د./ بولحية شهيرة- المركز الجامعي بريكة
د/ سويح دنيا زاد- جامعة باتنة 01

عنوان المقال

الاحتيال الإلكتروني

ملخص:

ارتبط إنتشار الجرائم المستحدثة بوجود الانترنت التي أفرزت نوعا جديدا يختلف عن الجرائم التقليدية، وساهم في توسعها الاستخدام الكبير للشبكة العنكبوتية، ونشوء مجتمع معلوماتي تسيطر فيه الأجهزة الإلكترونية على لأذهان مستخدميه، وخاصة مع الدراية الكافية بمختلف التقنيات والبيانات المخزنة، ويتسم هذا النوع من الجرائم بسهولة إرتكابها وسرعة انتشارها بين الدول والقارات، وتعد جريمة الإحتيال الإلكتروني إحدى أهم الجرائم الإلكترونية التي تعتمد على اسلوب الخداع والغش للاحتيال على مال الغير اعتماد على تقنية الشبكة المعلوماتية في البيانات والمعلومات الالكترونية.

الكلمات المفتاحية: الرقمنة- الاحتيال- الجرائم المعلوماتية- الأمن المعلوماتي.

Abstract :

The spread of cybercrime has been linked to the existence of the Internet, which has produced a new type of crime that differs from conventional crimes. The widespread use of the Internet has contributed to the spread of the Internet and the emergence of an information society in which the electronic devices dominate the minds of its users, especially with sufficient knowledge of the various technologies and stored data. Easily and rapidly spread between countries and continents, and the crime of electronic fraud is one of the most important electronic crimes, which rely on the method of deception and fraud to deceive the money of others to rely on the technology of the information network in the data and Electronic Information.

مقدمة:

أصبحت المعلومات في بيئة المجتمعات الحديثة ترتبط بمختلف جوانب الحياة ، وتمثل ركيزة نشاط الإنسان الإقتصادي والإجتماعي والسياسي، وتتيح المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، ويعود ذلك الى تطور التقنية وتهيئة البيئة العالمية المناسبة في تكنولوجيا المعلومات والإتصالات، وإنتقال كافة التغيرات من مكان لآخر دون مواجهة أية حواجز جغرافية[1].

ومع التوسع الهائل في إستخدام شبكات المعلومات إزدادت المخاطر التي تتعرض لها، وجدت الجريمة الإلكترونية التي أخذت أنماط جديدة من السلوكيات والأفعال الخارجة على القانون، وهي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني)، إذ هي ظاهرة إجتماعية تتوافق مع إنتقال نشاط الناس من الواقع المادي الى الواقع الافتراضي [2]، ولأن شبكة العنكبوتية والمنتديات وغرف الدردشة تكتنفها صفة المجهولية في تواصل مستخدميها، حيث يجدون

فيها الوسيلة المفتوحة للتعبير بحرية أكثر عما يدور بداخلهم، وتمكنهم أيضا من التمرد على الواقع الذي يعيش فيه الشباب في ظل مطالبتهم بالحرية المطلقة، مما يفتح شهية الجاني والفريسة في ممارسة ما تمنعه الضوابط العرفية الداخلية والدينية، وبموجب ذلك أصبحت الانترنت أداة ووسيلة لتنفيذ العمل الجرمي بكل سهولة من قبل المنحرفين لتحقيق اغراضهم المعادية للفرد والمجتمع [3]، خاصة وأن الحصول على المعلومات بالطريقة الإلكترونية لا يكلف الكثير من المال والجهد مما يجعل التعدي عليها إستنادا الى أساليب مختلفة كالتخريب والتجسس والإحتيال عملية سهلة، ومما يزيد الأمور تعقيدا أن التعدي على المعلومات وإستغلالها ضد الطرف الآخر تتم في خفاء ويصعب كشف الفاعل مما يشجع على إستمراريةإرتكابها بكل سهولة[4].

والإحتيال إحدى السلوكات المجرمة بجميع القوانين تختلف صوره بإختلاف الثقافات الى جانب تطور تقنية الإتصالات التي أضافت أنواع حديثة للجريمة أكثر عددا وأخطر كيفا مما عليه الجرائم بصورتها التقليدية، والإحتيال الإلكتروني أحدى أهم الجرائم المستحدثة بموجب وجود شبكة الأنترنت التي تسمح بالسرقة والإعتداء على هوية المستخدمين، وهذا ما نحاول توضيحه في الورقة البحثية التي نتناولها من خلال طرح الإشكالية التي تتمثل في: **ماذا نعني بجريمة الإحتيال الإلكتروني؟**

وهي الإشكالية التي ستحاول الإجابة عليها من خلال النقاط التالية:

أولا- الاطار المفاهيمي لجريمة الاختيال الالكتروني:

يتطلب تحديد مفهوم جريمة الإحتيال الالكتروني، الإشارة الى الاحتيال في اطاره العام، وفقا لمختلف التعاريف التي تضمنته كما سنوضحه في النقاط التالية:

1-تعريف الإحتيال الإلكتروني:

أ - **لغة:** الإحتيال هو الحذق، وجودة النظر، والقدرة على دقة التصرف[5]، والاحتيال والمحاولة: مطالبتك الشيء بالحيل، والحيلة هي المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف ما يقتضيه ظاهره[6].

ب - **إصطلاحا:** اختلف الفقهاء في الوصول الى تعريف محدد لجريمة الاحتيال لاختلافهم في الزاوية التي ينظر إليها منه، ومن تعريفاته الإصطلاحية نتناول على سبيل المثال:

-جريمة الاحتيال هي الاستلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال، وعرفها آخر بانها استعمال وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكا لغيره نتيجة الوقوع في الغلط[7]

وإختلفت القوانين في تسمية هذه الجريمة، كما هو الحال بالنسبة للقانون الفرنسي الذي تناول لأول مرة عبارة طرق إحتيالية، وإعتبر الإحتيال جريمة قائمة بذاتها في نص المادة (405)، التي نصت على انه "كل من يتوصل الى أن يسلب، أو يشرع في سلب مال أو بعض ثروة الغير"، وأضاف ظرفا مشددا لجريمة الإحتيال أو الشروع فيها، يتحقق عندما ترتكب إما بانتحال صفة ضابط في الشرطة القضائية، أو مأمور الضبط في دائرة الدولة المدنية، أو في الجيش الفرنسي الأجنبي[8].

أما المشرع الجزائري تناول جريمة الإحتيال في قانون العقوبات، ونص في المادة (372)، على أنها "كل من توصل إلى إستلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء

من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار."،

كما ربط المشرع الجزائري مفهوم هذه الجريمة بإنتحال الوظائف والألقاب أو الأسماء وإساءة إستعمالها وإعتبرت من قبيل جريمة إحتيال، لأن الإحتيال لا يكون الغرض منه العائد المالي فقط، بل قد يعود الى إعتبارات أخرى كالانتقام، ويأخذ أشكالا متعددة مثل ما أشارت اليه المواد (243 الى 246) من قانون العقوبات الجزائري:

-التدخل في غير صفة في الوظائف العمومية والمدنية والعسكرية، او القيام بعمل من اعمال هذه الوظائف.

-إستعمال شخص لقبا متصلا بمهنة منظمة قانونا أو شهادة رسمية أو صفة حددت السلطة العمومية شروط منحها أو إدعى لنفسه شيئا من ذلك بغير أن يستوفي الشروط المفروضة لحملها.

-من انتحل لنفسه بصورة عادية أو في عمل رسمي لقبا أو رتبة شرفية.

كما تناول المشرع العقابي المصري جريمة الاحتيال في المادة (336) من قانون العقوبات، حيث نصت على أن "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمى أو تسديد المبلغ الذى أخذ بطريق الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور ، وإما بالتصرف في مال ثابت أو منقول ليس مملوكا له ولا له حق التصرف فيه ، وإما باتخاذ اسم كاذب أو صفة غير صحيحة، معنى ذلك أن الإحتيال ينال بالإعتداء على حق مليكة المال العام المنقول والإستلاء على مال منقول مملوك للغير.

وجريمة الإحتيال الإلكتروني تحمل نفس المفهوم الذي تناولناه في النقاط السابقة، إلا أن الفارق الوحيد في الوسيلة التي يتم بموجبها تنفيذ هذه الجريمة، وتتمثل هذه الوسيلة في إعتمادها على وجود الحاسب الآلي وتوافر الشبكة العنكبوتية التي تعد جوهر جريمة الإحتيال الالكتروني، اذ وبدونها لا يكون هناك وجود للإحتيال الكتروني، وارتبط تعريفها بالمفهوم العام للجريمة الالكترونية التي يدخل الاحتيال في إحدى اساليبها، من تعريفاتها:

-هي الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي، وهذا ما ادى الى اطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[9].

-هي كل نشاط اجرامي تستخدم فيه التقنية الالكترونية – الحاسوب الالي الرقمي وشبكة الانترنت- بطريقة مباشرة او غير مباشرة كوسيلة لتنفيذ الفعل الاجرامي[10].

-الاحتيال المعلوماتي هو اي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي، وهو التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الالي، او الادخال غير المصرح به لمعلومات وبيانات صحيحة، او التلاعب في الاوامر والتعليمات التي تحكم عملية البرمجة، او اي وسيلة اخرى من

شأنها التأثير على الحاسب الالي حتى يقوم بعملياته بناء على هذه البيانات والاوامر او التعليمات، من اجل الحصول على ربح غير مشروع والحاق الضرر بالغير[11].

ومن خلال مجمل التعاريف فإن الإحتيال الإلكتروني يعتبر إحدى الطرق الحديثة المتطورة التي يتم اللجوء اليها للوصول وإختراق أهداف معينة بطرق غير مشروعة، إستنادا الى وجود شبكة الأنترنت دون النظر الى الأضرار المعنوية او المادية التي تترتب على التعدي على أجهزة وخصوصيات الآخرين، ويكون الفاعل في هذا النوع من الجرائم شخصا ذو مهارات تقنية عالية قادرا على إستخدام خبراته في إختراق البيانات السرية بغية الحصول على معلومات وإتصالات مجانية.

2-أساليب الإحتيال الإلكتروني:

هناك العديد من الدوافع التي والأسباب التي تؤدي الى إرتكابالإحتيال، من أهمها:

أ-إنتحال الشخصية:

تتطلب عملية الإحتيال الإلكتروني ذكاء وقدرة برمجية عالية تدفع العديد من الهواة الى تجريب قدرتهم وإثبات مهاراتهم البرمجية من خلال القيام بعمليات الإختراق لمواقع معينة سواء كانت شخصية أو عامة، واللجوء الى الخداع في تمويه وطمس الهوية من أجل سرقة حساب أو بريد إلكتروني والدخول باسم المستخدم وانتحال شخصيته للحصول على معلومات اختيارية من الضحية[12].

وانتحال الشخصية من الأساليب الأكثر شيوعا يقوم فيها المجرم المعلوماتي بإنتحال ضفة شخصيات معروفة وأكثر شيوعا من أجل الحصول على البيانات والمعلومات التي يحتاجها في الإحتيال، وهذا النوع من الإحتيال الشخصي يهدف الى الإستفادة من الإساءة الى سمعة الضحية أو الحصول على عوائد مالية .

ب-الاعتداء على المعطيات:

يعتمد في ذلك على تقنية الاختراق كذلك أو ما يعرف ب(haking)، بغرض الدخول على المعطيات السرية و المحمية أو الخصوصية الشخصية وعلى البيانات التي لها صفة بالحياة الفردية، من خلال إستخدام الانترنت والغرض من ذلك التزوير أو الاختلاس او تحقيق غايات شائنة، ما يجعل هذه الاعتداءات حديث المجالس والاجتماعات والرسائل الاعلامية والاجهزة الامنية ، لأنها تزعجهم وتفزعهم وتسلب خصوصياتهم الامر الذي يجعلهم متيقضين ومنتبهين على ما يجري حولهم، من اجل حماية انفسهم ضد اية خدع او انزلاقات، وهذا ما يدفع الافراد الى بذل المزيد من الحذر والحيطة والاحتفاظ بهويتهم الشخصية وخصوصيتهم الفردية [13]، ويترتب على هذا الاعتداء للحياة الشخصية أضرار منها[14]:

-التجسس على الحياة الخاصة: نعني به الاطلاع على حياة الاشخاص وخصوصياتهم من دون علمهم بذلك ودون اذنهم، وهي من الآفات السيئة من الناحية الاجتماعية والاخلاقية، ولا يختلف التجسس عن الإختراق الا من حيث الهدف، لأن الأساليب المتبعة هي ذاتها يراد من خلاله تمكين المتجسس من التعرف على محتويات الحاسوب المستهدف أول بأول دون الإضرار به، وغالبا ما تتم عمليات التجسس بإستخدام نوع من الفيروسات التي تنقل الى الحواسب وتعمل على إرسال نسخ من البيانات والمعلومات الى حاسوب آخر، أو تمكينه من التجسس الرقمي[15].

والمحتال في هذا المقام الذي يستخدم الانترنت لا يحصل على وصمة اجرامية من قبل افراد مجتمعه، لانه يتعامل مع السرقة والاحتيال في اجواء يطغى عليها المجهولية وعن بعد، وهذه احدى السمات التي تتسم بها جرائم الانترنت نقيض الانواع الاخرى من الجرائم التي يحصل فيها الجاني على صفة المجرم سواء كان هذا في الاجهزة الامنية او المجتمع المحلي.

-النصب في مجال الخدمات الالكترونية: يعتبر النصب وسرقة المال المعلوماتي في مجال المنتجات والخدمات التجارية التي تقدمها الشبكة العنكبوتية بوسائل غير مسبوقة احدى اهم الاساليب التي يعتمد عليها الجاني في احتياله على الاشخاص أو الشركات والمؤسسات، كاستخدام البريد الالكتروني او عرضها على مواقع على الشبكة واستخدام هذه الوسائل في عمليات النصب والإحتيال [16]، ويعتمد المحتالين عبر الانترنت خداع ضحاياهم على:[17]

-التعدي على البيانات: يقوم التعدي بالإطلاع عليها واستخدامها بطرق غير قانونية بعيدا عن تناول يد غير المصرح لهم والمسموح لهم بالإطلاع عليها، ويكون ذلك بالنسخ غير القانوني للبيانات وقرصنة برمجيات الحاسب، كما تقوم هذه العملية بناء على طلب الشخص المحتال من الضحية عبر الانترنت بحدوث خلل في البيانات في الحساب البنكي مثلا، يستلزم ذلك بسرعة اعادة ادخال بيانات جديدة من اسم الضحية وتاريخ ميلاده العنوان ورقم الحساب حتى تتم معاملاته البنكية.

-التزوير المعلوماتي: تتم عملية التزوير هي الأخرى بالدخول الى قاعدة البيانات وتعديل ما هو موجود فيها أو لإضافة معلومات مغلوطة بهدف الإستفادة غير المشروعة من ذلك [18]، وهو يعتبر من الطرق الفعالة التي يلجأ اليها المحتالين في تحقيق اغراضهم الإجرامية.

3-خصائص جريمة الإحتيال الإلكتروني:

يقوم الإحتيال الالكتروني على مجموعة من الخصائص تمثل خصائص الجريمة الالكترونية، وهي:

أ-الاحتيال الالكتروني من الجرائم العابرة للحدود:

يعني ذلك انها تمثل شكلا من اشكال الجرائم العابرة للحدود الاقليمية بين دول العالم كله، مع وجود اجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير ان تخضع لحدود الزمان والمكان، لذلك كان من السهولة ارتكاب الاحتيال مع عدم القدرة على كشفه، وهذه الخاصية خلقت العديد من المشاكل حول تحديد الدولة التي تكون صاحبة الاختصاص القضائي في حالة ما اذا كان المجرم من دولة والضحية من دولة اخرى، وكذا الاشكالية في القانون الواجب التطبيق واجراءات الملاحقة القضائية،

وبالنظر الى الطبيعة الخاصة لهذه الجريمة وخطورتها على المستوى الدولي، كان من الضروري التعاون الدولي في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الاعضاء من اجل التكفل بالإيقاع بالمجرم المعلوماتي ومحاكمته[19].

ب-الاحتيال الالكتروني من الجرائم التي يصعب اكتشافها:

تقع جريمة الاحتيال الالكتروني في بيئة افتراضية لا تترك اية آثار على مرتكبها، لأن الضحية لا يلاحظها رغم انها تقع اثناء وجوده على الشبكة، وهذا بفضل القدرات الفنية والتقنية التي يتمتع بها الجاني والتي تمكنه من جريمته بدقة[20].

ث-الاحتيال الالكتروني من الجرائم التي لا تقوم على العنف:

يعتمد ارتكاب هذا النوع من الجريمة على اسلوب لا يحتاج فيه الى مجهود عضلي كجرائم القتل والسرقة التقليدية، فهي تنفذ باقل جهد ولا تتطلب نوعا من الايذاء او الاختطاف او التكسير، بل تعتمد فقط المعرفة الواسعة بتقنية المعلوماتية وشبكة الانترنت والاحاطة ببعض البرامج التشغيلية، لذلك يطلق على هذا النوع من الجرائم بالجرائم الناعمة[21].

د-خصوصية المجرم المعلوماتي:

يطلق على المجرم الذي يرتكب هذا النوع من الجرائم بالمجرم المعلوماتي، ويتسم بخصائص معينة تميزه عن المجرم التقليدي، لأن جريمة الاحتيال الالكتروني من الجرائم التقنية التي يرتكبها ذوي الاختصاص في مجال المعلومات الالكترونية، او على الاقل الاشخاص الذين يكون لديهم حد ادنى من الدراية الكافية بالاستخدام والمعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت[22].

وعليه يمكن القول بان جريمة الاحتيال الالكتروني هي الجريمة التي تقوم على وجود عنصرين اساسيين، هما جهاز الكمبيوتر وشبكة الانترنت، والمجرم المعلوماتي فيها يقوم بالاحتيال على كل ما يعتبر حق للغير وليس له علاقة به، سواء كان ذلك مالا او معلومات او بيانات او اشياء خصوصية، عن طريق خداع المجني عليه والحاق الضرر به.

ثانيا- الحماية من الإحتيال الالكتروني:

بما أن الإحتيال الإلكتروني أحدى الجرائم المستحدثة التي أفرزتها التكنولوجيا المعاصرة، فإن الحماية من هذه الجريمة تكون هي الأخرى بإستخدام التقنيات التكنولوجية الحديثة، وتوفير الأمن المعلوماتي يعتبر وسيلة فعالة في التصدي له، لأنه يبحث في استراتيجيات توفير الحماية للمعلومة الإلكترونية من المخاطر التي تهددها ومن انشطة الإعتداء عليها، بالإعتماد على الوسائل والدوات والإجراءات اللازم توفيرها لضمان الحماية الداخلية والخارجية للمعلومات، ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى[23]

1-أساليب الأمن المعلوماتي:

يمكن تجنب العديد من الإعتداءات التي تتعرض لها البيانات والمعلومات المدونة إلكترونيا، والتحكم في الدخول اليها إلا لمن له الحق بذلك، وفقا لمجموعة من الآليات الدفاعية التي تمنع حدوث الإحتيالوالإختراق للمواقع والبيانات، من خلال [24].

أ-التحكم بالدخول للأصول المعلوماتية:

يكون هذا الإجراء عن طريق جهاز رقابة إيجابي يقوم بتحديد عما إذا كان الشخص طالب الدخول مصرحا له بذلك أم لا والعمل بموجب ذلك، كما يقوم هذا الجهاز الإيجابي بالتحري عن شخصية المتصل بربط عملية تصريح الدخول والتحري عن الشخصية، فتكون سرية المعلومات مضمونةوغير متاحة للكافة للإطلاع عليها او لإحتيالها بغير وجه حق.

ويدخل في إطار هذا العنصر، سياسات السماح بالدخول التي تساعد عملية التحكم بالدخول في فرض النشطة والأشخاص المسموح لهم بالدخول، وهذه السياسات تحكم العمال التي يسمح أن يقوم بها البشر فيما يخص الصول المعلوماتية، والبرامج التي تدخل على الأصول المعلوماتية وتستخدمها، وتطبق على أي وسط معلوماتي، البيئة المعلوماتية، المطبوعات، الأقراص، الأشرطة والإتصالات من نقطة الى أخرى، وكذلك وجود رقيب يتولى التحكم في الدخول شخصيا أو جهاز دخول ذا تحكم آلي او برنامجي يستخدم السمات البيولوجية كبصمة الإصبع والبصمة الصوتية. [25]

ب-ترشيح المعلومات:

يتثمل ترشيح المعلومات في وجود برنامج أو جهاز يقوم بمراقبة المعلومات الداخلية والخارجية من شبكة الحاسب الآلي، ينبني هذا القرار على المعلومات في مقدمة الرسالة المرسلة التي تشمل عناصر أساسية خاصة بالمرسل كالعنوان، ونوع الخدمة بالأترنت بريد إلكتروني ، ويب وغيرها، وتتجسد هذه المرشحات في كل من جدار الحماية الأمنية الذي هو عبارة عن مراقب بين الشبكة الداخلية للمنظمة وشبكة الأنترنت، أو بين شبكتين محليتين، يهدف الى منع دخول المتطفلين والبرمجيات القائمة على الإحتيال، مرشحات البريد غير المرغوب فيه(بريد القمامة)، تستخدم هذه البرامج عدة إستراتيجيات لتحديد أي الرسائل التي يتم التخلص منها، بقراءة خانة المرسل فإذا تبين من احد العناوين ضمن قائمة عناوين محددة لمن يقومون بهذه الأعمال يتم إزالة الرسالة ومسحها، اما مرشحات الشبكة فتستخدم لمنع إنزال مواد غير مرغوب فيها من الشبكة أثناء التصفح، وتعتبر بديلا عن التشريعات القانونية لحماية الأطفال خاصة من أخطار الأنترنت.

ج-إكتشاف التطفل وسوء الإستخدام:

يهدف إكتاف التطفل الى إكتشاف النشاط الضار في بدايته ويتحقق ذلك عن طريق مراقبة النشطة الحالية او مراجعة القوائم التي يتم تسجيل هذه النشطة فيها، وإن تم الإكتشاف في وقت مبكر يمكن إجهاض محاولة الإعتداء قبل حدوث الضرر، وحتى في حالة عدم التمكن من ايقاف النشاط فالعلم به في حد ذاته ينبئ مسؤولي الأمن الى الثغرات الأمنية لتلافيها.

2-وسائل تحقيق الأمن المعلوماتي:

حتى يكون للأمن المعلوماتي دور إيجابي في الحد من الجرائم التي ترتكب عبر الأنترنت، بما فيها الإحتيال الإلكتروني، يجب على كل الحكومات والمنظمات المعنية التأكيد على أهمية الأخذ بأمن المعلومات والتوجيهات المنظمة له إضافة الى ضرورة التنسيق والتعاون على تنفيذه على كافة المستويات وبالتالي تطوير وسائلأمن المعلومات التي تتمثل في[26]:

-إعداد معايير أمن عالمية تكون منسجمة ومتوافقة مع التطبيق الجغرافي المتسع والممتد على اوسع نطاق على العالم ، حيث يمثل تطوير توجهات ومعايير الأمن المنتج التعاوني بين الحكومات والمنظمات والمنتجين والموردين والمستخدمين لنظم المعلومات،

-ترويج الخبرة والمزاولة الأحسن لكل الأطراف المعنية بأمن نظم المعلومات على كافة مستوياتها، وتنويعها بترويج خبراتها وممارسة الأفضل في إعداد وتنفيذ سياسات أمن المعلومات الخاصة بها، ما اجل تعزيز ترقية الخبرة والوعي بمفاهيم الممارسة وتأمين النظم ومراجعتها.

-إبرام العقود الصحيحة بين الأطراف المختلفة المرتبطة بالمعاملات والتصرفات الإلكترونية، والمشاركين في نقل المعلومات سواء كانت الكترونية أو ورقية يردون من ذلك معرفة والتأكد من ان المعلومات المرسلة هي المرغوبة وترد من مصادر معتمدة وموثوق منها، كما انها تصل أهاف أطراف المعاملات الإلكترونية والورقية متشابهة الى حد كبير، فقط يكمن الفارق في طرق إنشاءها وإستخدامها وتخزينها.

-تخصيص المخاطر وتحديد المسؤولية القانونية استنادا الى قواعد ذات فعالية وكفاءة ترتبط بها كل الأطراف المتضمنة إجراءات الأمن كالباعين، مشتغلي الإتصالات، مقدمي الخدمات، المستخدمين وغيرهم، كما تتضمن نظما عديدة تستخدم في نقل المعلومات التي تكون خارج سيطرة او مراقبة معالج المعلومات المختص، وتتضح الحاجة لتواجد قواعد امن المعلومات المرتبطة بتخصيص المخاطر والمسؤولية القانونية عند السرقة والإحتيال وفقدان اعتمادات الإلكترونية .

-وجود العقوبات والجزاءات التي تعتبر وسائل مهمة في استخدام نظم المعلومات، لحماية الأطراف المعتمدة على هذه النظم، وتوافر بياناتها وسريتها في مواجهة أي هجمات تعرضها للضرر والإفشاء او الإحتيا بطرقه المختلفة.

ومن التشريعات التي حاولت تفعيل الأمن المعلوماتي في نصوصها القانونية لمواجهة الجريمة التي ترتكب عبر الأنترنت سواء كانت إحتيال أو قرصنة او تجسس، نجد المشرع الجزائري الذي عمد الى تعديل العديد من القوانين الوطنية لتتواكب مع التطورات الاجرامية في مجال تكنولوجيا الاعلام والاتصال، مثل القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والذي تم فيه تحديد الحالات التي تسمح باللجوء الى مراقبة الاتصالات الالكترونية بناء على ما ورد في المادة (04)، وتناول قانون العقوبات في الباب السابع منه عنوان المساس بأنظمة المعالجة الالية للمعطيات سعيا منه لضمان الحماية الجنائية للمعاملات الالكترونية، وتم انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلال المرسوم الرئاسي رقم 15-261.

ووضع المشرع الجزائري بموجب القانون قم 09-04، ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، سعيا منه للحفاظ على النظام العام ومستلزمات التحريات وحماية الأمن المعلوماتي من خلال:

-تحديد حالات مراقبة الاتصالات الالكترونية: تكون رقابة الإتصالات الإلكترونية في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وتوفر معلومات عن إحتمالإعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني، وجود

مقتضبات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية و تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، استنادا الى اذن مكتوب من السلطة القضائية المختصة.

-تفتيش المنظومات المعلوماتية: سمح المشرع للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد الى منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، منظومة تخزين معلوماتية وان وجدت اسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى وان هذه المعطيات يمكن الدخول اليها.

فجريمة الاحتيال الالكتروني تعد من الجرائم الناشئة مع نشأة وتطور استخدام الحاسوب، والشبكة العنكبوتية التي تسهل على الجاني الاستلاء والاعتداء على معلومات او برامج او معطيات تخص افرادا آخرين عن طريق خداعهم بأساليب تقنية متطورة لا يستطيع المجني عليهم اكتشافها، وهذه الجريمة تعتبر احدى الجرائم الالكترونية المتعددة التي ترتكز في تنفيذها على وجود الشبكة العنكبوتية .

خاتمة:

بيننا من خلال الدراسة التي تناولناها إحدى الجرائم الالكترونية الحديثة التي تعرف إنتشارا كبيرا مع زيادة إنتشار شبكة الانترنت، والتي اصبحت تمثل هاجسا يؤرق الكثير من الدول بسبب الاستخدام الغير مشروع لها، وعدم القدرة على إكتشاف مرتكبها الذي يعرف بالمجرم المعلوماتي في الكثير من هذه الجرائم، ورغم المحاولات العديدة التي تبذلها الدول في مجال تحقيق الأمن السيبراني كمصطلح جديد يتعلق بجرائم تكنولوجيات الاعلام والاتصال ومكافحتها، عن طريق توعية الأفراد وتحسيسهم بأهمية اليقظة في التحكم في التكنولوجيات الحديثة، ومحاولاتهم في تحقيق نوع من التوازن بين الوسائل التقنية المختلفة كعملية التشفير واستخدام برامج متخصصة ضد القرصنة لإستغلالها في التقليل من جرائم الاحتيال، وكل الإختراقات التي تعرفها أنظمة المعالجة المعلوماتية، إلا أنه لا تزال هناك الكثير من العقبات التي تعيق التصدي لهذا النوع من الجرائم بصورة كاملة، ومن التوصيات التي نقترحها إنطلاقا من هذه الدراسة:

-تفعيل وسائل الحماية من الجريمة الالكترونية في النصوص القانونية حتى تكون لها المرجع او الاساس الذي تنطلق منه الجهود المبذولة للتصدي لهذه الجرائم.

-تطوير التعاون بين مختلف الدول في شكل اتفاقيات ثنائية او جماعية، من اجل اعطاء اهتمام اكبر ومشترك للحوار ومبادلة الآراء حول الجريمة الالكترونية.

-إستحداث نصوص قانونية جديدة تكون اكثر صرامة وفاعليه مقارنة بالنصوص التقليدية، من خلال التشديد في العقوبات المقررة لمرتكبي جرائم الاحتيال الالكتروني وغيرها من الجرائم التكنولوجيا الحديثة.

-الاستعانة بأصحاب الخبرة في المجال التكنولوجي من طرف المشرع، للتعاون في كيفية التعامل مع هذا النوع من الاجرام على اعتبار ان القضاة او اعضاء الضبط القضائي ليست لهم الدراية الكافية بالأساليب التقنية لهذا النوع من الجرائم .

- انشاء محكمة خاصة بالجرائم المعلوماتية، يتولى تسييرها سلك قضائي خاضع لخبرة وتدريب فعال في مجال مكافحة الجرائم المعلوماتية والاستعانة بخبراء امن المعلومات.

قائمة الهوامش:

[1]-هيثم حمود الشلبي، إدارة مخاطر الإحتيال في قطاع الإتصالات، دار صفاء للنشر والتوزيع، طبعة 1، عمان، الأردن، 2009، ص، 28.

[2]- ذياب البداينية، الجرائم الإلكترونية، المفهوم والاسباب". الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية. الاردن. 2014، ص،3.

[3]- معن خليل العمر، الجرائم المستحدثة، دار وائل للنشر والتوزيع، عمان، الأردن، 2012، ص، 204.

[4]- ذياب البداينة، الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، طبعة 1، عمان، الأردن، 2006، ص، 17.

[5]- هيثم حمود الشلبي، مرجع سابق، ص، 22.

[6]- عبيد علي، ناصر موفق وآخرون، ماهية جريمة الإحتيال الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق، جامعة تكريت، بغداد موقع: www.iasj.net/iasj?func=fulltext&aId=124926، ص، 336.

[7]- المرجع نفسه، ص، 338.

[8]- طاهر جليل الحبوش، جرائم الاحتيال الاساليب والوقاية والمكافحة ". اكاديمية نايف العربية للعلوم الامنية، مركز الدراسات والبحوث، الرياض، 2001، ص، 8.

[9]- محمد عبيد الكعيبي، الجرائمالناشئةعنالاستخدامغيرالمشروعلشبكةالانترنت،دارالنهضةالعربية، القاهرة، 2009، ص، 32.

[10]- عبد المومن بن الصغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن". الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة. كلية الحقوق والعلوم السياسية. جامعة محمد خيضر. بسكرة، 2015،ص، 5.

[11]- عبيد علي، ناصر موفق وآخرون ، مرجع سابق، ص، 340.

[12]- هيثم حمود الشلبي، مرجع سابق ، ص، 197.

[13]- معن خليل العمر، مرجع سابق، ص، 225.

[14]- شريفي الشريف، " مدى احترام حق الخصوصية في الحسابات الالكترونية على الانترنت". الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة. كلية الحقوق والعلوم السياسية. جامعة محمد خيضر. بسكرة ، 2015، ص، 6

[15]- هيثم حمود الشلبي، مرجع سابق ، ص، 169.

[16]- معن خليل العمر، مرجع سابق، ص، 241.

[17]- ، ذياب البداينة، الأمن وحرب المعلومات ، مرجع سابق، ص، 227.

[18]- هيثم حمود الشلبي، مرجع سابق ، ص، 189.

[19]- عبيد علي، ناصر موفق وآخرون ، مرجع سابق، ص، 340.

[20]- عبد المومن بن الصغير، مرجع سابق، ص، 350.

[21]- عبيد علي، ناصر موفق وآخرون ، مرجع سابق ، ص، 349.

[22]- المرجع نفسه، ص، 351.

[23]- هيثم حمود الشلبي، مرجع سابق، ص، 211.

[24]- ذياب البداينة، مرجع سابق، ص، 381.

[25]- المرجع نفسه، ص، 384.

[26]- هيثم حمود الشلبي، مرجع سابق، ص، 258.