مجلة الصدى للدراسات القانونية والسياسية
المجلد 4 ، العدد 3
السنة 2022 ، ص23-ص46

دور الإدارة العراقية في مكافحة الجرائم المعلوماتية المخلة بالأمن العام

The role of the Iraqi administration in combating cybercrime against public security

م. سيف علاء حسين العبيدي[1] م. عمر عباس خضير العبيدي[2]
(1) وزارة التعليم العالي والبحث العلمي (العراق)
Saif.alaa1988@gmail.com
(2) وزارة التربية (العراق)
omarabbas93.aa@gmail.com

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر:
2022/07/10	2022/08/31	2022/09/27

الملخص:

في العقود الأخيرة برزت ثورة من نوع آخر متعلقة بوسائل الاتصال والمعلومات، نتيجة التطور الذي تجسد أساسا في انتشار أجهزة الحاسب الآلي والتي تطورت بشكل مستمر، بالإضافة إلى البرامج المتقدمة، وشبكات الاتصال التي قربت ملايين البشر بعضهم البعض، وأتاحت فرصا جديدة للاطلاع على المعلومات وتبادلها، وحتى التفاوض وإبرام عقود مختلفة خصوصا عبر شبكة الأنترنت، بل الأكثر من ذلك يمكن عبر هذه الأخيرة تسليم المنتجات كالبرامج، أو القطع الموسيقية، أو الصحف الالكترونية، أو تقديم الخدمات، مثل الاستشارات القانونية أو الطبية.

لكن ما دامت الجريمة ظاهرة اجتماعية، تتأثر طبيعتها وحجمها بالتحولات الاقتصادية والاجتماعية والثقافية دولياً ووطنياً، فقد ظهر للوجود نمط جديد من الإجرام، تجسد في انتشار الجرائم المعلوماتية أو الإلكترونية، والتي تعتبر من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكون هذه الجرائم تشمل في اعتداءاتها قيما جوهرية تخص الأفراد والمؤسسات، وليس على مستوى العراق فحسب بل وحتى الدول في كافة نواحي الحياة، كما أن هذه الجرائم تركت في النفوس شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار هذه الثورة الجديدة.

الكلمات المفتاحية: الجرائم، المعلوماتية، الإدارة العراقية، الأمن العام، الضبط الإداري،

Abstract:

1. المؤلف المرسل: م. سيف علاء حسين العبيدي Saif.alaa1988@gmail.com

In the last decades, a revolution of another kind related to the means of communication and information has emerged, as a result of the development that was mainly embodied in the proliferation of computers and which have developed continuously, in addition to advanced programs and communication networks that brought millions of people together, and provided new opportunities to view and exchange information, Even negotiating and concluding various contracts, especially via the Internet, but more than that, it is possible through the latter to deliver products such as programs, musical pieces, electronic newspapers, or provide services, such as legal or medical consultations.

But as long as crime is a social phenomenon, the nature and size of which are affected by economic, social and cultural transformations internationally and nationally, a new pattern of crime has emerged, embodied in the spread of information or electronic crimes, which is considered one of the biggest negatives of the information revolution, because these crimes include valuable Substantial concerns individuals and institutions, not only at the level of Iraq, but even countries in all aspects of life, and these crimes have left a feeling of mistrust regarding dealing and benefiting from the fruits of this new revolution.

Keywords: crimes, informatics, the Iraqi administration, public security, administrative control.

مقدمة:

إن ظاهرة جرائم الكمبيوتر والإنترنت، أو جرائم التقنية العالية، أو الجريمة المعلوماتية، ظاهرة إجرامية مستجدة نسبيا تقرع في جنباتها أجراس الخطر، لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها). فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية،

وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت.

أهمية البحث:

تتجلى أهمية هذه الدراسة في إلقاء الضوء على الدور الذي يجب أنْ تضطلع به الدول والجماعات والأفراد للتصدي لظاهرةِ الجرائم المعلوماتية والوقاية منها، كما يستمد هذا الموضوع أهميته إدراكاً من الواقع بأنَّ ظاهرة الجرائم المستحدثة قد غدتْ تشكلُ تحدياً حقيقياً للسياسات الجنائية السائدة في الدول وأجهزتها التشريعية والتنفيذية والقضائية، وكذلك الهدف من دراسة الموضوع هو إيجاد تعريف عام موحد للجرائم المعلوماتية.

إشكالية البحث:

تتلخص إشكالية البحث:

1- بعدم وجود تعريف متفق عليه للجرائم المعلوماتية، وهو يمثل قصوراً على المستوى الدولي والوطني فيما يتعلق في تعريف الجرائم المعلوماتية من أجل تحديد معياراً للجرائم المعلوماتية؟

2- وكذلك وجود قصور على المستوى التشريعي في معالجة هذه الجرائم مما ولد فجوة قانونية بين الحداثة في إعتماد الوسائل وقدم التشريعات النافذة التي تعالج هذه الجرائم.

منهجية البحث:

بالنظر للخصوصية التي يتميزُ بها موضوع الجرائم المعلوماتية والإهتمام الذي يحظى به من قبل الدول، حيث ستعتمدُ الدراسة في معالجتها لهذا الموضوع على المنهج التحليلي والإستقرائي والمقارن.

أهداف البحث:

1- التعرف على الجرائم المعلوماتية وصورها وآثارها على المجتمع.
2- معرفة التشريعات والقوانين المقارنة التي عالجت الموضوع ومعرفة البنود الموجودة لدينا مع دول مقارنة.
3- الاستفادة من تجارب الدول المتقدمة عربياً في هذا الميدان من أجل تحقيق الضبط الإداري المعلوماتي والحماية المجتمعية.

خطة البحث:

لبيان موضوع دور الإدارة العراقية في مكافحة الجرائم المعلوماتية المخلة بالأمن العام، وتقديم الحلول لمعالجة إشكاليات هذا الموضوع، سنقسمُ هذا الموضوع على مبحثين، وهما ما يأتي:

المبحث الأول: تعريف الجرائم المعلوماتية وصورها

المبحث الثاني: الآليات القانونية في مكافحة الجرائم المعلوماتية في العراق

المبحث الأول

تعريف الجرائم المعلوماتية وصورها

تعد الجرائم المعلوماتية صنفاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب التي تقتضي ضرورة تحقق أركان الجريمة طبقاً لمبدأ شرعية الجرائم والعقوبات. إذ يعد الأمن حاجة أساسية للمجتمع الإنساني، ومؤشراً على الاستقرار والازدهار والتقدم في الوطن، ويرى بعض الفقه أن الأمن الاجتماعي يعنى ببساطة سلامة الأفراد والجماعات من الأخطار الداخلية والخارجية، متمثلة في التهديدات الإلكترونية داخل المجتمع من قبل أفراد أو جماعات تمارس الابتزاز والسرقات مما يعد مؤشراً خطيراً لافتقاد الأمن الاجتماعي. وبقدر حاجة المجتمع للأمن الاجتماعي تكون حاجته لمقوماته وركائزه

الأساسية التي تسهم في توفير الأمن، وبناء المجتمعات الحديثة وعاملاً مهماً في تقدم الأمم ورقيها.

وعليه ومما تقدم سنتناول دراسة هذا المبحث على مطلبين، وهما ما يأتي:

المطلب الأول: تعريف الجرائم المعلوماتية

المطلب الثاني: صور الجرائم المعلوماتية

المطلب الأول: تعريف الجرائم المعلوماتية

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيراً، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة من جهة، ويكون وسيلة لارتكابها من جهة أخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان :"كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[1].

للجريمة المعلوماتية مسميات كثيرة، فالبعض يطلق عليها اسم جرائم الحاسب الآلي[2]. والبعض الأخر الجرائم المستحدثة، أو جرائم الكمبيوتر، أو الجرائم الإلكترونية [3].

ونظراً لاختلاف وتعدد التسميات التي تطلق على هذا النوع من الإجرام، ونظراً لحداثته والذي ولد نتيجة التطور العالمي والتكنلوجي الهائل والمتسارع الذي تشهده البشرية[4].

بالإضافة إلى الطبيعة الخاصة التي تتميز بها، فقد تنوعت التعريفات التي تناولت موضوع الجريمة المعلوماتية، الأمر الذي انعكس على الصعوبة التي واجهتنا عند وضع

تعريف جامع مانع للجريمة المعلوماتية. فقد ذهب البعض [5] إلى تعريف الجريمة المعلوماتية بالاعتماد على الوسيلة التي يتم ارتكاب الجريمة من خلالها، إلا وهي الحاسب الآلي: هي الجرائم التي يتم ارتكابها عن طريق الحاسب الآلي.

ويلاحظ أن عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها الغش المعلوماتي، أو الإختلاس المعلوماتي أو الجريمة المعلوماتية[6]. ونظرا لصعوبة إعطاء تعريف لهذه الظاهرة الإجرامية وذلك حصرها في مجال ضيق. ومن هذه التعاريف: "الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية"[7].

بينما أعطى خبير أمريكي مفهوما موسعا للجريمة المعلوماتية وقال: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل". ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جرائم الحاسوب بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا". وكذلك تعريف "David Tnompson" بأنها: "أية جريمة يكون متطلبا اقترافها، أن تتوفر لدى فاعلها معرفة تقنية للحاسب". وهناك جانب من الفقه الفرنسي، يحاول وضع تعريف لظاهرة الغش المعلوماتي حيث يرى الأستاذ "Massa" أن المقصود بها: "الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح". وفي الغالب ترتكب الجريمة المعلوماتية ليس بغرض تحقيق الربح، وإنما بدافع الإنتقام والسخرية من المنافسين أو غير ذلك من الدوافع. ويؤكد الأستاذ "Devéze" أنه ليس المقصود مجرد إخفاء وصف قانوني، ولكن وضع مفهوم إجرامي، والذي سيكون من الممكن أن يطبق عليه أحد التعاريف المعمول بها في القانون المدني أو الجنائي أو المالي[8].

في حين تبنى فقهاء أخرون أساس أخر لتعريف الجريمة المعلوماتية، ألا وهو موضوع هذه الجريمة، والمتمثل بالمعلومات والبيانات محل الجريمة، ذلك عندما يتجه قصد الجاني إلى الاعتداء عليها كأتلافها أو تخريب البرامج أو تزويرها [9].

وبهذا يبدو لنا أن أنصار هذا الاتجاه اعتبروا أن الجرائم المعلوماتية تقوم أساسا على التلاعب بالبيانات والمعلومات والبرامج، وذلك من خلال المعالجة الآلية للبيانات بتعديلها أو محوها أو تشويهها أو الغاءها [10].

إذ يتضح مما تقدم ومن خلال التعريفات السابقة يمكننا تعريف الجرائم المعلوماتية وهو كل سلوك غير مشروع أو الضار بالمجتمع يقوم به شخص يكون على إلمام كافي بتقنية المعلومات، بالاعتداء على نفس أو مال، أو معلومات، أو بيانات الغير عن طريق الحاسب الآلي، أو أي جهاز اخر.

المطلب الثاني: صور الجرائم المعلوماتية

للجرائم المعلوماتية عدة صور يمكن تسليط الضوء عليها من خلال بحثها في ثلاثة صور الأول منها لبيان غسيل الأموال في حين نخصص الثاني لبحث التزوير المعلوماتي إما الثالث فنتناول فيه جريمة الاتجار بالمخدرات عبر الإنترنت.

أولاً: جريمة غسل الأموال عبر الشبكة الدولية للمعلومات:

تعد جريمة غسل الأموال من أخطر جرائم العصر فهي التحدي الحقيقي أمام مؤسسات المال والإعمال فضلا عن كونها امتحان لقدرة القواعد القانونية على تحقيق فعالية في مواجهة الأنشطة الجرمية ومكافحة أنماطها المستجدة. وهي صورة من صور الجريمة المعلوماتية.

يقصد بغسيل الأموال توظيف الأموال داخل الدولة أو خارجها في أعمال مشروعة وذلك لطمس الأصل غير المشروع لهذه الأموال [11].

وغالباً ما يتم ذلك عن طريق تسلل الأموال إلى المشروعات الإقتصادية والتأثير فيها. ويعاد استغلالها بعد ذلك على إنها من مصدر ربح مشروع [12].

ونتيجة التطور فقد استفاد مجرمو غسيل الأموال من التقنية ومميزاتها لتحقيق أغراضهم الإجرامية.

أما السبب الذي حذا بهم إلى غسيل الأموال عبر هذه الوسائل المستحدثة، هي السرعة وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما إن البطاقات الذكية والتي تشابه بطاقات البنوك التي تستخدم في مكائن الصرف الآلية، تساعد على تحويل الأموال بواسطة المودم أو الأنترنت مع ضمان التشفير وأمان العملية [13].

وهذا الأمر جعل عمليات غسيل الأموال عبر الوسائل التقنية، وخاصة عبر شبكة الويب العالمية، تتم بسرعة ودون إن تترك أي أثار في الغالب [14].

هذا ويذهب البعض إلى إن العلاقة بين الأنترنت وغسيل الأموال، ذات حركة سريعة ولا تأخذ بعين الاعتبار الحدود الجغرافية. مما يجعلها محل جاذبية من قبل المجرمين الذين يهدفون إلى غسيل الأموال [15].

ثانياً: التزوير المعلوماتي:

يقصد بالتزوير: هو تغيير الحقيقة في محرر بقصد الغش وبإحدى الطرق التي حددها القانون تغييرا من شأنه إن يسبب ضررا. إلا إن هذا التزوير أصبح يتم أيضا باستخدام التقنية المعلوماتية، ولهذا ظهر ما يسمى بالتزوير المعلوماتي. وهو التزوير الذي يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تخرج عن طريق الطابعة أو كانت مخرجات مرسومة عن طريق الراسم.

وفي إطار هذه الجريمة تدخل أيضا جريمة استعمال المحرر المزور، إذا ما كان هنالك السلوك الإجرامي المتمثل بفعل الاستعمال. ومحل هذا الاستعمال يرد على المحرر المزور.

هذا ويتصور وقوع جريمة التزوير المعلوماتي، عند قيام الموظف بتغيير الحقيقة في البيان البنكي مثلا، وذلك عندما يحصل على بيانات ذوي الشأن فيثبت على سداد جزء من الفاتورة (فاتورة التلفون مثلا) في حين إن صاحب الشأن قد قام على سدادها كاملة. هذا وأكثر ما يحصل به التزوير، هو اساءة استخدام الصورة سواء كانت لأنسان أو حيوان أو جماد. فيما لو تم تغيير الصورة في الوثيقة المطبوعة سواء أكانت على شريط ممغنط أو مسجل وجرى عرضها على شاشة الحاسب الآلي[16].

ثالثاً: الإتجار بالمخدرات عبر الإنترنت:

كثيرا ما يحذّر أولياء الأمور أبناءهم من رفقاء السوء خشية من تأثيرهم السلبي فيهم ولاسيما في تعريفهم على المخدرات فالصاحب ساحب كما يقول المثل وهذا صحيح ولا غبار عليه لكن وفي عصر الإنترنت أضيف على كاهل أولياء الأمور مخاوف جديدة لا تقتصر على رفقاء السوء فقط بل يمكن إن يضاف إليها مواقع لا تتعلق بالترويج للمخدرات وتشويق الناشئ لاستخدامها بل تتعداه إلى تعليم كيفية زراعة المخدرات وصناعتها بأصنافها كافة وبأبسط الوسائل المتاحة.

والأمر هنا لا يحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى إي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخاوف أحد الخبراء التربويين في بتسبيرج بالولايات المتحدة والذي أكد إن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والإنترنت.

واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات وعقدت المؤتمرات والاتفاقيات الدولية المختلفة ومنها الاتفاقية الوحيدة لمكافحة المخدرات المنعقدة في لاهاي عام (1961م) واتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية المنعقدة في فينا عام (1988م)[17].

المبحث الثاني

الآليات القانونية في مكافحة الجرائم المعلوماتية في العراق

على الرغم من ان التشريعات العقابية التقليدية في العراق قد تناولت الجرائم التقليدية التي تقع على الأموال والأشخاص وغيرها بالتجريم، فأن هذه القوانين قد لا تطال غالبية الجرائم المعلوماتية وذلك لاختلاف هذه الجرائم الحديثة عن الجرائم التقليدية في الطبيعية أو في الأركان أو في المحل، وعلى الرغم من ان التطورات التشريعية الحديثة على مستوى الدول المتقدمة، فإن القانون الجزائي يتطور دائماً بنفس السرعة التي تتطور بها التكنلوجيا أو مهارة الذهن البشري في تسخير المبتكرات لإستخدام الشيء، فالأشكال الحديثة للجريمة لم يقتصر إعتدائها على القيم المادية التي كانت محمية بقانون العقوبات، بل إمتد هذا الإعتداء على القيم المعنوية مثل المعلومات والمعطيات، فأصبحت النصوص التقليدية في قانون العقوبات عاجزة عن مواكبة الجرائم المستحدثة من الإجرام الإلكتروني (المعلوماتي). كذلك عملت الجهود الإدارية العراقية في مكافحة مثل هذه الجرائم من خلال الجامعات العراقية من خلال إقامة الندوات العلمية، وكذلك وزارة الداخلية العراقية.

وعليه ومما تقدم سنتناول دراسة هذا المبحث على مطلبين، وهما ما يأتي:

المطلب الأول: موقف التشريع والقضاء العراقيين في مكافحة الجرائم المعلوماتية

المطلب الثاني: جهود المؤسسات الحكومية العراقية في مكافحة الجرائم المعلوماتية

المطلب الأول: موقف التشريع والقضاء العراقيين في مكافحة الجرائم المعلوماتية

لا يزال المشرع العراقي قيد إصدار قانون خاص ينظم الجريمة المعلوماتية. ولكن هذا لا يعني عدم خضوع الجريمة الإلكترونية للقانون. إذ لم يتوانى القضاء العراقي عن لعب دوره بشكل فاعل، فلم يقف ذلك حائلاً أمام معالجته للجرائم الإلكترونية إذ نجحت المحاكم العراقية في تسوية النزاعات المعروضة أمامها من خلال التشريعات النافذة كتطبيق قانون

العقوبات العراقي رقم 111 لسنة 1969 المعدل، وقانون المطبوعات رقم 206 لسنة 1968 الذي يخص الصحف والمجلات. أما بخصوص العقوبات التي تفرضها المحاكم فهي "التعويض" لأنها محاكم بداءة تنظر في الدعاوى المدنية أو الحبس مدة لا تقل عن 5 سنوات في حالة وجود جنحة.

وقد أجاز قانون المحكمة الجنائية العراقية لسنة 2005 للمحكمة أن تستعمل الوسائل الإلكترونية للتوصيل السمعي والبصري كالبريد الإلكتروني وما الى ذلك من الوسائل الإلكترونية الأخرى.

ومن هنا يظهر ضرورة إنشاء محكمة متخصصة في هذا النوع من الجرائم وتوفير كادر متدرب وذو كفاءة عالية للتعامل مع هكذا جرائم[18].

توجت النصوص المتناثرة في القوانين العربية، والتي جاءت كخطوة لمحاربة الاعتداء الذي يقع عليها عن طريق التقنية الرقمية، بإصدار عدد من الدول العربية قوانين خاصة بالجرائم المعلوماتية. ويعتبر العراق من الدول التي تصدت للجرائم المعلوماتية، إلا إنه ما زال مشروع قانون، حيث أورد المشرّع في المادة الأولى من هذا المشروع عدد من الفقرات التعريفية، حيث تولى المشرّع توضيحها والتعريف بها لكي لا تثير الغموض عند تطبيق نصوص القانون [19].

ومن ثم تطرق المشرّع العراقي إلى الأهداف التي يسعى إلى تحقيقها القانون، وهي توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات، ومعاقبة مرتكبي الأفعال التي تشكل اعتداء على حقوق مستخدميها من الأشخاص الطبيعية أو المعنوية ومنع إساءة استخدامه في ارتكاب جرائم الحاسوب.

وفي إطار الفصل الرابع من هذا المشروع، وتحديدا في المادة 30 منه، أشار المشرّع إلى تطبيق قانون العقوبات العراقي رقم 111 لسنة 1969، وقانون أصول المحاكمات الجزائية رقم 23 لسنة 1971، على كل ما لم يرد نص بشأنه في هذا القانون.

وفي هذا المقام لابد لنا من القول إن المشرّع العراقي قد احسن عندما قام على الإحاطة ببعض الجوانب الإجرائية للجريمة المعلوماتية كتحديد الجهة القضائية المختصة للنظر في هذه الجرائم، كما نلاحظ إن المادة 24 في بندها الثاني قد أشارت إلى عدم جواز المباشرة بإجراءات التفتيش إلا بأمر من القاضي المختص، وفي هذا تأكيد على مبدأ الشرعية الإجرائية في اطار الإجراءات الجنائية ، كما إنه تأكيد على حماية الحياة الخاصة التي اكد الدستور العراقي لسنة 2005 عليها في المادة 17 منه، بالإضافة إلى إنه سمح للقاضي الاستعانة بالخبرة الفنية لتجاوز بعض الصعوبات التي قد يواجهها القاضي المختص في مرحلتي التحقيق والمحاكمة سواء أكانت هذه الخبرة من داخل العراق أو خارجه ([20]).

كما أحسن صنعا عندما أعطى للقاضي عددا من الصلاحيات التي تمكنه السيطرة على تلك البيانات أو المعلومات التي قد يتوصل من خلالها إلى الدليل الذي يمكنه من الوصول إلى الحقيقة وإصدار الحكم على أساسه، إلا إن المشرّع العراقي قد أغفل عما إذا كانت هذه البيانات قد اخترقت شبكة تابعة لدولة أخرى، فلم يوضح الإجراءات التي لابد إن تتبع في هذه الحالة.

المطلب الثاني: جهود المؤسسات الحكومية العراقية في مكافحة الجرائم المعلوماتية

تنطوي هذه الجرائم على مخاطر جمة تلحق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (البيانات والمعلومات والبرامج في كل أنواعها)، وتطاول المعطيات المخزنة والمعلومات المنقولة عبر نظم المعلومات وشبكاتها. هذه المعطيات هي موضوع هذه الجريمة، وهذا يُظهر مدى خطورة الجريمة

الالكترونية، فهي تطاول الحق في المعلومات والحقوق المالية وحقوق الملكية الفكرية والحق المعنوي.

كذلك إنها تمس الحقوق والحريات الشخصية، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية، وتهدد إبداع وابتكار العقل البشري. ونظراً إلى ارتفاع مؤشر هذه الجرائم وتضاعف أعدادها وتطور أساليبها وأنواعها وما رافقها من استحداث أشكال جديدة لم تكن معروفة قبلاً بسبب التطور المضطرد والمتسارع في تكنولوجيا المعلومات، إذ حرصت المؤسسات العراقية على إقامة المؤتمرات والندوات العلمية لمكافحة هذه الجرائم، وهي كما يأتي:

أولاً: جهود وزارة التعليم العالي والبحث العلمي العراقية

عملت وزارة التعليم العالي والبحث العلمي على حث الجامعات بإقامة ندوات علمية بكيفية مكافحة الجرائم المعلوماتية وتثقيف الأفراد والموظفين في مجال مسؤولياتهم تجاه حماية معلومات الشركة، مثل مسؤولياتهم تجاه حماية كلمات المرور التي يستخدموها. وقد ترجمت الوزارة هذا الحث بإصدار كتاب الى الجامعات كافة بعنوان الأمن الإلكتروني المرقم (ب ت 4/ 1622 في 2018/2/25) والذي تضمن "ضرورة حث الباحثين في الجامعات والمؤسسات العلمية على إجراء المزيد من الدراسات المتعلقة بالأمن الإلكتروني ومواجهة التنظيمات الإرهابية التي تنشط على مواقع التواصل الاجتماعي وتستغل أجواء الحرية والانفتاح لحقيق مآربها الدينية".

وعملت بعض الجامعات التابعة الى وزارة التعليم العالي والبحث العلمي العراقية ومنها جامعة تكريت وجامعة بابل بإقامة ندوات علمية من أجل مكافحة الجرائم المعلوماتية، وهي ما يأتي:

أ- الندوة العلمية (مدى فاعلية البنية القانونية الدولية والوطنية لمكافحة جريمة الإرهاب الإلكتروني) 5/7/ 2018 جامعة تكريت كلية الحقوق/ العراق

تكمن أهمية هذه الندوة في مصطلح الإرهاب الإلكتروني الدولي الذي شاع استخدامه عقب التقدم الكبير الذي حققته تكنولوجيا المعلومات واستخدامات الحواسيب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، وهذا الأمر هو الذي دعا (30) دولة الى توقيع الإتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية بودابست عام (2001)، والذي يُعدُ من أشد أنواع الجرائم التي ترتكب عبر شبكة الإنترنت خطورة، حيث يتضحُ هذا جلياً من خلال النظر إلى فداحة الخسائر التي يمكن أنْ تُسببها عملية ناجحة واحدة تندرج تحت مفهوم الإرهاب الإلكتروني، إذْ دفع التطور في الوسائل التكنولوجية الحديثة وإنتشار وسائل الإتصالات الإلكترونية، والجماعات الإرهابية في استخدام تلك الوسائل، والترويج والتنظيم للمخططات الإرهابية، مما استلزم تحديد معالم الظاهرة الإرهابية المستحدثة التي تعتمد على استخدام أحدث التقنيات واستغلال وسائل الإتصالات وشبكة المعلومات الدولية، وتستمد أهمية الموضوع في توعية الأفراد من كافة المجتمعات والدول في الوسائل والطرق التي تلجأ إليها التنظيمات الإرهابية لغايات استقطاب وتجنيد هؤلاء الأفراد، كما تتجلى أهمية الندوة في إلقاء الضوء على الدور الذي يجب أنْ تضطلع به الدول والجماعات والأفراد للتصدي لظاهرةِ الإرهاب الإلكتروني والوقاية منها، كما يستمد هذا الموضوع أهميته إدراكاً من الواقع بأنَّ ظاهرة الجرائم المستحدثة ومنها الإرهاب الإلكتروني الدولي قد غدتْ تشكلُ تحدياً حقيقياً للسياسات الجنائية السائدة في الدول وأجهزتها التشريعية والتنفيذية والقضائية، وكذلك الهدف من دراسة الموضوع هو إيجاد تعريف عام موحد للإرهاب الإلكتروني على المستوى الدولي[21].

ب- الندوة العلمية (مخاطر الإرهاب الإلكتروني وسبل مكافحته) 2017/4/13 جامعة بابل كلية القانون/ العراق

وناقشت الدراسة موضوعاً مهماً من موضوعات الإرهاب، ألا وهو" الإرهاب الالكتروني "أو ما يسمى بـ" الإرهاب المعلوماتي "وهو إرهاب يرتبط بالتطورات الحديثة التي صاحبت ظهور الحاسوب الإنترنت، حيث لم تعد أفعال الإرهاب مقتصرة على جانبها التقليدي في التفجير والتفخيخ والإتلاف والقتل، إنما باتت العديد من أفعال الإرهاب ترتكب عن طريق أجهزة الحاسوب وشبكة الإنترنت، حتى بات الإرهابي يجلس في قارة من الكرة الأرضية خلف حاسوب وبضغطة زر واحدة يقوم بعل إرهابي ينفذه في قارةٍ أُخرى.

وبينت الدراسة ان هذا الأمر خلق مشكلات جديدة تتعلق بالقانون الواجب التطبيق على مثل هذه الأفعال فضلاً عن صعوبة إثباتها والأهم من ذلك مخاطرها التي باتت تتسع بشكل هائل مع الاستخدام الواسع لشبكة الإنترنت، ولعل خير دليل على ذلك ان الجهود الدولية اليوم قد تنبهت الى هذا الخطر القادم عبر تقنية المعلومات.

وبحسب الدراسة فان الإرهاب الالكتروني يعرف بأنه "إستخدام الموارد المعلوماتية والمتمثلة في شبكات المعلومات وأجهزة الكومبيوتر وشبكة الإنترنت من أجل أغراض التخويف أو الإرغام لأغراض سياسية" وعُرف أيضا بأنه "كل فعل أو إمتناع عن فعل يقوم به فردٌ أو جماعة منظمة باستخدام وسائل تقنية المعلومات أو الشبكات المعلوماتية، من شأنه إحداث ضرر أو تعريض مصلحة يحميها القانون لخطر، تنفيذاً لمشروع إرهابي". واستعرضت الدراسة عدد من الأمثلة على الإرهاب الالكتروني الذي يتسبب عن تحكم التكنولوجيا في العديد من مجالات الحياة مثل التسبب في سقوط الطائرات أو تصادمها عبر تزويدها بمعلومات ملاحية خاطئة أو تعطيل وسائل التحكم الالكترونية فيها والتلاعب في البرامج التي تتحكم بأجهزة صناعة الدواء ما ينتج عنه فوضى في المقادير المستخدمة بما

يسبب أضراراً جسيمة لا يمكن إكتشافها إلا بعد فترة متأخرة بل وبعد فوات الأوان وأيضاً تعطيل إشارات السير أو إحداث الفوضى في عملها خاصةً في المدن الكبرى وما ينتج عنه من أضرار لا يستهان بها ناتجة عن الفوضى وحوادث السير الناجمة عن ذلك وتعطيل محطات الكهرباء والماء وشبكة الاتصال والأنظمة المصرفية والبورصة، نظراً لوجود "فايروس" من خلاله يمكن السيطرة على أجهزة الهاتف في مجتمع ما وجعلها تتصل كلها برقم الطوارئ في وقت واحد لشل وتعطيل هذه الخدمة وفتح منافذ السدود وما ينتج عنها من أضرار الفيضانات والتلاعب في أنظمة تشغيل وإطلاق وتوجيه الصواريخ الاستراتيجية وأسلحة الدمار الشامل، مما يتسبب عنه ضررٌ ودمارٌ نتيجة الإطلاق العشوائي لها وهو ما قد يُسبب حرباً كونية والتسبب بتعطيل عمل المحطات النووية والكيمائية والبيولوجية عبر التلاعب بأنظمة تشغيلها المناطة بتكنولوجيا الحاسبات الآلية وما ينتج عنه من تسرب للإشعاعات الخطرة[22].

ثانياً: جهود وزارة الداخلية العراقية

اتخذت الحكومة العراقية العديد من الجهود والإجراءات خلال السنوات الأخيرة من أجل حماية مواطنيها من الجرائم الإلكترونية (المعلوماتية) والتي شهدت تزايداً ملحوظاً خلال السنوات العشر الأخيرة، لذلك جاءت الجهود من الحكومة ومن وزارة الداخلية العراقية تحديداً لمواجهة هذا التزايد والتقليل منه وذلك بإنشاء رقم مكافحة الجرائم الالكتروني (الإبتزاز)[23] في العراق الذي يمكنك كمواطن عراقي الاتصال عليه لحمايتك من هذه الجريمة.

دفع أجهزة وزارة الداخلية العراقية بعد استفحال الجرائم الإلكترونية وتهديدها لسلامة المجتمع، وتم إطلاق حملة "بتنه - تهمنه" لنشر الوعي بين أوساط الشباب العراقي

بمخاطر الدعاية والجرائم الإلكترونية، وخاصة علميات التجنيد التي يقوم بها داعش لجذب الشباب.

وهذه الحملة تمثل جهداً لوزارة الداخلية العراقية لأنها تفاعلت في حملتها هذه مع شباب المدراس والمعاهد والكليات لنشر الوعي في صفوفهم بضرورة تأمين حساباتهم الإلكترونية، وكيفية طلب المساعدة في حالة حدوث أي مشاكل، وتظافر مع إطلاق برنامج إذاعي للوزارة وعدد من الأفلام القصيرة لنشر الوعي من خطر التعرض للابتزاز خاصة بحق الفتيات الصغيرات ومحاولات استخدامهن في جرائم خطيرة مثل الإرهاب وتهريب المخدرات. إذ تبرز أهمية هذه الحملة التي تنفذها الداخلية العراقية، في أنها قد كشفت عن أن الابتزاز الإلكتروني يستهدف بشكل أكبر الفئة العمرية من 15 إلى 26 سنة، معظمهم من غير المتعلمين أو ممن يعيشون في أسر محافظة للغاية، وهذا يعني أن انتشار الجهل في صفوف هذه الضحايا كان سبباً في زيادة وقوع هذه الجرائم. ورغم أن الحكومة مسؤولة عن حماية وسلامة وأمن مجتمعها إلا أنها لم تتمكن من إصدار تشريع قانوني لمجابهة هذه الجرائم[24].

ونرى من جانبنا فأن وزارة الداخلية مطالبة بالتوسع في حملاتها التوعية في المدارس والجامعات، حاجتنا إلى إنشاء قسم بوليسي خاص مجهز بأحدث الوسائل التكنولوجية تكون مهمته تلقي هذه الأنواع من الجرائم الالكترونية ومعالجتها أسوة بما أتبعته بعض الدول في العالم من حولنا.

الخاتمة:

أولاً: الاستنتاجات:

1- ان الجرائم المعلوماتية جرائم جيدة وتعبير لم يرد في القوانين العقابية في العراق في استخدام التقنية الحديثة كما ان المجتمع العراقي لم يألف مثل هذه الجرائم وان الأفعال

المنطوية فيها أنما تم معالجتها في أكثر من قانون عقابي ومنها قانون العقوبات وقانون مكافحة الإرهاب وقوانين أخرى.

2- ان الجرائم المعلوماتية تختلف عن الجرائم العادية في أسلوب ارتكابها وشخص مرتكبها والوسيلة المستعملة في ارتكابها وهي من الجرائم الصعبة الاكتشاف كما أنها تحتاج الى خبراء مختصين في التحقيق فيها لان المجرم لا يترك أثراً عند ارتكابها.

3- ان الجرائم المعلوماتية كثيرة ومتشعبة فمنها ما يتعلق بالمساس بالحق العام ومنها توجد فيها اعتبارات شخصية وتتعدد صور ارتكابها بين الإرهاب والمخدرات والاتجار بالبشر الى السب والقذف والقرصنة والجرائم المالية واختراق المواقع ومنها ما يشكل جناية خطرة وتتدرج لتصل الى الجنح وهي جرائم يصعب حصرها مع التطور الكبير والتنوع والابتكار في أسلوب ارتكابها.

ثانياً: المقترحات:

1- ضرورة الإسراع في تشريع قانون مكافحة الجرائم المعلوماتية مع عدم المساس بالحريات الشخصية وان ينسجم القانون مع الدستور.

2- ان الجرائم المعلوماتية تحتاج الى إعادة النظر في قانون أصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل وذلك لأنها من الجرائم التي تختلف في وسائل إثباتها عن الجرائم الأخرى.

3- ان الجرائم المعلوماتية يجب ان يتم البدء بخطوات لحسن تطبيق قانونها ومنها تنظيم عمل مكاتب الإنترنت وشركات الاتصال المسؤولة عن توفيرها.

4- ان هناك اتجاها تشريعيا لتشريع قانون الجرائم المعلوماتية ولابد من إعادة النظر في العقوبات المنصوص عليها في مسودة قانون الجرائم المعلوماتية الموجودة في مجلس النواب لأنها مبالغ في بعضها.

5- ضرورة ان تكون هناك توعية قانونية بمخاطر استخدام الإنترنت من قبل ضعاف النفوس ومخاطر الاستخدام من قبل الأحداث في ان يكونوا صيدا سهلا لقراصنة الإنترنت وان تكون هناك توعية إعلامية بعد التوسع الكبير في استخدام الحاسوب في جميع مجالات الحياة.

قائمة المصادر والمراجع:

القران الكريم

أ-الكتب:

1- بيل غيتس: المعلوماتية بعد الأنترنت، ترجمة عبد السلام رضوان، عالم المعرفة سلسلة كتب ثقافية شهرية يصدرها المجلس الوطني للثقافة والفنون والآداب، الكويت، 1978.

2- د. خالد حمد محمد الحمادي: جريمة غسيل الأموال في عصر العولمة، دار النهضة العربية، القاهرة، 2006.

3- د. خالد ممدوح إبراهيم: حكومة الأنترنت، دار الفكر العربي، الإسكندرية، 2011.

4- ريتشارد روسينبرج، التأثير الاجتماعي للحاسبات، تعريب د. م، سرور علي أبراهيم سرور: دار المريخ للنشر، السعودية، الرياض، 2000.

5- د. عبد الفتاح بيومي حجازي: الجريمة في عصر العولمة، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

6- د. عبد الفتاح بيومي حجازي: جريمة غسيل الأموال بين الوسائط الالكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية، 2007

7- محمد العجلوني، د. زياد مشاقبة: استخدامات حاسوبية في الإدارة، ط1، دار اليازوري، الأردن، 2011.

8- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2004.

9- محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.

10- د. محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2004.

11- د. محمد علي قطب: الجرائم المستحدثة وطرق مواجهتها، ط1، دار الفجر للنشر والتوزيع، القاهرة، 2009.

12- منير الجنبيهي: ممدوح الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006.

13- د. هشام فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

14- د. هدى حامد قشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، 1992.

ب- الرسائل والأطاريح:

1- إسراء طارق جواد كاظم الجابري: جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012.

2- زينب إسكندر: التزامات المصارف في مكافحة غسيل الأموال، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2010.

3- شذى حسن عبد زلزلة: أهمية المعلومات في بناء استراتيجية التنمية العربية، أطروحة دكتوراه، المعهد العالي للدراسات السياسية والدولية، الجامعة المستنصرية، 2005.

4- لينا محمد متعب الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012.

ج- المقالات في المجلات:

1- د. واثبة السعدي: الحماية الجنائية لبرامج الحاسوب، بحث منشور في مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مج 18، ع1، 2004.

2- د. فائزة بابا خان: جريمة الإنترنت، بحث منشور في مجلة العدل نيوز، 2012/12/22.

د- المقالات على مواقع الإنترنت:

1- للمزيد حول الندوة يُنظر إلى الرابط الإلكتروني الآتي: http://claw.tu.edu.iq ، (آخر زيارة للموقع في2019/12/14، 11:30م).

2- للمزيد حول الندوة يُنظر إلى الرابط الإلكتروني الآتي: http://law.uobabylon.edu.iq (آخر زيارة للموقع في2019/12/20، 5:40م).

3- للمزيد حول المقال يُنظر إلى الرابط الإلكتروني الآتي: https://theglobalcoalition.org، (آخر زيارة للموقع في2019/12/24، 9:10م).

الهوامش:

(1) د. هشام فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص29.

(2) الحاسب الآلي: آلة تتكون من وحدات مستقلة يطلق عليها المكونات الصلبة حيث يقوم كلاً منها بمهمة مستقلة، والجزء الأخر يطلق عليه المكونات اللينة والذي يكون من برمجيات مختلفة لتشغيل الجهاز، ومنها

ما هو تطبيق للجهاز. محمد العجلوني، د. زياد مشاقبة: استخدامات حاسوبية في الإدارة، ط1، دار اليازوري، الأردن، 2011، ص 14.

(3) د. محمد علي قطب: الجرائم المستحدثة وطرق مواجهتها، ط1، دار الفجر للنشر والتوزيع، القاهرة، 2009، ص 131؛ د. خالد ممدوح إبراهيم: حكومة الأنترنت، دار الفكر العربي، الإسكندرية، 2011، ص 356؛ ريتشارد روسينبرج، التأثير الاجتماعي للحاسبات، تعريب د. م، سرور علي أبراهيم سرور: دار المريخ للنشر، السعودية، الرياض، 2000، 352.

(4) بيل غيتس: المعلوماتية بعد الأنترنت، ترجمة عبد السلام رضوان، عالم المعرفة سلسلة كتب ثقافية شهرية يصدرها المجلس الوطني للثقافة والفنون والآداب، الكويت، 1978، ص 15.

(5) منير الجنبيهي: ممدوح الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص13.

(6) د. محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2004، ص43.

(7) محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص7.

(8) د. محمد علي العريان: المصدر السابق، ص 44.

(9) د. واثبة السعدي: الحماية الجنائية لبرامج الحاسوب، بحث منشور في مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مج 18، ع1، 2004، ص62. وهو ما أخذ به المشرّع الإماراتي في القانون الاتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات في الأمارات العربية المتحدة: "كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به"؛ كما أتجه البعض الأخر إلى: (مجموعة الجرائم التي تتصل بالمعلوماتية). د. هدى حامد قشقوش: جرائم الحاسب الألكتروني في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، 1992، ص 5.

(10) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2004، ص19.

(11) د. خالد حمد محمد الحمادي: جريمة غسيل الأموال في عصر العولمة، دار النهضة العربية، القاهرة، 2006، ص27.

[12] د. عبد الفتاح بيومي حجازي: الجريمة في عصر العولمة، ط1، دار الفكر الجامعي، الإسكندرية، 2007، ص 204.

[13] زينب إسكندر: التزامات المصارف في مكافحة غسيل الأموال، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2010، ص 33 وما بعدها.

[14] د. عبد الفتاح بيومي حجازي: جريمة غسيل الأموال بين الوسائط الالكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية، 2007، ص 17 وما بعدها.

[15] زينب إسكندر، مصدر سابق، ص 34. لقد جاء النص على هذه الجريمة، المادة 19 من القانون الإماراتي النافذ، والمادة 21 من القانون العُماني النافذ.

[16] لينا محمد متعب الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012، ص32.

[17] إسراء طارق جواد كاظم الجابري: جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012، ص52.

[18] د. فائزة بابا خان: جريمة الإنترنت، بحث منشور في مجلة العدل نيوز، 2012/12/22.

(19) وهذه المصطلحات هي الحاسوب، المعالجة الآلية للبيانات، بيانات الحاسوب، البرامج، جهات تزويد الخدمات المعلوماتية، بيانات المرور، بيانات الاشتراك، البطاقة الالكترونية، شبكة المعلومات، التوقيع الالكتروني، الوسائل الالكترونية، المعلومات، المحرر الالكتروني، نظام معالجة المعلومات، شهادة التصديق الالكتروني. شذى حسن عبد زلزلة: أهمية المعلومات في بناء استراتيجية التنمية العربية، إطروحة دكتوراه، المعهد العالي للدراسات السياسية والدولية، الجامعة المستنصرية، 2005، ص 153.

[20] لينا محمد متعب الأسدي: مصدر سابق، ص57.

[21] للمزيد حول الندوة يُنظر إلى الرابط الإلكتروني الآتي: http://claw.tu.edu.iq ، (آخر زيارة للموقع في2019/12/14، 11:30م).

[22] للمزيد حول الندوة يُنظر إلى الرابط الإلكتروني الآتي: http://law.uobabylon.edu.iq (آخر زيارة للموقع في2019/12/20، 5:40م).

[23] تعريف الإبتزاز الإلكتروني: هي عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو إستغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية، وإعادة ما يتم تصيد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الإجتماعي المختلفة كـ الفيس بوك، تويتر، وإنستكرام وغيرها من وسائل التواصل الإجتماعي نظراً لانتشارها الواسع وإستخدامها الكبير من قبل جميع فئات المجتمع، وتتزايد عمليات الإبتزاز الإلكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الإجتماعي والتسارع المشهود في أعداد برامج المحادثات المختلفة.

[24] للمزيد حول المقال يُنظر إلى الرابط الإلكتروني الآتي: https://theglobalcoalition.org ،(آخر زيارة للموقع في2019/12/24، 9:10م).