مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة

مجلة علمية محكمة

للعلوم القانونية

المجلد 17، العدد 1
شوال 1441 هـ / يونيو 2020م

الترقيم الدولي المعياري للدوريات 2616-6526

الطبيعة القانونية للهجوم السيبراني وخصائصه

شيخه حسين الزهراني

كلية القانون - جامعة الشارقة

الشارقة - الإمارات العربية المتحدة

تاريخ الاستلام: 17-01-2019 **تاريخ القبول: 05-06-2019**

ملخص البحث:

الهجوم السيبراني هو ظاهرة إجرامية نشأت في مجال تكنولوجيا المعلومات، وتتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية للمؤسسات العامة أو الخاصة بغرض: إما تدمير تلك النظم أو الحصول أو الحصول على المعلومات السرية المخزنة سواء أكانت عسكرية أو الاقتصادية.

هذه الظاهرة الإجرامية لها طبيعة خاصة، فهي لا تنصب على شيء مادي ملموس بل تقع على البيانات أو المعلومات المخزنة داخل الحاسب الآلي فيكون الهدف من الهجمة السيبرانية إما معرفة المعلومة السرية المخزنة على الحاسب الآلي أو إزالة المعلومة من على الحاسب الآلي، والذي يؤدي إلى خسارة المجني عليه سواء بسبب معرفة المعلومة أو مسحها. وبذلك أصبحت المعلومة تقوم بالمال ويمكن الاعتداء عليها وأن تكون محلا للجريمة إذا توافر فيها شروط معينة.

كذلك تتميز الجريمة السيبرانية بقلة حالات اكتشافها حيث لا يشوب ارتكابها أي عنف ولا تترك وراءها أية آثار مما يؤدي إلى صعوبة إثباتها، وكذلك يتميز المجرم المعلوماتي عن المجرم التقليدي من حيث الغرض من ارتكاب الجريمة أو دوافع ارتكابها.

الكلمات الدالة: التعاون الدولي، الإنتربول، تسليم المجرمين، الإنابة القضائية، المساعدات القضائية.

المقدمة:

أصبحنا اليوم نعيش عصر تكنولوجيا المعلومات والاتصالات التي صارت هي الأساس الذي يعتمد عليه في شتى المجالات، ولدى جميع المؤسسات سواء أكانت مؤسسات عامة تملكها حكومات الدول أو مؤسسات خاصة يمتلكها الأفراد، فتقنية المعلومات وشبكات الاتصالات هي الأداة الأساسية المستخدمة في إدارة شؤون الدول وتقديم وتسهيل الخدمات عن طريقها.

وقد أدى التطور السريع مجال تقنية المعلومات والاتصالات وشبكة الإنترنت في العالم كله إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب معه خلق ظاهرة إجرامية جديدة وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، والتي تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بغرض إما تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه إلى وجود مخاطر على الصعيد الدولي والوطني إذا لم يتم تدارك هذه الظاهرة التي سوف ينشأ عنها، إذا ما تركت، خسائر هائلة على المستوى العسكري والاقتصادي والاجتماعي لجميع دول العالم. مما يستوجب معه والحال كذلك إيجاد سبل للتصدي لهذه الظاهرة.

فالهجوم السيبراني هو «هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير المرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى».

فالخصائص المميزة لشبكة الإنترنت أنها لا تعرف الحدود الدولية، فالمستخدم لشبكة الإنترنت يمكنه التنقل بين أرجاء العالم وهو في مكانه أمام شاشة الحاسب الآلي أو التليفون المحمول. ويترتب على الطبيعة الدولية لشبكة الإنترنت ان الجرائم التي ترتكب من خلالها تكون لها صفة الجرائم الدولية، أو الجرائم العابرة للحدود.

أهمية البحث:

ومثل أي ظاهرة إجرامية جديدة تظهر في المجتمع، وحتى يمكننا التصدي ومكافحة تلك الظاهرة الإجرامية، فكان لزاما علينا أن نقف على ما تتمتع به تلك الظاهرة من طبيعة قانونية وخصائص تميزها عن غيرها من الجرائم التقليدية، وذلك من خلال تحليلها للوقف على أسباب ظهورها ومعرفة الطريق المناسب لمكافحتها والتصدي لها. وحيث إن الظاهرة الإجرامية تتكون من الفعل المجرم الذي ينكره المجتمع والذي يمثل موضوع الجريمة، ومقترف هذا الفعل أو السلوك -الذي وصفه المجتمع بأنه جريمة- وهو الفاعل أو المجرم، فبعد تحديد الطبيعة القانونية لهذه الظاهرة، لا بد أن نبين خصائص تلك الجريمة، وخصائص مرتكبها، حتى نتمكن من معالجتها.

إشكالية البحث:

الإشكالية التي يثيرها هذا البحث والتي تقتضي البحث لها عن إجابة هي: هل يتمتع الهجوم السيبراني كظاهرة إجرامية بذات الطبيعة القانونية والخصائص التي تتمتع بها الجرائم التقليدية أم أن لها خصوصيتها التي تتميز بها؟، كذلك: هل المجرم السيبراني أو الإلكتروني هو شخص له خصائص يتميز بها وحده أم يتمتع بذات خصائص المجرم التقليدي؟

حصر نطاق البحث:

نحصر البحث في معرفة الطبيعة القانونية للهجوم السيبراني من خلال معرفة طبيعة الجرائم السيبرانية القانونية وخصائصها وخصائص المجرم السيبراني دون التطرق لطبيعة وخصائص الجريمة التقليدية والمجرم التقليدي حتى لا نخرج عن موضوع البحث.

منهج البحث:

إن إشكالية البحث لها دور رئيس في اختيار المنهج الذي يجب اتباعه في مقطع تناول موضوع البحث وعلى ذلك اتبع الباحث المنهج التحليلي والاستقصائي، وذلك من خلال تحليل الموضوع من أمهات الكتب والمراجع ذات العلاقة والأبحاث والدارسات التي تناولت الموضوع مع بيان رأي الفقه في تلك المسألة.

خطة البحث:

تناولت هذا الموضوع في مبحثين في محاولة من الباحث للإحاطة بجميع جوانب الموضوع دون الخروج عنه فجاءت الخطة كالاتي:

المبحث الأول: محل الجرائم السيبرانية

المبحث الثاني: خصائص الهجوم السيبراني

المبحث الأول: خصائص الهجوم السيبراني

الجريمة السيبرانية، كأي جريمة تتكون من فعل غير مشروع بمقتضى القانون وفاعل لهذه الجريمة وهو المجرم، إلا أن جريمة السيبرانية تتميز خصائص تختلف عن الجريمة التقليدية في عدة أمور، كذلك يختلف المجرم السيبراني من حيث خصائصه عن المجرم التقليدي. وعلى ذلك سوف نعرض في هذا المبحث لخصائص كلٍ من الجريمة السيبرانية والمجرم السيبراني، وذلك على النحو الآتي:

المطلب الأول: خصائص الجريمة السيبرانية

أولا- خصوصية الجريمة السيبرانية:

تتميز الجريمة السيبرانية بقلة عدد الحالات التي تم اكتشافها بالفعل إذا ما قارنا ذلك على ضوء ما يتم اكتشافه من الجرائم التقليدية. ويرى البعض أن من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف، كما أنها لا تترك أثارًا، وإنما يتمثل مظهرها في تغيير أو محو الأرقام والبيانات الموجودة بأنظمة الحاسبات الآلية. ولا تترك أثرًا خارجيًّا مرئيًّا أو ملموسًا.[1] إلا أنه يرى البعض الآخر صعوبة قبول هذا الرأي المتقدم على إطلاقه، فمن ناحية لا يقتصر أثر جرائم المعلوماتية على تغيير أو محو الأرقام والبيانات 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 والتي تتسم في اغلب 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 أن تستخدم كدليل في الإثبات في مدة قد تقل عن ثانية واحدة.[2]

ولا يتمثل الاختلاف بين الجريمة السيبرانية والجريمة التقليدية في معدل ارتكابها ومقدار الخسائر الناجمة عنها فقط، بل تتميز الجريمة السيبرانية أيضا بكونها لا تتسم بالعنف الذي تتسم به غيرها من الجرائم التقليدية. فحالات الإتلاف المعلوماتي التي قد يصاحبها استخدام للعنف قليلة نسبيا إذا قورنت بغيرها من الجرائم، حتى إنه يمكن القول إنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة السيبرانية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم. فالصورة التقليدية للمجرم تكاد تختفي في الجرائم السيبرانية، بل على العكس من ذلك فإن المجرم السيبراني 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 السيبراني نادرًا ما يكون محترفًا للإجرام أو عائدا فهو نمط مختلف عن المجرمين على نحو ما سوف نبين لاحقًا، حتى إن المجتمع في كثير من الأحيان لا ينظر إليه كمجرم بالمعنى المتعارف لهذه الكلمة. كما أن الأسباب أو العوامل التي تقف وراء ارتكاب الجريمة

(1) د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992، ص 41، انظر أيضا، د.نائلة قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط 2005 ، ص 49

(2) د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992، ص 42، انظر أيضًا، د. نائلة قورة، المرجع السابق، ص 49.

السيبرانية قد تختلف أيضًا بالمقارنة بالجريمة التقليدية فمجرد إظهار القدرات التقنية قد يكون واحد من هذه الأسباب، وهو ما لا نراه في الجرائم التقليدية.[1]

وتختلف الجريمة السيبرانية أيضا من حيث رد فعل المجني عليه تجاهها وتجاه مرتكبها فمن ناحية فإن المجني عليه في هذه الجرائم نادرًا ما يقوم بالإبلاغ كما سبق الإشارة. ويرجع ذلك لأسباب تتعلق بسمعة المؤسسة التي يمثلها والتي قد تتأثر إذا ما نما إلى علم المتعاملين معها تعرض أنظمة المعلومات الخاصة بها للتلاعب. ومن ناحية أخرى فإن للمجني عليه في هذه الجرائم دورًا مثيرًا للريبة في بعض الأحيان، فهو قد يشارك بطريق مباشر أو غير مباشر في ارتكاب الفعل فالبعض يرى أن للمجني عليه في الجرائم السيبرانية دورًا غير مباشر؛ وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للهجوم السيبراني مرتفع بشكل كبير. ويرجع ذلك إلى القصور الذي يعتري أنظمة الحاسبات الآلية والذي قد يساعد على ارتكاب الفعل الإجرامي ترتب على ذلك نتيجة أخرى تميز الجريمة السيبرانية. وهي أن إمكانية الحيلولة دون وقوع هذه الجريمة مرتفع بالمقارنة بغيرها من الجرائم؛ إذ يعتمد أساسًا 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.[2]

ويرى رأي من الفقه أن الأثر الرادع للقانون الجنائي ليس له ذات التأثير في جرائم المعلوماتية كما هو الحال في الجرائم التقليدية الأخرى طالما أن هذه الجرائم هي نتاج حسابات عقلية يضع الجاني فيها نصب عينيه عقوبة الفعل الذي 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 إن كثيرًا 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[3].

---

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

انظر أيضا، د. نائلة قورة، المرجع السابق، ص 50

(2) د. نائلة قورة، المرجع السابق، ص 51

(3) Parker(Donn), Op.Cit, p. 139

ثانيًا- من حيث الدافع على الارتكاب:

تستهدف الجرائم السيبرانية 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، قياسًا بالجرائم التقليدية، كما أتاحت الجرائم السيبرانية تسهيل ارتكاب جرائم أخرى لتحصيل مكاسب مادية جعلت حتى ملاحقة الجرائم التقليدية أمرًا صعبًا متى تم ارتكابها باستخدام نظام معلوماتي.(1)

ثالثًا- الجريمة السيبرانية 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 الجريمة ذا طبيعتين مختلفتين، إحداهما تتمثل في الجانب المادي، والأخرى تتمثل في جانب غير مادي، وذلك ليس على مكونات النظام ذاته بل يشمل ظهور المحل الواحد بمظهرين: أحدهما مادي والآخر 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 الآخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة معلوماتية حتى إن 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.(2)

رابعًا- من حيث موضوعها بالنسبة لمراحل تشغيل نظام المعالجة الآلية للبيانات:

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

(1) د/ طارق إبراهيم الدسوقي، المرجع السابق، ص 163

(2) د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، ط 1999، ص 42 وما بعدها، انظر أيضا، د. أيمن عبد الله فكري، المرجع السابق، ص 106

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 الحاسب الآلي كدس تعليمات غير مصرح بها فيها أو تشغيل برامج جديدة تلغي عمل البرامج الأصلية. والجرائم المرتكبة في هذه المرحلة تتطلب توافر معرفة فنية عميقة لدى الفاعل واكتشافها صعب، وغالبًا 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.[1]

خامسًا- الطبيعة متعدية الحدود للجريمة السيبرانية:

يمكن القول إن من اهم الخصائص التي تميز الجريمة السيبرانية 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 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 أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة السيبرانية وحجم المعلومات والأموال المستهدفة و المسافة التي قد تفصل الجاني عن هذه المعلومات و الأموال قد ميزت الجريمة السيبرانية عن الجريمة التقليدية بصورة كبيرة.[2]

سادسًا- صعوبة الإثبات في مجال الجريمة السيبرانية:

نظرًا للطابع الخاص الذي تتميز به الجرائم السيبرانية. فإن إثباتها يحيط به كثير من الصعوبات التي تواجه سلطة الاستدلال أو التحقيق الجنائي في استخلاص الدليل الجنائي.[3] والتي تتمثل في صعوبة اكتشاف هذه الجرائم؛ لأنها لا تترك أثرا خارجيا. فالجرائم السيبرانية 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 السيبرانية هي جرائم فنية تتطلب تكتيك معين في مجال الحاسبات الآلية. وهي جريمة هادئة لا تتطلب العنف ورغم ذلك فإن البعض يشبه

(1) د. طارق إبراهيم الدسوقي، المرجع السابق، ص163، 164

(2) د. نائلة قورة، المرجع السابق، ص 52

(3) د. عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الإنترنت، دراسة متعمقة في جرائم الحاسب الآلي و الإنترنت، بدون ناشر، ط 2009، ص 24

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 اضف إلى ذلك عدم ظهور الدليل المادي للجريمة المعلوماتية واستحالة رؤيتها وعجز وسائل الفحص التقليدية عن ضبط أثارها.[1] فإذا تم اكتشاف الجريمة السيبرانية، 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 اقل من ثانية، إلى جانب إمكانية ارتكابها عبر الوطنية والدول والقارات وذلك باستخدام شبكات الاتصال ودون تحمل عناء الانتقال. وإلى جانب ذلك الرغبة في استقرار حركة المعاملات ومحاولة إخفاء أسلوب ارتكاب الجريمة حتي لا يتم تقليدها من جانب الآخرين.[2]

المطلب الثاني: المجرم السيبراني وخصائصه

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضًا على تمييز المجرم المعلوماتي عن غيره من المجرمين.[3]

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 التنبؤ بهم أو معرفتهم، فإذا كان هذا النمط موجود بالفعل إلا ان النمط السائد هو المجرم الذي تربطه بالمجني عليه صلة ما والتي غالبًا 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.[4]

ومع ذلك يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتي، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين. ويعد الأستاذ Parker واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي

(1) د. محمد علي العريان، المرجع السابق، ص 65، انظر أيضا د. طارق إبراهيم الدسوقي، المرجع السابق، ص 166

(2) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، ص 1 وما بعدها.

(3) د. نائلة قورة المرجع السابق، ص 56

(4) Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, Heinemann: London 1987, p 134

بصفة خاصة. والذي يرى أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبًا 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[1]، وان كانت -في رأيه- لا تتطابق معها. فالمجرم المعلوماتي من ناحية ينتمي في أكثر الأحوال إلى وسط اجتماعي متميز، كما أنه على درجة من العلم و المعرفة وهو ما يميز بشكل عام ذوي الياقات البيضاء، وإن كان ليس 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 أنّ الفاعل في الحالتين يبرر جريمته، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.[2]

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه عن غيره من المجرمين، وهي المهارة والمعرفة والوسيلة والسلطة وأخيرًا الباعث. وذلك على التفصيل الاتي:[3]

أولا- المهارة:

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم السيبراني. فتنفيذ الجريمة السيبرانية بصفة عامة يتطلب قدرًا 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 السيبراني على قدر كبير من العلم في هذا المجال أو أن تكون لديه الخبرة فيه بل إن الواقع العملي أثبت أن بعض أنجح مجرمي الجرائم السيبرانية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتبية من العمل في هذا المجال.[4]

---

(1) جرائم ذوي الياقات البيضاء مصطلح يطلق على الجرائم غير العنيفة والمرتكبة لدوافع مالية من قبل رجال الأعمال وأصحاب النفوذ. في علم الجريمة عرّف المتخصص بعلم الاجتماع إدوين سذرلاند المصطلح لأول مرة في عام 1939 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.

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

(3) Parker (Donn B) , Op.cit., p 136

(4) د. نائلة قورة، المرجع السابق، ص 57، انظر أيضا، د. طارق إبراهيم الدسوقي، المرجع السابق، ص 171

ثانيا- المعرفة:

أما المعرفة فتتلخص في التعرف على جميع 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 يكوِّن تصورًا كاملًا 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.[1]

ثالثا- الوسيلة:

يراد بالوسيلة الإمكانيات التي يتزود بها الفاعل لإتمام جريمته. ففيما يتعلق بالمجرم السيبراني فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في اغلب 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. والحقيقة 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 الأفراد هم عادة القائمون على تشغيل النظام، وذلك على عكس الأنظمة الشائعة الاستعمال.[2]

رابعًا- السلطة:

يقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم السيبراني 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.[3]

---

(1) د. نائلة قورة، المرجع السابق، ص 58، انظر أيضا، د. طارق إبراهيم الدسوقي، المرجع السابق، ص171

(2) الإشارة السابقة.

(3) د. نائلة قورة، المرجع السابق، ص 58، انظر أيضا، د/ طارق ابراهيم الدسوقي، المرجع السابق، ص 172

خامسًا- الباعث:

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 أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجنائي،[1] وأن الباعث لا أثر له في وجود القصد الجنائي،[2] وإذا كان الاستخدام العادي للتعبيرات المشار إليها 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 والبغضاء والانتقام، وهو إذاً 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 والجنس ودرجة التعليم وغير ذلك من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر.[3] أو هو الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو سلب مال المجني عليه في جريمة القتل.[4]

والأصل أن الباعث والغاية 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 فإن القانون يسبغ عليهما في بعض الأحيان أهمية قانونية خاصة.[5]

ولا يختلف باعث الجاني على ارتكاب الجريمة السيبرانية 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 السيبرانية،[6] ثم يأتي بعد ذلك مجرد

(1) د. محمود نجيب حسني، شرح قانون العقوبات- القسم العام، الطابعة السادسة، دار النهضة العربية، 1989، ص 1052

(2) د. احمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام -، ط 1991، دار النهضة العربية، ص 427

(3) د. فوزية عبد الستار، شرح قانون العقوبات – القسم العام – دار النهضة العربية، ط 1992، ص 479

(4) د. أيمن فكري رمضان، المرجع السابق، ص 132

(5) د. محمود نجيب حسني، المرجع السابق، ص 480

(6) ويرى البعض أن أغلب مجرمي السيبرانية ليس لديهم اطماع مادية بقدر ما يحاولون حل مشكلات مادية لديهم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى.

الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية الموجودة حوله وأخيرا الانتقام من رب العمل أو احد الزملاء.[1]

و الحقيقة انه أيا ما كان الباعث وراء ارتكاب الجريمة السيبرانية فإنه يوجد شعور دائما لدى مرتكب الفعل بأن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن ان 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 الإضرار بمؤسسة أو جهة تستطيع اقتصاديا تحمل نتائج تلاعبهم.[2]

ويتصف مجرمو المعلوماتية أيضًا وبصفة خاصة، بالخوف من كشف جرائمهم وافتضاح أمرهم. صحيح أن هذه الخشية إنما تصاحب المجرمين على اختلاف أفعالهم الإجرامية إلا أنها تميز مجرمي السيبرانية بصفة خاصة لما يترتب على افتضاح أمرهم من ارتباك مالي وفقد للمركز الوظيفي في كثير من الأحيان. ويساعد مرتكبو الجرائم السيبرانية في الحفاظ على سرية أفعالهم طبيعة الحاسبات الآلية نفسها فإن اكثر ما يعرض المجرم إلى اكتشاف أمره أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها في حين أن أهم الأسباب التي تساعد على نجاح الجريمة السيبرانية 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 وهو ما يساعد على عدم كشف الجريمة طالما ان جميع خطوات التنفيذ معروفة مسبقا بحيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة.[3]

وعلى ذلك استطاع الفقه أن يضع أنماط مختلفة لمرتكبي الجرائم السيبرانية، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مرتكبي الجرائم السيبرانية. ولا يعني بطبيعة الحال أن كل مجرم يندرج تحت طائفة محددة دون غيرها بل من الممكن أن يكون المجرم الواحد مزيجا من اكثر من طائفة، الطائفة الأولى جناة التسلية و المزاح (pranksters)، الطائفة الثانية هم المخترقون (Hackers)، الطائفة الثالثة المخترق المؤذي (Malicious hackers)، الطائفة الرابعة حل المشاكل الشخصية (Personal Problem Solves)، الطائفة الخامسة المجرم الممتهِن (Career Criminals)،

(1) د. هشام فريد رستم، المرجع السابق، ص 38

(2) د. نائلة قورة، المرجع السابق، ص 59

(3) د. نائلة قورة، المرجع السابق، ص 60

والطائفة السادسة المتطرفين (Extreme Advocates).

ويرى الباحث أن بين كل هذه الطوائف لم يذكر الفقه الحالة التي يكون من ارتكب الجريمة السيبرانية دولة من الدول، وذلك عندما يكون الهدف أو الباعث على ارتكاب تلك الجريمة هو باعث سياسي، حيث إن للدوافع السياسية دورًا لا يمكن إنكاره في ارتكاب الجرائم السيبرانية حيث سخرت الإنترنت في الصراعات السياسية الدائرة اليوم وشهدت السنوات القليلة الماضية محاولات دولية لاختراق شبكات حكومية في مختلف دول العالم فالتجسس عبر الإنترنت يتم يوميا من قبل أجهزة المخابرات، وكذلك فإن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، وخير مثال على ذلك عندما استطاع حزب الله اللبناني اختطاف أربعة جنود من قوات الاحتلال الإسرائيلي في جنوب لبنان بعد انتفاضة عام 2000م، بادر الجانب الإسرائيلي إلى مهاجمة موقع حزب الله على الإنترنت ونجحوا في تعطيله مما أنشأ صورة أخرى من الصراعات وهو الصراع الإلكتروني.[1]

وعلى ذلك هل نستطيع أن نقول إن تلك الصراعات عبر الإنترنت بين الدول تمثل جرائم سيبرانية. وأنه إذا ما تم اكتشاف ومعرفة الدولة التي اقترفت الفعل الإجرامي هل تسأل دوليا عن هذا الفعل الذي يمثل عدوان على دولة أخرى. وهل تستطيع الدولة المعتدى عليها استخدام حق الدفاع الشرعي عن نفسها والرد على هذا الاعتداء. وهل يعد هذا الاعتداء عن طريق شبكات الإنترنت من حيث طبيعته القانونية الدولية مثل الاعتداء باستخدام القوة العسكرية، مما يعطي الحق للدولة المعتدى عليها بالرد باستخدام القوة العسكرية.

المبحث الثاني: محل الجرائم السيبرانية

إن الهجوم السيبراني كجريمة يتميز بطبيعة خاصة مختلفة عن الجرائم التقليدية؛ لأنها في اغلب الأحوال عندما ترتكب تكون في مجال المعالجة الإلكترونية للبيانات و المعلومات، وذلك لأن الهدف من الهجوم السيبراني لدى المجرم هو، إما الحصول على تلك البيانات أو المعلومات أو إعاقة وصولها إلى مكان التخزين أو إتلاف تلك البيانات والمعلومات الموجودة على الحاسب الألي.

فالهجوم السيبراني لا يقع على الأجهزة الآلية كمنقولات مادية من أجل تخريبها ماديا بل تقع على ما تحويه تلك الأجهزة من بيانات ومعلومات مهمة وسرية والتي تكون محل الاعتداء أو الهجوم .

(1) د. طارق إبراهيم الدسوقي، المرجع السابق، ص 177

فالطبيعة القانونية للهجوم السيبراني حتى يمكن تحديدها، لا بد من تحديد معنى المعلومات أو البيانات وطبيعتها باعتبارها هي محل الاعتداء.

وعلى ذلك يمكن إن نقسم هذا المبحث إلى مطلبين، المطلب الأول سوف نقوم فيه بالحديث عن ماهية المعلومات، أما المطلب الثاني فيأتي فيه الحديث عن طبيعة المعلومات باعتبارها محل الاعتداء في الهجوم السيبراني.

المطلب الأول: ماهية المعلومات

1. تعريف المعلومات:

يمكن تعريف المعلومات بصفة عامة بأنها «مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا لتبادل و اتصال أو للتفسير و التأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل أو أشكال مختلفة.[1]

إلا أن بعض الفقه قد ميز في التعريف فين البيانات والمعلومات، فيرى أن البيانات تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للاستخدام والتي تخلو من المعنى الظاهر في اغلب الأحيان، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات.[2] وقد أيد بعض الفقه هذه التفرقة مدللا عليها بان عبارة « Le soliel brille » باللغة الفرنسية تعني أن الشمس مشرقة وهي لا تعدو أن تكون بيانا لحالة الشمس ولا يمكن أن تتحول إلى معلومة لدى شخص إلا بتوافر شرطين الأول أن يطلع عليها بالفعل والثاني أن يكون هذا الشخص على علم باللغة الفرنسية حتى يستطيع تفهمها. والى أن يتحقق هذان الشرطان تظل البيانات مجموعة من الحروف ولا يمكن أن تتحول إلى معلومة إلا بتوافرهما. ويرى رأي آخر أنه لا جدوى من التمييز بين المعلومات والبيانات فالذي يعنينا في هذا المقام هو حماية المعلومات بصفة عامة وطالما أن المعلومات هي المعنى المستخلص من البيانات فالحماية تشملهما معًا، ومن ناحية أخرى قد لا تكون المعلومة مفهومة لدى متلقيها وهو ما يجعلها تخرج عن دائرة المعلومات طبقا لهذه التفرقة ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر متن الخطورة فالذي يعنينا هو حماية

(1) Parker (Donn B) Fighting computercrime – A new Farmework for Protecting Information, john Wiley & sons, Inc., 1998, p 27

(2) د. هشام فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ط 1992، ص26

المعلومات بغض النظر عن فهم محتواها. [1]

وعرفها رأي آخر وفقا للعلاقة بين المعلومات والبيانات بأنها «مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة شكل حروف أو أرقام أو أشكال خاصة تصف أو تمثل فكرة أو موضوع أو هدفا أو شرطا أو أية عوامل أخرى وتشكل البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات.[2]

ويرى آخر أن البيانات هي معلومات في حالة كمون، والمعلومات هي البيانات في حالة نشاط، ولذلك فإن البيانات تمثل حقائق رقمية أو غير رقمية أو مشاهدات واقعية لا تصورية أو قياسات تتم بطريقة منهجية يمكن لآحاد الناس قراءتها وفهم دلالتها البسيطة بدون دخول في عمليات استنباطية أو استقرائية لدلالتها المعقدة سواء من حيث الربط فيما بين اكثر من بيان منها أو استخلاص أية نتيجة مترتبة عليها فإن تم ذلك بدأ دخول منطقة أخرى هي منطقة المعلومات . فالمعلومات هي كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالتها أو استنباط ما يمكن استنباطه منها وحدها أو متداخلة مع غيرها أو تفسيرها على نحو سديد يثري معرفة متخذي القرار في الحكم على الظواهر و المشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية[3]، فالمعلومة لدى انصار الرأي السابق تأتي في مرحلة تالية ومتأخرة على البيانات وتعد المعلومة هي القيمة المضافة إنما البيانات فهي المادة الخام بالنسبة لها.[4]

هذا وقد عرفها رأي آخر بأنها النشاط القادر على أن يحمل للجمهور بعض الوقائع أو الآراء من خلال وسائل بعدية أو سمعية تتضمن رسائل فكرية لهم أو هي شكل له قيمة اقتصادية من وجهة نظر الجمهور الذي يرغبها.[5]

وتتميز المعلومات بصفة عامة بقابليتها للدمج فقد تضاف معلومة إلى أخرى لتكوِّنا معا معلومة جديدة تختلف في قيمتها وأهميتها، ومن ثم في مقدار الحماية اللازمة لها عما كانت عليه قبل عملية الدمج، فمثلا، رقم حساب عميل في البنك معلومة على قدر من الأهمية وتحتاج هذه المعلومة بطبيعة الحال إلى حمايتها، إلا أنه إذا أضفنا إلى

(1) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط 2005، ص 97

(2) انظر، د. محمد السعيد خشبة، مقدمة في التجهيز الإلكتروني للبيانات، القاهرة، جامعة الأزهر، ط 1984، ص4

(3) د. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، ط 2001، ص 62

(4) د. أيمن عبدالله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، ط 2015، ص 40

(5) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الالي، دار النهضة العربية، ط 2000، ص 30

هذه المعلومة معلومة أخرى كاسم البنك واسم العميل وحجم الرصيد فإن قيمة المعلومة وأهميتها في هذه الحالة تتضاعف وتتطلب من ناحية أخرى قدرا أكبر من الحماية. إذا فلكل معلومة قيمة اقل بدون دمجها مع معلومة أخرى.

2. خصائص المعلومات:

للمعلومات بصفة عامة خصائص تساعد على التعرف على طبيعتها، وأهميتها، وعلى مقدار الحماية اللازمة لها. وان اكتساب المعلومة لأهميتها يستلزم تحوليها إلى شكل ملموس حتى يمكن الوقوف على وجودها، ومن ثم التمكن من حمايتها. فنحن نتعرف على المعلومة بالإشارة إليها وذكر اسمها، ونتمكن من معرفة وجود ملف ما من قراءة اسمه في فهرس ملفات البيانات التي في الحاسب الآلي .

وعلى ذلك لكل معلومة قيمة ما وتكون المعلومة تبعا لهذه القيمة جديرة بالحماية، ولكي تكتسب هذه المعلومة القيمة لا بد أن تظهر في إطار معين يعطيها هذه القيمة، وهذا الاطار يتحدد بمجموعة من الخصائص، و تنقسم تلك الخصائص إلى طائفتين وذلك على التفصيل التالي:

ترتكز خصائص المعلومات على أربعة ركائز أساسية، وهي:

الركيزة الأولى نوع المعلومة:

فتختلف المعلومات فيما بينها من حيث النوع، و تختلف من حيث الأهمية تبعا إلى ذلك، فالمعلومة قد تكون نوعا من المعرفة، وقد تكون في شكل رسم هندسي وقد تكون مجموعة من الأوامر، والإرشادات، وقد تتعلق بأمور مالية أو على العكس قد تكون ذات طبيعة فنية أو أدبية أو غير ذلك من مئات الأشكال التي قد توجد المعلومة عليها.

المعلومات التي تتخذ شكل التعليمات في مجال تكنولوجيا الحاسبات الآلية:

حاز هذا النوع من المعلومات على أهمية، وقيمة خاصة نظرا لاستخدامها في مجال الحاسبات الآلية، فالمعلومات في هذه الحالة، والتي تتخذ شكل برامج للحاسب الآلي « software » تعطي التعليمات اللازمة لتشغيل الحاسب لقيامه بالعمليات المطلوبة منه، ومن ثم كانت هذه البرامج وسيلة مهمة لارتكاب كثير من الجرائم المعلوماتية. ومن هنا كانت ضرورة الاهتمام بتوفير الحماية اللازمة لهذه البرامج. ولا يختلف الأمر سواء كانت هذه البرامج مصدرية أو أصليه أم كانت برامج هدف[1]، ففي كلتا الحالتين يمكن التلاعب

(1) تعد البرامج المصدرية وبرامج الهدف نوعي البرامج المستخدمة لتشغيل الحاسبات الالية، لمزيد من التفصيل،

فـي البرنامـج وتغييـره سـواء كان التلاعـب مقصـودا فـي ذاتـه أم كان مقصـود منـه ارتـكاب جريمـة أخـرى بمسـاعدته. ولا توجـد صعوبـة كبيـرة فـي اكتشـاف التلاعـب الـذي قـد يلحـق ببرامـج المصـدر علـى عكـس الحـال فيمـا يخـص برامـج الهـدف إذ يصعـب اكتشـاف التلاعـب الـذي لحـق بهـذا النـوع مـن البرامـج بـدون مقارنـة دقيقـة مـع نسـخة أخـرى مـن نفـس البرنامـج.

- **النقود في عالم الحاسبات الآلية:**

أصبـح الآن لبعـض المعلومـات قيمـة نقديـة خاصـة بعـد الدخـول فـي عصـر الحاسـبات الآليـة وتـدل المؤشـرات علـى نمـو عـدد الجرائـم التـي تقـع علـى هـذا النـوع مـن المعلومـات لذلـك بـدأت تتجـه الجهـود نحـو توفيـر اكبـر قـدر ممكـن مـن الحمايـة لهـذا النـوع مـن المعلومـات. ولقـد اصبـح التعامـل النقـدي فـي الوقـت الراهـن يتـم بصـورة كبيـرة عبـر الحاسـبات الآليـة بحيـث أصبـح اسـتخدام اصطـلاح النقـود الإلكترونيـة يتزايـد مقارنـة بالنقـود العاديـة. فأصبحـت الآن الصفقـات تبـرم بالكابـل عـن طريـق شـبكات الإنترنـت ويتـم تبـادل السـلع أو الخدمـات إلكترونيـا وكذلـك الوفـاء بقيمـة تلـك السـلع إلكترونيًـا.[1]

الركيزة الثانية: الصورة التي توجد عليها المعلومات:

إن الركيـزة الثانيـة للخصائـص الأوليـة للمعلومـات هـي الصـورة التـي توجـد عليهـا تلـك المعلومـة، فالمعلومـة قـد تكـون مشـفرة أو غيـر المشـفرة كمـا قـد تكـون مقـروءة أو مسـموعة، وتتوقـف قيمـة المعلومـة، والحمايـة اللازمـة لهـا فـي كثيـر مـن الأحيـان علـى الصـورة التـي توجـد عليهـا فتغييـر حـرف فـي معلومـة مشـفرة يختلـف اختلافـا كبيـرا عنـه فـي معلومـة غيـر مشـفرة فالتغييـر فـي الحالـة الأولـى يـؤدي إلـى تدميـر لمعنـى هـذه المعلومـات إلا أنـه لا يـؤدي بالضـرورة إلـى تلـك النتيجـة فـي الحالـة الثانيـة إذ قـد يقتصـر الأمـر علـى مجـرد الانتقـاص مـن صحتهـا.[2]

وقـد تتغيـر الصـورة التـي توجـد عليهـا المعلومـة بسـبب التلاعـب بهـا بحيـث تظـل المعلومـة موجـودة ولكـن بـدون معنـى أو فائـدة. فإدخـال أحـد البرامـج الخبيثـة إلـى الحاسـب الآلـي مـن شـأنه أن يغيـر مـن صـورة المعلومـة علـى نحـو سـلبي، وقـد يـؤدي إلـى تحويـل المعلومـة علـى الشاشـة إلـى مجموعـة مـن الحـروف المبعثـرة التـي تتهـاوى بسـرعة كبيـرة إلـى القـاع مكونـة كومـة كبيـرة مـن الحـروف. علـى الرغـم مـن أن المعلومـة مازالـت موجـودة علـى الشاشـة إلا أنهـا قـد فقـدت كل أهميـة لهـا مـا لـم يمكـن إعادتهـا إلـى الصـورة الأولـى بالاسـتعانة بنسـخة

والايضاح انظر د. نائلة قورة، المرجع السابق، هامش ص 102

(1) د. طارق إبراهيم الدسوقي، المرجع السابق، ص 56

(2) د. طارق إبراهيم الدسوقي، المرجع السابق، ص 57

إضافية يحتفظ بها كضمان في حالة فقد أو تدمير الأصل. كما قد يقوم هذا الفيروس أيضا بتغيير صورة المعلومات في ذاكرة الحاسب وذلك بتغيير ملف البيانات الذي يحتوي على المعلومات في ذاكرة الحاسب الآلي، وتحويلها إلى خيط من الحروف.[1]

وتقتضي حماية البيانات إذا الحفاظ على كل صورة توجد عليها وكذلك حماية البرامج المسؤولة عن تحويل المعلومات من صورة إلى أخرى كلما اقتضى الأمر، وأخيرًا حماية الوسيلة التي يتم من خلالها عرض هذه الصورة كشاشة عرض المعلومات وذلك بتحديد من لهم حق الاطلاع عليها.[2]

أما الركيزة الثالثة فهى شكل المعلومة:

ويقصد بالشكل في مجال المعلوماتية أو تكنولوجيا المعلومات الطريقة التي تكتب بها المعلومة من خلال الحاسبات الآلية ويتضمن ذلك أسلوب المبرمج في كتابة البرنامج، الحروف التي تتعلق بالطباعة، اللغة البرمجية، القواعد اللغوية، قواعد التشفير، الهيئة أو شكل الطباعة أو النسق، وحجم الذاكرة أو حجم الملف أو المستند

ويرى رأي وبحق انه من الضروري امتداد الحماية إلى القواعد المتصلة بالشكل وذلك لمنع التلاعب بالمعلومات عن طريق المساس بهذه القواعد. فتغيير شكل المعلومة قد يترتب عليه تغيير في معناها، أو فقدانها تماما. ويأتي الإتلاف المتعمد في هذه الحالة عن طريق تغيير الشكل إلى شكل آخر لا قيمة له، وأعطى هذا الرأي مثالًا على ذلك بأنه عندما يقوم احد الأشخاص بتشفير جميع النسخ المتعلقة بملف معين ثم يقوم بتدمير المفتاح المسؤول عن فك هذه الشفرة فتصبح المعلومات بهذا الشكل عديمة القيمة[3].

وأخيرا الركيزة الرابعة هي تخزين المعلومات:

تتطلب المعلومة لما لها من طبيعة خاصة، وجود وسط تخزن فيه حتى لو كان هذا الوسط هو مجرد العقل البشري. وتختلف وسائط تخزين المعلومات فقد تكون أحبارا أو ألوانا وينطبق ذلك على جميع المعلومات المدونة في أوراق، أو ذبذبات كهربائية في الفضاء كموجات الراديو أو قطع ووصل الكتروني كالإشارات الرقمية في الحاسبات الآلية، وإن أي تلاعب قد يقع على هذا الوسط من شأنه ان يؤدي إلى تعريض المعلومة للخطر.

(1) د. نائلة قورة، المرجع السابق، ص 106

(2) Parker, (Donn) , Op.Cit., p 41

(3) انظر، د. نائلة عادل قورة، المرجع السابق، ص 107

المطلب الثاني: طبيعة المعلومات باعتبارها محل الاعتداء في الهجوم السيبراني.

ثار جدل طويل حول الحماية القانونية للمعلومات في حد ذاتها منظورًا إليها بمعزل عن الوسيط المادي الذي يمكن أن يندمج فيه. فعلى الرغم من الأهمية الاقتصادية للمعلومات فإنها تظل مجرد أفكار غير قابلة للسرقة أو ان 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 توافرها ابتداء في المعلومة حتى يمكن أن تتمتع بالحماية القانونية ثم نبين الطبيعة القانونية للمعلومة وهل لها طبيعة خاصة ام أنها شكل جديد من أشكال القيم المادية وذلك على التفصيل الآتي.

أولا- شروط يلزم توافرها في المعلومات:

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

- **أن تكون المعلومة مبتكرة ومحددة:**

إن المعلومة التي تفتقر لصفة التحديد لا يمكن ان تكون معلومة حقيقة. فاذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ والتبادل عن طريق علامات أو إشارات مختارة فينبغي أن 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 وأن يكون هذا الشيء بدوره محلا لحق محدد. كذلك يجب أن 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]

(1) د. طارق ابراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ط 2015، ص 44

- **أن تتصف المعلومة بالسرية والاستئثار:**

كلما اتسمت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها محددا بمجموعة معينة من الأشخاص وبدون هذا التحديد فإنه لا يمكن ان 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 اذا 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 وصاحبها عندما يكون موضوع هذه المعلومة فكرة أو عمل ذهني أو إعداد أو تنسيق أمر ففي هذه الحالة ينظر مؤلف المعلومة إليها باعتبارها ملكا خاصا خالصا له وهو على حق في ذلك، فإذا تمكن الغير من الاستيلاء عليها وعلى نحو غير مشروع فسوف يشعر صاحبها بأنه قد سلب منه شيء يمتلكه.[1]

(1) د.طارق إبراهيم الدسوقي، المرجع السابق، ص 45، 46

ثانيا- الطبيعة القانونية للمعلومات:

كما أوضحنا سلفا تتمتع بعض المعلومات بقيمة اقتصادية إلا أن ذلك يثير التساؤل عما كانت المعلومات في ذاتها منفصلة عن الوسيط المادي الذي يعبر عنه تعد من القيم المالية التي يمكن إذا الاعتداء عليها وقد انقسم الفقه عند الإجابة عن 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 انصار 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 والخدمات، فللمعلومات في رأي أنصار هذا الاتجاه علاقة مباشرة بفكرة المنفعة أو الخدمة فمن ناحية فإن نشأة المعلومة غالبا ما تكون استناد إلى عمل سابق عليها. ومن ناحية أخرى، فإن 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. (1)

إلا أن استبعاد المعلومات من نطاق القيم المالية، لم يمنع الفقه والقضاء 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 والتطبيق الموسع لنظرية التصرفات الطفيلية وتأسيس الخطأ على نظرية الإثراء بلا سبب وأخيرًا، تأسيسه على فكرة المسؤولية التقصيرية.(2)

(1) د. نائلة قورة، المرجع السابق، ص 116

(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاستها على قانون العقوبات، دار النهضة العربية، ص 180، انظر أيضا د. محمد علي العريان، الجرائم المعلوملتية، دار الجامعة الجديدة، ط 2011، ص 62، انظر أيضا، د. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط 2002، ص 163 وما بعدها.

الاتجاه الثاني: المعلومات طائفة جديدة من القيم[1]:

يذهب انصار هذا الاتجاه إلى اعتبار المعلومات قيمة تضاف إلى غيرها من القيم الأخرى، ولقد تبنى جانب من الفقه الفرنسي هذا الاتجاه وعلى رأسهم كل من الأستاذ «Pierre Catala » والأستاذ «Michel Vivant» . فتعد المعلومة طبقا للأستاذ CATALA واستقلالا عن دعامتها المادية من قبيل المال للحيازة ولتدعيم هذا الوصف فقد أشار بأن المعلومة قابلة للحيازة عندما لا يحظر السوق، وهي قيمة تقوم لسعر السوق وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها. وأن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية وهي علاقة المالك بالشيء الذي يملكه وانها 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 ان تستند إلى مال معنوي بحيث يكون هذا المال من قبيل الأموال الاقتصادية وانه جدير بحماية القانون. أما الحجة الثانية هي ان كل الأشياء المملوكة ملكية معنوية والتي 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 ولكنها 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 ان المعلومة حتما من قبيل المال بسبب قيمتها الاقتصادية، فإن 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 انه يقرر وبحسم على فكرة ان المعلومة يمكن ان تكون محلا لعقد بيع طالما أن الإبداع يرتبط بصاحبه، بل يمكن علاوة على ذلك نقل حق الانتفاع بالمعلومة أو استغلالها، ويضيف إن لصاحب المعلومة أن يتنازل عنها بموجب عقد أو قيد استخدامها أو أن يرفضه.

(1) د/ عبد الله حسين على محمود، المرجع السابق، ص 169، 170، 171، انظر أيضا د/ نائلة قورة، المرجع السابق، ص 119، 120، انظر أيضا، د/ محمد على العريان، المرجع السابق، ص 63، 64 .

الخاتمة:

النتائج:

- من خلال الدراسة توصلنا إلى أن المعلومات أو البيانات هي محل الاعتداء في الجرائم السيبرانية بعض النظر من كون الاعتداء تم على البيانات التي لم تتحول إلى معلومة عن طريق البرمجة أم تم الاعتداء على المعلومة المخزنة داخل الحاسب الآلي بعد معالجتها برمجيا.

- كذلك ليس كل المعلومات المخزنة على الحاسب الآلي تعد محلا للاعتداء في الهجوم السيبراني، ومن ثم تكتسب الحماية القانونية، بل يلزم ان تتوافر في تلك المعلومة شروط معينة منها ان تكون المعلومة مبتكرة ومحددة وأن تتصف بالسرية والاستئثار، لأن المعلومة المتاحة للجميع لا تعد محلا للاعتداء في الهجوم السيبراني ولا حاجة لحمايتها من الناحية القانونية.

- كذلك توصلت الدراسة إلى ان المعلومة هي نوع من القيم، أي أنها تقوم بالمال وترتبط بصاحبها بعلاقة قانونية وهي علاقة مالك الشيء بالشيء الذي يملكه، فهي من قبيل المال بسبب قيمتها الاقتصادية.

- كذلك توصلت الدراسة إلى أن صعوبة إثبات الجريمة السيبرانية لعدم توافر أدلة مادية عادة وخوف المجني عليه على سمعة المؤسسة المعتدى عليها والذي يترتب عليه عدم قيامه بالإبلاغ بالإضافة إلى الطبيعة العابرة للحدود للجريمة السيبرانية هم الأسباب الرئيسة في زيادة تلك الظاهرة الإجرامية.

- كذلك توصلت الدراسة إلى أن المجرم السيبراني يختلف من حيث الصفات والبواعث على ارتكاب الجريمة عن المجرم التقليدي فالأول يجب أن تكون لدية المهارة الفنية العالية لاستخدام الحاسب الآلي حتى يتمكن من ارتكاب جريمته والتي عادة لا يكون لها آثار مادية

- كذلك تختلف دوافع وأنماط المجرم السيبراني عن المجرم التقليدي فمنهم من يقوم بالعمل الإجرامي من باب التسلية ومنهم من يقوم بها من باب إشباع رغبة داخلية بأنه قادر على اختراق أي نظام الكتروني ومنهم من يرتكبها بغرض الحصول على المال ومنهم من يرتكبها بغرض سياسي

التوصيات:

لذلك توصي الباحثة لما تختص به هذه الجريمة من خصوصية بما يلي:

- وضع قواعد إجرائية سريعة تتناسب مع سرعة هذه الجريمة لكي يسهل تقديم الأدلة ومعرفة مرتكبها وإثباتها.
- زيادة التعاون بين الدول للقضاء على تلك الظاهرة الإجرامية، وذلك لما تختص به تلك الجريمة من خاصية اللاحدودية حيث لا تستطيع دولة بمفردها مهما بلغ تقدمها ان تحمي نفسها من تلك الهجمات السيبرانية دون التعاون مع دول العالم الأخرى.
- وضع قانون دولي موحد لمكافحة الجرائم السيبرانية؛ وذلك لأن الفعل المرتكب قد يمثل جريمة في الدولة المرتكب فيها الجريمة، ولا يمثل ذات الفعل جريمة في الدولة التي يتواجد فيها المجرم مما يصعب التعاون من الناحية الإجرائية أو المحاكمية بين الدولتين لاختلاف القوانين بينهم.
- تدريب أفراد الأمن القائمون على مكافحة الجريمة السيبرانية بشكل مستمر يتواكب ويتزامن مع التطور التكنولوجي الذي قد تكون عليه الهجمات السيبرانية.
- التطوير المستمر لبرامج الحماية داخل أجهزة الحاسبات الآلية للمؤسسات الحكومية والاقتصادية داخل الدول بشكل يصعب معه اختراقه من أي مجرم سيبراني.
- عمل تحريات مستمرة على الأشخاص الذين لديهم سلطة الدخول على أنظمة الحاسبات الآلية للمؤسسات الحكومية والاقتصادية وتأكد من قيامهم بما يلزم لتأمين تلك الأجهزة من اية هجمات خارجية.

قائمة المصادر والمراجع:

المراجع العربية:

المراجع العامة:

1. د. محمود نجيب حسني، شرح قانون العقوبات- القسم العام، الطبعة السادسة، دار النهضة العربية، 1989.
2. د. أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام -، ط 1991، دار النهضة العربية
3. د. فوزية عبد الستار، شرح قانون العقوبات – القسم العام – دار النهضة العربية، ط 1992.

المراجع المتخصصة:

4. د. هشام فريد رستم، قانون العقوبات و مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ط 1992.

5. د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، ط 2005
6. د. محمد السعيد خشبة، مقدمة في التجهيز الإلكتروني للبيانات، القاهرة، جامعة الأزهر، ط 1984.
7. د. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، ط 2001.
8. د. أيمن عبدالله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، ط 2015.
9. د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، ط 2000
10. د. طارق إبراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ط 2015 .
11. د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية
12. د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، ط 2011.
13. د. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط 2002.
14. د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992
15. د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، ط 1999
16. د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بدون ناشر، ط 2009
17. د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية.

Transliteration Arabic References: **الترجمة الحرفية لمصادر ومراجع اللغة العربية:**

Almaraaj'e al'arabiah:

Almaraj'e al'aammah:

1. Dr. Mahmuod Najib Husniy, sharh qanuon al'uquobaat - alqism al'aam, at-tab'ah as-sadisah, dar an-nahdah al'arabiat, 1989.
2. Dr.Ahmad Fathy Suruor , alwaseet fi qanuon al'uquobaat - alqism al'aam – tab'at 1991, dar an-nahdah al'arabiat.
3. Dr.Fawziah Abdulsitar, sharh qanuon al'uquobat - alqism al'am - dar an-nahdah al'arabiat, tab'at 1992.

Almaraaj'e almutakhassisah:

4. Dr. Hisham Farid Rustum, qanuon al'uquobaat wa makhatir tikniat alm'aluomat, maktabat al'aalaat alhadeethah, tab'at 1992.
5. Dr. Na'ilah Adil Muhammad Farid Quorah, jaraa'im alhaasib al'aaly al'iqtisaadiyah, manshuorat alhalaby alhuquoqiyah, tab'at 2005.
6. Dr.Muhammad Alsaed Khashabah, muqaddimah fi at-tajheez al'iliktruony lilbayaanat, alqaahirah, jami'at al'azhar, tab'at 1984.

7. Dr.Muhammad shita, fikrat alhimayah aljina'iyah libaraamij alhaasib al'aaly, dar aljami'ah aljadeedah, al'iskandariat, tab'at 2001.
8. Dr.Ayman Abdallah Fekry, aljara'im alm'aluomatiyah, maktabat alqanuon waliqtisaad, alriyad, tab'at 2015.
9. Dr.Ahmad Hussam Taha Tammaam, aljara'im an-naashi'ah 'an istikhdam alhaasib al'aaly, dar an-nahdah al'arabiah, tab'at 2000.
10. Dr.Tariq Ibrahim Aldusuoqy, al'amn alm'aluomaaty, dar aljaami'ah aljadeedah, al'iskandariah, tab'at 2015.
11. Dr.Muhammad Sami Alshwwa, thawrat alm'aluomat wan'ekaasaatuha 'alaa qanuon al'uquobaat, dar an-nahdah al'arabiah.
12. Dr.Muhammad Aly al'eryaan, aljaraa'im alm'aluomatiyah, dar aljami'ah aljadeedah, tab'at 2011.
13. Dr.Abdallh Hussain Aly Mahmuod, sariqat alm'aluomaat almukhazzanah fi alhasib 'al'aaly, dar an-nahdah al'arabiah, tab'at 2002.
14. Dr.Hisham Farid Rustum, qanuon al'uquobat wa makhaatir tikniyat alm'aluomaat, maktabat al'aalaat alhadeethah, 1992
15. - Dr.Saeid Abdullatif Hassan, 'ithbaat jara'im alcompuoter waljara'im almurtakabah 'abr al'intrnt dar an-nahdah al'arabiah, tab'at 1999.
16. Dr. Abdulfattah Baiuomy Hajaazy, 'ad-daleel aljinaa'y wat-tazweer fi jara'im alkombiutir wal'intarnit, dirasah mut'ammiqah fi jaraa'im alhasib al'aaly wal'intarnit , bidun nashir, tab'at 2009.
17. Dr. Jameel Abdulbaqi Alsaghir, alqanuon aljina'iy wat-tiknuoloujia, alkitaab al'awwal, aljaraa'em an-nash'ah 'an istikhdam alhasib al'aly, dar an-nahdah al'arabiah.

المراجع الأجنبية:

Parker (Donn B) Fighting computercrime – A new Farmework for Protecting Information, john Wiley & sons, Inc., 1998

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

Clough (Bryan) & Mango (Paul), Approaching Zero: Data Crime and the Criminal Underworld, , Faber and Faber London Boston, 1992

Cornwall (Hugo), Datatheft, Computer Fraud, Industrial Espionage and Information Crime, Heinemann: London 1987

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

The Legal Nature and Characteristics of Cyberattack

Shaikha Hussain Alzahrani

College of Law - University of Sharjah

Sharjah - U.A.E.

Abstract:

Cyberattack is a criminal phenomenon that arose in the field of information technology and is carried out through attacks, penetrations and infiltrations within the information systems of public or private institutions with the purpose of either destroying these systems or obtaining confidential information stored, be it military or economic. This criminal phenomenon has a special nature, as it does not focus on a concrete physical object but rather on the data or information stored inside the computer. The cyberattack therefore seeks to either know the secret information stored on the computer or remove information from it, which leads to the victim's loss of data and its being known or surveyed. In this way, the information becomes worth a lot of money and subject to criminal assault if certain conditions are met. Cybercrime is also characterized by the limitation of its discovery as it does not involve violence and does not leave traces behind, which makes it difficult to prove. This is added to the fact that cybercrime is different from traditional crime in terms of its purpose or of the motives for committing it.

Keywords: International Cooperation, Interpol, Extradition, Judicial Delegation, Legal Aid.