتكبة بهدف الوصول إلي الحقيقة واقتناع عدالة المحكمة به ( ) ٠ ويشترط المشرع الجنائي لمباشرة التفتيش باعتباره إجراء من إجراءات التحقيق، شروط معينة وهي:

[الشرط الأول] سبق وقوع جريمة: استلزم المشرع الجنائي لصدور الأمر بالتفتيش أن تقع جريمة الكترونية ـــ جناية أو جنحة ـــ معاقب عليها وفقاً لقانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م، وهذه الجرائم أوردها المشرع في الباب الثالث من القانون، ومن أمثلتها، جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها (م١٣) وجريمة الدخول غير المشروع (م١٤) وجريمة تجاوز حدود الحق في الدخول (م١٥) وجريمة الاعتراض غير المشروع (م١٦) وجريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية (م١٧) وجريمة الاعتداء علي البريد الالكتروني أو المواقع أو الحسابات الخاصة (م١٨) وجريمة الاعتداء علي تصميم موقع (م١٩) وجريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة (م٢٠) وجريمة الاعتداء علي سلامة الشبكات المعلوماتية (م٢١) ٠ ومن الجدير بالذكر، أن التفتيش لا يكون صحيحاً إذا كانت الجريمة مخالفة ٠

[الشرط الثاني] صدور الأمر بعد وقوع الجريمة: اشترط المشرع الجنائي أن يصدر الأمر بالتفتيش بعد وقوع جريمة من الجرائم السابقة، لأن الأمر بالتفتيش إجراء تحقيق، والتحقيق لا يبدأ إلا من بعد وقوع الجريمة ٠ والغرض منه جمع الأدلة علي الجريمة التي وقعت٠ فإذا لم تكن هناك جريمة قد وقعت لم يكن هناك محل لإجراء تحقيق وبالتالي لإجراء التفتيش٠ ومن الجدير بالإشارة، أنه لا يعني وقوع الجريمة وجوب تمامها، إذ يصح التفتيش ولو وقفت الجريمة عند حد الشروع، لأن الشروع لا يغير من وصف الجريمة، وإنما يخفف من عقوبتها فقط ٠ وقد قضي في هذا الخصوص بأن العبرة في القول بوقوع الجريمة كشرط لإصدار الأمر هي بظاهر الحال بصرف النظر عما يسفر عنه إجراء التفتيش، فلا يخل بسلامة الأمر عدم ضبط شيء أو يسفر التفتيش علي أن الجريمة الصادر بشأنها لم تقع أصلاً، كما لو أدعي شخص كذباً علي المتهم بأنه أرسل عبارات السب والقذف عبر رسائل البريد التقني أو مواقع التواصل الاجتماعي المختلفة، وكذلك لـــــــو ثبت بعد التفتيش أن مرتكب الجريمة شخص آخر بخلاف المتهم ٠

ومن الجدير بالتنويه، أنه إذا كانت الجريمة لم تقع بعد، فإن التفتيش لا يجوز، ولو كانت علي وشك الوقوع ، فلا يجوز إصدار أمر التفتيش عن جريمة مستقبلية، كما لو أثبتت التحريات أن المتهم يتواصل مع أحد القراصنة لتعلم كيفية اختراق المواقع الحكومية والبنوك، وأنه ينوي اختراق هذه المواقع، أو أنه دخل علي أحد المواقع التقنية التي تتيح المعلومات حول تصنيع القنابل البدائية ، في الوقت الذي أكدته فيه التحريات ميوله الارهابية، وبصفة عامة لا يجوز التفتيش لاكتشاف الجريمة، ومن قبيل ذلك طلب مأمور الضبط القضائي من المحقق إصدار إذن التفتيش بشأن شخص معين تثار بشأنه الشبهات بأنه يتواصل مع الأطفال القصر لتحريضهم علي الفجور ( ) ٠

وخلاصة القول، لا يجوز أن يكون التفتيش من أجل ضبط جريمة مستقبلية، ولو دلت التحريات علي أنها سوف تقع حتماً ( ) ٠

[الشرط الثالث] وجود دلائل كافية ضد شخص معين: استلزم المشرع الجنائي لصحة صدور الأمر بالتفتيش ضرورة أن يكون هناك اتهام موجه ضد شخص فاعل أو شريك في ارتكاب جريمة الكترونية وقيام دلائل كافية علي ذلك ( ) ٠ ومؤدي ذلك، أنه لا يكفي مجرد توجيه الاتهام إلي شخص معين بأنه قد ساهم في ارتكاب جريمة سواء بوصفه فاعلاً أو شريكاً لتفتيش شخصه أو مسكنه أو الولوج داخل نظامه المعلوماتي، وإنما يتعين توافر دلائل كافية تسمح بتوجيه هذا الاتهام أو توافر إمارات

(ISSN: 2356 - 9492)

قوية أو قرائن تدل علي وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدي المتهم ٠ كما لا يكفي التبليغ عن الجريمة لإجراء التفتيش أو الإذن به، وإنما يجب أن تسبقه تحريات واستدلالات تسفر عن توافر دلائل كافية علي نسبة الاتهام إلي شخص معين، وتمارس محكمة الموضوع رقابتها علي مدي ما تضمنته الاستدلالات من شبهات معقولة تكفي لترجيح وقوع الجريمة ونسبتها إلي المتهم ٠

ويقصد بالدلائل الكافية ـــ بصفة عامة ـــ شبهات مستمدة من الواقع والقرائن تنبئ عن ارتكاب شخص لجريمة من الجرائم ٠ وتعرف الدلائل الكافية في الجرائم الإلكترونية بأنها:" مجموعة من المظاهر أو الأمارات المعينة التي تنهض علي السياق العقلي والمنطقي لملابسات الواقعة وكذلك علي خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية ـــ الإلكترونية ـــ إلي شخص معين بوصفه فاعلاً أو شريكاً " ٠ ومن أمثلة الدلائل الكافية لجرائم تقنية المعلومات؛ الربط بين نقل الصور الفاضحة وعنوان إنترنت بروتوكول مع رقم حساب المتهم لدي مزود الخدمة، ووجود رقمين للتليفون لديه يُستخدمان في ذلك، وكذلك الربط بين وسائل التحريض علي الفسق والتهديد بنشر الصور الفاضحة المرسلة إلي المجني عليها بعد عدة عناوين بريدية مرتبطة مع عنوان بروتوكول المتهم في منزله وعنوان بروتوكول آخر في محل عمله حال وجود خلافات عائلية سابقة بينه وبين المجني عليها ٠ علي أنه ينبغي ملاحظة أنه إذا قامت لدي المحقق أسباب جدية دعته إلي اتهام شخص معين واقتضي الأمر تفتيش جهاز الحاسوب الخاص به، فإنه لا ينال من صحة هذا التفتيش ما قد يسفر عنه التحقيق أو المحاكمة مستقبلاً من براءة هذا الشخص من الجريمة التي تم التفتيش بسببها، وبناء علي ذلك إذا أسفر أمر التفتيش عن اكتشاف جريمة أخري فإن ما تم اكتشافه يصح الاعتداء به قانوناً، لأنه تفتيش صحيح، وتطبيقاً لذلك إذا أثبتت التحريات أن المتهم أرسل عبارات السب والقذف إلي المجني عليها مستخدماً في ذلك جهاز الحاسوب الخاص به المرتبط بشبكة الإنترنت من خلال هاتف أرضي معين ، وبناء علي إذن المحقق تم تفتيش الحاسوب الخاص بالمتهم، وتبين أنه يحتوي علي صور جنسية خاصة بالأطفال ـــ وهي الجريمة المؤثمة بموجب المادة ١١٦/أ من قانون الطفل رقم ١٢ لسنة ١٩٩٦ م ـــ والمعدل بالقانون رقم ١٢٨ لسنة ٢٠٠٨م ـــ فإن الجريمة الأخيرة قد صادف صحيح القانون، ولا يؤثر في ذلك ما تسفر عنه التحقيقات بشان الجريمة الأصلية من أن نجل المتهم هو من أرسل تلك العبارات بواسطة جهاز الحاسوب المحمول الخاص به ( ) ٠

[الشرط الرابع] وجودة فائدة من التفتيش: استلزم المشرع الجنائي لصحة صدور الأمر بالتفتيش أن تكون الغاية من التفتيش ضبط أو سحب أو جمع أو التحفظ علي

البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه (م ٦ الفقرة ١ من جرائم التقنية) وبناء علي ذلك يجب أن يتوافر لدي المحقق أسباب كافية علي أنه يوجد علي نظام الحاسوب أو النظام المعلوماتي بيانات أو معلومات لها فائدة في ظهور الحقيقة علـــــي ارتكاب

جريمة من الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات ٠ فالتفتيش لا يتم إلا إذا توافرت لدي المحقق أسباب كافية علي أنه يوجد في المكان أو لدي الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء متحصلة منها أو أية مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة ( ) لدي المتهم المعلوماتي أو غيره٠ وبالتالي فإن مجرد وقوع جريمة من نوع الجناية أو الجنحة واتهام شخص معين بارتكابها أو المشاركة فيها لا يكفي لحث سلطة التحقيق إلي إصدار إذنها بالتفتيش ومباشرته ( ) ٠

ويتضح مما سبق، إنه إذا لم يكن للتفتيش غاية يستهدفها أو يسعي إلي الوصول إليها، أو كان يستهدف غير ما حدده المشرع فهو مشوب بعيب التعسف في استعمال السلطة٠ ومثال الحالة الأولي أن تكون الواقعة هي إطلاع غير مصرح به علي ملفات بيانات مخزنة داخل نظام حاسب إحدى الجهات من قبل احد القائمين علي تشغيله، فإنه واضح من البداية لا طائل من ورائه، ومثال الحالة الثانية أن تكون الجريمة المرتكبة سباً وقذفاً عن طريق الانترنت، وأن تكون الغاية المرجوة من التفتيش هي معرفة حسابات المتهم لدي البنوك ( ) ٠

ـــــ محل التفتيش: المحل الذي يقع عليه التفتيش للحصول علي في الجرائم المعلوماتية لاسيما الجرائم المتعلقة بالأنترنت هو جهاز الحاسب الآلي بمكوناته المادية والمنطقية وشبكات الاتصال به ( ) وهذه الأخيرة تشتمل علي الخادم والمزود الآلي والملحقات التقنية والتي قد توجد في حوزة شخص أو تكون موضوعه في مكان في مكان له حرمة المسكن ٠ ويقصد بالشخص كمحل لتفتيش نظم الحاسب الآلي قد يكون من مستغلي أو مستخدمي الحاسب الآلي أو من خبراء البرامج سواء أكانت برامج نظام أو برامج تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة والاتصالات، أو من مديري النظم المعلوماتية، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة أو تليفونات متصلة بجهاز المودم أو مستندات٠ وكذلك يقصد بالمنازل وما في حكمها ـــــ كمحل لتفتيش نظم الحاسب الآلي ـــــ كافة محال الإقامة أو المأوي والملحقات المخصصة لمنافعها ، والتي يشغلها الشخص سواء بصفة دائمة أو مؤقتة ، وسواء كانت ثابتة أو

(ISSN: 2356 - 9492)

متنقلة، متي ما وجدت فيها مكونات الحاسب الآلي سواء كانت مكونات مادية أو منطقية أو شبكات اتصال خاصة ( ) ٠

وفي فرنسا، فقد نصت المادة [٩٤] من قانون الإجراءات الجنائية الفرنسي والمعدلة بالقانون رقم ٤٧ لسنة ٢٠١٠م علي أنه: " يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها علي ماديات أو بيانات معلوماتية يكون كشفها مفيداً في إظهار الحقيقة" ( ) ٠ كما نصت المادة (١٧) فقرة (أ) من القانون الفرنسي رقم ٢٣٩ لسنة ٢٠٠٣ بشأن الأمن الداخلي الصادر في ١٨ مارس سنة ٢٠٠٣ م بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي علي البيانات التي تهم عملية البحث والتحري ٠ فتنص المادة ١٧ منه علي أنه:" لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش علي البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات المتصلة في شبكة واحدة مع النظام الرئيس أو يتم الدخول إليها أو تكون متاحة ابتداء من النظام الرئيس " ٠

ـــ السلطة المختصة بإصدار أمر التفتيش: نصت المادة [٦] من القانون ١٧٥ لسنة ٢٠١٨ م في شأن مكافحة جرائم تقنية المعلومات علي أنه: " لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين" ومفاد تلك المادة، أن السلطة المختصة بإصدار أمر التفتيش هي جهة التحقيق ، وهي أما أن تكون النيابة العامة ، وإما قاضي التحقيق بحسب الأحوال ٠ وفي فرنسا جعل المشرع الفرنسي قاضي التحقيق هو صاحب الاختصاص الأصيل في إصدار إذن التفتيش ٠ أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس ، ومتي اختص قاضي التحقيق بالدعوي، فمن حقه إجراء التفتيش علي النحو الذي يراه مفيداً في كشف الحقيقة، سواء كان ذلك لدي المتهم أو غيره ٠

ـــ الضمانات الشكلية لإذن التفتيش المعلوماتي: لم يستلزم القانون شكلاً معيناً لإذن التفتيش ـــ بصفة عامة ـــ كما لم يشترط عبارات خاصة يصاغ بها، ولكن يشترط أن يكون صريحاً ومكتوباً ومؤرخاً وأن يتضمن اسم ووظيفة من أصدره وأسم المتهم والجريمة المنسوبة إليه، وأن يحمل الإذن توقيع مصدره كما يتضمن من البيانات ما يحدد نوع الجريمة التي يهدف إلي التوصل إلي دليل بشأنها كما يجب تحديد محل التفتيش شخصاً كان أم منزلاً أو أحد نظم الحاسب الآلـــي وتحديد الميقات الزمني الذي ينفذ فيه الإذن ( ) ٠

الفرع الثالث

تسليم المعلومات

أجازت المادة السادسة من قانون جرائم تقنية المعلومات، لجهة التحقيق المختصة، بحسب الأحوال أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته، وحركة الاتصالات التي تمت علي ذلك النظام أو النظام التقني ٠ وقد عرف المشرع مقدم أو مزود الخدمة بأنه:" أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنية المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات " ٠ (المادة الأولي من قانون جرائم تقنية المعلومات) ٠

واشترطت الفقرة ثانياً من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات بأنه مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب علي مقدم الخدمة أن يوفر لمستخدمي خدماته ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة ، البيانات والمعلومات الاتية: [١] اسم مقدم الخدمة وعنوانه [٢] معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الالكتروني [٣] بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها [٤] أي معلومات أخري يقدر الجهاز أهميتها لحماية مستخدمي الخدمة ويصدر بتحديدها قرار من الوزير المختص ٠

والحقيقة الدقيقة، أن الأمر بالتسليم يكون موجهاً لمقدمي الخدمات، ومحله كافة البيانات أو المعلومات التي تتصل بارتكاب جريمة ما، ويشمل ذلك أيضاً بيانات مستخدمي الخدمة وحركة الاتصالات التي تمت، لتحديد تاريخ ووقت ومدة ونوع الاتصال ، ولتحديد معدات الاتصال المستخدمة وكذلك تحديد موقع المعدات الطرفية والاتصالات ( ) ٠ وهو إجراء يهدف إلي تمكين سلطات التحقيق من كشف الحقيقة وجمع الأدلة الرقمية ذات الصلة بجرائم تقنية المعلومات ( ) ٠ وقد حرضت العديد من المواثيق الدولية علي تقرير الأمر بتسليم المعلومات لسلطات التحقيق، من أبرزها الاتفاقية الأوربية في شأن الجرائم المعلوماتية (بودابست) والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فقد أجازت المادة (١٨) من اتفاقية بودابست إمكانية إصدار أمر لأي شخص لتقديم بيانات محددة موجودة علي حاسب آلي بحوزته أو تحت

(ISSN: 2356 - 9492)

سيطرته والمخزنة داخل نظام معلوماتي أو علي أي وسيط تخزين بيانات أخر ٠ ويجب على الهيئات أو الأشخاص المعنيين إتاحة المعلومات المطلوبة إلكترونيًا أو "محوسبًا" في أسرع وقت ممكن ( ) ٠

المطلب الثالث

اجراءات المحاكمة الخاصة بجرائم تقنية المعلومات

تقسيم:

نتناول هذا المطلب من خلال الفرعين التاليين:

[الفرع الأول] الاختصاص المكاني لجرائم تقنية المعلومات ٠

[الفرع الثاني] الاختصاص القضائي بنظر جرائم تقنية المعلومات ٠

الفرع الأول

الاختصاص المكاني لجرائم تقنية المعلومات

نصت المادة [٣] من القانون ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات علي أنه: " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون علي كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون، متي كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في الأحوال الآتية:

١- إذا ارتكبت الجريمة علي متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدي جمهورية مصر العربية أو تحمل علمها ٠

٢- إذا كان المجني عليهم أو أحدهم مصرياً ٠

٣- إذا تم الاعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليهما أو تمويلها في جمهورية مصر العربية ٠

٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية ٠

٥- إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج ٠

٦- إذا وجد مرتكب الجريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه ٠

ومفاد تلك المادة، أن المشرع الجنائي قد حدد نطاق تطبيق جرائم تقنية المعلومات من حيث المكان، وذلك علي النحو الآتي:

[أولاً] قواعد الاختصاص المكاني العامة في التشريع الجنائي المصري: حيث تخضع جرائم تقنية المعلومات ـــــ والواردة بالقانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ـــــ لقواعد الاختصاص العامة في قانون العقوبات المصري وهي؛ قواعد الإقليمية والشخصية الإيجابية والعينية، وذلك علي النحو التالي:

[أ] قاعدة الإقليمية: اعتنق القانون المصري مبدأ إقليمية القاعدة الجنائية ـــــ كقاعدة عامـــة ـــــ بتقريره في المادة الأولي من قانون العقوبات المصري بقوله: « تسري أحكام هذا القانون علي كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه » ٠ وما أضافته الفقرة الأولي من المادة الثانية من ذات القانون بقولها : « تسري أحكام هذا القانون أيضاً علي الأشخاص الآتي ذكرهم: (أولاً) كل من ارتكب في خارج القطر فعلاً يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها فـــــــــــــي القطر المصري »٠ ويعني ذلك، انطباق قانون العقوبات المصري علي كافة الجرائم التي ترتكب علي إقليم دولة مصر، بصرف النظر عن جنسية مرتكبيها سواء من الوطنيين أو من الأجانب ٠ بينما لا محل لسريان هذا القانون علي ما يقع من جرائم خارج هذا الإقليم أياً كانت جنسية مرتكبيها ٠ وقد سار المشرع المصري بهذه القاعدة مع ما تسير عليه سائر دول العالم وهو إقليمية القانون الجنائي ٠ ويأخذ المشرع الفرنسي، بمبدأ الإقليمية حيث تنص المادة [٢-١١٣] من قانون العقوبات علي أنه: " يطبق القانون الفرنسي علي الجرائم المرتكبة علي إقليم الجمهورية ٠ وتعتبر الجريمة قد ارتكبت علي إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع علي هذا الإقليم " ( ) ٠ ومفاد ما تقدم، أن كل من القانون المصري والفرنسي يطبق علي كثير من الجرائم المتعلقة بتقنية المعلومات ، طالما أن الجريمة قد وقعت فوق الإقليم المصري أو الفرنسي ٠

[ب] قاعدة الشخصية في شقها الإيجابي: تقتضي قاعدة الإقليمية عدم تطبيق قانون العقوبات المصري علي الجرائم المرتكبة خارج إقليم الدولة ولو كان مرتكبها من مواطني الدولة ٠ لكن المواطن الذي يرتكب جريمة في الخارج ثم يهرب إلي وطنه

(ISSN: 2356 - 9492)

يستطيع بهذا الشكل أن يفلت من العقاب، إذ أن الدولة التي ارتكب الجريمة فيها لا تستطيع أن تعاقبه عن جريمته، لأنها لو طالبت بتسليمه فلن يستجاب لطلبها، لأن كل دولة تحظر تسليم مواطنيها ٠ لذلك يتعين الخروج علي قاعدة الإقليمية بأن تقوم الدولة بمحاكمة مواطنيها الذين يرتكبون جرائم في الخارج ثم يعودون إلي وطنهم إذا لم يحاكموا في الدولة التي ارتكبوا الجرائم فيها أو إذا كانوا قد أدينوا ولم يستوفوا العقوبة المحكوم عليهم بها ٠ ويعد هذا الاستثناء من قاعدة الإقليمية، إعمالاً لما يُعرف بمبدأ الاختصاص الشخصي، الذي يُمكن من معاقبة المواطن بموجب القانون الجنائي لدولته إذا ارتكب جريمته خارج الدولة ٠ وقد نصت علي هذا الاستثناء من قاعدة الإقليمية المادة الثالثة من قانون العقوبات بقولها:" كل مصري ارتكب وهو في خارج القطر فعلاً يعتبر جناية أو جنحة في هذا القانون يعاقب بمقتضي أحكامه إذا عاد إلي القطر وكان الفعل معاقباً عليه بمقتضي قانون البلد الذي ارتكب فيه " ٠

ولقد أخذ المشرع الفرنسي، بمبدأ الشخصية في جانبها الإيجابي ، فقد نصت المادة [٦-١١٣] من قانون العقوبات علي أنه:" يطبق القانون الفرنسي علي كل جناية يرتكبها فرنسي خارج إقليم الجمهورية ٠ ويطبق هذا القانون أيضاً علي الجنح التي يرتكبها فرنسي خارج فرنسا إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي ارتكبت فيها ٠ وتطبق احكام هذه المادة حتي ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه " ٠

[جـ] قاعدة العينية: تقتضي قاعدة الإقليمية تطبيق قانون العقوبات المصري علي كل من يرتكب جريمة في إقليم الدولة، غير أن الأخذ بمبدأ الإقليمية علي إطلاقه يؤدي إلي نتائج لا يمكن قبولها ٠ فبعض الجرائم التي ترتكب خارج الدولة قد تكون من الخطورة بحيث تهدد كيانها أو تضر بمصالحها الحيوية، وهي برغم خطورتها لا تعني غيرها من الدول، وعلي هذا لا ينبغي التمسك بمبدأ الإقليمية وإلا أدي ذلك إلي إفلات مرتكبي هذه الجرائم الخطيرة من العقاب ٠ من أجل ذلك يأخذ مشرعنا الجنائي ـــــ إلي جانب قاعدة الإقليمية ـــ بما يعرف بمبدأ الاختصاص العيني؛ ومقتضاه أن يمتد نطاق تطبيق قانون العقوبات إلي خارج إقليم الدولة ليسري علي الجرائم التي ترتكب في الخارج وتنال من مصالحها الأساسية ٠

ولقد أخذ قانون العقوبات المصري بمبدأ الاختصاص العيني في حدود معينة نصت عليها المادة الثانية (ثانياً) ٠ فقد نصت هذه المادة علي سريان أحكام هذا القانون علي كل من ارتكب في خارج مصر جريمة من الجرائم الآتية:

(أ) جناية مخلة بأمن الحكومة مما نص عليه في البابين الأول والثاني من الكتاب الثاني من قانون العقوبات ٠

(ب) جناية تزوير مما نص عليه في المادة ٢٠٦ من قانون العقوبات ٠

(جـ) جناية تقليد أو تزييف أو تزوير عملة ورقية أو معدنية مما نص عليه في المادة ٢٠٢ أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلي مصر أو إخراجها منها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها مما نص عليه في المادة ٢٠٣ بشرط أن تكون العملة متداولة قانونا في مصر " ٠ ومن هذه الجرائم ما يمكن ارتكابه ـــ بطبيعة الحال ـــ عن طريق الانترنت، مثل جريمة السعي أو التخابر لدي دولة أجنبية (المواد ٧٧/ب ، ٧٧/ج ، ٧٧/د من قانون العقوبات) وجريمة تسليم أو إفشاء أسرار الدفاع عن البلاد (م ٨٠ عقوبات) وجريمة إنشاء أو تأسيس أو تنظيم أو إدارة جمعيات أو هيئات أو منظمات تهدف إلي سيطرة طبقة اجتماعية علي غيرها من الطبقات (م ٩٨/أ عقوبات) ٠

ولقد أخذ المشرع الفرنسي بمبدأ عينية النص الجنائي، حيث تنص المادة [١٠-١١٣] من قانون العقوبات الفرنسي علي أنه:" يطبق القانون الفرنسي علي الجنايات والجنح التي ترتكب في الخارج والتي تشكل اعتداء علي المصالح الأساسية للأمة المنصوص عليها في الباب الأول من الكتاب الرابع، وكذلك علي جرائم تقليد وتزوير أختام الدولة وتزييف العملة المعدنية أو الورقية أو السندات العامة والمعاقب عليها بالمواد ٤٤٢-١ ، ٤٤٢-٢، ٤٤٢-٥، ٤٤٢-١٥، ٤٤٣-١ ، ٤٤٤-١ وعلي أية جناية أو جنحة ترتكب ضد اعضاء أو أماكن البعثات الدبلوماسية أو القنصلية في الخارج " ( ) ٠ وبتطبيق هذه الأحكام والقواعد علي الجرائم المتعلقة بتقنية المعلومات ، نجد أن الاختصاص ينعقد للمشرع المصري او الفرنسي للجرائم الواردة في المادة ٢/ ثانياً والمادة ١١٣-١٠ ـــ والسابق الإشارة إليهما ـــ والتي يمكن ارتكابها عن طريق شبكة الإنترنت ، حتي ولو كان الموقع الذي توجد عليه هذه الجرائم خارج الإقليم المصري أو الفرنسي، وبصرف النظر عن جنسية الجاني ٠

[ثانياً] أحوال التوسع في الاختصاص المكاني لجرائم تقنية المعلومات: حرص المشرع الجنائي علي توسيع نطاق اختصاصه بنظر جرائم تقنية المعلومات التي تقع في الخارج، من خلال النص علي الأخذ بمبدأ عالمية النص الجنائي، ومبدأ الشخصية في شقه السلبي، وامتداد اختصاصه ليشمل الاعمال التحضيرية للجريمة، وتجريم

(ISSN: 2356 - 9492)

أنشطة جماعات الجريمة المنظمة التي تباشر أنشطتها في مصر ، وتوضيح ذلك فيما يلي:

١- إذا ارتكبت الجريمة علي متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدي جمهورية مصر العربية أو تحمل علمها ٠

فمما لا شك فيه، أن الجريمة لو وقعت علي متن وسيلة نقل جوي أو بري أو مائي مصرية، وهي خارج القطر المصري، فإن أحكام قانون العقوبات المصري علي التي تسري عليها باعتبارها في حكم الإقليم، وذلك بالنسبة لما يقع عليها من جرائم ٠ ولكن المشرع الجنائي قد توسع في نطاق السريان الإقليمي لقانون مكافحة جرائم تقنية المعلومات بشأن الجرائم التي تقع علي متن وسائل النقل الجوي أو البري أو المائي متي كانت وسيلة النقل هذه مسجلة لدي جمهورية مصر العربية أو تحمل علمها، وفي أي مكان وجدت وسيلة النقل ٠

٢- إذا كان المجني عليهم أو أحدهم مصرياً ٠

وهو تطبيق لمبدأ الشخصية في شقه السلبي، ومقتضاه إعمال قانون العقوبات المصري ليسري

علي الجرائم التي تقع علي مواطني الدولة المصرية، أياً كان مكان ارتكاب الجريمة أو أياً كانت جنسية مرتكبيها، ومن ثم يخضع للقانون المصري الذي يرتكب خارج الجمهورية، جريمة علي أحد مواطني جمهورية مصر العربية، حتي ولو وقعت من أجنبي خارج مصر ٠ وقد اشترط المشرع الجنائي في المجني عليه أو أحدهم أن يكون مصرياً أي متمتعاً بالجنسية المصرية، ويستوي أن يحمل الجنسية المصرية وحدها أو مع غيرها ٠ والعبرة بصفة المجني عليه وقت ارتكاب الجريمة لا بعدها ، فإذا غير المجني عليه جنسيته من المصرية إلي جنسية أخري بعد وقوع الجريمة فلا يحول ذلك دون سريان قانون جرائم تقنية المعلومات ٠

ولقد أخذ المشرع الفرنسي بالجانب السلبي لمبدأ الشخصية، فقد نصت المادة [١١٣-٧] من قانون العقوبات الفرنسي الجديد علي أن:" يطبق القانون الفرنسي علي أيه جناية، وكذلك علي أيه جنحة يعاقب عليها بالحبس يرتكبها فرنسي أو أجنبي في الخارج إذا كان المجني عليه فرنسياً لحظة ارتكاب الجريمة " ٠ وعليه فإن اختصاص القانون الفرنسي وفقاً للمادة سالفة الذكر، هو أن يكون المجني عليه فرنسياً، باعتبار أنه يهدف إلي حماية المجني عليه الفرنسي ضد الجرائم التي تقع عليه في الخارج ٠ ويترتب علي ذلك أن فاعل الجريمة التي ترتكب بواسطة الإنترنت علي إقليم دولة

أجنبية ضد مواطن فرنسي يحاكم في فرنسا، حتي ولو كان هذا الفعل غير معاقب عليه في البلد الأجنبي ٠

٣- إذا تم الاعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليهما أو تمويلها في جمهورية مصر العربية ٠

الأصل العام هو اختصاص المحاكم الجنائية بنظر الأفعال التي تشكل في ذاتها جريمة وفقاً لقانونها، ويخرج من نطاق التجريم الأعمال التحضيرية للجريمة علي اعتبار أنها لا تدخل في النموذج القانوني المكون للجريمة، وتشجيعاً للجناة علي ترك الجريمة، ولا يكون العقاب علي الأعمال التحضيرية إلا إذا كانت تلك الأفعال تشكل في نظر القانون جريمة بذاتها٠ ونظراً إلي الطابع التنظيمي لجرائم تقنية المعلومات وارتكابها من جانب جماعات إجرامية منظمة، وجسامة مثل هذه الجرائم وخطورتها علي المجتمع ، علاوة علي عدم تجريم تلك الأفعال من شأنه عدم إمكان مساءلة مرتكبي الجريمة، فقد حرص المشرع الجنائي علي مد اختصاصه الجنائي ليشمل الاعمال التحضيرية في جرائم تقنية المعلومات التي ترتكب داخل مصر ولو وقعت هذه الجريمة في الخارج، من خلال تقرير اختصاص المحاكم المصرية بنظر الاعمال التحضيرية التي تتم داخل مصر، وتشمل أفعال الاعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها ( ) ٠

٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية ٠

والمقصود بالجماعة هنا، أكثر من فرد سواء اتخذوا شكل جمعية أو هيئة أو منظمة أو عصابة مؤلفة من ثلاثة أشخاص علي الأقل أو كيان تثبت له هذه الصفة أياً كان شكله القانوني أو الواقعي، وسواء كانت داخل البلاد أو خارجها وأياً كان جنسيتها أو جنسية من ينتسب إليها، وقد اشترط المشرع لسريان القانون في هذه الحالة، أن تكون هذه الجماعة تمارس أنشطتها الإجرامية في أكثر من دولة من بينها مصر ٠

ومن الجدير بالذكر، أن قانون جرائم تقنية المعلومات لم يتضمن تعريف للجماعة الإجرامية المنظمة، علي عكس قانون مكافحة الإتجار بالبشر وقانون مكافحة الهجرة غير الشرعية، حيث عرفتها بأنها : " الجماعة المؤلفة وفق تنظيم معين من ثلاثة أشخاص على الأقل للعمل بصفة مستمرة أو لمدة من الزمن بهدف ارتكاب جريمة محددة أو أكثر من بينها جرائم تهريب المهاجرين وحدها أو مع غيرها، وذلك من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مادية أو معنوية أو لأى

(ISSN: 2356 - 9492)

غرض آخر، ولا يلزم أن يكون لأعضائها أدوار محددة أو أن تستمر عضويتهم فيها " (المادة الأولي من قانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين رقم ٨٢ لسنة ٢٠١٦) ٠

٥- إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج ٠

تسري أحكام قانون جرائم التقنية، علي كل من ارتكب خارج جمهورية مصر العربية من غير المصريين، جريمة من الجرائم المنصوص عليها في هذا القانون، متي كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني، إذا كانت الجريمة من شأنها إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها بغض النظر عن جنسيته ، أو كان من شأن الفعل إلحاق ضرر بأمنها أو بأي من مصالحها ، سواء كانت هذه المصالح في الداخل أو الخارج ( ) ٠

٦- إذا وجد مرتكب الجريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه ٠

ومقتضي هذه الحالة، سريان اختصاص المحاكم الجنائية المصرية بنظر جرائم تقنية المعلومات التي يتم القبض علي مرتكبيها في مصر، أياً كانت جنسيتهم وأياً كان مكان ارتكاب جريمتهم، ليشمل بذلك جرائم تقنية المعلومات التي ارتكبت خارج مصر ولو لم ترتكب من مصري، متي وجد مرتكب الجريمة بمصر سواء كان فاعلاً أم شريكاً، ولا شك في أن هذا التوسع في اختصاص قانون العقوبات المصري يتناسب مع طبيعة جرائم تقنية المعلومات عبر الوطنية، والتي قد ترتكب بمعرفة جماعات الجريمة المنظمة، وهو ما من شأنه تحقيق مواجهة فعالة لهذه الجرائم في التشريع الجنائي المصري ( ) ٠

الفرع الثاني

الاختصاص القضائي بنظر جرائم تقنية المعلومات

نصت المادة الرابعة من قانون رقم ١٢٠ لسنة ٢٠٠٨ الخاص بإنشاء المحاكم الاقتصادية ـــ والمعدل بالقانون رقم ١٤٦ لسنة ٢٠١٩م ـــ علي أنه: " مع عدم الإخلال بالاختصاصات المقررة للمحاكم الاقتصادية المنصوص عليها في أي قانون آخر، تختص المحاكم الاقتصادية بدوائرها الابتدائية والاستئنافية، دون غيرها، نوعيًا ومكانيًا بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها في القوانين الآتية:

١- قانون العقوبات في شأن جرائم المسكوكات والزيوف المزورة ٠

٢- قانون الإشراف والرقابة على التأمين في مصر ٠

٣- قانون شركات المساهمة وشركات التوصية بالأسهم والشركات ذات المسئولية المحدودة وشركات الشخص الواحد.

٤- قانون سوق رأس المال.

٥- قانون تنظيم نشاطي التأجير التمويلي والتخصيم.

٦- قانون الإيداع والقيد المركزي للأوراق المالية.

٧- قانون التمويل العقاري ٠

٨- قانون حماية حقوق الملكية الفكرية.

٩- قانون البنك المركزي والجهاز المصرفي والنقد.

١٠- قانون الشركات العاملة في مجال تلقى الأموال لاستثمارها.

١١- قانون تنظيم إعادة الهيكلة والصلح الواقي والإفلاس.

١٢- قانون حماية الاقتصاد القومي من الآثار الناجمة عن الممارسات الضارة في التجارة الدولية.

١٣- قانون حماية المنافسة ومنع الممارسات الاحتكارية.

١٤- قانون حماية المستهلك.

١٥- قانون تنظيم الاتصالات.

١٦- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

١٧- قانون مكافحة غسل الأموال.

١٨- قانون تنظيم الضمانات المنقولة.

١٩- قانون تنظيم نشاط التمويل متناهي الصغر.

٢٠- قانون الاستثمار.

(ISSN: 2356 - 9492)

٢١- قانون مكافحة جرائم تقنية المعلومات.

ومفاد تلك المادة ، أن المحاكم الاقتصادية هي الجهة المختصة بنظر جرائم تقنية المعلومات وقد ذهب البعض إلي أن المشرع المصري قد أحسن صنعاً بالنص صراحة علي اختصاص المحاكم الاقتصادية بنظر جرائم تقنية المعلومات ( ) والتي تستلزم قضاة متخصصون بالفصل في هذه النوعية من الجرائم ( ) ٠

خاتمة

اخترنا موضوع المواجهة الجنائية لجرائم تقنية المعلومات ـــــ والمنصوص عليها في القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات ـــــ نظراً لما يمثله هذا الموضوع من أهمية بالغة علي الصعيدين العلمي

والعملي ٠ فهذا الموضوع لم يحظى بدراسة قانونية كافية بين دراسي القانون لاسيما القانون الجنائي ٠ كما أنه يمثل حجر الزاوية في تحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة علي المعلومات وكفالة سريتها وعدم إفشائها أو التصنت عليها إلا بأمر قضائي مسبب، وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها ٠

ففي ظل التطور المستمر في نظم معالجة البيانات والمعلومات الآلية وتخزينها وتبادلها وتخليقها وتطويرها وتعدد المواقع والحسابات الخاصة والاتساع المضطرد في استخدام البريد الالكتروني والأجهزة والمعدات التقنية إلي جانب التطور المذهل في وسائل الاتصال المعلوماتي، كل ذلك كان له انعكاسات حتمية في تقنية المعلومات، إذ ترتكب جرائم بواسطة تلك الأنظمة والتقنيات باعتبارها من وسائلها وأدواتها، وهي ما يطلق عليها الأن تقنية المعلومات التي تكون المعلومات محلاً للجرائم أو أداة في ارتكابها ٠ من هذا المنطلق، كانت الحاجة ماسة إلي صدور القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات، وهو ما يستدعي الدراسة لبيان ما تضمنه من قواعد موضوعية وأحكام إجرائية بصدد تلك الجرائم ٠

ويقتضي التمهيد لتلك الدراسة أن نتعرض في البداية لماهية الجريمة المعلوماتية في المبحث الأول، تناولنا في المطلب الأول تعريف الجريمة المعلوماتية، بينما تعرضنا في المطلب الثاني للتطور التاريخي للجريمة المعلوماتية ٠ ووقوفاً علي ماهية القواعد الموضوعية لجرائم تقنية المعلومات، فقد عرضنا في المبحث الثاني للأحكام الموضوعية لجرائم تقنية المعلومات، عرضنا في المطلب الأول لجرائم الدخول غير المشروع، وتجاوز حدود الحق في الدخول، والاعتراض غير المشروع٠ تناولنا في الفرع الأول جريمة الدخول غير المشروع ، بينما عرضنا في الفرع الثاني لجريمة تجاوز حدود الحق في الدخول، وفي الفرع الأخير تعرضنا لجريمة الاعتراض غير المشروع ٠ بينما تعرضنا في المطلب الثاني لجرائم الاعتداء علي سلامة البيانات، والبريد الإلكتروني، وتصميم الموقع ٠ تناولنا في الفرع الأول جريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية، وفي الفرع الثاني جريمة الاعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة وفي الفرع الثالث جريمة الاعتداء علي تصميم موقع٠ وقد عرضنا في المطلب الثالث لجرائم الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة، وسلامة الشبكة المعلوماتية، تناولنا في الفرع الأول جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة ٠ وفي الفرع الثاني جريمة الاعتداء علي سلامة الشبكة المعلوماتية ٠

(ISSN: 2356 - 9492)

ولما كانت القواعد الإجرائية تمثل عاملاً رئيسياً في نجاح المواجهة الجنائية لجرائم تقنية المعلومات فقد أفردنا المبحث الثالث لبيان الأحكام الإجرائية لجرائم تقنية المعلومات، كرسنا المطلب الأول، لإجراءات الاستدلال الخاصة بجرائم تقنية المعلومات، تناولنا في الفرع الأول مأموري الضبط القضائي في جرائم تقنية المعلومات، بينما عرضنا في الفرع الثاني لإجراءات الاستدلال في جرائم تقنية المعلومات ٠ وبعد ذلك انتقلنا في المطلب الثاني، لإجراءات التحقيق الخاصة بجرائم تقنية المعلومات كرسنا الفرع الأول للتحفظ علي البيانات والمعلومات، بينما عرضنا في الفرع الثاني للتفتيش في النظم المعلوماتية، وفي الفرع الثالث تسليم المعلومات ٠

هذا، وقد أفردنا المطلب الأخير للحديث عن اجراءات المحاكمة الخاصة بجرائم تقنية المعلومات ٠ تكلمنا في الفرع الأول عن الاختصاص المكاني لجرائم تقنية المعلومات، ثم عرضنا في الفرع الثاني للاختصاص القضائي بنظر جرائم تقنية المعلومات ٠

وفي ضوء ما تقدم، نوصي في نهاية الدراسة بالآتي:

[أولاً] إدراج تعريف للجماعة الإجرامية المنظمة في قانون مكافحة جرائم تقنية المعلومات، وذلك علي غرار التعريف الوارد بقانون مكافحة الإتجار بالبشر، وقانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين ٠

[ثانياً] تقرير اعفاء من العقاب لمن يبادر من مرتكبي الجرائم المعلوماتية بإبلاغ السلطات بأمرها والطريقة التي استخدمها في ارتكابها والثغرات أو الفجوات التي استغلها في النظام لتنفيذ جريمته بشرط أن يكون ذلك قبل العلم بها وقبل وقوع الضرر ٠ لكن إذا تم الإبلاغ بعد علم السلطات بالجريمة، فإنه يجب لإعفاء المبلغ أن يؤدي الإبلاغ إلي ضبط باقي الجناة في حالة تعددهم أو يؤدي الإبلاغ إلي ضبط الأدوات المستخدمة في الجريمة ٠

[ثالثاً] نناشد المشرع الجنائي بأن يضع نصاً في قانون مكافحة جرائم تقنية المعلومات، يلتزم الشاهد بمقتضاه بالإعلام في الجرائم المعلوماتية ٠

[رابعاً] نناشد المشرع الجنائي بنقل نطاق تطبيق القانون من حيث المكان من الباب الأول من قانون مكافحة جرائم تقنية المعلومات إلي الباب الثاني المتعلق بالأحكام والقواعد الإجرائية، لارتباط الموضوع بالقواعد الإجرائية ٠

[خامساً] حث الدول ودعوتها إلي الاهتمام بالمؤسسات العلمية المتخصصة في مجال تقنية المعلومات وتقديم الدعم المادي والمعنوي لها لتكون مصدر دعم متكامل لمؤسسات الدولة القائمة علي مكافحة الجريمة في مواجهة الجرائم الإلكترونية، وإعداد أجهزة متخصصة للخبرة في مواجهة الجرائم المتعلقة بتقنية المعلومات ٠

[سادساً] دعوة وسائل الاعلام لإبراز الدور الهام لمكافحة الجرائم المتعلقة بتقنية المعلومات ٠

[سابعا] تكثيف الاهتمام التربوي للنشء من قبل مؤسسات المجتمع لاسيما المؤسسات التعليمية وذلك بتوعيتهم بالمخاطة الأمنية لشبكة الإنترنت وتوضيح العقوبات التي توقع علي مرتكبي هذه الجرائم ٠

[ثامناً] تدريس مادة جرائم تقنية المعلومات لطلاب الدراسات العليا بكليات الحقوق بالجامعات المصرية، لاسيما في هذا العصر عصر تكنولوجيا المعلومات التي أصبحت تتطور وبسرعة هائلة حيرت كل العقول، والتي لا تعكف عما هو جديد في كل عام ٠

[تاسعاً] ضرورة مواكبة التشريعات للتطورات المتسارعة في مجال تقنية المعلومات والبرامج، للحد من انتشار جرائم تقنية المعلومات، ومتابعة كل ما هو جديد ومستحدث في هذا المجال ٠

[عاشراً] نناشد المشرع الجنائي بأن يضع نصاً في قانون مكافحة جرائم تقنية المعلومات ، يجرم بمقتضاه عدم الإبلاغ عن جرائم تقنية المعلومات ٠

تلك عشرة توصيات، استخلصتها من خلال البحث والدراسة في موضوع جرائم تقنية المعلومات، في محاولة متواضعة من الباحث لدراسة وتحليل النصوص القانونية الواردة بالقانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ٠

"والله من وراء القصد "

المراجع التي أشير إليها في هذا البحث

[أولاً] المراجع العربية:

(ISSN: 2356 - 9492)

[أ] كتب عامة:

[١] د/ عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، عام ٢٠١٧م٠

[٢] د/ محمد زكي أبو عامر، الإجراءات الجنائية ، دار المطبوعات الجامعية بالإسكندرية، عام ١٩٨٤م٠

[٣] د/ نجاتي سيد أحمد سند، مبادئ الإجراءات الجنائية في التشريع المصري ، الجزء الأول، بدون ناشر، طبعة ٢٠١٥م٠

[ب] كتب خاصة:

[١] م/ بهاء المري، شرح جرائم تقنية المعلومات، منشأة المعارف بالإسكندرية، عام ٢٠١٩م ٠

[٢] د/جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية، عام ٢٠٠١م٠

ـــ د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، عام ٢٠٠١م ٠

[٣] د/ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، عام ٢٠٠٩م٠

[٤] د/ عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، دراسة مقارنة، دار النهضة العربية، عام ٢٠٠٩م٠

[٥] م/ عمر محمود الحوتي، الوجيز في الحماية الجنائية من جرائم تقنية المعلومات، وفق أحكام القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، دار النهضة العربية، عام ٢٠٢١م٠

[٦] د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها علي قانون العقوبات، دار النهضة العربية، عام ١٩٩٨م٠

[٧] د/ محمود رجب فتح الله، الوسيط فـــــي الجرائم المعلوماتية، دار الجامعة الجديدة، عام ٢٠١٩م٠

[٨] د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، عام ١٩٩٢م٠

[٩] د/ هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، الطبعة الأولي، عام ١٩٩٧م٠

[ج] رسائل:

[١] د/ إبراهيم إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية ، دراسة قانونية نفسية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، عام ١٩٨٠م٠

[٢] د/ أيمن عبد الله فكري، جرائم نظم المعلومات، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، عام ٢٠٠٥/٢٠٠٦م٠

[٣] د/ حسن فضيل خليف المناصير، جريمة الدخول غير المشروع إلي النظام المعلوماتي والتعدي علي محتوياته، دراسة مقارنة، رسالة ماجستير، عمادة البحث العلمي والدراسات العليا جامعة الأردن، عام ٢٠١٦م٠

[٤] د/ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، عام ٢٠٠٥م٠

[٥] د/ محمد سليمان خوالدة، جريمة الدخول غير المشروع إلي موقع الكتروني أو نظام معلومات وفق التشريع الأردني، دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا الجامعة الأردنية، عام ٢٠١٢م ٠

[د] دوريات ومقالات:

[١] د/ أحمد السيد الشوادفي علي، الحماية الإجرائية للشهود، دراسة مقارنة، مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد الرابع والثمانون، أكتوبر ٢٠١٨م٠

[٢] د/ أسامة بن غانم العبيدي، جريمة الدخول غير المشروع إلي النظام المعلوماتي، دراسة مقارنة، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، العدد [١٤] مايو ٢٠١٢م٠

[٣] د/ أحمد عبد اللطيف الجار الله، الحماية الجنائية للمعاملات الالكترونية، مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، المجلد [٤٠] العدد الأول، مارس ٢٠١٦م ٠

(ISSN: 2356 - 9492)

[٤] د/ أسامة بن غانم العبيدي، الجهود الدولية لمكافحة الجرائم المعلوماتية، مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، المجلد [٣٩] العدد [٤] ، ديسمبر ٢٠١٥م ٠

[٥] د/ بدر أحمد الجاسر الراجحي، الأحكام العامة للمواجهة الجنائية لظاهرة جرائم تقنية المعلومات، دراسة مقارنة، مجلة الحقوق ، جامعة الكويت ، مجلس النشر العلمي، المجلد [٤٤] العدد الرابع، ديسمبر ٢٠٢٠م ٠

[٦] د/ حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، دراسة تحليلية مقارنة، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد السابع (ملحق) ، يونيه ٢٠٢١م ٠

[٧] د / حسين خليل مطر، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون جامعة الكوفة، المجلد [١١] العدد [٣٦] ، إبريل ٢٠١٨م٠

[٨] د/ خليل يوسف جندي الميراني، المواجهة التشريعية للجريمة المعلوماتية علي المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة كركوك، المجلد السابع، العدد [٢٦] أغسطس ٢٠١٨م٠

[٩] د/ رامي متولي القاضي، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون ١٧٥ لسنة ٢٠١٨ مقارناً بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد [٧٥] مارس ٢٠٢١م٠

[١٠] د/ سالم سعيد محمد عبد الله، الضبطية القضائية في مواجهة الجرائم المستحدثة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنوفية، العدد [٥١] أكتوبر ٢٠٢٠م٠

[١١] د/ سعود علي اللوغاني، التفتيش في الجريمة الإلكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة الإسكندرية، العدد الثاني، عام ٢٠١٧م٠

[١٢] د/ سرحان حسن محمد حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد [٢٠] العدد [٧٩] ، أكتوبر ٢٠١١م ٠

[١٣] د/ سميرة معاشي، ما هي الجريمة المعلوماتية، مجلة المنتدي القانوني، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد السابع، إبريل ٢٠١٠م٠

[١٤] د/ سعيد سالم المزروعي، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقاً للتشريع الإماراتي، مجلة العلوم الاقتصادية والإدارية والقانونيـــــــــــــــــة، المركز القومي للبحوث ، غزة، المجلد الثاني، العدد [١٣] أكتوبر ٢٠١٨ م٠

[١٥] د/ عبد الإله محمد النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية، دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، المجلد [١٠] العدد الأول ، يونيو ٢٠١٦م٠

[١٦] د/ علياء علي القحطاني، الحماية الجنائية من جرائم التعدي علي أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، دراسة مقارنة، مجلة القانون والأعمال، جامعة الحسن الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، مختبر البحث قانون الاعمال ، العدد [٧٥] ، عام ٢٠١١م٠

[١٧] د/ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة الاسكندرية، العدد الأول، عام ١٩٩٢م٠

[١٨] د/ عبد الله ذيب عبد الله، جريمة الدخول غير المصرح به الواقعة علي الشبكات الإلكترونية الحكومية، دراسة مقارنة، مجلة المنارة للبحوث والدراسات، جامعة آل البيت، عمادة البحث العلمي، المجلد [٢٧] العدد الأول، عام ٢٠٢١م ٠

[١٩] د/ غنام محمد غنام ، ذاتية الإجراءات الجنائية في مجال جرائم تقنية المعلومات، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة العدد [٤٤] أكتوبر ٢٠٠٨م ٠

[٢٠] د/ محمد بن حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد [٢١] العدد [٨١] إبريل ٢٠١٢م ٠

[٢١] د/ مهند وليد اسماعيل الحداد، التنظيم القانوني لجريمة الدخول غير المصرح به إلي نظام الحاسب الآلي، دراسة مقارنة، مجلة العلوم الشرعية، جامعة القصيم، المجلد [١١] العدد الأول، سبتمبر ٢٠١٧م٠

(ISSN: 2356 - 9492)

[٢٢] د/ مصطفي علي خلف، التفتيش وفقاً لأحكام القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، المجلد [٦٣] العدد [٣] نوفمبر ٢٠٢٠م ٠

[٢٣] د/ ميادة مصطفي محمد المحروقي، ذاتية الضوابط الإجرائية للأدلة الجنائية الرقمية في الأنظمة القانونية ذات الأصل اللاتيني والأنجلو أمريكي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة الإسكندرية، العدد الثاني ، عام ٢٠١٨م٠

[٢٤] د/ نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، (المعاينة والتفتيش) مجلة الأندلس للعلوم الإنسانية والاجتماعية، جامعة الأندلس للعلوم والتقنية، المجلد [١٥] العدد [١٣] ، يناير ٢٠١٧م٠

[٢٥] د/ هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون ، أكاديمية شرطة دبي ، المجلد السابع، العدد الثاني ، يوليو ــ ربيع الأول ١٩٩٩م٠

[٢٦] د/ هدي حامد قشوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، المجلد [٣٥] العدد الثاني، يوليو ١٩٩٣م٠

[ثانياً] المراجع الفرنسية:

1. Julien Mucchielli, Cybercriminalité : « la situation française, en terme de ressources humaines, est proche de l'artisanal, Dalloz actualité 22 juillet 2014

2. Gabriel Thierry, Rapport sur le droit pénal à l'épreuve des cyberattaques, Des nouvelles propositions pour faire avancer la cyberjustice, Dalloz actualité 29 avril 2021
3. Frédérique Chopin, Infractions liées aux technologies de l'information et de la communication (Cybercriminalité) - Août 2020,Fiches d'orientation ,

4. S. Lavric, Renforcement de la lutte contre la cybercriminalité, Conclusions du Conseil JAI, 27 novembre 2008, Dalloz actualité 04 décembre 2008
5. - Cécile Duhil de Bénazé,Maintien frauduleux dans un fichier et vol de données: l'occasion peut faire le larron,Dalloz actualité 05 juin 2015
6. Cécile Duhil de Bénazé, Maintien frauduleux dans un fichier et vol de données : l'occasion peut faire le larron, Dalloz actualité 05 juin 2015 .
7. Lucile Priou-Alibert,Vol d'informations : nouvel épisode,Dalloz actualité 13 juillet 2001
8. -٨Méryl Recotillet,Consommation de la suppression d'un jugement dans un système de traitement automatisé de données,Dalloz actualité 25 juin 2021
9. M. Léna, Informatique : code d'accès valide mais non valable, Dalloz actualité 31 octobre2007
10. Alice RoqueśTrafic de moyens et atteintes aux STAD : précisions sur éléments constitutifs,Dalloz actualité, 7 février 2020
11. Dorothée Goetz, Atteintes aux systèmes de traitement automatisé de données : précisions sur la compétence de la justice parisienne,d alloz actualité 12 octobre 2018

(ISSN: 2356 - 9492)

12. Cécile Crichton,Précisions sur l'accès aux métadonnées à des fins de sécurité publique,Dalloz actualité 12 avril 2022
13. Cécile Crichton, Conservation de données > à des fins de sécurité nationale et de lutte contre la criminalité, Dalloz actualité 13 octobre 2020
14. Sofian Goudjil, Réquisition de données informatiques > dans le cadre d'une information judiciaire, Dalloz actualité 08 juillet 2022
15- Sébastien Fucini, Enquête préliminaire : accès à la partie privée d'un site internet, Dalloz actualité 19 novembre 2013
15. Cloé Fonteix, Saisies pénales > : n'est pas special qui veut, dalloz actualité 20 septembre 2019 .

16. Mélanie Bombled,Validité de la saisie globale de données informatiques,Dalloz actualité 27 novembre 2013
17. Gabriel Thierry,La délicate montée en puissance de la justice dans les affaires de cybercriminalité,Dalloz actualité 03 octobre 2018,p.4. ; Dorothée Goetz, Atteintes aux systèmes de traitement automatisé de données : précisions sur la compétence de la justice parisienne,d alloz actualité 12 octobre 2018