Journal Of the Iraqia University (70-1) November (2024)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.iasj.net/iasj/issue/2776

التحديات القانونية لمكافحة الجرائم الإلكترونية في العصر الرقمي

م. علي فاضل جويد

قسم القانون-كلية الإمام الجامعة-العراق

"Legal Challenges to Combating Cybercrime in the Digital Age"

M. Ali Fadhel Jawad
Department of Law - Imam University College - Iraq
Le3na94@gmail.com

المستخلص

يشهد العصر الرقمي تزايدًا مستمرًا في استخدام التكنولوجيا الحديثة، الأمر الذي أدى إلى بروز مجموعة جديدة من التحديات القانونية المرتبطة بمكافحة الجرائم الإلكترونية. تشمل هذه التحديات صعوبة تتبع الجناة بسبب الطبيعة العابرة للحدود للجرائم الإلكترونية، والتطور السريع في أدوات وتقنيات الجريمة، والقصور في التشريعات الوطنية التي قد تكون غير محدثة لتغطية التطورات التقنية الحديثة. إضافة إلى ذلك، يواجه المشرعون تحديات تتعلق بحماية حقوق الخصوصية وحرية التعبير أثناء محاولة ضبط الأنشطة الإجرامية على الإنترنت. تتطلب مكافحة الجرائم الإلكترونية نهجًا متعدد الجوانب يشمل تحديث التشريعات، تعزيز التعاون الدولي، وتطوير القدرات التقنية للمؤسسات القانونية. يهدف هذا البحث إلى تحليل هذه التحديات القانونية واستكشاف سبل تطوير آليات مكافحة الجرائم الإلكترونية بما يتوافق مع المتغيرات التكنولوجية السريعة.**الكلمات المفتاحية : التحديات القانونية , الجرائم الالكترونية , العصر الرقمي.**

Abstract

The digital age is witnessing a continuous increase in the use of modern technology, leading to the emergence of a new set of legal challenges related to combating cybercrime. These challenges include the difficulty of tracking offenders due to the cross-border nature of cybercrimes, the rapid evolution of crime tools and techniques, and the inadequacy of national legislation that may not be updated to address recent technological advancements. Additionally, lawmakers face challenges related to protecting privacy rights and freedom of expression while attempting to regulate criminal activities on the internet. Combating cybercrime requires a multi-faceted approach, including updating legislation, enhancing international cooperation, and developing the technical capacities of legal institutions. This research aims to analyze these legal challenges and explore ways to develop mechanisms for combating cybercrime in line with the rapid technological changes.

Keywords: Legal challenges, Cybercrime, Digital age

المقدمة

إن الجرائم الإلكترونية هي نتيجة ثانوية للتقدم السريع في تكنولوجيا المعلومات، وتعتبر واحدة من أهم التحديات الأمنية وأكثرها خطورة التي تواجه جميع المجتمعات البشرية اليوم، وخاصة في مجال تكنولوجيا المعلومات والاتصالات التي تستخدمها الكيانات والأفراد في القطاعين العام والخاص. وقد تميز القرن العشرين بالابتكارات التكنولوجية الهامة، ولا سيما ظهور أجهزة الكمبيوتر الإلكترونية، التي تطورت لتسهيل إنشاء شبكات وأنظمة المعلومات، مما أدى في النهاية إلى تسمية هذه التكنولوجيا بنظام المعلومات.تمثل جرائم الكمبيوتر، والتي يشار إليها أيضًا باسم جرائم المعلومات نظرًا لارتباطها بأنظمة معالجة المعلومات الآلية، ظاهرة إجرامية حديثة نسبيًا مرتبطة بتكنولوجيا الكمبيوتر. وقد أدى هذا الارتباط إلى تعزيز الشعور بالغموض، مما دفع البعض إلى التأكيد على أن جرائم الكمبيوتر تشبه الأسطورة ولا تشكل تهديدًا حقيقيًا. وعلاوة على ذلك، حتى إذا كانت

بعض الأنشطة غير القانونية مرتبطة بأجهزة الكمبيوتر، فإنها تُعتبر جرائم تقليدية يمكن تطبيق قوانين العقوبات التقليدية عليها.تواجه الجرائم الإلكترونية العديد من المشاكل القانونية. فهناك عقبات إجرائية، وقضايا تتعلق بسلطة فرض العقوبات والتحقيق، وتعقيدات تتعلق بالقانون المناسب لهذه الفئة من الجرائم. وتنبع أصول هذه التحديات من حداثة هذا النوع من الجرائم وعدم كفاية تطوير التشريعات الجنائية لمعالجتها.

إشكالية الدراسة

إن فعالية القانون الوطني في مكافحة الجريمة تشكل معياراً لتقييم مدى تطوره وقدرته على تحقيق أهدافه القانونية. ولا شك أن التشريع يسعى إلى حماية الأفراد من الأنشطة الإجرامية؛ إلا أن الجرائم الإلكترونية تطرح قضايا فريدة تتطلب فهم طبيعتها وتحديد هذه التحديات.

تساؤلات الدراسة

سيقوم الباحث من خلال الدراسة بالأجابة على التساؤلات الأتية :ما المقصود بالجريمة الإلكترونية ؟ ما هي خصائص الجريمة الإلكترونية ؟. ما هي أهم مظاهر التحديات التى تواجه الجرائم الإلكترونية على المستوى القانوني ؟ .

أهدف الدراسة

تهدف الدراسة إلى الوقوف على عدة نقاط الوقوف على تعريف الجريمة الإلكترونية التعرف على أهم الخصائص التى تتمتع بها الجريمة الإلكترونية الوقوف على أهم التحديات الإجرائية التى تواجه مكافحة الجرائم الإلكترونيةالتعرف على أهم تحديات القانون الواجب التطبيق على الجرائم الإلكترونية

منهج الدراسة

يبع الباحث في معالجة الموضوع المنهج التحليل والمنهج الإستنباطي

المنهج التحليل

وذلك بتحليل نصوص القانوني المرتبطة بمكافحة الجرائم الإلكترونية ، مثل قوانين تقنية المعلومات ، من أجل الوقف على مناطق الضع والقوة

المنهج الإستباطي : والقائم على أستنباط الأفكار والحلول بعد تحليل النصوص.

خطة الدراسة

المبحث الأول: الجرائم الإلكترونية في العصر الرقمي المبحث الثاني: أهم الإشكاليات التي تواجهة مكافحة الجرائم الإلكترنية في العصر الرقمي

المبحث الأول الجرائم الإلكترونية في العصر الرقمي

تمهيد وتقسيم تشمل الجرائم الإلكترونية مجموعة واسعة من الأنشطة. وقد أصيبت المجتمعات في الآونة الأخيرة بظاهرة إجرامية ناجمة عن انتهاك الحقوق التكنولوجية والخصوصية. وقد ظهرت وجهات نظر عديدة بشأن هذه الفئة الجديدة من الجرائم، سواء في التشريعات المقارنة أو الأمريكية، مما دفع إلى إجراء تحقيقات مختلفة لوضع تعريف كامل لهذه الجريمة العالمية.لقد ظهرت تعريفات عديدة، تركزت جميعها حول فكرة أن الجريمة الإلكترونية تشكل عملاً إجرامياً يتم تنفيذه من خلال وسائل تكنولوجية. وقد ظهرت العديد من الاستفسارات حول التصنيف القانوني للجريمة الإلكترونية. وينشأ هذا من كثرة وجهات النظر حول هذه الفئة من الجرائم، حيث ظهرت العديد من التفسيرات الفقهية في محاولة لتوضيح مفهوم الجريمة الإلكترونية وتقديم توصيف قانوني نهائي لهاإن تعريف الجريمة الإلكترونية يتطلب فهم أهدافها وعناصرها الإجرائية، فضلاً عن دراسة المكونات المختلفة التي تتجمع لتشكل الجريمة وتقدير أبعادها التكنولوجية.سيتم تناول هذه القضية في قسمين على النحو المبين أدناه:

المطلب الأول تعريف الجريمة الإلكترونية

لم يتفق الفقه على تعريف نهائي وشامل للجرائم الإلكترونية، وذلك نتيجة لعدم وجود تنظيم تشريعي في العديد من الدول وظهور هذه الجرائم في الآونة الأخيرة مقارنة بجرائم أخرى، فضلاً عن غياب تعريف قانوني لهذا النوع من الجرائم في أغلب الدول، فضلاً عن عدم وجود مصطلح قانوني موحد لوصف الجرائم الناجمة عن الاستغلال والاستخدام غير المشروع لتكنولوجيا المعلومات.واستجابة لهذا الفراغ القانوني، سعى الفقه إلى تقديم تفسير للجرائم الإلكترونية. وينقسم الفقه إلى اتجاهين رئيسيين على أساس المنظور الذي يتم من خلاله تحليل هذا الشكل من أشكال الجريمة. ويقيد الاتجاه الأول تعريف الجريمة الإلكترونية، في حين يسعى الاتجاه اللاحق إلى توسيع نطاقها.

أولاً : التعريف الضيق للجريمة الإلكترونية أحد التعريفات التي طرحها مؤيدو هذا الاتجاه هو تعريف الجريمة الإلكترونية، حسب الخبير القانوني ميروي، والتي تعرف بأنها أي فعل غير قانوني يرتكب باستخدام جهاز الكمبيوتر، أو أي فعل إجرامي يكون الكمبيوتر هو الأداة الأساسية فيه، أو أي مزيج من السلوكيات غير القانونية التي ترتكب من خلال المعالجة الآلية للبيانات (الدسوقي , ٢٠٠٩ : ١٥٣) ويصفها جانب آخر من الفقه

بأنها: "الجرائم التي تكون فيها البيانات وبرامج المعلومات الحاسوبية جزءًا لا يتجزأ منها، أو أي فعل غير مشروع يكون فيه الكمبيوتر بمثابة الأداة الرئيسية"(المضحاكي , ٢٠١٤ : ٢٥)كما عرفتها الدكتورة هدى قشقوش هي: " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، كما عرفتها بأنها " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات"(قشقوش , ب.س: ٢٥).

ثانيًا : التعريف الواسع للجريمة الإلكترونية تناول رأي أخر من الفقه تعريف الجريمة الإلكترونية بأنها : "عمل أو إمتناع يأتيه الإنسان إضرار بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابًا "(الدسوقي , ٢٠٠٩ : ١٥٨)تصنف المنظمة الأوروبية للتعاون الاقتصادي والتنمية الجريمة الإلكترونية على أنها أي فعل أو امتناع عن فعل من شأنه أن يؤدي إلى اعتداء على ممتلكات مادية أو غير مادية، تنشأ بشكل مباشر عن استخدام تكنولوجيا المعلومات الإلكترونية.(المضحاكي , ٢٠١٤ : ٢٧)تم تحديد تعريف الجريمة الإلكترونية في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، الذي انعقد في فيينا عام ٢٠٠٠، حيث جاء فيه أن "الجريمة الإلكترونية تشير إلى أي جريمة ترتكب من خلال نظام أو شبكة كمبيوتر، أو داخل نظام كمبيوتر، بما في ذلك جميع الجرائم التي يمكن أن تحدث في بيئة إلكترونية" (الحلبي , ٢٠١١ : ٢٨)ويشير هذا الاتجاه إلى توسع كبير في تعريف الجريمة الإلكترونية، التي تواجه انتقادات بسبب تصنيف السلوكيات باعتبارها جرائم إلكترونية فقط بسبب استخدام الكمبيوتر في السلوك غير المشروع. ولا يمكن تصنيف بعض الجرائم، مثل سرقة الكمبيوتر أو الأقراص، باعتبارها جرائم إلكترونية فقط بسبب تصرفات الجاني، حيث كان الكمبيوتر أو مكوناته المادية مجرد هدف للاختلاس.

المطلب الثاني خصائص الجريمة الإلكترونية

إن الارتباط بين الجريمة الإلكترونية والتكنولوجيا الرقمية أعطى هذا النوع من الجريمة بعض الصفات التي تميزه عن الجرائم التقليدية والتي يمكن تلخيصها على النحو التالي:

أولا : الجريمة الإلكترونية جريمة عابرة للحدودإن السمة الأساسية للجرائم الإلكترونية هي قدرتها على تجاوز الحدود الجغرافية، وذلك بسبب ارتباطها بالإنترنت وتكنولوجيا المعلومات، الأمر الذي يسمح بتأثر عدة دول في وقت واحد بهذه الجرائم بسبب تنفيذها السريع. فقد يرتكب الجاني الجريمة في دولة ما بينما يقيم الضحية في دولة أخرى خلال فترة زمنية وجيزة في العصر الرقمي، سهّل انتشار الإنترنت ربط عدد لا يحصى من أجهزة الكمبيوتر على مستوى العالم، مما سهّل الاتصالات ونقل البيانات، شريطة معرفة عنوان المتلقي أو إمكانية الوصول إلى كلمة المرور. وبصرف النظر عما إذا كانت هذه الإجراءات تُنفَّذ من خلال وسائل قانونية أو غير قانونية، يمكن وصف الجرائم المتعلقة بالتكنولوجيا بأنها جرائم عابرة للحدود الوطنية، حيث يقيم الجاني في كثير من الأحيان في دولة واحدة بينما يقع الضحية في دولة أخرى، مما قد يتسبب في ضرر في دولة ثالثة في نفس الوقت. وبالتالي، تتجلى الجرائم الإلكترونية كفئة جديدة من الجرائم التي تتجاوز الحدود الوطنية أو الإقليمية أو القارية (المناعسة , ٢٠١٤ : ٩٣)لقد خلقت طبيعة الجرائم الإلكترونية العديد من التحديات في تحديد الاختصاص القضائي، وتحديد القوانين المناسبة، ومعالجة عمليات المقاضاة، إلى جانب القضايا الأخرى المرتبطة بالجرائم العابرة للحدود الوطنية بشكل عام (باطلي , ٢٠١٥ : ٤٩).

ثانيًا : صعوبة الإكتشاف والإثباتإن الخصائص الفريدة للجرائم الإلكترونية تجعل إثباتها صعباً، ويرجع ذلك في الغالب إلى صعوبة اكتشاف هذه الجرائم، لأنها لا تترك أدلة خارجية. وتتميز الجرائم الإلكترونية بالتلاعب أو حذف البيانات والمعلومات الرقمية الموجودة في ذاكرة الكمبيوتر، دون أي علامات واضحة على الاختراق المادي أو العنف. والجرائم الإلكترونية هي جرائم تكنولوجية غير عنيفة تتميز بطبيعتها السرية (الطائي , ٢٠٠٧ : ٥٣).تعتبر الجريمة الإلكترونية جريمة جديدة، وتشكل ظاهرة إجرامية مميزة ذات صلة بقانون الجرائم المعلوماتية، حيث تحدث في نطاق معالجة البيانات الإلكترونية، وتتضمن جمع أو إدخال البيانات في جهاز كمبيوتر مرتبط بشبكة معلومات، بقصد الحصول على معلومات محددة. ويمكن أن تحدث هذه الجرائم من خلال التلاعب الشفهي أو النصي، مما يسمح للمستخدم بتعديل المستندات والنصوص على الكمبيوتر مع إمكانية التصحيح والتغيير والحذف والتخزين والاسترجاع والطباعة(كامل , ٢٠٠٧ : ٢٧٠) .

ثالثًا : الجرائم الإلكترونية مغرية للمجرمين إن الجرائم التقليدية تتطلب استخدام أدوات مادية وعادة ما تتضمن العنف، كما هو الحال في جرائم المخدرات والإرهاب والسطو المسلح؛ وعلى النقيض من ذلك، تُعرَّف الجرائم الإلكترونية بأنها جرائم غير عنيفة لا تتطلب استخدام القوة. ويحتاج مجرم الإنترنت فقط إلى الكفاءة التقنية للتعامل مع الكمبيوتر المستخدم في الأنشطة غير المشروعة. وهو يحتاج إلى وجود شبكة معلومات عالمية، إلى جانب الإرادة لتحقيق الهدف غير القانوني، وكل هذا خالٍ من العنف(محمد, ب.س : ٣٧).

المبحث الثاني أهم الإشكاليات التي تواجهة مكافحة الجرائم الإلكترونية في العصر الرقمي

تمهيد وتقسيم لقد كان لإرتباط الجريمة الإلكترونية بجهاز الحاسب الآلي من جهة وشبكة الإنترنت من جهة أخرى أن نتج عن ذلك عدة صعوبات سواء في طابع الجريمة أن أساليب مواجتها أم أساليب التحقيق فيهالقد أدى دمج تقنيات الحوسبة والاتصالات إلى ظهور تكنولوجيا المعلومات، مما سهل التدفق الواسع للمعلومات والبيانات المتنوعة ضمن إطار رقمي. وقد أدى الاستخدام غير السليم لتكنولوجيا المعلومات إلى الجرائم الإلكترونية، والتي تفرض تحديات كبيرة على السلطات التشريعية والقضائية والأمنية في معالجتها.تعتبر الجريمة المعلوماتية من جرائم العصر الرقمي التي تمس المعمومات بكافة أشكالها والتي تمخضت عن الاستغلال السيئ لتكنولوجيا المعلومات، فقد تسببت في إنقلاب خطير في مفهوم النظرية التقليدية للجريمة والتي ترتكب من قبل المجرم المعموماتي، وقد نتج عن هذا الأمر ضرورة استحداث أساليب خاصة للتحري و التحقيق فيها ، وكذا آليات مسبقة للوقاية منها سواء على مستوى الوطني أو الدولي بإعتبارها من الجرائم العابرة للحدود والتي لا تعترف بالحدود الجغرافية ، بمعنى تتيح شبكة الانترنت لأي مستخدم على مستوى أغلب دول العالم تحميل و نشر البيانات و المعمومات في غضون ثوان معدودة و بمجرد ضغطة زر على لوح المفاتيح هذا ما نتناوله في هذا المبحث والذي قسمته إلى ثلاث مطالب على النحو الأتي المطلب الأول : مظاهر التحديات الإجرائية المطلب الثاني : التحديات المتعلقة بسلطة التحري والعقاب المطلب الثالث : التحديات المتعلقة بالقانون الواجب التطبيق

المطلب الأول مظاهر التحديات الإجرائية

تتخذ الصعوبات الإجرائة عدة صور في مجال الجريمة الإلكترونية ، وتتبع تلك الصعوبات من ذاتية الجريمة الإلكترونية وما تتمتع به من سمات تميزها عن غيرها من الجرائم التقليدية ، وطبيعتها الخاصة .

أولا : التحديات المتعلقة بذاتية الجريمة الإلكترونية

تنشأ التحديات من نشأة الجريمة الإلكترونية، حيث تتكاثر الجرائم المرتكبة بواسطة جهاز واحد، مما يؤدي إلى ظهور مظاهر مختلفة من هذه الجرائم:الجريمة المادية : وتتسبب الجريمة في إحداث ضرر مادي للضحية أو المستهدف بالخداع، وتتجلى في أحد الأشكال الثلاثة التالية (حجازي , ٢٠٠٦ : ٩٦).

- السرقة الإلكترونية تتضمن الاستيلاء على ماكينات الصراف الآلي والبنوك في العديد من الدول، حيث يتم نسخ البيانات الإلكترونية لبطاقات الصراف الآلي واستخدامها لاحقًا لأخذ الأموال من حساب الضحية.
- إنشاء ملف شخصي على الإنترنت يشبه إلى حد كبير موقع بنك بارز أو مؤسسة مالية كبيرة.
- رسائل بريد إلكتروني من مصادر غير مألوفة تطلب التبرعات للإفراج عن الأموال الأجنبية من خلال تقديم جزء من الإجمالي، أو تلك التي تضلل المتلقي للاعتقاد بأنه فاز بجائزة أو يانصيب.

الجريمة الثقافة : تتمثل هذه الجريمة في قيام الجاني بالاستيلاء غير المشروع على الحقوق الفكرية والادعاء بأنها ملك له دون موافقة الضحية، وتتجلى في أحد الأشكال التالية (نعيم , ٢٠١٣ : ٣١) :

- قرصنة البرمجيات هي النسخ أو الاستنساخ غير المصرح به للبرمجيات من شركة دولية على أقراص مضغوطة لإعادة بيعها بسعر مخفض.
- اختراق القنوات الفضائية المشفرة ونشرها على الإنترنت باستخدام تقنية "النسخ الناعمة".
- جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة .

الجريمة السياسية والاقتصادية: تستخدم المنظمات الإرهابية حاليًا تكنولوجيا المعلومات لتمكين أنشطتها الإجرامية التقليدية. فهي تستخدم بسهولة أساليب متطورة مثل الاتصالات والتنسيق ونشر المعلومات المضللة واستخدام القاصرين وتقديم الدعم المالي لتحقيق أهدافها. وتتجلى هذه الجريمة في عدة أشكال، بما في ذلك.

– الاستيلاء على المواقع الحرجة، واستخراج المعلومات، وامتلاك القدرة على نشر الفيروسات.

– توضيح المغالطات التي يقع فيها الشباب حول الإرهاب والإدمان والزنا والفساد الحكومي، والتي غالبا ما تكون لأسباب سياسية واقتصادية.

الجريمة الجنسية: وقد تتجلى هذه الفئة من الجرائم في أحد الأشكال التالية:

– الإبتزاز : يتضمن أحد أنواع الابتزاز السائد قيام شاب بالوصول بشكل غير قانوني إلى جهاز فتاة أو الحصول عليه، والذي يحتوي على مجموعة من صورها، وإكراهها على علاقة أو تهديدها بالكشف عن الصور التي يمتلكها.

– التغرير والاستدراج : هذا هو السيناريو المعتاد عندما يتعرف شاب على فتاة عبر تطبيقات الدردشة. يدخل في علاقة معها، ثم يغريها بالوعود اللفظية، فيجعلها تعتقد أنه ينوي الزواج منها، وبالتالي يعزز ثقتها. ثم يرغمها على استخدام الصور والتسجيلات الصوتية التي بحوزته إذا لم تذعن لمطالبه(سليمة , ٢٠١٨ : ٢٥).جرائم الواقعةعلى الأفراد: تتضمن هذه الجرائم الوصول غير المشروع إلى هويات الأشخاص الإلكترونية، بما في ذلك حسابات البريد الإلكتروني وكلمات المرور الخاصة بهم، وقد تشمل أيضًا انتحال الهوية واستخراج صور ومعلومات مهمة من أجهزتهم بقصد إلحاق الأذى بهم. وتشمل هذه الفئة من الجرائم كل ما يلي(نور الدين , ٢٠١٨ : ٢٧٢) :

- جرائم التشهير بهدف تشويه سمعت الأفراد.

-جرائم السب والشتم والقذف.

-جرائم المطاردة الالكترونية .

ثانيًا : صعوبات مكافحة الجريمة الناتجة عن طبيعتها الإلكترونية لقد أدت ظاهرة الجرائم الإلكترونية إلى ظهور العديد من التحديات، بما في ذلك انتشار الأنشطة الإجرامية الإلكترونية واستخدام التقنيات الحديثة من قبل المجرمين في مجال تكنولوجيا المعلومات والاتصالات. وقد سهل هذا التقدم تنفيذ مثل هذه الأنشطة على المستويين المحلي والدولي، مما دفع المنظمات والمؤتمرات الدولية إلى التركيز على هذه الجريمة وحث الدول على معالجتها ومكافحتها. وتفلت بعض الأنشطة من التصنيفات الجنائية التقليدية في الأطر القانونية الوطنية والدولية، في حين يبدو نظام الملاحقة الإجرائية غير كافٍ لاستيعاب هذه الظاهرة الإجرامية الناشئة، مما يؤثر على جهود الملاحقة الجنائية الوطنية والدولية من أهم التحديات التى تواجه الجريمة الإلكترونية تلك الصعوبة الناتجة عن طبيعتها الإلكترونية ، فيعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية، وذلك للأسباب التالية(الطائي ,٢٠٠٧ : ٢٢٠):

– يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.

– صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام إسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.

– تنازع القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين سوف يخضع لها الجاني؟.

– التحدي المتمثل في تحديد المسؤولية الجنائية عن السلوك الإجرامي، كما هو الحال عندما يدخل أحد الأفراد إلى موقع ويب ويصادف محتوى إباحي. هل يجب استشارة مشغل الاتصالات أو مزود الموانئ أو مزود المعلومات أو أصحاب المصلحة الآخرين في قطاع الإنترنت بشأن هذه الجريمة؟.

المطلب الثاني التحديات المتعلقة بسلطة التحري والعقاب

يتعرض التحقيق والبحث والتحري في الجرائم المعموماتية للعديد من العراقيل والصعوبات التي تعيق الوصول للحقيقة وإثباتها نسبتها لمرتكبيها ، مما يسجل عجز جهات التحقيق عن مواجية الإجرام المعموماتي التصدي لها ، إما بسبب الطبيعة الخاصة للإجرام العملوماتي و الجهات المتضررة ، أو معوقات خاصة بجهات التحقيق ، وأخرى تشريعية :

أولاً : الصعوبات الخاصة بالجهات المتضررة

بالنسبة للصعوبات المتعلقة بالجهات المتضررة فتمثل في النقاط التالية :

١– عدم إدراك مسؤولي المؤسسات لخطورة الجرائم المعلوماتية التي تهدد كيانها كونها تستخدم النظام المعلوماتي لتقديم خدماتها لعملائها بشكل أسرع(الشدي ,١٤٢٣ : ٢١٠) .

٢– إحجام المتضررين من الجريمة المعموماتية من أفراد و مؤسسات عن الإبلاغ عنها ، إما لعدم علمهم بها أصلا أو خوفا من الفضيحة أو الظهور بمظهر مشين أمام الآخرين ، و يعطي انطباعا بقمة خبرة هذه المؤسسات و عدم اتخاذها إجراءات الحماية الأمنية لأنظمتها المعموماتية وتقرر تفضيل سمعة المؤسسة و مصداقيتها على الإبلاغ عنها(الحلبي , ٢٠١١ : ٢٢٥).

يستطيع الجاني أن يتخلص بسرعة من الأدلة ضده أو يمحوها، مما يعوق قدرة السلطات على كشف الجريمة إذا علمت بها. وفي هذا السيناريو، يسعى الجاني إلى التخلص بسرعة من الأدلة التي تدينه، وبالتالي منع السلطات من إثبات قضيتها والتهرب من المساءلة عن أفعاله، ونسب الحادث بدلاً من ذلك إلى عطل في نظام الكمبيوتر أو الشبكة أو الأجهزة.إن عدم قدرة المسؤولين في المؤسسات المتضررة على الاعتراف بخطورة

الجرائم الإلكترونية يشكل عائقاً كبيراً أمام التحقيقات. فضلاً عن ذلك فإن تجاهل تثقيف المستخدمين فيما يتصل بخطورة الجرائم المرتبطة بالإنترنت، إلى جانب المنافسة بين الشركات الرامية إلى تبسيط العمليات وتعزيز قابلية استخدام البرمجيات والأجهزة وملحقاتها، ينتقص من التركيز على التدابير الأمنية لصالح تقديم الخدمات. ويؤدي هذا إلى التردد في الإبلاغ عن الجرائم، التي تعتبر قضية مهمة وخطيرة في عملية الإبلاغ عن الجرائم الإلكترونية، حيث يمتنع الأفراد في كثير من الأحيان عن إخطار السلطات المختصة بالجرائم المرتكبة ضدهم، وخاصة عندما يتعلق الأمر بمؤسسات مالية أو كيانات مماثلة (جفال , ٢٠١٦ : ٤٣) .

ثانيًا : صعوبات تتعلق بالجهات القائم بالتحقيق

إن التحقيق في الجرائم الإلكترونية محفوف بالعديد من التحديات التي تعيق العملية، مما يؤدي إلى عواقب نفسية على المحقق، الذي قد يعاني من انخفاض الثقة بنفسه، كما قد يفقد المجتمع الثقة في وكالات إنفاذ القانون التي تفشل في الحماية من هذه الجرائم ومحاسبة الجناة.

1–قلة خبرة القائمين بالتحقيق في هذه الجرائم إن الافتقار إلى الخبرة الفنية اللازمة للتحقيق في هذه الفئة من الجرائم، إلى جانب عدم إتقان استخدام الكمبيوتر والإنترنت، وعدم الفهم الكافي لمنهجيات الجرائم الإلكترونية، والافتقار إلى الخبرة التحقيقية في جرائم الكمبيوتر والإنترنت، والمعرفة المحدودة باللغات الأجنبية . وخاصة وأن المحترفين في مجال الكمبيوتر يستخدمون مصطلحات متخصصة تميز تواصلهم وفهمهم . يعوق التحقيق الفعال. وعلاوة على ذلك، قام المحترفون في هذا المجال بتكثيف المصطلحات في اختصارات، مما أدى إلى ظهور لهجة غريبة يشار إليها بلغة الاختصارات.

٢– الصعوبات التقنية لإستخدام بروتوكول TCP / IP في الإثبات (١)

هناك تحديات عند استخدام المحقق بروتوكول TCP / IP ، كدليل إلكتروني للإثبات وهي(الحلبي , ٢٠١١ : ٢٢٦):

- بروتوكول IP هو وحدة معلوماتية تخص الكمبيوتر وليس الأفراد، مما يجعل من الصعب إثبات أن شخصًا معينًا ارتكب السلوك غير المشروع. ومع ذلك، قد يعمل هذا البروتوكول بمثابة افتراض قانوني ضد مالك الجهاز ما لم يتم دحضه.

- يستخدم الجاني عناوين ومعلومات خاطئة أو غير مشروعة عبر جهاز الكمبيوتر الشخصي الخاص به داخل ملف خدمات عامة للتهرب من تحديد الهوية. ويستخدم عنوان IP مشتركًا بين العديد من المستخدمين، ثم ينهي الاتصال ثم يعيد الاتصال، وبالتالي ينشر النشاط الإجرامي عبر عدة عناوين.

- يتم نقل المعلومات إلى عنوان المصدر، مما يخلق الوهم بأنها نشأت من جهاز IP بعنوان مصدر مزيف، في حين أنها في الواقع نشأت من جهاز كمبيوتر مختلف.

٣– أرتفاع تكاليف جمع الدلة إن التحقيق في هذه الجرائم يتطلب خبرة متخصصة، تتطلب تدريبًا مستمرًا يتماشى مع التطورات في التكنولوجيا الإلكترونية. وهذا يستلزم نفقات باهظة، ويتطلب البحث عن الأدلة التدقيق في آلاف الصفحات، وخاصة عندما لا تسفر هذه الصفحات عن نتائج قاطعة.

٤– إن النقص في الأدوات والبرمجيات المعاصرة لكشف الجرائم الإلكترونية والقبض على مرتكبيها يفرض الاعتماد على وحدات تحقيق متخصصة من محققين قضائيين وخبراء فنيين متخصصين في تكنولوجيا المعلومات وتطوراتها(مبارك , ٢٠١٤ : ٣٦١).

ثالثا : الصعوبات التشريعية

لقد أدى تقدم العلم في قطاع المعلومات إلى ظهور جرائم معلوماتية جديدة وتطور مظاهرها، كما أدى ركود النصوص التشريعية في معالجة هذه القضايا إلى تقييد تصنيف هذه الجرائم وتحديد عناصرها ووضع العقوبات المناسبة، مما أدى إلى خلق العديد من التحديات القانونية. فالقاضي الجنائي مقيد بمبدأ الشرعية فيما يتعلق بالجرائم والعقوبات القانونية الموضوعية، مما يمنعه من تجريم أفعال لم يحددها المشرع صراحة، بغض النظر عن ضررها أو خطورتها المحتملة وكذا حصر القياس في النصوص الجزائية الموضوعية .

المطلب الثالث التحديات المتعلقة بالقانون الواجب التطبيق

في حين يزعم البعض أن القوانين الحالية تعالج الجرائم الإلكترونية بشكل مناسب، فإننا نؤكد أنه على الرغم من أن بعض القوانين الحالية قد تعالج أنشطة إجرامية محددة عبر الإنترنت، فمن غير الممكن أن ننكر أن لوائح أخرى تواجه تحديات كبيرة في التنفيذ.

أولا :عدم وجود أتفاق حول طبيعة النشاط الإجرامي ولم تتوصل الأنظمة القانونية في العديد من الدول إلى توافق بشأن إطار موحد للجرائم الإلكترونية، وبالتالي فإن الأفعال التي تعتبر جنائية في بعض الولايات القضائية قد لا تعتبر كذلك في ولايات أخرى(حجازي , ٢٠٠٦ : ١٨٨).

فعدم الاتفاق على صور الإجرام المعلوماتي جعل من البيئة الالكترونية فضاءًا لقراصنة الحاسب الآلي لارتكاب جرائمهم العابرة للحدود.

ثانيا :اختلاف النظم القانونية في تحديد مكان الجريمة الإلكترونية

وقد يؤدي هذا التفاوت إلى أن تكون إجراءات التحقيق والاستجواب والمقاضاة التي تكون فعّالة في دولة ما غير فعّالة أو غير مقبولة إجرائياً في دولة أخرى، كما يتضح من المراقبة الإلكترونية. وعلاوة على ذلك، قد تحظر دولة ما استخدام الأدلة التي تم الحصول عليها باستخدام أساليب تعتبرها الدولة الأخرى غير قانونية أو انتهاكاً للحريات الشخصيةغالبًا ما يحكم اختصاص القانون الجنائي الوطني أحد المبادئ الأربعة التالية: الإقليمية، أو الشخصية، أو الموضوعية، أو العالمية. وتختلف أهمية هذه المبادئ فيما بينها، ويتم ترتيب قيمتها وفقًا لتسلسلها. تستخدم معظم القوانين الجنائية مفهوم الإقليمية كمبدأ أساسي، ثم تعززه بعناصر أخرى.إن تنفيذ التطبيق الإقليمي للقانون الجنائي، وفقاً لأحد المبادئ الأربعة المذكورة آنفاً، محفوف بالتحديات. وقد تؤدي هذه التحديات إلى تضارب إيجابي في الاختصاص بين التشريعات الوطنية المتعددة، أو بدلاً من ذلك، تضارب سلبي في الاختصاص، مما يمنع أي دولة من مقاضاة الجاني. ونادراً ما ينشأ هذا النوع الأخير من الخلاف عندما تحدد التشريعات الوطنية سلطتها على أساس معايير ثابتة [٢] ؛ في حالات الصراعات القضائية المتزامنة بين دول متعددة تلاحق نفس الجريمة الجنائية، أو في الحالات التي تنطوي على جرائم عابرة للحدود الوطنية حيث ينتشر السلوك الإجرامي عبر عدة أقاليم، أو عندما تفقد جوانب معينة من هذا السلوك خصائصها الملموسة، كما هو الحال في القرصنة الإلكترونية وأشكال المشاركة الإجرامية التي تيسرها تكنولوجيات الاتصال المعاصرة؛ فإن مثل هذه الظواهر تتطلب صراعاً قضائياً وتؤدي إلى غموض في وضع المعايير، وبالتالي تتطلب حلولاً مبتكرة وتطوير مفاهيم قانونية جديدة، كل ذلك مع الحفاظ على مبادئ الشرعية الجنائية الأساسية لمعظم الأنظمة القانونية الوطنية.

ثالثا :التجريم المزدوج

تشكل الجريمة المزدوجة شرطًا أساسيًا حاسمًا لتسليم المجرمين، مما قد يعيق التعاون الدولي في تسليم الأفراد المتورطين في الجرائم الإلكترونية، خاصة وأن العديد من الدول لا تزال تفتقر إلى الأحكام القانونية التي تعالج هذه الظاهرة الإجرامية.إن المصلحة الجماعية للدول تتطلب استكشاف الأساليب اللازمة للتغلب على هذه التحديات وإقامة تعاون دولي حقيقي يتماشى مع خصائص هذا النوع الجديد من الجريمة، ويضمن التوحيد بين الأنظمة القانونية الجزائية المحلية (نعيم , ٢٠١٨ : ٩٥)وقد أدركت البلدان أهمية التعاون الدولي واعتبرته أمرا ضروريا لمعالجة القضايا التي تفرضها الجرائم الإلكترونية، مما دفع العديد منها إلى إبرام اتفاقيات ثنائية لتبسيط التحقيق في هذه الجرائم(البشري , ١٠٨٧) ، في عام ١٩٨٣، أجرت منظمة التعاون الاقتصادي والتنمية دراسة لاستكشاف جدوى تنفيذ القوانين الجنائية الوطنية وتعديل أحكامها لمعالجة القضايا التي تفرضها الجرائم الإلكترونية واستغلالها. وفي عام ١٩٨٥، نشرت هذه المجموعة ورقة تحدد الحد الأدنى من الأفعال المتعلقة بإساءة استخدام الكمبيوتر والتي يجب على الدول حظرها ومعاقبتها في تشريعاتها. ومن أمثلة هذه الأفعال: الاحتيال أو التزوير باستخدام الكمبيوتر، وتغيير برامج الكمبيوتر أو المعلومات المخزنة، وسرقة البيانات السرية من قواعد بيانات الكمبيوتر، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية. كما تناولت اتفاقية فيينا لعام ١٩٨٨ هذه القضية وطلبت من العديد من الدول إبرام اتفاقيات ثنائية للمساعدة في التحقيق في هذه الجرائم. وأبرز الاجتماع التمهيدي الإقليمي لعام ١٩٨٩ لآسيا والمحيط الهادئ، والذي سهل انعقاد المؤتمر الثامن للأمم المتحدة في كوريا عام ١٩٩٠، نتائج التقدم التكنولوجي والتقدم فيما يتعلق بالجرائم الإلكترونية، ودعا إلى تعزيز التعاون الدولي لمعالجة هذه القضية. وحث المؤتمر الأخير، في قراره بشأن الجرائم المتعلقة بالكمبيوتر، الدول الأعضاء على تعزيز جهودها لمعالجة الجرائم الإلكترونية عبر عدة أبعاد(عوض , ١٩٩٣ : ٣٦٢).

الخاتمة

تعتبر الجرائم الإلكترونية جرائم جديدة نسبيا وتحتاج إلى بحوث مستقبلية لوضع قواعد شاملة تنطبق على كافة الجرائم المرتبطة بالتطورات الإلكترونية والمعلوماتية ووسائل الاتصال المعاصرة. وهذا يتطلب اتخاذ إجراءات تشريعية لتوفير الحماية القانونية الكاملة وإزالة أي ثغرات في القوانين الجنائية الحالية، وضمان مواكبتها للتطورات في تكنولوجيا المعلومات.وقد ارتبط هذا التطور بارتفاع معدلات الجرائم الإلكترونية الناجمة عن سوء استخدام تكنولوجيا المعلومات وأجهزة الكمبيوتر، مما أدى إلى أضرار واسعة النطاق تعرض أمن البيانات للخطر وتنتهك حريات الأفراد والمؤسسات.وتواجه هذه الجرائم العديد من التحديات في سبيل مواجهتها ، فهناك التحديات الإجرائية والتحديات المتعلقة بالتحري والعقاب والتحديات الخاصة بالقانون الواجب التطبيق .

النتائج

- أن مفهوم الجريمة الإلكترونية يعنى كل فعل إجرامي متعمّد أيًا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.

- إن الجريمة الإلكترونية لها بعد تكنولوجي وفني وأخلاقي غير محسوس ولا يمكن إدراكه بالحواس التقليدية، ويتطلب إدراكها الاستعانة بتقنيات وأجهزة وتقنيات الكمبيوتر.

- إن عملية مكافحة الجريمة الإلكترونية تقابلها عدة صعوبات ترجع إلى حدثة مثل هذا النوع من الجرائم ، والتى تتطلب مكافحتها تضافر الجهود الدولية وإجراء تعديلات تشريعة تتناسب مع طبيعتها .

التوصيات

- ندعو إلى وضع لوائح جديدة للتعامل مع الجرائم الإلكترونية، مع الأخذ في الاعتبار الخصائص الفريدة لهذه الجرائم، وخاصة فيما يتعلق بالأدلة في الإجراءات القانونية، سواء كانت جنائية أو مدنية أو تأديبية. ولابد من مراجعة اللوائح التي تحكم الإجراءات الجنائية لاستيعاب هذه الجرائم.

- ندعو إلى التنسيق والتعاون القضائي والإجرائي الدولي في مجال مكافحة الجرائم الإلكترونية.

- ندعو إلى إنشاء وحدة شرطة متخصصة للتعامل مع الجرائم الإلكترونية، تضم رجال شرطة ماهرين في التعامل مع الكمبيوتر والإنترنت.

- نوصي بتدريب وتحديث رجال الادعاء العام أو النيابة لعامة والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت .

المراجع

الكتب

أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة ، دار الثقافة للنشر و التوزيع ، عمان ، ٢٠١٤

د. جعفر حسن الطائي،جرائم تكنولوجيا المعلومات ، رواية جديدة للجريمة الحديثة،ط ١،جامعة عمر المختار، ٢٠٠٧

د. حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤

خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، ٢٠١١

د. خليفة محمد،الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية ، ص

د. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013

د. طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية ، مصر، ٢٠٠٩

د. طارق عبدالله الشدي ، آلية البناء لنظم المعلومات ، دار الوطن للطباعة والنشر ، الرياض ، ١٤٢٣ هـ

د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن دار الجامعة الجديدة،الإسكندرية، ٢٠١٠

د. عبد الفتاح بيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006

د. عفيفي كامل ،جرائم الكمبيوتر و حقوق المِؤلف والمصنفات الفنية و دور الشرطة و القانون"دراسة مقارنة"، منشورات الحلبي الحقوقية ،الإسكندرية، ٢٠٠٧

عنية باطلي الجريمة الإلكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، ٢٠١٥

د. نواوي سليمة ، دور الدرك الوطنى في محاربة الجريمة الإلكترونية ، جامعة المسيلة ، ٢٠١٨

د. هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، بدون سنة نشر

يوسف جفال، التحقيق في الجرايمة الإلكترونية ، بدون ناشر ، ٢٠١٦

الرسائل

سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة للماجيستير ، جامعة مولود معمري ، الجزائر ، ٢٠١٨

الدوريات

د. بن سولة نور الدين، الجرائم الالكترونية في ضوء التشريع الجزائري، مجلة الحوار المتوسطى، المجلد التاسع، العدد1 ، مارس2018

المؤتمرات

د.محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة منن ١ – ٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات

د. محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ٢٥ –٢٨ أكتوبر ، ١٩٩٣

هوامش البحث

(١) هو اختصار لكلمة Transmission Control Protocol بروتوكول التحكم في نقل البيلنات وكلمة Internet protocol وبرتوكول TCP/IP

هو العصب المحرك للانترنت يضم مجموعة بروتوكولات مطورة كطريق للتواصل بين مختلف أنواع الحواسيب

(٢) الأمر يدق بالنسبة لجريمة غسيل الأموال أو استخدام عائدات الأنشطة الإجرامية غير المشروعة في الدول التي تجرم تشريعاتها هذا النشاط على أساس أنه فعل من أفعال الاشتراك أو كصورة من صور الإخفاء وليس بوصفه جريمة مستقلة ، وفي الحالتين نكون بصدد جريمة تبعية يتبع الاختصاص بملاحقتها الجريمة الأصلية ، وبالتالي يخرج عن اختصاص إحدى تلك الدول ملاحقة مرتكب جريمة غسيل الأموال ، خاصة إذا كان المتهم لا يتمتع بجنسيتها؛ إذن للتغلب على هذا النوع من التنازع السلبي في الاختصاص يتعين تقرير مبدأ الاختصاص العالمي الذي يعطي لدولة القبض على المتهم الاختصاص بملاحقته إذ كان يحمل جنسيتها ، فإن لم يمكن كذلك ، وجب تسليمه في حالة المطالبة به من دولة أخرى وفقا لمبدأ الإقليمية أو الشخصية

References

Books

Osama Ahmed Al-Manasa, Jalal Mohammed Al-Zoubi, Electronic Information Systems Technology Crimes, Third Edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2014

Dr. Jaafar Hassan Al-Taie, Information Technology Crimes, A New Novel of the Modern Crime, 1st Edition, Omar Al-Mukhtar University, 2007

Dr. Hanan Rayhan Mubarak Al-Madhhaki, Information Crimes, First Edition, Al-Halabi Legal Publications, Beirut, 2014

Khaled Ayyad Al-Halabi, Investigation and Procedures in Computer and Internet Crimes, First Edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2011

Dr. Khalifa Mohammed, Criminal Protection of Computer Data in Algerian and Comparative Law, Dar Al-Jamiah Al-Jadida, Alexandria, p.

Dr. Saeedani Naeem, Research and Investigation Mechanisms for Information Crime in Algerian Law, 2013

Dr. Tariq Ibrahim Al-Desouky Attia, Information Security The Legal System for Information Protection, Dar Al-Jamia Al-Jadida, Alexandria, Egypt, 2009

Dr. Tariq Abdullah Al-Shadi, The Mechanism of Building Information Systems, Dar Al-Watan for Printing and Publishing, Riyadh, 1423 AH

Dr. Aisha Bin Qara Mustafa, The Authority of Electronic Evidence in the Field of Criminal Evidence in Algerian Law and Comparative Law, Dar Al-Jamia Al-Jadida, Alexandria, 2010

Dr. Abdel Fattah Bayoumi Hijazi, Combating Internet Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, First Edition, 2006

Dr. Afifi Kamel, Computer Crimes, Copyright and Artistic Works, and the Role of the Police and the Law "A Comparative Study", Al-Halabi Legal Publications, Alexandria, 2007

Aniya Batali, Electronic Crime "A Comparative Study", Algerian House for Publishing and Distribution, Algeria, 2015

Dr. Nawawi Salma, The Role of the National Gendarmerie in Combating Cybercrime, University of M'Sila, 2018

Dr. Hoda Hamed Qashqoush, Computer Crimes in Comparative Legislation, Dar Al Nahda Al Arabiya, Cairo, no year of publication

Youssef Jaffal, Investigation into Cybercrime, no publisher, 2016