جامعة الأزهر
كلية الشريعة والقانون بأسيوط
المجـــلة العلميـــة

مدى فاعلية التشريعات الوطنية للحد من الجرائم المعلوماتية

إعداد
د/ حمدان بن درويش الغامدي
أستاذ القانون التجاري الدولي المساعد
جامعة أم القرى
معهد خادم الحرمين الشريفين لأبحاث الحج والعمرة
قسم البحوث الإدارية والإنسانية
المشرف علي وحدة بحوث الأنظمة والقانون

(العدد الثاني والثلاثون الإصدار الثاني يوليو ٢٠٢٠م الجزء الأول)

مدى فاعلية التشريعات الوطنية للحد من الجرائم المعلوماتية

حمدان بن درويش الغامدي.

قسم القانون التجاري الدولي، جامعة أم القرى، مكة المكرمة، المملكة العربية السعودية.

البريد الالكتروني: HDGHAMDI@gmail.com

ملخص البحث:

أدى تقدم تكنولوجيا المعلومات إلى خلق نوع جديد من الجرائم، والتي تنصب الأفعال المكونة لها على البيانات والمعلومات المخزنة على الأنظمة المعلوماتية والحسابات الخاصة والمواقع الإلكترونية بهدف سرقتها أو حرمان صاحبها منها، إذ أصبحت تلك المعلومات والبيانات من الأشياء التي تقوم بالمال. ويرجع ذلك إما لأهمية المعلومة نفسها لمساسها مثلا بحق من حقوق الملكية الفكرية، وإما لخسارة مالية ستلحق بصاحب المعلومة إذا فقدها أو حرم منها، من أجل ذلك، ونظرا للأضرار والخسائر الضخمة التي قد تلحق بأفراد والمؤسسات العامة والخاصة بسبب وقوع تلك الأفعال غير المشروعة، اتجه العالم إلى محاولة الحد من ارتكاب تلك الأفعال، فنصت المعاهدات الدولية والقوانين الداخلية على تجريم تلك الأفعال.

وتوصلت الدراسات والأبحاث إلى الوصول مفهوم تلك الجرائم وبيان خصائصها وخصائص مرتكبيها والأسباب التي تعوق اكتشافها وملاحقة مرتكبيها، وكذلك الإمكانيات القانونية التي يجب توفيرها في النصوص القانونية للدول من أجل تحقيق تلك الجرائم وتقديم مرتكبها للعدالة مع أدلة إسناد تثبت ارتكابه تلك الجريمة.

ومن أجل ذلك أيضا حاول المشرع السعودي أن يضع نظام يقرر فيه تجريم الأفعال التي تمس بسلامة البيانات والمعلومات والأنظمة المعلوماتية والمواقع الإلكترونية والحسابات، بالإضافة إلى تجريم الأفعال التي تكون تكنولوجيا المعلومات وسيلة لارتكابها.

الكلمات المفتاحية: **التشريعات الوطنية، الجرائم المعلوماتية، الملكية الفكرية، تكنولوجيا المعلومات.**

The effectiveness of national legislations on reducing information crimes

Hamdan bin Darwish Al-Ghamdi

Department of International Trade Law, Umm Al-Qura University, Makkah Al- Mukarramah, Kingdom of Saudi Arabia.

Email: HDGHAMDI@gmail.com

Abstract:

The advancement of information technology has created a new type of crimes, whose formation actions focus on data and information stored on information systems, private computer accounts and websites with the aim of robbing them or depriving owners of their accounts. Such information and data have to do with properties and making money. This can be attributed either to the importance of the piece of information itself as it is related, for example, to an intellectual property right, or to a financial loss incurred on the owner of information when he loses it or is deprived of it. Given the huge damages and losses that may be inflicted on individuals and public and private institutions due to the occurrence of these illegal acts, the world has turned to crackdown on these acts. International treaties as well as internal laws have stipulated the criminalization of those acts. Studies and research papers have explored the concept of those crimes, underlined their characteristics as well as the features of their perpetrators, and highlighted the reasons that hinder their detecting and the prosecution of their perpetrators. They have also discussed the legal capabilities that must be provided for in the legal texts of states in order to thoroughly investigate these crimes and bring their

perpetrators to justice with supporting evidence to prove their commission of such crimes. To this end, the Saudi legislator has also attempted to set a legal system in which it provides for criminalizing acts that affect the integrity of data, information, information systems, websites and accounts, in addition to criminalizing acts that information technology is a means of their commission.

Keywords: National Legislations، Information crime، Intellectual property، Information technology.

مُقَدِّمَة

أدى التطور التقني لنظم المعلومات، والتقدم السريع، والمتواصل للأجهزة، والبرامج المعلوماتية، واعتماد الدول على التقنية المعلوماتية في شتى المجالات إلى اتساع دائرة ومجالات استخدام الحاسبات الإلكترونية، و النظم المعلوماتية، وأصبحت معظم الأجهزة، والمؤسسات العامة، والخاصة تعتمد على أجهزة الحاسب الآلي في تسيير شئونها وتقليل الاعتماد على المستندات الورقية. وحيال هذا التقدم التكنولوجي أصبح لزاما على الدولة ممثلة في سلطتها التشريعية ان تبسط حمايتها على هذه النظم الحديثة وتوفر لها وسائل التأمين من الناحية القانونية التي تتفق وطبيعتها.

إلا أن المشكلة في إضفاء الحماية القانونية على نظم المعلومات هي ما تتميز به تلك الجرائم من خصائص، و التي تصل بالقائمين على الحماية من تلك الجرائم إلى صعوبة اكتشاف الجريمة المعلوماتية، حيث أنها هادئة لا تتسم بالعنف وهي جريمة فنية لا يتخلف عنها آثار مادية ملموسة كتلك التي تخلفها جريمة السرقة أو جريمة الاعتداء على الآخرين.

كذلك كلما تقدم الإنسان في فهم تكتيك العمل في الأنظمة المعلوماتية كلما استطاع أن يرتكب جريمته دون ان يترك أثار يمكن عن طريقها الوصول اليه. وعلى ذلك تعد الجريمة المعلوماتية من اهم الجرائم التي تحتاج إلى حماية جنائية كافية.

ومن الملاحظ أن النصوص الجنائية التقليدية التي تكفل الحماية القانونية للحق في الخصوصية كالنصوص التي تحمي حرمة المسكن، و الحياة الخاصة، و المحادثات لا تكفي لكفالة هذه الحماية في مواجهة خطر الإجرام المعلوماتي.

واذا كان القضاء يقوم بدور تفسير النصوص الجنائية في الحدود، و النطاق التي تمتد اليه عبارات النصوص، فان ذلك يعد مقبولا مادام في اطار مبدأ الشرعية الجنائية وما يتفرع منه من خطر حظر القياس في مواد التجريم، و العقاب.

لذلك كان لابد على المشرع ان يمارس سلطاته في تجريم ما يستجد من الأفعال الضارة بالمصالح الجوهرية في المجتمع. وهوما حدا بالمشرع السعودي، والدول العربية، وغيرها عندما تلمس انه في اشد الحاجة إلى سن قوانين تجرم الأفعال والجرائم الخاصة بأمن المعلومات.

أهمية البحث:

تأتي أهمية البحث من أهمية الدور الذي تلعبه التشريعات الوطنية في الحد من الجرائم المعلوماتية، لا أقول على المستوى الوطني فقط بل على المستوى الدولي أيضا، الجريمة المعلوماتية لا علاقة لها بدولة متقدمة أو غير متقدمة، فالدول المتقدمة لا تستطيع ان تحمي نفسها من تلك الجرائم مهما تقدم بدون تعاون مع الدول الأخرى، ويأتي هذا التعاون من خلال سن قوانين داخلية في جميع الدول تجرم تلك الأفعال بشكل متفق عليه حتى تتمكن الدولة التي تم الاعتداء على احد مؤسساتها الخاصة او العامة من ملاحقة المجرم المعلوماتي الذي ارتكب الجريمة.

إشكالية البحث:

يثير هذا البحث عدة تساؤلات أولها هل للجريمة المعلوماتية مفهوما يختلف عن مفهوم الجريمة التقليدية وما هو محل تلك الجريمة وما هي طبيعته القانونية؟ وهل هناك خصوصية للجريمة المعلوماتية و المجرم المعلوماتي؟ هل

ما نص عليه المشرع السعودي في نظام مكافحة جرائم المعلوماتية كافي للحد من تلك الجريمة؟

أهداف البحث:

يهدف البحث الى التعرف على مفهوم الجريمة المعلوماتية ومحلها وتطبيعته القانونية، كذلك الوقوف على خصائص الجريمة المعلوماتية و المجرم المعلوماتي. كذلك معرفة مدى فاعلية القوانين الوطنية لاسيما السعودي و المصري في الحد من تلك الجرائم وهل ما وضعه المشرع المسعودي و المصري من نصوص كافي للحد من تلك الجريمة.

منهج البحث:

أدت إشكالية البحث بالباحث الى إستحدام المنهج الوصفي التحليلي، كذلك ستخدم الباحث في الإجابة على التساؤلات التي يثيرها البحث المنهج المقارن، وذلك لمقارنة النظام السعودي بالقانون المصري في مسألة الجرائم المعلوماتية.

خطة البحث

قسم الباحث بحثه إلي مبحثين، المبحث الأول يعرض فيه لماهية الجرائم المعلوماتية ، اما المبحث الثاني نبين فيه الدور الذي قام به النظام السعودي و القانون المصري للحد من تلك الجرائم. وعلى ذلك فقد انقسم البحث الى ما يلي:

المبحث الاول : ماهية الجريمة المعلوماتية

المبحث الثاني: دور التشريعات الوطنية في مكافحة الجرائم المعلوماتية

المبحث الأول

ماهية الجريمة المعلوماتية

الجريمة في حد ذاتها هي سلوك انساني غير مشروع صادر عن إرادة إجرامية يفرض له القانون جزاء جنائيا.(١) والجريمة المعلوماتية لا تختلف في تعريفها كثيرا عن التعريف التقليدي للجريمة بوجه عام. إلا أنها تتمتع ببعض الخصائص التي لا تتمتع به الجريمة التقليدية. كذلك المجرم المعلوماتي له من الخصائص التي تختلف عن خصائص المجرم التقليدي. وعلى ذلك سنبين في هذا المبحث تعريف الجريمة المعلوماتية، ثم نبين خصائص الجريمة المعلوماتية والمجرم المعلوماتي وذلك في المطلبين التاليين.

المطلب الأول

التعريف بالجريمة المعلوماتية

عرف رأي في الفقه الجريمة المعلوماتية بأنها " كل إشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب الالي".(٢)

وعرفه رأي آخر بأنها نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه.(٣)

---

(١) فتوح عبد الله الشاذلي، شرح قانون العقوبات ، القسم العام، دار المطبوعات الجامعية، ط ٢٠٠١، ص ٦٣

(٢) منير محمد الجهيني ، ممدوح محمد الجهيني، جرائم الانترنت و الحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ط ٢٠٠٦ ، ص ١٤ ، انظر ايضا هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية، ط ١٩٩٩، ص ١١٠

(٣) هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ط ١٩٩٢ ، ص ٥

كذلك ذهب جانب من الفقه الى أن الجريمة المعلوماتية هي أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لارتكابه، و التحقيق فيه وملاحقته قضائيا.(١)

وعرفها قانون مكافحة جرائم المعلوماتية السعودي بأنها أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

ويرى الباحث أن الجريمة المعلوماتية هي كل فعل غير مشروع عمدي أو غير عمدي يمثل مساسا بالبيانات و المعلومات الموجودة داخل الأنظمة المعلوماتية أو الشبكات المعلوماتية أو المواقع الالكترونية أو الحسابات والبريد الالكتروني .

- **المعلومات هي محل الجرائم المعلوماتية**:

ثار جدل طويل حول الحماية القانونية للمعلومات في حد ذاتها منظورا اليها بمعزل عن الوسيط المادي الذي يمكن أن يندمج فيه. فعلى الرغم من الأهمية الاقتصادية للمعلومات فإنها تظل مجرد أفكار غير قابلة للسرقة أو أن تكون هذه المعلومات محلا لعدد من الجرائم كالنصب أو خيانة الأمانة ومن ناحية أخرى ، فإنه قد لا تتوافر في هذا المعلومات مقومات الملكية الفكرية حتى تحميها النصوص الخاصة بحماية هذا النوع من الملكية وقد أدى الجدل المتقدم للتشكيك في توافر الحماية اللازمة لهذه المعلومات على الرغم مما تتمتع به من قيمة اقتصادية كبيرة. ومن خلال هذا المطلب سوف نبين طبيعة المعلومات باعتبارها محلا يمكن الاعتداء عليه من الناحية القانونية وذلك من خلال بيان الشروط اللازم

(١) سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، ٢٥الي ٢٨ اكتوبر، ص ٥١٦

توافرها ابتداء في المعلومة حتى يمكن أن تتمتع بالحماية القانونية ثم نبين الطبيعة القانونية للمعلومة، وهل لها طبيعة خاصة أم أنها شكل جديد من أشكال القيم المادية، و ذلك على التفصيل الاتي.

أولا: شروط يلزم توافرها في المعلومات:

يلزم أن تتوافر في المعلومات بصفة عامة – سواء أكان التعبير عنها يتم من خلال وسيط مادي ، ام كانت بمعزل عن هذا الوسيط – بعض الصفات التي يمكن أن تتمتع بالحماية القانونية، و تتمثل هذه الصفات فيما يلي :

ـ أن تكون المعلومة مبتكرة، و محددة:

أن المعلومة التي تفتقر لصفة التحديد لا يمكن ان تكون معلومة حقيقة . فاذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ، و التبادل عن طريق علامات أو إشارات مختارة فينبغي ان تكون محددة فالمعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها وتحديد جوانبها وهو ما يعد ضروريا في حالة الاعتداء على الأموال لأن هذا الاعتداء يجب أن يكون منصبا على شيء محدد، و ان يكون هذا الشيء بدوره محلا لحق محدد. كذلك يجب ان تنصب صفة الابتكار على الرسالة التي تحملها المعلومة فالمعلومة غير المبتكرة هي معلومة عامة متاحة للجميع ولا يمكن نسبتها إلى شخص محدد أو طائفة من الأشخاص.[1]

ـ أن تتصف المعلومة بالسرية، و الاستئثار:

كلما اتسمت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها محددا بمجموعة معينة من الأشخاص وبدون هذا التحديد فانه لا يمكن أن

(١) د/ طارق ابراهيم الدسوقي،الامن المعلوماتي، دار الجامعة الجديدة ، ط ٢٠١٥ ، مصر ، ص ٤٤

تكون المعلومة محلا يعتدى عليه بالسرقة أو النصب على سبيل المثال، فالمعلومة غير السرية تكون صالحة للتداول ومن ثم تكون بمنأى عن أي حيازة كالمعلومات التي تتعلق بحقيقة معينة(كحالة الجو) أو بحدث معين أو بخدمة متاحة للجمهور وهي جميعها معلومات تفتقر السرية.

وقد تستمد المعلومة سريتها من طبيعتها كاكتشاف في أحد المجالات التي تتميز بالسرية أو لرغبة صاحبها في ذلك أو للسببين معا كما في حالة الشفرة السرية الخاصة باستعمال بطاقات الائتمان. وفي جميع الحالات فان السرية التي تتمتع بها المعلومة هي التي تحدد نطاق استعمالها في دائرة محددة بحيث يستفيد أصحابها من الخاصية الثانية، و هي الاستئثار بالمعلومة.

وتعد خاصية الاستئثار بالمعلومة أمرا ضروريا لأنه في مختلف الجرائم التي تنطوي على اعتداء قانوني على الأموال فان الفاعل يعتدي على حق يخص الغير على سبيل الاستئثار ويتوافر للمعلومة هذه الصفة إذا كان الوصول اليها غير مصرح به إلا لأشخاص محددين. إلا أن الاستئثار بالمعلومة قد يرجع إلى سلطة شخص ما على المعلومة في التصرف فيها، وفي هذه الحالة يكون الاستئثار لمؤلف المعلومة، ويرتبط بهذا الشكل من أشكال الاستئثار بالمعلومة نوع من الرابطة نجدها متحققة في حالتين:

الحالة الأولى: تتعلق بالمعلومات التي ينصب موضوعها على بيان حقيقة أو أمر ما ، وهذا النوع من المعلومات هو بحسب الأصل غير سري ومتاح للجميع أما إذا قام شخص بتجميع وحفظ هذه المعلومات ذاتها فهو ينشأ عن طريق هذا التجميع معلومة جديدة يمكن أن يستأثر بالتصرف فيها بمفرده أو لمن يسمح له بالاطلاع عليها من خلال رمز سري معين.

وتتحقق الحالة الثانية عند توافر الرابطة بين المعلومة، و صاحبها عندما يكون موضوع هذه المعلومة فكرة أو عمل ذهني أو إعداد أو تنسيق امر ففي هذه الحالة ينظر مؤلف المعلومة اليها باعتبارها ملكا خاصا خالصا له وهو على حق في ذلك ، فاذا تمكن الغير من الاستيلاء عليها وعلى نحو غير مشروع فسوف يشعر صاحبها بأنه قد سلب منه شيء يمتلكه.(١)

ثانيا : الطبيعة القانونية للمعلومات:

كما أوضحنا سلفا تتمتع بعض المعلومات بقيمة اقتصادية، إلا أن ذلك يثير التساؤل عما إذا كانت المعلومات في ذاتها، منفصلة عن الوسيط المادي الذي يعبر عنها، تعد من القيم المالية التي يمكن الاعتداء عليها وقد انقسم الفقه عند الإجابة على هذا التساؤل إلى اتجاهين على النحو التالي :

الاتجاه الأول: للمعلومات طبيعة قانونية من نوع خاص:

يرفض هذا الاتجاه إدراج المعلومات ضمن القيم المالية التي يمكن الاعتداء عليها فهذه القيم يجب أن تكون قابلة للتملك ويترتب على ذلك أن الأشياء التي يمكن الاستئثار بها هي وحدها التي تدخل في عداد القيم أما المعلومات لما لها من طبيعة معنوية فلا يمكن الاستئثار بها ولا تندرج في مجموعة القيم المحمية، ما لم تكن تنتمي إلى المواد الأدبية أو الفنية أو الصناعية التي تحميها حقوق الملكية الأدبية أو الفنية أو الصناعية ولا ينكر أنصار هذا الاتجاه ما للمعلومات من قيمة اقتصادية وهو ما أدى بالبعض إلى إدخال المعلومات في عداد الحقوق المالية مع استبعادها من طائفة القيم المالية، وإدخالها في طائفة المنافع، و الخدمات ، فللمعلومات في رأي انصار هذا الاتجاه علاقة مباشرة بفكرة المنفعة أو الخدمة فمن ناحية فان نشأة المعلومة غالبا ما تكون استناد إلى عمل سابق عليها .،

(١) د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص ٤٥، ٤٦

ومن ناحية أخرى ، فان الإلمام بالمعلومة يساعد بصفة عامة على القيام بعمل ما بصورة أسهل، وأسرع . لذا يمكن في هذه الحالة اعتبار المعلومات خدمة أو منفعة تقوم بالمال، وهو ما يؤدي إلى الخلط ووصف المعلومات بأنها قيمة مالية. (١)

إلا أن استبعاد المعلومات من نطاق القيم المالية ، لم يمنع الفقه، و القضاء الفرنسي من محاولة إيجاد حماية قانونية لها في حالة الاستيلاء غير المشروع عليها ولقد اتخذت هذه المحاولة عدة أشكال تنوعت بين الاستعانة بدعوى المنافسة غير المشروعة، و التطبيق الموسع لنظرية التصرفات الطفيلية، وتأسيس الخطأ على نظرية الإثراء بلا سبب وأخيرا، تأسيسه على فكرة المسئولية التقصيرية.(٢)

الاتجاه الثاني: المعلومات طائفة جديدة من القيم(٣):

يذهب أنصار هذا الاتجاه إلى اعتبار المعلومات قيمة تضاف إلى غيرها من القيم الأخرى، ولقد تبنى جانب من الفقه الفرنسي هذا الاتجاه وعلى رأسهم

---

(١) د/ نائلة قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، ط ٢٠٠٥، ص ١١٦

(٢) د/ محمد سامي الشوا، ثورة المعلومات، و انعكاستها على قانون العقوبات، دار النهضة العربية ، ص ١٨٠ ، انظر أيضا د/ محمد علي العريان، الجرائم المعلوملتية ، دار الجامعة الجديدة ، ط ٢٠١١، ص ٦٢ ، انظر أيضا ، د/ عبد الله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الالي، دار النهضة العربية ، ط ٢٠٠٢ ، ص ١٦٣ وما بعدها.

(٣) د/ عبد الله حسين على محمود ، المرجع السابق ، ص ١٦٩، ١٧٠، ١٧١، انظر أيضا د/ نائلة قورة ، المرجع السابق ،ص ١١٩، ١٢٠، انظر أيضا ، د/ محمد على العريان ، المرجع السابق ، ص ٦٣، ٦٤ ..

كلا من الأستاذ "Pierre Catala "، و الأستاذ "Michel Vivant" . فتعد المعلومة طبقا للأستاذ CATALA واستقلالا عن دعامتها المادية من قبيل المال للحيازة، و لتدعيم هذا الوصف فقد أشار بأن المعلومة قابلة للحيازة عندما لا يحظر السوق ، وهي قيمة تقوم لسعر السوق وانها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها. وأن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية وهي علاقة المالك بالشيء الذي يملكه وأنها تنتمي إلى مؤلفها بسبب علاقة التبني التي تربط بينهما.

ويؤكد الأستاذ VIVANT هذا الرأي مستندا إلى حجتين الأولى هي إن فكرة الشيء أو المال والذي يغلب عليه الطابع المعنوي وان صفة محل الحق يجوز أن تستند إلى مال معنوي بحيث يكون هذا المال من قبيل الأموال الاقتصادية وأنه جدير بحماية القانون. أما الحجة الثانية هي أن كل الأشياء المملوكة ملكية معنوية، و التي يعترف بها القانون ترتكز على الإقرار بأن للمعلومة قيمة عندما تكون بصدد براءة اختراع أو علامات أو رسومات أو نماذج أو من قبيل حق المؤلف، ومنشأ المعلومة هو الذي يقدم ويكشف ويطلع الجماعة على شيء ما بغض النظر عن الشكل أو الفكرة فهو يقدم لهم المعلومة بمعنى واسع ولنها خاصة به ويجب أن تعامل هذه الأخيرة بوصفها مالا وتصبح محلا للحق، فلا يوجد ما يسمى بالملكية المعنوية بدون الاعتراف بالقيمة المعلوماتية.

ويستخلص من ذلك أن المعلومة باعتبارها مالا فهي مجموعة تندرج في نطاق القانون الوضعي، فمن وجهة نظر هذا الرأي أن المعلومة حتما من قبيل المال بسبب قيمتها الاقتصادية ، فان هذا المال ليس بمال مستحدث لأنه يدخل في مجموعة قائمة من قبل خاصة بالأموال المعلوماتية والتي وفقا لرأيه متاحة ومعترف بها عن طريق الملكية الأدبية ، وحينئذ يفهم أنه يقرر وبحسم على فكرة

أن المعلومة يمكن ان تكون محلا لعقد بيع طالما أن الإبداع يرتبط بصاحبه، بل يمكن علاوة على ذلك نقل حق الانتفاع بالمعلومة أو استغلالها، ويضيف ان لصاحب المعلومة ان يتنازل عنها بموجب عقد أو قيد استخدامها أو ان يرفضه.

المطلب الثاني

خصائص الجريمة المعلوماتية

أولا: خصوصية الجريمة المعلوماتية:

من خصائص هذه الجريمة انها ليست عادية او تقليدية ترتكب بصورة عشوائية أو غير مدروسة. بل أنها جريمة تنفذ بواسطة خبراء على درجة عالية جدا من التخصص والكفاءة في استخدام الحاسب الآلي، والانترنت، على درجة من سعة الأفق و الحيلة. ويتمتع هؤلاء الخبراء بمكانة اجتماعية ولديهم قدر من العلم والتقنية التكنولوجية ومهارات، ومعارف فنية في مجال الكمبيوتر والانترنت، وكيفية التعامل معها ، بحرفية عالية.(١)

كذلك أن تحديد وتصنيف الافعال التي تتحقق بها الجرائم المعلوماتية ، أمر لا يخلو من الصعوبات. ويرجع ذلك الى التطور التكنولوجي المستمر. فالجريمة المعلوماتية تلاحق هذا التطور في كل صورة، نظرا للارتباط الوثيق بينهما. وقد القى هذا الوضع بظلاله على صياغة النصوص الواردة في التشريعات التي تعاقب على الجرائم المعلوماتية، سواء فيما يتعلق بتحديد المصالح المحمية، او بتحديد الاساليب و الانماط المختلفة للصياغة التشريعية الخاصة بهذه الجرائم.(٢)

---

(١) حسن بن احمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وابحاث ، جامعة الجلفة ، ٢٠٠٩ ، ص ٥١٧

(٢) محمد امين الشوابكة، جرائم الحاسوب و الانترنت – الجريمة المعلوماتية، دار الثقافة للنشر و التوزيع، عمان ،ط ٢٠٠٧ ، ص ٤٥

إلا أن الفقه اختلف ومن وراءه التشريعات الجنائية في تصنيف الجرائم المعلوماتية، اختلافا يجد أساسه في تباين المعايير التي يتبناها كل فقيها وتشريع على حده، إلا أن هذه الاختلافات كان هناك قاسما مشتركا بينهم ، وهو أنه يمكن اختزال هذه الجرائم في نمطين رئيسيين. أولهما الجرائم التي يستعان فيها بالحاسب الالي لارتكابها ، وهذا النوع من الجرائم لا يعدو أن يكون فيها الحاسب الآلي مجرد أداة أو وسيلة لارتكابها بحيث تتم الجريمة لو استعان الجاني بأداة أخرى ، وهذا النوع يعد من الجرائم التقليدية وبالتالي امكانية اخضاعها للحماية الجنائية وفقا لقواعد القانون الجنائي التقليدي.(١)

أما النمط الثاني من جرائم الحاسب الآلي، فهي تلك الجرائم التي يكون فيها الحاسب الالي موضوعا لها بعنصريها المادي و المعنوي. وهنا يفرق بين حالتين، الحالة الأولي ، هي التي يكون محل الجريمة المكونات المادية للحاسب الآلي من أجهزة و معدات وكابلات وشبكة ربط والات طباعة وتصوير وغيرها من أجهزة. فهنا نحن أمام جريمة تقليدية تقع على أشياء مادية سواء تم سرقتها ام اتلافها. اما الحالة الثانية ، هي الحالة التي يكون فيها محل الجريمة البيانات و المعلومات التي بداخل الحاسب الآلي ، فهي الجريمة المعلوماتية التي يقصدها البحث، وهي جريمة تتميز بخصائص تختلف عن الخصائص التي تخضع للقوانين الجنائية التقليدية.(٢)

---

(١) James Richard, " Transational criminal organization cybercrime, and money laundering" ed 1998 , p 40

(٢) نهلة عبد القادر المونمي، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان ، ط ٢٠٠٤ ، ص ٤٩ .

انظر ايضا، محمد كرام ، صعوبات اثبات الجرائم المرتكبة عن طريق التقنيات الحديثة، مجلة المحامي ، العدد ٤٤ ، ٢٠٠٤ ، ص ٣٣١.

وتتميز الجريمة المعلوماتية بقلة عدد الحالات التي تم اكتشافها بالفعل إذا ما قارنا ذلك على ضوء ما يتم اكتشافه من الجرائم التقليدية . ويرى البعض ان من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف، كما أنها لا تترك أثار وإنما يتمثل مظهرها في تغيير أو محو الأرقام، و البيانات الموجودة بأنظمة الحاسبات الآلية. ولا تترك اثر خارجيا مرئيا أو ملموسا.(١) إلا أنه يرى البعض الأخر صعوبة قبول هذا الرأي المتقدم على إطلاقه، فمن ناحية لا يقتصر أثر جرائم المعلوماتية على تغيير أو محو الأرقام، و البيانات من الملفات المخزنة في ذاكرة الحاسب الآلي حتى في هذه الحالة فمجرد تغيير أو محو هذه البيانات يعد أثرا على ارتكاب الفعل فصعوبة اكتشافها وإثباتها يرجع إلى عدة أسباب من بينها وسيلة تنفيذها، و التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد . بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم. فضلا عن إمكانية تدمير المعلومات التي يمكن ان تستخدم كدليل في الإثبات في مدة قد تقل عن ثانية واحدة.(٢)

ولا يتمثل الاختلاف بين الجريمة المعلوماتية، و الجريمة التقليدية في معدل ارتكابها ومقدار الخسائر الناجمة عنها فقط، بل تتميز الجريمة المعلوماتية أيضا بكونها لا تتسم بالعنف الذي تتسم به غيرها من الجرائم التقليدية، فالجريمة المعلوماتية جريمة هادئة بمعنى انها لا تحتاج الى اي مجهود عضلي كالاغتصاب

(١) د/ هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، ١٩٩٢، ص ٤١ ، انظر أيضا / د/ نائلة قورة ، المرجع السابق ، ص ٤٩

(٢) د/ هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، ١٩٩٢، ص ٤٢ ، انظر أيضا / د/ نائلة قورة ، المرجع السابق ، ص ٤٩

أو القتل وركنها المادي قد لا يتجاوز مجرد لمسات بسيطة على لوحة مفاتيح الحاسب الآلي[١]. فحالات الإتلاف المعلوماتي التي قد يصاحبها استخدام للعنف قليلة نسبيا إذا قورنت بغيرها من الجرائم، حتى أنه يمكن القول أنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم. فالصورة التقليدية للمجرم تكاد تختفي في الجرائم المعلوماتية، بل على العكس من ذلك فان المجرم المعلوماتي عادة ما يكون على قدر كبير من العلم ، كما أنه ينتمي إلى مستوى اجتماعي مرتفع نسبيا عن غيره من المجرمين ومن ناحية أخرى فإن المجرم المعلوماتي نادرا ما يكون محترفا للإجرام أو عائدا فهو نمط مختلف عن المجرمين على نحو ما سوف نبين لاحقا ، حتى أن المجتمع في كثير من الأحيان لا ينظر اليه كمجرم بالمعنى المتعارف لهذه الكلمة. كما ان الأسباب أو العوامل التي تقف وراء ارتكاب الجريمة المعلوماتية قد تختلف أيضا بالمقارنة بالجريمة التقليدية فمجرد إظهار القدرات التقنية قد يكون واحد من هذه الأسباب، وهو ما لا نراه في الجرائم التقليدية.[٢]

---

(١) سعاد الكمال ، خطر الجرائم المعلوماتية ، ورقة بحثية مقدمة في المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ICACC ، جامعة للامام محمد بن سعود الاسلامية، ٢٠١٥ ، ص ٢٠٨ .

(٢) Wasik (Martian) criminal damage and the computerized saw, new law journal, vol. 136 , 1986 , p 19.

Stefan Frederick Fafinski, computer use and misuse, the constellation of control, submitted in accordance with the requirements for the degree of doctor of philosophy , the university of leeds, school of law , September 2008 , p 101

انظر أيضا ، د/ نائلة قورة ، المرجع السابق ، ص ٥٠ .

وتختلف الجريمة المعلوماتية أيضا من حيث رد فعل المجني عليه تجاهها، وتجاه مرتكبها فمن ناحية فان المجني عليه في هذه الجرائم نادرا ما يقوم بالإبلاغ كما سبق الإشارة .، ويرجع ذلك لأسباب تتعلق بسمعة المؤسسة التي يمثلها، و التي قد تتأثر إذا ما نما إلى علم المتعاملين معها تعرض أنظمة المعلومات الخاصة بها للتلاعب.، و من ناحية أخرى فان للمجني عليه في هذه الجرائم دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريق مباشر أو غير مباشر في ارتكاب الفعل فالبعض يرى أن للمجني عليه في الجرائم المعلوماتية دورا غير مباشر وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للهجوم المعلوماتي مرتفع بشكل كبير. ويرجع ذلك إلى القصور الذي يعتري أنظمة الحاسبات الآلية، و الذي قد يساعد على ارتكاب الفعل الإجرامي ترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية. وهي أن إمكانية الحيلولة دون وقوع هذه الجريمة مرتفع بالمقارنة بغيرها من الجرائم اذ يعتمد أساسا على تطوير نظم الأمن الخاصة بأنظمة الحاسبات الآلية دون الدخول في المشكلات التي تتعلق بظروف الجاني أو الأسباب التي أدت إلى ارتكاب الجريمة لإصلاحها أو الحيلولة دون ارتكابها وهو ما لا يتحقق في مواجهة الجرائم الأخرى.[1]

ويرى رأي من الفقه أن الأثر الرادع للقانون الجنائي ليس له ذات التأثير في جرائم المعلوماتية كما هو الحال في الجرائم التقليدية الأخرى طالما ان هذه الجرائم هي نتاج حسابات عقلية يضع الجاني فيها نصب عينيه عقوبة الفعل الذي

---

(١) د/ نائلة قورة ، المرجع السابق ، ص ٥١

ا نظر أيضا ، احمد بن على المقصودي، الجرائم المعلوماتية خصائصها و كيفية مواجهتها قانونا، المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ، جامعة الامام محمدج بن سعود ، كلية علوم الحاسب الاليو المعلومات، الرياض، ٢٠١٥ ، ص٢٤

يقدم عليه بجانب ما يعود عليه من فائدة كما أنه لا يوجد شعور عام بعدم أخلاقية الفعل أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها ، بل أن كثيرا من العاملين في مجال المعلوماتية لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو في نسخ البرامج بدلا من شرائها واستعمال الحاسبات الآلية للمؤسسات التابعين لها لأغراض شخصية(١).

ثانيا: من حيث الدافع على الارتكاب:

تستهدف الجرائم المعلوماتية إدخال تعديل على عناصر الذمة المالية ويكون الطمع الذي يشبعه الاستيلاء على المال دافعها. وبريق المكسب السريع محركها وقد ترتكب أحيانا لمجرد قهر نظام الحاسب الآلي وتخطي حواجز الحماية المفروضة حوله أو بدافع الانتقام من رب العمل أو احد الزملاء.

ويستهدف السلوك الإجرامي في الجريمة المعلوماتية معنويات وليس ماديات ولذلك يثار في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي حيث تنطوي هذه الجرائم على سلوكيات غير مألوفة، نتج عنها خسائر مادية كبيرة قياسا بالجرائم التقليدية، كما أتاحت الجرائم المعلوماتية تسهيل ارتكاب جرائم أخرى لتحصيل مكاسب مادية جعلت حتى ملاحقة الجرائم التقليدية أمرا صعبا متى تم ارتكابها باستخدام نظام معلوماتي.(٢)

ثالثا : الجريمة المعلوماتية تتميز بوجود ازدواجية في محل الجريمة:

نظرا لأن النظام المعلوماتي ذاته ليس من طبيعة واحدة فهو يتكون من عناصر مادية وأخرى غير مادية بما يسمح من إمكانية ان يكون موضوع

---

(١) Parker(Donn) , Op.Cit, p. 139

(٢) د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص ١٦٣

الجريمة ذا طبيعتين مختلفتين أحدهما يتمثل في الجانب المادي، و الأخر يتمثل في جانب غير مادي وذلك ليس على مكونات النظام ذاته بل يشمل ظهور المحل الواحد بمظهرين أحدهما مادي ولآخر غير مادي كما هو الحال بالنسبة للمعلومات فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي أي أنها في حالة غير مادية، والشكل الأخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة معلوماتية حتى أن المعلومات بطبيعتها غير مادية يمكن أن تخضع لأكثر من نص قانوني وفقا لما إذا كانت في شكل مادي أو غير مادي وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له مثال ذلك اعتبارها مصنف أدبي مما يوجد مشكلة تعدد الأوصاف القانونية على ذات المحل.(١)

رابعا: من حيث موضوعها بالنسبة لمراحل تشغيل نظام المعالجة الآلية للبيانات

على الرغم من إمكانية ارتكاب الجرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام معالجة البيانات (الإدخال ، المعالجة ، الإخراج) فان لكل مرحلة منها نوعية خاصة من الجرائم لا يمكن بالنظر لطبيعتها ارتباطها إلا في وقت محدد يعتبر بالنسبة لمراحل التشغيل الأمثل لذلك.

ففي مرحلة المدخلات، حيث تترجم المعلومات إلى لغة مفهومة من قبل الحاسب يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية. وفي هذه المرحلة يرتكب الجانب الأكبر من الجرائم السيبرانية. وفي مرحلة المعالجة يمكن إدخال أية تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج

(١) د/ سعيد عبد اللطيف حسن ، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية ، ط ١٩٩٩، ص ٤٢ وما بعدها ، انظر أيضا ، د/ ايمن عبد الله فكري، المرجع السابق ، ص ١٠٦

الحاسب الآلي كدس تعليمات غير مصرح بها فيها أو تشغيل برامج جديدة تلغي عمل البرامج الأصلية.، و الجرائم المرتكبة في هذه المرحلة تتطلب توافر معرفة فنية عميقة لدى الفاعل واكتشافها صعب وغالبا ما يكون اكتشافها مصادفة. أما في المرحلة الأخيرة المتعلقة بالمخرجات يقع التلاعب في النتائج التي يخرجها الحاسب بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة.(١)

خامسا : الطبيعة متعدية الحدود للجريمة المعلوماتية:

تعتبر الجريمة المعلوماتية ، جريمة عابرة للحدود ، اذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد اخر. وقد يكون الضرر المحتمل في بلد ثالث. وعلى ذلك تعد الجرينة المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية، ويؤدي التباعد الاقليمي الى صعوبة ضبط الجاني لاختلاف الانظمة القانونية من بلد الى اخر.(٢)

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود. فبعد ظهور شبكات المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من

(١) د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص١٦٣، ١٦٤

(٢) حاتم المهدي ، خصائص الجريمة المعلوماتية، مقالة، مجلة الإرشاد القانوني ، ٢٠١٨ ، ص ٢١٣

انظر أيضا: محمود فتوح محمد سعدات ، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، ورقة بحثية مقدمة للمؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ، جامعة الامام محمد بن سعود ، ٢٠١٥ ، ص ٣٨

المعلومات بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها ان أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد. كما ان السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات، والأموال المستهدفة، و المسافة التي قد تفصل الجاني عن هذه المعلومات، والأموال قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.(١)

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك، حيث أدى التوسع الكبير في إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لجرائم الإحتيال المعلوماتي بصفة خاصة. فربط وسائل الإتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية التي تتم بوسائل إلكترونية وبصفة خاصة من خلال التحويل الإلكتروني للأموال، و التبادل الإلكتروني للمعلومات. ولا يقتصر الأمر على المعاملات المالية فقط بل ان الطبيعة الدولية للجريمة المعلوماتية تظهر في أنماط أخرى من السلوك فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث. وكذلك فيما يتعلق بالإتلاف المعلوماتي فإعداد احد البرامج الخبيثة (الفيروسات) يمكن ان يحدث في دولة ما، ثم يتم نسخ هذا البرنامج آلاف المرات ويرسل إلى دول متفرقة من العالم.(٢)

---

(١) د/ نائلة قورة ، المرجع السابق، ص ٥٢

انظر ايضا : الناجم كوبان ، الطبيعة الاستثنائية للجرائم المعلوماتية ، مجلة القانون المغربي، دار السلام للطباعة ، ط ٢٠١٦ ص ١٥٧

(٢) د/ نائلة قورة ، المرجع السابق، ص ٥٣

ومن القضايا التي لفتت النظر إلى البعد الدولي لجرائم الحاسبات الآلية، قضية عرفت باسم مرض نقص المناعة المكتسبة (الإيدز). وتتلخص وقائعها عام ١٩٨٩ في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة. إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس، وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل اليه على عنوان ببنما حتى يتمكن المجني عليه من الحصول على مضاد للفيروس. وفي الثالث من فبراير ١٩٩٠ تم القاء القبض على المتهم بالولايات المتحدة الأمريكية وتقدمت المملكة المتحدة بطلب تسليمه لمحاكمته أمام القضاء الإنجليزي حيث ان إرسال هذا البرنامج قد تم داخل المملكة المتحدة. وبالفعل وافق القضاء الأمريكي على تسليم المتهم وتم توجيه احدى عشرة تهمة ابتزاز اليه وقعت معظمها في دول مختلفة. إلا ان إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. وأيا ما كان الأمر فان لهذه القضية أهميتها من ناحيتين : الأولى أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة سيبرانية،، و الثانية أنها المرة الأولى التي يقدم فيها شخص بتهمة إعداد برنامج خبيث.[١]

(١)Clough (Bryan) & Mango (Paul), Approaching Zero: Data Crime and the Criminal Underworld, 1992, pp 136-146

انظر ايضا سوير سفيان ، الجرائم المعلوماتية ، رسالة ماجستير ، كلية الحقوق، جامعة ابو بكر بلقايد ، تلمسان ، الجزائر ، ٢٠١٠ ، ص ١٢

سادسا: صعوبة الإثبات في مجال الجريمة المعلوماتية:

لا شك انه كلما تقدم الإنسان في فهم تقنية العمل في الحاسبات كلما استطاع أن يرتكب جريمة دون أن يخلف وراءه أية آثار يمكن الاهتداء إليه من خلالها، ولهذا تعتبر هذه الجريمة من اهم الجرائم التي تحتاج الى حماية جنائية كافية .(١)

ونظرا للطابع الخاص الذي تتميز به الجرائم المعلوماتية . فإن إثباتها يحيط به كثير من الصعوبات التي تواجه سلطة الاستدلال أو التحقيق الجنائي في استخلاص الدليل الجنائي.(٢) والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا. فالجرائم المعلوماتية لا عنف فيها ولا سفك دماء ولا آثار اقتحام لسرقة أموال وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات وليس لها أي اثر خارجي مرئي. بمعنى آخر إن الجرائم المعلوماتية هي جرائم فنية تتطلب تكتيك معين في مجال الحاسبات الآلية. وهي جريمة هادئة لا تتطلب العنف ورغم ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالية بالولايات المتحدة الأمريكية نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف أضف إلى ذلك عدم ظهور الدليل المادي للجريمة المعلوماتية واستحالة رؤيتها وعجز وسائل

---

(١) نبيل ادريس ، الجريمة المعلوماتية بين المفاهيم و النصوص التشريعية ، مجلة القانون والمجتمع ، جامعة ادرار ، الجزائر ، ٢٠١٧ ، ص ٣٣ .

(٢) د/ عبد الفتاح بيومي حجازي، الدليل الجنائي، و التزوير في جرائم الكمبيوترو الانترنت، دراسة متعمقة في جرائم الحاسب الآلي، و الانترنت، بدون ناشر ، ط ٢٠٠٩ ، ص ٢٤ .

الفحص التقليدية عن ضبط أثارها.[١] فإذا تم اكتشاف الجريمة المعلوماتية، فلا يكون ذلك إلا عن طريق الصدفة نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات حيث يتم بالنبضات الإلكترونية نقل المعلومات. ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها عبر الوطنية، و الدول، و القارات وذلك باستخدام شبكات الاتصال ودون تحمل عناء الانتقال. والى جانب ذلك الرغبة في استقرار حركة المعاملات، و محاولة إخفاء أسلوب ارتكاب الجريمة حتي لا يتم تقليدها من جانب الآخرين.[٢]

المطلب الثالث

المجرم المعلوماتي وخصائصه

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين.[٣]

ولقد اختلف الباحثون في تحديد سمات المجرم المعلوماتي ، كما ثبت عدم جدوى النظرة التقليدية للمجرم المعلوماتي التي سادت في كتابات الباحثين لفترة من الزمن فمجرمو المعلومات ليسوا دائما مجموعة من النوابغ الذين لا يمكن

(١) د/ محمد علي العريان، المرجع السابق ، ص ٦٥ ، انظر أيضا د/ طارق ابراهيم الدسوقي ، المرجع السابق، ص ١٦٦

(٢) د/ جميل عبد الباقي الصغير ، القانون الجنائي، و التكنولوجيا، الكتاب الاول، الجرائم الناشئة عن استخدام الحاسب الالي، دار النهضة العربية، ص ١ وما بعدها
انظر ايضا ، غنية باطلي، الجريمة الالكترونية دراسة مقارنة ، الدار الجزائرية للنشر و التوزيع ، ط ٢٠١٥ ص ٢٨ وما بعدها

(٣) د/ نائلة قورة المرجع السابق ، ص ٥٦

التنبؤ بهم أو معرفتهم ، فإذا كان هذا النمط موجود بالفعل إلا أن النمط السائد هو المجرم الذي تربطه بالمجني عليه صلة ما، و التي غالبا ما تكون صلة وظيفية. ولهذا يمكن القول بأن ثمة حقيقة واحدة اتفق عليها الباحثون وهي أن العدد الأكبر من جرائم المعلوماتية قد تم ارتكابها عن طريق أشخاص تربطهم علاقة بالمجني عليهم سواء أكانت علاقة وظيفية أو أي علاقة أخرى مباشرة.(١)

ومع ذلك يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتي،، و التي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين. ويعد الأستاذ Parker واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة، و بالمجرم المعلوماتي بصفة خاصة. والذي يرى أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه. فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب من سماتها من جرائم ذوي الياقات البيضاء(٢)، وإن كانت – في رأيه – لا تتطابق معها. فالمجرم المعلوماتي من ناحية ينتمي في اكثر الأحوال إلى وسط اجتماعي متميز، كما أنه على درجة من العلم، و المعرفة وهو ما يميز بشكل عام ذوي الياقات البيضاء، وان كان ليس

---

(١)Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, 1987, p 134

(٢) جرائم ذوي الياقات البيضاء مصطلح يطلق على الجرائم غيرالعنيفة والمرتكبة لدوافع مالية من قبل رجال الأعمال وأصحاب النفوذ . في علم الجريمة عرّف المتخصص بعلم الاجتماع إدوين سذرلاند المصطلح لأول مرة في عام ١٩٣٩ بأنه"جريمة يرتكبها فرد من ذوي الطبقات الاجتماعية العليا وله مكانة مرموقة في نطاق مهنته". وتشمل جرائم ذوي الياقات البيضاء: الاحتيال والرشوة ومخططات بونزي والتجارة من الداخل والاختلاس والجرائم الإلكترونية وانتهاك حقوق الطبع وغسيل الأموال وانتحال الشخصية والتزييف .

من الضروري أن ينتمي المجرم المعلوماتي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء. كما يتفق مجرم المعلوماتية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته، بل أنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.(١)

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه عن غيره من المجرمين،، و هي المهارة، و المعرفة، و الوسيلة، و السلطة، و أخيرا الباعث. وذلك على التفصيل الاتي:(٢)

أولا: المهارة:

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي. فتنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني بالضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو أن تكون لديه الخبرة فيه بل إن الواقع العملي أثبت أن بعض أنجح مجرمي الجرائم المعلوماتية لم يتلقوا

(١)Suthreland (Edwin H) , " White-collar criminality", Geis (Gilbert) (ed), in White collar criminal: The Offender in Business and the Professions, Atherton press, 1968.

(٢)Parker (Donn B) , Op.cit., p 136

المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتبية من العمل في هذا المجال.[1]

ثانيا: العلم :

أما المعرفة فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على المحيط الذي تدور فيه حتى لا يواجهون بأشياء غير متوقعة من شأنها إفشال أفعالهم أو الكشف عنهم. وتميز المعرفة بمفهومها السابق مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المسرح الذي يمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع ان يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

ثالثا: الأدوات:

يراد بالأدوات الإمكانيات التي يتزود بها الفاعل لإتمام جريمته. ففيما يتعلق بالمجرم المعلوماتي فان الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها. فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج اليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي.، و الحقيقة أنه كلما كان نظام الحاسب الآلي الذي يحتوي على المعلومات المستهدفة غير مألوف كانت الوسائل المتطلبة أكثر صعوبة في الحصول عليها لإقصارها على عدد قليل من

(١) د/ نائلة قورة ، المرجع السابق ، ص ٥٧ ، انظر أيضا ، د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص ١٧١ .

الأفراد هم عادة القائمون على تشغيل النظام وذلك على عكس الأنظمة الشائعة الاستعمال.[١]

رابعا: السلطة:

يقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي، والتي تمكنه من ارتكاب جريمته. فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة. وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو أو تعديل المعلومات التي تحتوي عليها. وقد تتمثل السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على أنظمة الحاسبات الآلية. وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية، كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.[٢]

خامسا: الدافع:

الدافع أو الباعث أو الغرض أو الغاية تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي. تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا ذلك ان القاعدة القضائية تقرر ان الباعث ليس من عناصر القصد الجنائي،[٣] وأن الباعث لا أثر له في وجود القصد

(١) الاشارة السابقة

(٢) د/ نائلة قورة ، المرجع السابق ، ص ٥٨ ، انظر أيضا ، د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص ١٧٢

(٣) د/ محمود نجيب حسني ، شرح قانون العقوبات- القسم العام ، الطابعة السادسة ، دار النهضة العربية ، ١٩٨٩ ، ص ١٠٥٢

الجنائي،[١] واذا كان الاستخدام العادي للتعبيرات المشار اليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية.

فالباعث ، هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي، كالمحبة، والشفقة، و البغضاء، والانتقام، وهو إذا قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى، تبعا لاختلاف الناس من حيث السن، و الجنس ودرجة التعليم وغير ذلك من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة من شخص لأخر.[٢] أو هو الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل.[٣]

والأصل أن الباعث، و الغاية ليس لهما أثر قانوني في وجود القصد الجنائي الذي يقوم على عنصرين هما علم الجاني بعناصر الجريمة واتجاه إرادته إلى تحقيق هذه العناصر أو قبولها، ولا تأثير للباعث أو الغاية على قيام الجريمة أو العقاب عليها فالجريمة تقوم بتحقق عناصرها سواء كان الباعث نبيلا أو خسيسا وسواء كانت الغاية شريفة أو دنيئة، وإذا كانت القاعدة أن الباعث أو الغاية لا أثر لهما على قيام الجريمة فان القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة.[٤]

---

(١) د/ احمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام – ، ط ١٩٩١ ، دار النهضة العربية ، ص ٤٢٧

(٢)١ د/ فوزية عبد الستار ، شرح قانون العقوبات – القسم العام – دار النهضة العربية ، ط ٩٩٢ ، ص ٤٧٩

(٣) د/ ايمن فكري رمضان ، المرجع السابق ، ص ١٣٢

(٤) د/ محمود نجيب حسني ، المرجع السابق ، ص ٤٨٠

ولا يختلف باعث الجاني على ارتكاب الجريمة المعلوماتية في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية،[١] ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية الموجودة حوله وأخيرا الانتقام من رب العمل أو احد الزملاء.[٢]

والحقيقة أنه أيا ما كان الباعث وراء ارتكاب الجريمة المعلوماتية فانه يوجد شعور دائما لدى مرتكب الفعل بأن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن أن يتصف باللاأخلاقية، وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسب الآلي وتخطي الحماية الموجودة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الأضرار بمؤسسة أو جهة تستطيع اقتصاديا تحمل نتائج تلاعبهم.[٣]

ويتصف مجرمو المعلوماتية أيضا وبصفة خاصة، بالخوف من كشف جرائمهم وافتضاح أمرهم. صحيح أن هذه الخشية إنما تصاحب المجرمين على اختلاف أفعالهم الإجرامية إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على افتضاح أمرهم من ارتباك مالي وفقد للمركز الوظيفي في كثير من الأحيان. ويساعد مرتكبو الجرائم المعلوماتية في الحفاظ على سرية أفعالهم طبيعة

---

(١) ويرى البعض ان اغلب مجرمي المعلوماتية ليس لديهم اطماع مادية بقدر ما يحاولون حل مشكلات مادية لديهم لا يستطيعون حلها باللجوء إلى الجرائم الاخرى:انظر د/ احمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر العربي ، ط ٢٠٠٥ الاسكندرية ، ص ٩٩

(٢) د/ هشام فريد رستم ، المرجع السابق ، ص ٣٨

(٣) د/ نائلة قورة ، المرجع السابق ، ص ٥٩ انظر ايضا محمد بن علي بن حميد البلوشي ، التحقيق في الجريمة المعلوماتية، رسالة ماجستير ، عمان ، ص ١٠، ١١

الحاسبات الآلية نفسها فان أكثر ما يعرض المجرم إلى اكتشاف أمره أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها في حين إن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحاسبات الآلية سواء كانت المحل الذي يرد عليه السلوك الإجرامي أو الوسيلة المستخدمة لتنفيذه إنما تؤدي عملها بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى، و هو ما يساعد على عدم كشف الجريمة طالما أن جميع خطوات التنفيذ معروفة مسبقا بحيث لا يحتمل ان تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة.(١)

كما تتميز الجرائم المعلوماتية عادة بوجود اكثر من فاعل للنشاط الإجرامي الواحد أو انه هناك تعاون، و تواطؤ على الأضرار . فمن الملاحظ فيما يخص الجرائم المعلوماتية أن الأشخاص الذين يتمتعون بقدرات تقنية عالية بحيث يستطيعون خلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي. فالجرائم المعلوماتية تتطلب عادة شخصين على الأقل أحدهما متخصص في الحاسبات يقوم بالجانب الفني من العمل الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب، و تحويل المكاسب اليه.(٢)

وعلى ذلك استطاع الفقه أن يضع أنماط مختلفة لمرتكبي الجرائم المعلوماتية، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مرتكبي الجرائم المعلوماتية. ولا يعني بطبيعة الحال أن كل مجرم يندرج

(١) د/ نائلة قورة ، المرجع السابق ، ص ٦٠

(٢) د/ هشام فؤيد رستم ، المرجع السابق ، ص ٣٩

تحت طائفة محددة دون غيرها بل من الممكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يلي:[١]

الطائفة الأولى جناة التسلية، و المزاح (pranksters)[٢]:

تضم هذه الطائفة الأشخاص الذين يرتكبون جرائم سيبرانية بغرض التسلية، و المزاح مع الآخرين بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث)

الطائفة الثانية هم المخترقون (Hackers)[٣]:

تضم هذه الطائفة أشخاص يستهدفون من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول اليها كسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

الطائفة الثالثة المخترق المؤذي (Malicious hackers):[٤]

وهم أشخاص هدفهم الحاق خسائر بالمجني عليهم دون أن يكون الحصول على المكاسب المادية من ضمن الأهداف ويندرج تحت هذه الطائفة الكثير من مخترقي المواقع من مخترعي فيروسات الحاسبات الآلية وموزعيها.

---

(١) د/ نائلة قورة ، المرجع السابق ، ص ٦١ وما بعدها ، انظر أيضا ، د/ طارق ابراهيم الدسوقي ، المرجع السابق ، ص ١٧٣وما بعدها

Parker (Donn.) Op.cit., pp. 144-146

(٢) عبد الغفور الوزاني ، تصنيفات المجرم المعلوماتي بين الدوافع واختلاف الاهداف ، مجلة المنارة للدراسات القانونية و الادارية، ٢٠١٦ ، ص ٢٧٢

(٣) عبد الغفور الوزاني ، المرجع السابق، ص ٢٧٣

(٤) عبد الغفور الوزاني ، المرجع السابق، ص ٢٧٤

الطائفة الرابعة حل المشاكل الشخصية (Personal Problem Solvers):

هذه الطائفة أكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم معلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه ولا يكون الباعث على ارتكاب الجريمة تحقيق ربح مادي بقدر ما هو رغبة في إيجاد حلول لمشكلات مادية تواجه الجاني ولا يستطيع حلها بالوسائل الأخرى، بما فيها اللجوء إلى الجرائم التقليدية، كما أنهم يتمتعون بقدر معقول من الخبرة في مجال الحاسبات الآلية وذلك بحكم عملهم. ويبرر المنتمون إلى هذه الطائفة أفعالهم دائما بحيث لا يجدون غضاضة في ارتكاب الفعل بحجة أن المجني عليه – والذي غالبا ما يكون مؤسسة مالية أو اقتصادية أو شركة ينتمي اليها الجناة – يستطيع أن يتحمل الخسائر الناجمة عن أفعالهم.

الطائفة الخامسة: **طائفة الموظفين** (Career Criminals)

وهم الذين يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة. ويعمل المنتمون إلى هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة من سمات المجرم التقليدي.

الطائفة السادسة : **طائفة الارهابيين** (Extreme Advocates)

يدخل في عداد هذه الطائفة الجماعات الإرهابية أو المتطرفة والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية، وسياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي ويتركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص، والممتلكات من اجل لفت الأنظار إلى ما يدعون اليه ولقد بدأ اهتمام الجماعات

الإرهابية وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي إلا وهو الاجرام المعلوماتي، فاعتماد المؤسسات المختلفة داخل الدول، و الأجهزة المسئولة على أنظمة الحاسبات الآلية في إنجاز الأعمال والأهمية القصوى للمعلومات التي تحتويها في أغلب الأحوال جعل من هذه الأنظمة هدفا جذابا لتلك الجماعات.

المبحث الثاني

دور التشريعات الوطنية في مكافحة الجرائم المعلوماتية

المبدأ انه لا جريمة ولا عقوبة إلا بنص، فقد وضع المشرع السعودي نظام مكافحة جرائم المعلوماتية ، والذي وضع نصوص جرمت أفعال معينة، و التي تتمثل في جرائم الاعتداء على الحماية المعلوماتية للمؤسسات العامة، و الخاصة، ووضع كذلك عقوبة لتلك الأفعال المجرمة.

وعلى ذلك سوف ينصب حديثنا على ما وضعه المشرع السعودي من تعريفات للمصطلحات الفنية المتعلقة بجرائم تقنية المعلومات على اعتبار أن هذه الجريمة إثباتها مرتبط الى حد كبير بأمور فنية، ثم الأفعال التي عدها المشرع السعودي جرائم من قبيل الجرائم المعلوماتية لمساسها بالمواقع الالكترونية أو نظام المعلومات الالكتروني أو شبكة المعلومات بهدف اتلافها أو تخريبها أو الحصول على معلومات سرية، والتي وضع لها عقوبة، وذلك من خلال تحليل القانون سالف الذكر فيما قرره من جرائم تتعلق بأفعال لم ينص عليها قانون العقوبات التقليدي، ومقارنة ذلك قانون بقانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م .

المطلب الأول

التعريفات الفنية المتعلقة بجرائم المعلوماتية الواردة في القانون السعودي والمصري

ففي إطار مسايرة المشرع السعودي ركب الدول المعنية بحماية النظام الإلكتروني، و البرامج المعلوماتية، أصدر المشرع السعودي نظاما لمكافحة الجرائم المعلوماتية.

وجاءت المادة الأولى من هذا النظام لتضع تعاريف وتحدد المعاني المقصودة للألفاظ، و المصطلحات الفنية، و القانونية الواردة بهذا النظام ليسد بذلك المشرع إلى طريق على التأويل أو التفسير غير الصحيح للمعاني المقصودة.

فعرفت المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي، النظام المعلوماتي بأنه " مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية". وكذلك لم يخرج المشرع المصري في تعريفه للنظام المعلوماتي عما أورده النظم السعودي من تعريف. كما عرف المشرع السعودي برنامج الحاسب الالي بأنه" مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي ، أو شبكات الحاسب الآلي ، وتقوم بأداء الوظيفة المطلوبة". أما المشرع المصري فقد عرف البرنامج المعلوماتي، ولم يربط المصطلح بالحاسب الآلي فقط بل بسطه على أية برنامج معلوماتي يعمل على أجهزة الحاسب الآلي وما في حكمها من أجهزة حديثة تقوم مقامها، وقد عرف المشرع المصري البرنامج المعلوماتي بانه " مجموعة الأوامر والتعليمات المعبر عنها بأية 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". فالبرنامج طبقا للقانون المصري هو ما يتم تشغيله على الحاسب الآلي أو أي نظام معلوماتي آخر غير الحاسب الالي. فدقة المصطلح تمنع من التأويل في تفسير المعنى وتمنع التحايل على القانون و الافلات من العقاب.

كذلك عرفت المادة الأولى من النظام السعودي، الشبكة المعلوماتيى بأنها" ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت). كما عرفها المشرع المصري بأنها " 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 .

ثم جاء المشرع السعودي بتعريف للبيانات بشكل عام فقرر أنها " المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي ، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي ، كالأرقام والحروف والرموز وغيرها". كذلك عرف المشرع المصري البيانات بشكل عام بأنها " كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها".

ويلاحظ على تعريف القانون المصري للبيانات أنها جاءت بشيء من التفصيل لا يدع مجالا للاجتهاد و التلاعب بالالفاظ لعدم الافلات من العقاب، بل الاكثر من ذلك فقد فرق المشرع المصري بين نوعين من البيانات، البيانات الشخصية وهي أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل

مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى. والبيانات الحكومية، وهي بيانات متعلقة بالدولة أو إحدى سلطاتها، أو أجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة أو الأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها. وجاءت هذه التفرقة اختلاف عقوبة التعدي على البيانات الخاصة عن البيانات الحكومية من حيث الجسامة.

كما عرف النظام السعودي الحاسب الالي بأنه، أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرامج ، والأوامر المعطاة له. ولم يخرج المشرع المصري عندما عرف الحاسب عن التعريف السابق، فنص على أن الحاسب هو، كل جهاز أو معدة تقنية تكون قادرة على 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 أو تبادلها أو تحليلها أو للاتصالات.

وبمطالعة التعريفين السابقين نجد أن كلا من المشرع المصري و السعودي وضعا تعريفا موسعا للحاسب، لايقتصر على الحاسب الالي التقليدي او الحاسب الالي المحمول (لاب توب) ، بل إن هذا التعريف يشمل الى جانب ما سبق، الهواتف المحمولة الذكية بجميع أنواعها، وما قد يستجد في عالم التكنولوجيا من أجهزة تقوم بنفس الوظائف ولها نفس الخواص؛ وذلك حتى تدخل أية أجهزة موجودة في الوقت الحالي أو غير موجودة وستوجد في المستقبل تحت مظلة قوانين مكافحة الجرائم المعلوماتية.

كذلك وضعت المادة الأولى من النظام السعودي تعريفا للموقع الالكتروني فنصت أن الموقع الالكتروني هو مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد . وعرفه المشرع المصري بأنه " مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة.

وبالمقارنة بين النظام السعودي و القانون المصري تبين أن المشرع المصري قد أورد في قانون مكافحة جرائم تقنية المعلومات تعريفات لمصطلحات لم ينص عليها المشرع السعودي وهي، المعالجة الالكترونية، تقنية المعلومات، مقدم الخدمة، المستخدم، مدير الموقع، الحساب الخاص، البريد الالكتروني، حركة الاتصال، ودعامة الكترونية.

ولا يقال إن السبب في عدم ايراد تلك المصطلحات الفنية في نظام مكافحة جرائم المعلوماتية السعودي انه قصور من المشرع؛ لأن الهدف من إيراد تلك المصطلحات الفنية و تعريفها هو بيان معاني هذه المصطلحات لورودها داخل نصوص مواد القوانين، و لتي رأى المشرع اهمية لتعريفها حتى لا يترك التعريف لاجتهاد الفقه و القضاء، وليمنع تأويل الالفاظ و المعاني لقصد لم يريده المشرع. والسبب في ورود مصطلحات فنية في القانون المصري لم تورد في النظام السعودي هو أن المشرع المصري قد عالج مسائل لم يعالجها المشرع السعودي.

وبعد عرض المصطلحات الفنية التي أوردها كلا من المشرع السعودي و المصري سنبين لاحقا الأفعال التي جعل المشرع السعودي و المصري إتيانها جريمة من الجرائم المعلوماتية، ووضع عقوبات متفاوتة لها حسب الفعل المرتكب وذلك في المطلب الثاني من هذا المبحث

المطلب الثاني

الأفعال التي تم تجريمها لمساسها بالمواقع والنظام الالكتروني والشبكات في القانوني السعودي والمصري

جاءت الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات سواء القانون السعودي أو القانون المصري على نوعين، النوع الأول، هي جرائم الهدف من ارتكابها في حد ذاته المساس بالمواقع الالكترونية أو النظام المعلوماتي والشبكات. و النوع الاخر هو الجرائم المرتكبة بواسطة انظمة وتقنيات المعلومات ويكون للمجرم فيها هدف يتم الوصول اليه عن طريق استخدامه انظمة وتقنية المعلومات، وهذه الجرائم لن تكون محل تعليق لأنها في رأي الباحث تعد من الجرائم التقليدية والتي يكون أداة أو وسيلة ارتكابها هي تقنية المعلومات. فجرائم المعلوماتية طبقا لرأي الباحث هي الجريمة التي يكون محلها معلومة أو بيان، اما للحصول عليها أو حذفها أو اتلافها أو حرمان صاحبها منها. وعلى ذلك سيكون الحديث عن النوع الأول الخاص بالأفعال التي تم تجريمها لمساسها بالمواقع والنظام الالكتروني والشبكات وذلك على النحو التالي:

أولا: جريمة الدخول غير المشروع:

عرف المشرع السعودي الدخول غير المشروع بأنه " دخول شخص بطريقة متعمدة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها" . ووضع المشرع السعودي في نظام مكافحة الجرائم المعلوماتية عدة صور لجريمة الدخول غير المشروع وميز كل صورة عن الأخرى بالباعث او الهدف من الدخول و القصد من الدخول، وكذلك بالعقوبة التي تطبق على كل صورة.

فجاءت المادة الثالثة من النظام السعودي على أنه " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

٣- الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

كذلك نصت المادة الخامسة من النظام السعودي على انه " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

ونصت المادة السابعة من النظام السعودي على انه" يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية:

٢- الدخول غير المشروع إلى موقع إلكتروني ، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

ويلاحظ ان المشرع السعودي عندما جرم فعل الدخول غير المشروع، جعل هذا الفعل عن قصد وعمد، الدخول الذي يعلم مرتكبه انه عمل غير مشروع، ثم اقرن بعد ذلك الدخول غير المشروع بالهدف أو الغاية من الدخول و التي يبتغيها المجرم المعلوماتي من الدخول. معنى ذلك ان الدخول بطريق الخطأ أو الدخول بقصد الدخول دون العلم بعدم المشروعية طبقا للنظام السعودي لا يعاقب عليه لعدم نص المشرع السعودي على المعاقبة على الدخول غير العمدي. فتعريف

الدخول غير المشروع و على ما قرره المشرع السعودي جاء واضح ليس به لبس فهو خاص بالدخول العمدي.

أما المشرع المصري عندما تحدث عن جريمة الدخول غير المشروع، فقد ساوى بين الدخول غير المشروع العمدي و الدخول غير المشروع غير العمدي مع البقاء. فنص على أنه " 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 عمدا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه .

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على 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" .

ويلاحظ على هذا النص انه غلظ العقوبة اذا نتج عن الدخول ضرر، وساوي المشرع في تغليظ العقوبة بين الضرر الناتج عن الدخول العمدي والدخول غير المعمدي مع البقاء.

ثم وضع المشرع المصري افتراضا لم ينص عليه المشرع السعودي، فقد جرم المشرع المصري فعل تجاوز حدود الحق في الدخول، فقد يكون للشخص حق الدخول الى الموقع الالكتروني وذلك لتسجيل بيانات أو نقل بيانات، الا انه يدخل ويتجاوز الحد المسموح له بالدخول سواء من حيث الزمان أو المكان، فيعد بذلك الفعل طبقا لما قرره المشرع المصري قد ارتكب جريمة تجاوز حدود الحق في الدخول. فنص المشرع المصري على انه" 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 إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

ثانيا: جريمة الاعتراض غير المشروع:

جاءت المادة الثالثة من النظام السعودي في فقرتها الأولى تنص على انه " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.

والتصنت هو استراق السمع أو التجسس، فقد يكون الدخول الى الشبكة المعلوماتية دخولا مشروعا، إلا أن المجرم المعلوماتي يتصنت عن طريق اعتراض البيانات المرسلة الى شخص اخر. والتصنت هنا لا يعني بالضرورة أن يسمع المتصنت شيئا بأذنيه بل التصنت الذي يعنيه المشرع السعودي هو التجسس سواء أكان بالسمع أو بالرؤية. اما الالتقاط فهو كما عرفته المادة الاولى من النظام " مشاهدة البيانات أو الحصول عليها دون مسوغ نظامي صحيح.

وفي جميع الأحوال يعد التصنت او الالتقاط اعتراضا لما هو متداول على شبكة المعلومات، وهو ما نص عليه المشرع المصري في المادة ١٦ من القانون مكافحة جرائم تقنية المعلومات والتي جاءت على انه" 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 الحاسب الآلي وما في حكمها".

وعرفت المادة الأولى من القانون المصري الاعتراض بأنه " مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق".

وبذلك نجد أن مصطلح الاعتراض الذي نص عليه المشرع قد اشتمل على جميع الافعال التي نص عليها المشرع السعودي في المادة الثالثة، بل الأكثر من ذلك شمل التعريف على أفعال لم ينص عليها المشرع السعودي الأمر الذي جعل التشريع المصري في تلك المسألة يقدم حماية قانةنية عالية المستوى للنظم العلوماتية و الشبكات المعلوماتية:

ثالثا: جريمة الاعتداء على الشبكات المعلوماتية:

نصت المادة الخامسة من النظام السعودي على أنه " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت

وعلى الصعيد الاخر نجد المشرع المصري قد اتى بتجريم نفس الفعل بأن نص في مادته الحادية والعشرين من قانون مكافحة جرائم تقنية المعلومات على انه " 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 متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو

التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها .

ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين .

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

وبمطالعة النصوص السالفة نجد أن المشرع السعودي لم يحدد عما إذا كان الفعل المجرم هو الفعل العمدي و غير العمدي أم الفعل العمدي فقط، فهو نص يحتمل التأويل فقد يفهم منه أن الأفعال العمدية فقط هي التي يعاقب عليها أما الإيقاف غير العمدي أو بطريق الخطأ لا يعاقب عليه. وقد يفهم من هذا النص أن الأفعال العمدية وغير العمدية يعاقب عليها . وذلك ان دل يدل على ان الصياغة تحتمل التأويل.

إلا أن الباحث يرى أن نص المشرع السعودي جاء للافعال العمدية فقط، وان كانت الصياغة تحتمل التأويل،ىذلك لان القاعدة العامة انه لا جريمة ولا عقوبة إلا بنص، فإذا لم ينص المشرع صراحة على الأفعال العمدية فلا يجوز الاجتهاد و القول بان النص يشمل الفعلين العمدي و غير العمدي ومن ثم فلا يجوز العقاب على الايقاف غير العمدي.

أضف إلى ذلك أنه يستحيل ان تكون العقوبة على الجرائم العمدية في نفس قدر العقوبة على الجرائم غير العمدية، فالجريمة العمدية يكون فيها الجاني

قاصدا للفعل و النتيجة معا، أما الجرائم غير العمدية وان قصد الجاني الفعل فانه لا يريد النتيجة التي وقعت.

وأدلل على ذلك أيضا بأن المشرع المصري نص على عقوبة لتلك الافعال اذا صدرت عن عمد ووضع عقوبة اخف لتلك الافعال اذا وقعت بطرق الخطأ. كذلك فرق المشرع المصري في العقوبة على تلك الافعال في حالة ما اذا وقعت على شبكة معلوماتية خاصة بالدولة او احد الاشخاص الاعتبارية العامة او ممتلكاتها او المرافق التي تدار بمعرفة الدولة او احد مؤسساتها العامة. فقد شدد المشرع المصري في العقوبة عن تلك الافعال التي تقع على شبكات الدولة عن اية شبكة اخرى خاصة بالافراد. فانتقل بالعقوبة من الحبس الذي لا يزيد على ثلاث سنوات الى السجن المشدد الذي قد يصل الى خمسة عشر عاما.

تلك هي جرائم الاعتداء على سلامة الشبكات و انظمة تقنية المعلومات التي نص عليها المشرع السعودي، واشترك معه في تجريم نفس الافعال المشرع المصري. واذا كان المشرع السعودي قد اهتم بالجانب الموضوعي لمكافحة جرائم المعلوماتية الا انه لم يتطرق من قريب او من بعيد الى جانب غاية في الاهمية وبدونه لن يتم تفعيل الجانب الموضوعي، وهو الجانب الاجرائي لمكافحة جرائم المعلوماتية. وذلك بعكس ما فعله المشرع المصري الذي اورد فصلا كاملا في قانون مكافحة جرائم تقنية المعلومات، خاص بالاجراءات الجنائية التي من شأنها ان تساعد في الكشف عن الجريمة المعلوماتية واثباتها و الوصول الى مرتكبيها، وذلك لعدم قدرة القواعد و الاحكام الواردة في قانون الاجراءات الجنائية ان تقوم بهذه المهمة لتمتع الجريمة المعلوماتية بخواص غير متوفرة في الجرائم التقليدية على نحو ما قد بيناه عند الحديث عن خصائص الجريمة المعلوماتية. وسنبين تلك الاجراءات التي نص عليها المشرع المصري في المطلب تالي.

المطلب الثالث

الأحكام و القواعد الإجرائية التي قررها القانون المصري

أولا : التزامات مقدم الخدمة: [1]

يلتزم مقدمو الخدمة بما يلى :

(1) حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات لمدة ١٨٠ يوما متصلة وتتمثل البيانات الواجب حفظها وتخزينها فيما يلى :

أ- البيانات التى تمكن من التعرف على مستخدم الخدمة.

ب – البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرته.

ج – البيانات المتعلقة بحركة الاتصال

د- البيانات المتعلقة بالاجهزة الطرفية للأتصال.

ه – أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

(2) المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم افشائها أو الافصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته أو أى بيانات أو معلومات متعلقه بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها.

(3) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.

١- راجع نص المادة الثانية من قانون مكافحة جرائم تقنية المعلومات المصري

ثانيا : مع عدم الإخلال بأحكام قانون حماية المستهلك الصادر بالقانون رقم ٦٧ لسنه ٢٠٠٦، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة، فى الشكل، وبالطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الاتية:

(1)اسم مقدم الخدمة وعنوانه.

(2) معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الاليكترونى.

(3) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لاشرافها.

(4) أيه معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويحددخا قرار من الوزير المختص.

ثالثا : مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومى، ووفقا لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون.

رابعاً : يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين ويحظر على غير هؤلاء القيام بذلك

ثانيا: في مجال التعاون الدولى لمكافحة جرائم تقنية المعلومات. [١]

نص المشرع المصري على ان تعمل السلطات المصرية المختصة على تيسير التعاون بالبلاد الاجنبية فى إطار الاتفاقيات الدولية والاقليمية والثنائية

(١) راجع نص المادة الرابعة من القانون المصري

المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات. على أن يكون المركز الفننى للأستعداد لطوارىء الحاسب والشبكات بالجهاز هو المنقطة الفنية المعتمدة فى هذا الشأن.

ثالثا: مأمورى الضبط القضائي: (١)

يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومى، بالنسبة إلى الجرائم التى تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم.

رابعا: الأوامر القضائية المؤقتة: (٢)

لجهة التحقيق المختصة – بحسب الأحوال- أن تصدر أمراً مسبباً، لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ٣٠ يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلى :

١- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو انظمة المعلومات، وتتبعها فى أى مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة أن كان لها مقتضى.

(١) راجع نص المادة الخامسة من القانون المصري

(٢) راجع نص المادة السادسة من القانون المصري

٢- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.

٣- أن تأمر مقدم الخدمة بتسليم مالدية من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو الجهاز التقنى، وفى كل الاحوال يحب أن يكون أمر جهة التحقيق المختصة مسببا.

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة فى المواعيد، ووفقا للإجراءات الجنائية.

خامسا: الإجراءات والقرارات الصادرة بشأن حجب المواقع :[1]

لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أى عبارات أو أرقام أو صور أو أفلام أو أية م مواد دعائية، أو ما فى حكمها مما يعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدا للأمن القومى أو تعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا.

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة فى غرفة المشورة، خلال ٢٤ ساعة، مشفوعا بمذكرة برأيها، وتصدر المحكمة قرارها فى الأمر مسببا، فى مدة لا تجاوز ٧٢ ساعة من وقت عرضه عليها، بالقبول أو بالرفض.

ويجوز فى حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع من ارتكاب جريمة، أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز – (فى

(١) راجع نص المادة السابعة من القانون المصري

إشارة للجهاز القومى لتنظيم الاتصالات) – ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المواقع أو الروابط أو المحتوى المذكور فى الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

وعلى جهة التحرى والضبط المُبلغة أن تعرض محضرا تثبت فيه ما تم من إجراءات على جهة التحقيق المختصة، وذلك خلال ٤٨ ساعة من تاريخ الإبلاغ الذى وجهته للجهاز، وتتبع فى هذا المحضر ذات الاجراءات المبينه بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها فى هذه الحالة، أما بتأييد ما تم من إجراءات حجب أو بوقفها. فإذا لم يعرض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد، يعد الحجب الذى تم كأن لم يكن.

ولمحكمة الموضوع أثناء نظر الدعوى أو بناء على طلب جهة التحقيق أو الجهاز أو ذوى الشأن – أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه. وفى جميع الأحوال يسقط القرار الصادر بالحجب بصدور أمر بأن لا وجه لإقامة الدعوى الجنائية أو بصدور حكم نهائى فيها بالبراءة."

سادسا: التظلم من القرارات الصادرة بشأن حجب المواقع : [١]

لكل من صدر ضدة أمر قضائى من المنصوص عليه بالمادة ٧ من هذا القانون، وللنيابة العامة، ولجهة التحقيق المختصة، ولكل ذوى الشأن، أن يتظلم منه، أو من إجراءات تنفيذه، أمام محكمة الجنايات المختصة بعد انقضاء ٧ أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال، فإذا رُفض تظلمة فله أن يتقدم بتظلم جديد كلما انقضت ٣ أشهر من تاريخ الحكم برفض التظلم.

(١) راجع المادة الثامنة من القانون المصري

يكون التظلم – فى جميع الأحوال – بتقرير فى قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز لكل ذى شأن، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز ٧ أيام من تاريخ التقرير به.

سابعا: المنع من السفر:[١]

يجوز للنائب العام أو من يفوضة من المحاميين العامين الأول بنيابات الاستئناف، ولجهاا التحقيق المختصة، عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام فى ارتكاب أو الشروع فى ارتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون، أن يأمر بمنع المتهم من السفر خارج البلاد أو بوضع اسمه على قوائم ترقب الوصول بأمر مسبب لمدة محددة.

ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال ١٥ يوما من تاريخ علمه به، فإذا رفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ٣ أشهر من تاريخ الحكم برفض التظلم.

ويحصل التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تعلم بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز ١٥ يوما من تاريخ التقرير به، بحكم مُسبب بعد سماع أقوال المتظلم وسلطة التحقيق المختصة، ولها فى سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها فى هذا الشأن.

(١) راجع المادة التاسعة من القانون المصري

ويجوز للنيابة العامة وجهات التحقيق المختصة فى كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع اسمه من على قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة لذلك.

وفى جميع الأحوال ينتهى المنع من السفر بمرور سنه من تاريخ صدور الأمر، أو بصدور قرار بأن لا وجه لإقامة الدعوى الجنائية أو بصدور قرار نهائى فيها بالبراءة أيهما أقرب.

ثامنا: الخبراء :[1]

ينشأ بالجهاز سجلان لقيد الخبراء يقيد بأولهما الفنيون والتقنيون العاملون به، ويقيد بالأخر الخبراء من الفنين والتقنين من غير العاملين بالجهاز. ويطبق عليهم فى ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والاحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء.

واستثناء من تلك القواعد تسرى قواعد المساءلة الإدارية والتأديبية على الخبراء المقيدين بالسجل الثانى قواعد وأحكام وإجراءات القيد فى كل من السجلين.

تاسعا: في الأدلة الرقمية: [2]

يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو النظام المعلوماتى أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية فى الاثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية.

(١) المادة العاشرة من القانون المصري

(٢) المادة الحادية عشر من القانون المصري

الخاتمـــة

النتائج و التوصيات

توصلت الدراسة الى:

- ان الجريمة المعلوماتية هي كل فعل غير مشـــروع عمـــدي او غيـــر عمدي يمس البيانات و المعلومات الموجودة على الانظمة المعلوماتية او الشبكات المعلوماتية او المواقع الالكتونية او الحسابات او البريـــد الالكتروني.
- الجريمة المعلوماتية تتمتع بخصوصية تختلف عن الجرائم التقليديـــة، فالجريمة المعلوماتية يقوم بارتكابها خبراء متخصصين فـــي مجـــال تقنية المعلومات و علوم الحاسبات، وهي من الجرائم التـــي يصـــعب اثباتها لصعوبة التوصل الى دليل يسند الاتهام بارتكابها الى شـــخص معين فهي لا تترك اثار مادية مثل الجرائم التقليدية، كذلك فهي مـــن الجرائم العابرة للحدود والتي يصعب في كثير من الاحيان اذا عـــرف شخص مرتكبها ان يتم القيض عليه.
- المجرم المعلوماتي يختلف عن المجرم التقليدي في عـــدة خصـــائص فهو لابد وان تكون لديه مهارة في علـــوم الحاســـبات و تكنولوجيـــا المعلومات، وان يكون لديه العلم و الادوات اللازمين للوصـــول الـــى هدفه.
- لا يوجد توحيد للافعال المجرمة في قوانين الدول؛ فمـــن الممكـــن ان يكون الفعل مجرم في دولة، ويكون نفس الفعل مباح في دولة اخرى. فهناك افعال تم تجريمها في قانون مكافحة جرائم تقنيـــة المعلومـــات المصري، لم يجرمها نظام مكافحة جرائم المعلوماتية السعودي.

- المشرع المصري رغم حداثة قانونه الا انه وضع قانون لمكافحة الجرائم المعلوماتية يتطابق الى حد كبير مع النموذج الوارد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- المشرع المصري وضع فصلا كاملا في قانون مكافحة جرائم تقنية المعلومات عن الجراءات الجزائية التي تمكن جهات التحقيق من كشف الجريمة و ملاحقة الجاني و القبض عليه حتى لو كان خارج البلاد. وهو ما لم يرد في النظام السعودي.
- لذلك يوصي الباحث:

- يوصي الباحث المشرع السعودي بادراج جميع الافعال التي تمس النظم المعلوماتية و الشبكات و المواقع و الحسابات الخاصة و البريد الالكتروني الواردة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ضمن الجرائم المعلوماتية ووضعها في النظام السعودي لمكافحة جرائم المعلوماتية وذلك لتوحيد الافعال المجرمة بين الدول للمساعدة في عملية تسليم المجرمين بين الدول.
- يوصي الباحث المشرع السعودي باصدار نصوص تتضمن قواعد اجراءات جزائية خاصة بالجرائم المعلوماتية و تتناسب مع خصائص تلك الجريمة؛ لكي تساعد جهات التحقيق في الكشف عن الجريمة و اثباتها وملاحقة الجناه.
- تفعيل دور التعاون القضائي الدولي داخل المملكة العربية السعودية بما يتناسب مع ما نصت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات و التي وقعت عليها المملكة العربية السعودية في عام ٢٠١٠.

قائمة المراجع

- منير محمد الجهيني ، ممدوح محمد الجهيني، جرائم الانترنت و الحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ط ٢٠٠٦
- هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية، ط ١٩٩٩
- هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ط ١٩٩٢
- سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، ٢٥الي ٢٨ اكتوبر
- د/ محمد سامي الشوا، ثورة المعلومات، و انعكاستها على قانون العقوبات، دار النهضة العربية
- د/ عبد الله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الالي، دار النهضة العربية ، ط ٢٠٠٢
- حسن بن احمد الشهري، نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وابحاث ، جامعة الجلفة ، ٢٠٠٩
- محمد امين الشوابكة، جرائم الحاسوب و الانترنت – الجريمة المعلوماتية، دار الثقافة للنشر و التوزيع، عمان ،ط ٢٠٠٧
- نهلة عبد القادر المونمي، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان ، ط ٢٠٠٤
- محمد كرام ، صعوبات اثبات الجرائم المرتكبة عن طريق التقنيات الحديثة، مجلة المحامي ، العدد ٤٤ ، ٢٠٠٤

- د/ هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، ١٩٩٢
- د/ هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، ١٩٩٢
- سعاد الكمال ، خطر الجرائم المعلوماتية ، ورقة بحثية مقدمة في المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ICACC ، جامعة للامام محمد بن سعود الاسلامية، ٢٠١٥
- احمد بن على المقصودي، الجرائم المعلوماتية خصائصها و كيفية مواجهتها قانونا، المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ، جامعة الامام محمدج بن سعود ، كلية علوم الحاسب الاليو المعلومات، الرياض، ٢٠١٥
- د/ سعيد عبد اللطيف حسن ، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية ، ط ١٩٩٩
- حاتم المهدي ، خصائص الجريمة المعلوماتية، مقالة، مجلة الارشاد القانوني ، ٢٠١٨
- محمود فتوح محمد سعدات ، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، ورقة بحثية مقدمة للمؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ، جامعة الامام محمد بن سعود ، ٢٠١٥
- الناجم كوبان ، الطبيعة الاستثنائية للجرائم المعلوماتية ، مجلة القانون المغربي، دار السلام للطباعة ، ط ٢٠١٦

- سوير سفيان ، الجرائم المعلوماتية ، رسالة ماجستير ، كلية الحقوق، جامعة ابو بكر بلقايد ، تلمسان ، الجزائر ، ٢٠١٠
- نبيل ادريس ، الجريمة المعلوماتية بين المفاهيم و النصوص التشريعية ، مجلة القانون والمجتمع ، جامعة ادرار ، الجزائر ، ٢٠١٧
- د/ عبد الفتاح بيومي حجازي، الدليل الجنائي، و التزوير في جرائم الكمبيوترو الانترنت، دراسة متعمقة في جرائم الحاسب الآلي، و الانترنت، بدون ناشر ، ط ٢٠٠٩
- د/ جميل عبد الباقي الصغير ، القانون الجنائي، و التكنولوجيا، الكتاب الاول، الجرائم الناشئة عن استخدام الحاسب الالي، دار النهضة العربية
- غنية بالطي، الجريمة الالكترونية دراسة مقارنة ، الدار الجزائرية للنشر و التوزيع ، ط ٢٠١٥
- د/ محمود نجيب حسني ، شرح قانون العقوبات- القسم العام ، الطابعة السادسة ، دار النهضة العربية ، ١٩٨٩
- د/ احمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام – ، ط ١٩٩١ ، دار النهضة العربية
- د/ فوزية عبد الستار ، شرح قانون العقوبات – القسم العام – دار النهضة العربية ، ط ١٩٩٢
- د/ احمد خليفة الملط، الجرائم المعلوماتية ، دار الفكر العربي ، ط ٢٠٠٥ الاسكندرية
- محمد بن علي بن حميد البلوشي ، التحقيق في الجريمة المعلوماتية، رسالة ماجستير ، عمان

- عبد الغفور الوزاني ، تصنيفات المجرم المعلوماتي بين الدوافع واختلاف الاهداف ، مجلة المنارة للدراسات القانونية و الادارية، ٢٠١٦
- د/ ايمن عبدالله فكري ، الجرائم المعلوماتية ، مكتبة القانون، و الاقتصاد ، الرياض ، ط ٢٠١٥ .
- د/ طارق ابراهيم الدسوقي عطية ، الامن المعلوماتي، دار الجامعة الجديدة ، ط ٢٠١٥ ، مصر .
- د/ محمد علي العريان، الجرائم المعلوماتية ، دار الجامعة الجديدة ، ط ٢٠١١ .
- د/ نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، ط ٢٠٠٥.

مراجع اجنبية:

- James Richard, " Transational criminal organization cybercrime, and money laundering" ed 1998
- Wasik (Martian) criminal damage and the computerized saw, new law journal, vol. 136 , 1986

Stefan Frederick Fafinski, computer use and misuse, the constellation of control, submitted in accordance with the requirements for the degree of doctor of philosophy , the university of leeds, school of law , September 2008

- Clough (Bryan) & Mango (Paul), Approaching Zero: Data Crime and the Criminal Underworld, 1992
- Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, 1987
- Suthreland (Edwin H) , " White-collar criminality", Geis (Gilbert) (ed), in White collar criminal: The Offender in Business and the Professions, Atherton press, 1968

فهرس الموضوعات