PERDANA
INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH
eISSN: 2600-9463

CYBERCRIME: A COMPARATIVE STUDY

الجريمة الإلكترونية: دراسة مقارنة

Ashraf Abdelkader Kandel[1]

[1] Associate Professor, Sharjah Police Academy, United Arab Emirates. ashrafabdelkader145@gmail.com

Vol. 9. No. 1
December Issue
2020

Abstract

This research aims to identify what cybercrime is, reveal its characteristics, identify the traditional and modern methods used to prove the crime and to prove the authenticity and legitimacy of the electronic evidence, its authority before the judge and his appreciation of the evidence. There are many problems related to cybercrime - what means are used to prove it? Are traditional procedural rules sufficient to control and inspect electronic evidence, so that it has the evidentiary power and therefore has an authority to the judge? The descriptive analitical approach will be used to be exposed to a number of terms when dealing with the inspection of the information system, in addition to the comparative method so that the researcher can address the global nature of cybercrime. The results of the studi indicated the need to develop criminal evidence methods in order to deal with cybercrime. The studi also demonstrated that the evidentiary mechanisms in cybercrime are the same as those of committing the crime, and that the methods of criminal evidence reli primarili on modern science, provided that the facts are based on scientific law or scientific theory.

Keywords: *Cybercrime, Characteristics, Electronic, Evidence, Authority*.

ملخص البحث

هدف هذا البحث إلى التعرف على ماهية الجريمة الإلكترونية، والكشف عن خصائصها، والوقوف على الوسائل التقليدية والحديثة التي يتم استخدامها لإثبات الجريمة ولإثبات صحة ومشروعية الدليل الإلكتروني، وحجيته أمام القاضي وتقديره للدليل، وهناك العديد من الإشكاليات التي تتعلق بالجريمة الإلكترونية – ما هي الوسائل المستخدمة لإثبات وقوعها؟ وهل تعد القواعد الإجرائية التقليدية كافية لضبط وتفتيش الأدلة الإلكترونية حتى تمتلك القوة الثبوتية وبالتالي يكون لها حجية لدى القاضي؟، وسيتم استخدام المنهج التحليلي الوصفي للتعرض إلى عدد من المصطلحات عند تناول تفتيش النظام المعلوماتي، بالإضافة إلى المنهج المقارن حتى

يتمكن الباحث من تناول الطبيعة العالمية للجريمة الإلكترونية، وقد جاءت نتائج الدراسة لتشير إلى ضرورة تطوير آليات الإثبات الجنائي حتى تتم مواجهة الجرائم الإلكترونية، كما أثبتت الدراسة أن آليات الإثبات في الجريمة الإلكترونية هي نفس آليات ارتكابها، كما أن آليات الإثبات الجنائي تعتمد في الأساس على العلوم الحديثة، بشرط أن تكون الحقائق مستندة على قانون علمي أو إلى نظرية علمية.

الكلمات المفتاحية: الجريمة الإلكترونية، الخصائص، الإلكتروني، الحجية، القاضي.

مقدمة

إن الجريمة الإلكترونية هي أحد أنواع الجرائم المستحدثة نظرًا لارتباطها بمجال تكنولوجيا المعلومات والاتصالات، ويتم ارتكاب هذا النوع من الجرائم بشكل أساسي من خلال أجهزة الحاسوب وملحقاته، بالإضافة إلى اعتمادها على مختلف الأجهزة التقنية المتطورة الحديثة أو التي ستظهر في المستقبل.

ومن الجدير بالذكر أن مصطلح الجريمة الإلكترونية يشوبه الغموض، حيث كانت هناك العديد من المحاولات لوضع تعريف جامع له، ولكن لم يوفق أي منها بالتوصل إلى التعريف الشامل له، فقد رأى البعض أن الجريمة الإلكترونية هي نفس الجريمة التقليدية ولكنها ترتكب من خلال وسائل متطورة.

ولذلك ذهبوا إلى عدم وضع تعريف محدد للجريمة الإلكترونية، فيمكن القول أن الجريمة الإلكترونية هي الصورة المتطورة من الجريمة التقليدية، ولذلك فإنه من الصعب مواجهتها والتعامل معها.

وقد واجه المتخصصون في هذا المجال مشكلة فيما يتعلق بمواجهة هذا النوع من الجرائم لتعلقها بالبيانات والمعلومات، أي بيئتها الالكترونية، الأمر الذي ميزها بشكل كبير عن غيرها من الجرائم التقليدية، وذلك لكون أساليب ارتكابها غير تقليدية.

وبالنظر إلى الحاجة إلى تواجد الدليل الإلكتروني كدليل لإثبات وقوع الجريمة ولنسبتها إلى مرتكبها، أصبح من الضروري أن يتم استخلاصه من البيئة الإلكترونية، من خلال البيئة أو الموقع الذي ارتكبت من خلاله الجريمة الإلكترونية، حيث أنها تعد ظاهرة مستحدثة بشكل نسبي مما جعلها تختلف عن غيرها من الجرائم التقليدية.

وبالنظر إلى أن الوسائل التكنولوجية والتقنيات الرقمية تستخدم بشكل كبير من قبل الأفراد في العالم أجمع، أدى ذلك إلى انتشار الجرائم الإلكترونية بشكل كبير في الآونة الأخيرة، فمنذ بداية الالفية الثانية وهي في تنامي وتطور مستمر تقوم باستهداف جميع الأفراد والجماعات والمنشآت والبلدان، وخاصة مما ليست لديهم معرفة كافية بتلك التطورات التكنولوجية، الأمر

الذي تطلب وضع قوانين تختص بالجوانب الإجرائية أكثر منها في الجوانب الموضوعية.

الهدف من البحث

تهدف الدراسة موضوع البحث إلى معرفة الجريمة الالكترونية وخصائصها، والوسائل التقليدية والحديثة لإثباتها وما ينتج عنها من مشروعية الدليل الالكتروني، وحجيته أمام القاضي الجنائي، وذلك بهدف التوصل إلى الضوابط التي يلتزم بها القاضي لوزن وتقدير الدليل الجنائي (الرقمي)، والذي يتم استخلاصه من مسرح الجريمة الإلكترونية.

إشكالية البحث

إن لسلطة القاضي الجنائي التقديرية دورًا هامًا، حيث أنه يعد دورًا مكملًا للعدالة الجنائية، يرجع ذلك إلى أهمية الدور الذي يلعبه مبدأ حرية الإثبات في عملية التأثير على القاضي الجنائي، ولذلك فإن هناك العديد من الإشكاليات التي تحيط بحداثة الجريمة الإلكترونية، ومنها ما يلي:

- ما هي الوسائل التقليدية والحديثة التي يمكن من خلالها إثبات الجريمة الآليكترونية؟
- هل تعد القواعد الاجرائية التقليدية كافة لضبط وتفتيش أدلة الجرائم الالكترونية؟
- ماهية القوة التدليلية للأدلة الإلكترونية التي يعتمد عليها القاضي في اثبات الجريمة الالكترونية؟
- ماهي الشروط اللازمة لقبول الدليل الالكتروني؟
- مدي اقتناع القاضي بالدليل ووزنه بقوته الثبوتية العلمية القاطعة أو المرجحة؟

منهج البحث

تعتمد الدراسة على المنهج التحليلي الوصفي الذي يمكن من خلاله التعرض لعدد من المصطلحات، على سبيل المثال عند تناول تفتيش النظام المعلوماتي، بالإضافة إلى المنهج المقارن نظرًا لطبيعة الجرائم الإلكترونية العالمية، حيث سيتم من خلال هذا البحث المقارنة بين التشريعات الفرنسية والعربية التي تتمثل في كل من التشريع المصري والإماراتي.

المبحث الاول: الجريمة الإلكترونية ماهيتها خصائصها

لقد ظهرت العديد من المحاولات لوضع تعريف واضح ومحدد يتم من خلاله التعرف على معالم الجريمة الإلكترونية في مختلف المجالات، ولذلك ظهرت العديد من الآراء فيما يتعلق بتعريف الجريمة الإلكترونية، حيث تبنى كل منهم مفهومًا خاصًا.

المطلب الاول: ماهية الجريمة الإلكترونية

لم يتفق الباحثون في مجال الجرائم الإلكترونية على تبني مصطلح بعينه للجرائم الناشئة من البيئة الإلكترونية، سواء أكان ذلك على المستوى الفقهي أو التشريعي، ويرجع التحديث والتطوير في مجال الجريمة المستحدثة للتطور الكبير في مجال التقنيات الإلكترونية والاتصالات.

ولذلك ظهرت العديد من المصطلحات، ففي بعض الأحيان يطلق عليها الجرائم الالكترونية، وأحيانًا أخرى تسمى بالجرائم المعلوماتية، وهو السبب في الصعوبة التي يواجهها

المشرع لوضع نص تشريعي يمكن من خلاله تجميع النماذج التجريمية الالكترونية.

الفرع الأول: ماهية الجريمة الالكترونية فنيًا وتقنيًا

لقد قام البعض بتعريف الجريمة الإلكترونية بكونها جميع الأفعال والامتناع عن الأفعال التي تتعدى على العناصر المادية والمعنوية للحاسب الآلي، ويجب أن تكون تلك الأفعال لها صلة مباشرة أو غير مباشرة بالتقنيات الحديثة (محمد، ٢٠١٦).

وبالنظر إلى ذلك التعريف فإن جوهر الجريمة يكمن في مكونات الحاسب الآلي المادية (harduare) التي تشمل الماوس والشاشة وما على ذلك، والمكونات المعنوية (software) مثل البرمجيات والنظم، ومن هنا نستنتج أن ارتكاب هذا النوع من الجرائم يعتمد بشكل أساسي على توافر جهاز الحاسوب.

أما بالنسبة للجانب الفقهي، فقد قام بتعريف الجريمة الإلكترونية بكونها نشاط من الأنشطة الإجرامية التي تستعمل التقنيات الحديثة بشكل مباشر أو غير مباشر للوصول لغايات تتمثل في السلوك الإجرامي.

وهنا نجد أن هذا التعريف قد اعتمد على الجانب الفني والتقني للجريمة الإلكترونية، وذلك دون التعرض إلى الجانب القانوني لها، ويتفرع من هذا التعريف ثلاث تعريفات هي كالآتي:

تعريف الجريمة الإلكترونية وفقًا للصفات الشخصية للمجرم (المجرم المعلوماتي)

يعتمد هذا التعريف على تحديد أنواع المجرمين الذين يرتكبون جرائم الانترنت، ويعتمد أصحاب هذا التعريف على بعض الجوانب الشخصية المتمثلة في أن يكون الجاني على دراية بالتقنيات الحديثة واستعمال الحاسب الآلي (راجح، ٢٠١١)، ووفقًا لمن التزموا بالتعريف التقني فإن الجريمة الإلكترونية عبارة عن جريمة يتم استعمال التقنيات الحديثة في تنفيذها سواء بشكل مباشر أو بشكل غير مباشر.

وقد اتجه أصحاب الاتجاه الفقهي إلى تعريف جرائم الحاسب الآلي قانونيًا، حيث يجب الوصول للمفردات التي تختص بالجريمة مثل الحاسب الآلي والأنظمة التي تشغله ووحدات الدخول، والخدمات، وما إلى ذلك.

ويعترض البعض على هذا التعريف، ويرجع هذا الاعتراض إلى اهتمامه بالفعل الإجرامي كعامل أساسي، وتجاهل العديد من العوامل الأخرى التي تختص بالجريمة الإلكترونية والأدلة التي تشملها.

تعريف الجريمة الآليكترونية وفقًا لوسائل تنفيذ الجريمة

وتعرف الجريمة الآليكترونية أيضًا وفقًا للوسائل التي يتم استعمالها لتنفيذ الجريمة، بأنها الجريمة التي يتم استعمال أجهزة الحاسب الآلي في ارتكابها، وذلك العامل الأساسي في وجود الجريمة، ووفقًا لذلك فقد عرف "جون فوستر" الجريمة الإلكترونية بأنها أفعال إجرامية يتم استعمال أجهزة الحاسب الآلي لتنفيذها باعتبارها أداة للجريمة، كما عرف مكتب التقنية في الولايات المتحدة الامريكية الجريمة

الإلكترونية بأنها كل الأفعال الإجرامية التي يستعمل المجرمين لتنفيذها البيانات المحفوظة على أجهزة الحاسب الآلي.

ويمكن تعريف الجريمة الإلكترونية بأنها جميع جوانب السلوك غير المشروع الذي يتم تنفيذه عن طريق الحاسب الآلي، ويستعمل المجرمون برامج حديثة وتقنيات مختلفة لتنفيذ تلك الجرائم.

تعريف الجريمة الآليكترونية وفقًا لموضوع الجريمة

تعرف الجريمة الإلكترونية وفقًا للموضوع الخاص بالجريمة بأنها الجرائم التي يدخل في ارتكابها استعمال العديد من الأنظمة المعقدة والتقنيات الحديثة وتزوير البيانات للوصول لقواعد بيانات.

واعتمدت قرارات الأمم المتحدة هذا الاتجاه، حيث قامت بتعريف الجريمة الإلكترونية بأنها سلوكيات غير مشروعة يتم تنفيذها عن طريق عمليات إلكترونية مختلفة من شأنها المساس بأمن الأنظمة المعلوماتية وكل ما يتعلق بها من مواضيع تلك الأنظمة على معالجتها.

الفرع الثاني: تعريف الجريمة الآليكترونية قانونيًا

لقد ذهب البعض إلى أنه يمكن تعريف الجريمة المعلوماتية على أنها "القيام بعمل أو الامتناع عنه وإحداث أضرار عن طريق برامج الحاسب الآلي وبرامج الاتصال المختلفة، ويفرض قانون العقوبات عقوبات على ذلك".

كما يذهب بعض الآراء إلى تعريف الجريمة الإلكترونية بأنها مجموعة من النشاطات التي يعاقب عليها القانون ويمكن إطلاق لفظ فعل إجرامي عليها، وتقع تلك الأفعال في نطاق الثورة التكنولوجية، كما تعرف بأنها الأنشطة الجنائية التي تشكل انتهاك للحقوق باستعمال الحاسب الآلي.

وهناك رأي آخر يذهب إلى تعريف الجريمة الإلكترونية بأنها انتهاكات للقوانين من خلال شبكات المعلومات للوصول لأرباح مادية.

موقف المشرع المصري

في عام ٢٠١٨م، قامت جمهورية مصر العربية بإصدار القانون رقم ١٧٥ المتعلق بمكافحة جرائم تقنية المعلومات، والغرض منه التصدي للجرائم التي يتم ارتكابها من خلال تكنولوجيا المعلومات والاتصالات.

وقد جاءت المادة الأولى من هذا القانون لتعريف مفهوم المعالجة الإلكترونية، بحيث عرفته على أنه: جميع العمليات الإلكترونية والتقنية سواء بشكل جزئي أو كلي، وذلك عن طريق استخدام تلك الوسائل لتسجيل، أو تجميع، أو تخزين، أو دمج، أو إرسال، أو عرض، أو تداول، أو نشر، أو محو، أو تعديل البيانات، أو المعلومات المختلفة في الأجهزة الحديثة، وذلك من خلال مجموعة من الوسائط والأجهزة الإلكترونية والضوئية والمغناطيسية، أو ما يستحدث من تقنيات أو وسائط أخرى.

ويتصدى القانون للجرائم التي تهدد الحياة الخاصة للأفراد وتهدد شرف الفرد وسمعته، كما تستعمل تلك الجرائم في تهديد الأمن القومي للدول، وذلك يشمل بعض الجرائم التي يتم تنفيذها من خلال البطاقات الائتمانية والدفع الإلكتروني.

وقد حدد القانون مواد لمواجهة تلك الجرائم التي تضر بمصالح الناس عن طريق سوء استعمال التقنيات الحديثة، ويشمل ذلك جرائم الانتفاع بلا حق بخدمات الاتصالات وجرائم الدخول غير المشروع على المواقع، وجرائم التعدي على حقوق الدخول للشبكات والتعدي على سرية البيانات والمعلومات على البريد الإلكتروني والشبكات الخاصة، كما توجد بعض القوانين الخاصة بحماية حقوق المليكة الفكرية، وتواجه القوانين استعمال التقنيات الحديثة في نشر الأفكار المتطرفة التي تروج للإرهاب والتطرف (خليل، ٢٠٠٤).

موقف المشرع الفرنسي

في ٥ يناير لعام ١٩٨٨م، قام المشرع الفرنسي بإصدار القانون رقم (٨٨-١٩ المعدل و المتمم لقانون ع ف) الذي يتناول قضية "الغش المعلوماتي"، حيث أنه يتم قام بوضع تنظيم قانوني يتعلق بجرائم الاعتداء على نظم المعالجة الآلية، والتي تم إدراجها ضمن جرائم الأموال.

فبالنظر إلى ما ورد في الباب الثالث من الكتاب الثالث في قانون العقوبات الفرنسي الخاص بالجنايات والجنح ضد الأموال، نجد أن المشرع الفرنسي قام بتخصيص هذا الجزء لجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، ومن ثم قام بوضع العقوبات الملائمة لهذا النوع من الجرائم بما يتراوح بين الغرامة والحبس في جرائم الدخول غير المشروع والبقاء، بالإضافة إلى جرائم تدمير البرامج أو النظم المعلوماتية.

موقف المشرع الإماراتي

في عام ٢٠٠٦م، قام المشرع الإماراتي بإصدار القانون الاتحادي رقم (٢)، والذي تلاه المرسوم بقانون رم (٥) الصادر عام ٢٠١٢م المتعلق بمكافحة جرائم تقنية المعلومات، ومن ثم تم تعديل هذا المرسوم بقانون اتحادي رقم (١٢) لعام ٢٠١٦م الذي يسعى إلى مواكبة التطورات التكنولوجية والتقنية التي يشهدها عصر المعلوماتية، على سبيل المثال ما يعرف بالحكومة الإلكترونية، والتجارة الإلكترونية، فضلًا عن ظهور ما يعرف بالمستند الإلكتروني، والفضاء الإلكتروني.

ويعد الأساس في جميع العمليات المعلوماتية الحديثة هو الحاسب الآلي (Computer)، حيث اندمج بما يشهده هذا المجال من تطورات هائلة، الأمر الذي أدى إلى انتشار الجرائم التي يتم ارتكابها من خلال الحواسيب، وقد أوردت المادة الأولى من القانون السابق ذكره عدد من مفاهيم الملومات الإلكترونية، والنظام المعلوماتي الإلكتروني، ووسائل تقنية المعلومات.

ففي هذا القانون قام المشرع بتحديد الجرائم الإلكترونية، وكمثال على ذلك نجد جرائم التعدي على الحرمات الشخصية للأفراد، وجرائم النصب والاحتيال الإلكتروني، فضلًا عن الجرائم التي تضر بأمن الدولة بمصالحها، كما تعرض القانون إلى كيفية التصدي لهذا النوع من الجرائم.

المطلب الثاني: خصائص الجريمة الإلكترونية وسماتها

هناك العديد من الخصائص التي تميز الجرائم الإلكترونية عن غيرها من الجرائم التقليدية، ويرجع

السبب في ذلك إلى اعتمادها الأساسي على أجهزة الحاسوب وشبكات الإنترنت، ومن أهم تلك الخصائص ما يلي: الالكترونية تتميز بمجموعة من الخصائص عن باقي الجرائم التقليدية نظرًا لارتباطها بجهاز الحاسوب وشبكة الإنترنت، ومن هذه الخصائص ما يلي:

١- الصفة الدولية للجريمة الإلكترونية

وتعد أحد أهم الخصائص التي تتميز بها الجرائم الإلكترونية هي كونها جريمة عابرة للحدود الجغرافية للدول، ولذلك نجد أنها اتصفت بالصفة الدولية، وذهب البعض أن الجريمة الإلكترونية هي جريمة عابرة للحدود، وخاصة عند ظهور شبكة المعلومات الدولية التي أدت إلى تلاشي الحدود الملموسة أو المرئية والتي تقوم على منع انتقال البيانات والمعلومات من دولة لأخرى.

فأصبح الحاسوب ذو قدرة هائلة على نقل وتبادل المعلومات بين مختلف الأجهزة عبر الدول المختلفة ولمسافات شاسعة، مما نتج عنها تأثر العديد من المنشآت والشركات وغيرها من المؤسسات القائمة في مختلف الدول، والتي تبعد عن بعضها البعض بمسافات شاسعة، بالجريمة الإلكترونية التي يتم ارتكابها في وقت واحد وبسرعة كبيرة، بالإضافة إلى حجم المعلومات التي ميزت الجريمة الإلكترونية عن غيرها من الجرائم التقليدية بشكل كبير (أحمد، ٢٠١١).

وتعد البنوك من أهم المنشآت التي تتأثر بهذا النوع من الجرائم، فبالنظر إلى تطور إجراء المعاملات المصرفية ليتم إجرائها من خلال شبكات المعلومات الدولية، أدى ذلك إلى ظهور البعد الدولي للجرائم المعلوماتية والسبب في ذلك هو القيام بزيادة المعاملات المالية عن طريق الاستعانة بوسائل إلكترونية وتقنية تتمثل في وسائل الاتصال والحاسبات الآلية، وخاصة من خلال عليات التحويل الإلكتروني للأموال، فضلًا عن التبادل الإلكتروني للمعلومات، مما يشير إلى أن تلك المعاملات لا تقتصر على المعاملات المالية فقط.

ولكن هناك العديد من الأنماط الأخرى التي اتخذتها الجريمة الإلكترونية نظرًا لطبيعتها الدولية، والمقصود بذلك أن الجاني يمكنه ارتكاب الجريمة في دولة ما وهو في دولة أخرى من خلال الولوج إلى ذاكرة الحاسب الآلي المتواجد في الدولة المستهدفة، بل ويمكنه من خلال ذلك الإضرار بمصلحة فرد ما متواجد في دولة ثالثة، ومثال على ذلك جرائم الاحتيال المعلوماتية.

٢- جرائم صعبة الإثبات

من السمات التي تختص بها الجريمة الإلكترونية غياب الآثار المادية عند ارتكابها، ولهذا نجد أنه من الصعب اكتشافها، حيث أنها تعتمد على عمليات تحرك وانتقال لذبذبات ونبضات إلكترونية تتم عن طريق استخدام النظم المعلوماتية وشبكات الاتصال (أحمد، ٢٠١١).

ولذلك فإن أدلة الإدانة فيها في الغالب غير كافية، ويرجع السبب في ذلك إلى غياب الآثار المادية الملموسة، مثل الجرائم التقليدية التي يتم عن طريقها نقل المعلومات من خلال النبضات

المغناطيسية، بالإضافة إلى ذلك نجد أن الجاني يمكنه إتلاف أدلة الإدانة، ويضاف قلة خبرة رجال الشرطة والقضاء العملية والعلمية، فضلًا عن عدم كفاية القوانين الاجرائية الحالية للتصدي للجرائم المعلوماتية.

٣- صعوبة اكتشاف الجريمة الالكترونية

من أهم خصائص الجريمة الإلكترونية هي صعوبة اكتشافها لكونها تحدث في بيئة إلكترونية، أي أنه ليس هناك آثار مادية متخلفة عن ارتكاب هذا النوع من الجرائم، بل ويمن للجاني أن يقوم بمحو الأدلة المتخلفة عن ارتكاب تلك الجرائم بشكل سريع وفوري، ولذلك فإنه أصبح من الصعب أن يتم الكشف عن الجرائم الإلكترونية من قبل سلطات البحث والتحري، والتعرف على مرتكب الجريمة وتقديمه للعدالة.

كما نجد أن أن المتهم لا يتواجد في مسرح الجريمة عند ارتكابها، حيث يمكن أن يخطط وينفذ في دولة أخرى بعيدة عن الدولة التي يتم ارتكاب الجرم بها، بالإضافة إلى ذلك نجد أن في العديد من الجرائم لا يقوم المجني عليه بالإبلاغ عن الجرائم الإلكترونية للكشف عنها.

ويرجع الدور السلبي للمجني عليه في هذه الحالة إلى سببين أساسيين، الأول هو تصديقه في صعوبة التوصل إلى هوية المجرم الإلكتروني، والثاني هو خوفهم على سمعتهم ومكانتهم، والسبب الرئيسي حتى لا تتزعزع الثقة لدى المتعاملين معهم، وخاصة إذا كانت شركات كبرى، وقد ينتج عن ذلك خسائر مادية فادحة لهذه الشركات .

وقد تمت الإشارة إلى أن أغلب هذه الرائم لم يتم الكشف عنها، وأن ما تم تسجيله من جرائم لدى السلطات المختصة لا يدل على الواقع، وبالنظر إلى ما تم تقديمه للقضاء من جرائم فإن أدلة الإدانة لا تعد كافية لدراسة وسائل ارتكابها، والآليات القانونية للتصدي لها، والتعرف على الفجوات والإشكاليات.

٤- الجريمة الالكترونية جريمة عابرة للحدود

نظرًا للتوسع الكبير الذي شهدته شبكة الاتصال العالمية والإنترنت في العالم أجمع، حيث ظهرت القدرة على ربط أعداد هائلة من الحواسيب في العالم بهذه الشبكة، أصبح من المحتمل أن يكون المجني عليه في بلد ويقوم بارتكاب جريمته في بلد أخر، حث أنه لا توجد أي حدود جغرافية تحد الشبكات التي تخترق الأماكن والأزمنة فيما يتعلق بالمجتمع المعلوماتي.

فبالنظر إلى شبكات الإنترنت المعروفة بشبكات المعلومات الدولية، نجد أنه يمكن من خلالها تحويل المبالغ المالية إلى أي بلد في العالم وذلك عن طريق النظام المعلوماتي الخاص بها، كما يمكن للفرد الكشف عن كلمة السر المرتبطة بأي شبكة في العالم، وبالتالي يتمكن من الاتصال بها وبث ما يريد من معلومات، ومن هنا يتم ارتكاب جرائم الابتزاز الإلكتروني، بالإضافة إلى جرائم الاحتيال والنصب الإلكتروني.

٥- الجرائم الالكترونية جرائم هادئة ولا تحتاج إلى عنف

أحد السمات التي تميز الجرائم الإلكترونية هي أنها جرائم هادئة ناعمة لا يتم فيها ارتكاب أعمال العنف، الأمر الذي يميزها عن الجرائم التقليدية التي تتسم باستخدام العنف في أغلب الأحيان، وهي ما نجدها في جرائم القتل والضرب.

فعلى النقيض، نجد أن الجرائم الإلكترونية تتطلب سمات الذكاء، والتميز الفني والتقني، ومهارات التعامل مع شبكة الإنترنت، حيث أن جرائم الدخول غير المشروع للحواسيب، أو عمليات القرصنة والسطو الإلكتروني على بيانات العملاء، والأرصدة، وبطاقات الائتمان، وغيرها من الجرائم التي يتم ارتكابها إلكترونيًا، نجد أنها لا تتطلب عنف، فلا يقوم الجاني ببذل أي جهد جسدي، ولذلك فإنها تعتبر جريمة هادئة بطبيعتها.

المبحث الثاني: وسائل إثبات الجريمة الالكترونية

المشرع الإجرائي وضع عدد من الإجراءات بضوابط محددة، تقوم على حماية مشروعية هذه الإجراءات، والتي يمكن عن طريقها التوصل إلى الدليل الإلكتروني المستخلص من الجريمة الإلكترونية.

فعلى سبيل المثال، نجد أن تلك الإجراءات تضمنت تفتيش وضبط الأنظمة المعلوماتية، بالإضافة إلى المعاينة والخبرة التقنية، وهذه الإجراءات مكنت من خلالها كشف هوية المتهم بنسبة كبيرة، وبسبب ظهور ما يعرف ب "ثورة المعلومات" اكتسبت هذه الأدلة أهمية كبيرة، وأحبت في حاجة إلى التطور الدائم حتى تتمكن من مواكبة التطور الحادث في الجرائم الإلكترونية، ولذلك سوف نتناول في هذا المبحث الإجراءات التقليدية، كما يلي:

المطلب الاول: الوسائل التقليدية لأثبات الجريمة الالكترونية

الفرع الأول: مشروعية التفتيش على البيئة الالكترونية والضبط

لا يوجد اختلاف في مفهوم التفتيش القانوني فيما يتعلق بالجرائم الإلكترونية عنه في الإجراءات الجزائية، حيث أنه يقصد به قيام السلطة المختصة بإجراءات التحقيق التي تهدف الولوج إلى المعالجة الآلية للبيانات بالبيئة الالكترونية، والتوصل إلى كل ما تتضمنه من مدخلات ومخرجات وتخزين.

والغرض من ذلك هو الكشف عن الأفعال غير المشروعة والتي قد تشكل جريمة جناية أو جنحة، فضلًا عن الكشف عن أي أدلة أو قرائن يمكن من خلالها إثبات الجريمة (واللازمة للتحقيق والاتهام) والتوصل إلى الجاني.

أ- سبب تفتيش نظم المعلوماتية

يجب أن تعتمد عملية التفتيش على توافر المبررات الكافية والواضحة والجدية التي يمكن عن طريقها التعرف على السبب من التفتيش والغرض منه.

وتتمثل هذه المبررات فيما يلي:

- وقوع جريمة معلوماتية.

- لتوجيه التهمة واسنادها إلى شخص ما، يجب القيام بإجراء التفتيش للوصول إلى الأدلة التي ستساعد في عملية إثبات وقوع الجريمة، كما يجب توافر اتهام بعينه يتم توجيهه إلى فرد أو عدد

من الأفراد، وذلك إما بصفته فاعل أو شريك يمتلك لأشياء مرتبطة بالجريمة الإلكترونية.

والمقصود بذلك تواجد أدلة قوية وكافية لإدانة من قم بارتكاب الجريمة من خلال إجراء التفتيش نظرًا لوجود اعتقاد بمشاركته في ارتكاب الجريمة المعلوماتية، فإن مرحلة تجميع الأدلة لإثبات وقوع الجريمة ولنسبتها إلى فاعلها ليست كافية، حيث أنه من الضروري أن يتم اتخاذ إجراءات بعينها والعمل على تنفيذها وفقًا لما تم التوصل إليه من ظروف وملابسات للجريمة، وطبقًا لما تم التوصل إليه من أدلة وبراهين يمكن عن طريقها الجزم في موقف المشتبه بهم والحكم سواء بالإدانة أو بالبراءة.

ب– محل تفتيش نظم المعلوماتية

الهدف الرئيسي لإجراء التفتيش يكمن في التوصل إلى ما يخفيه الشخص من أشياء مادية أو غير ملموسة، وبالنسبة إلى الجرائم الإلكترونية، فإن عملية التفتيش هنا تركز بشكل أساسي على كل ما يتعلق بتلك النظم من برامج، وآلات، وأجهزة إلكترونية، وغيرها.

وفي هذه الحالة فإن محل التفتيش يتمثل في الغالب في منازل الأفراد أو الأجهزة التي تتواجد بها والشبكات المعلوماتية، وقد يرد التفتيش على المكونات المادية للحاسب الآلي وملحقاته، وقد ظهر خلاف هنا حول حكم خضوعها للتفتيش والضبط وفقًا لما ورد في أحكام قانون الإجراءات الاحترازية.

أما بالنسبة للمكونات المعنوية للحاسب الآلي فهي كافة المكونات غي المادية للحاسوب المتمثلة في البرمجيات كنظم التشغيل وبرامج التطبيقات، وهناك نوعيين رئيسيين للبرامج المعنوية للحاسوب، وهما: الأول المتعلق ببرامج تشغيل الجهاز ذاته والقائم على تحسين سرعته، أما الثاني فهو الخاص بتيسير أعمال من يقوم باستخدام الجهاز، ومثال على ذلك برامج Microsoft office، ولتخزين بيانات ومعلومات، مثل برنامج الكتابة Word وبرنامج المحاسبة Excel (قنديل، ٢٠١٥).

ج– اجراءات تنفيذ تفتيش نظم المعلوماتية

يجب أن يتمتع القائم على تنفيذ عملية التفتيش بصفة قانونية طبقًا لما ورد في الأحكام والقوانين الإجرائية، كما يجب تنفيذه ضمن الإطار الزمني المحدد له قانونًا، فإذا خرج عنه سوف يتسم بالبطلان.

ونظرًا لصعوبة التوصل إلى الدليل الإلكتروني لما تتسم به هذه العملية من تعقد وتشابك، فضلًا عن صعوبة التوصل إلى مرتكب هذا النوع من الجرائم ونسبها إليهم، فنجد أن قيام الشخص القائم على التفتيش بمراعاة خصوصية جرائم المعلومات يفرض عليه ضرورة مراعاة الدقة والمهنية الفنية والتقنية في المعاملة مع الأجهزة والبرامج التي تتضمنها، فضلًا عن اتباع الاحتياطات الضرورية، ولهذا أصبح من الضروري الاستعانة بأهل الخبرة، حيث أن هذا الإجراء يتطلب عمليات فنية دقيقة للدخول لأنظمة الوسائل الإلكترونية نتيجة استخدام الشفرات

والأكواد السرية.

الفرع الثاني: مشروعية ضبط الأدلة المتحصلة من الوسائل الإلكترونية

تهدف عملية التفتيش التي تتم في البيئة الإلكترونية إلى التوصل إلى أدلة عن الجريمة التي تم ارتكابها حتى يتمكنوا من الوقوف على الحقائق من خلال وسيلة تقنية تتمثل في عملية الضبط، فمن خلال عملية الضبط يمكن جمع الأدلة الإلكترونية واستخلاصها من البيئة الإلكترونية، والتي تهدف إجراءات الإثبات الجنائي إلى جمعها.

وتتضمن عملية الضبط فيما يتعلق بالجرائم الإلكترونية كل ما تم استخدامه لارتكابها، ومن أمثلة ذلك نجد آلات النسخ والتسجيل لبرامج الحاسوب، بالإضافة إلى أجهزة ربط مع الشبكات الإلكترونية يطلق عليها Modem، وأجهزة اختراق الاتصالات، وأجهزة تحليل الشفرات، وكشف كلمات السر، فضلًا عن جميع البرامج المقلدة والمنسوخة، وأوراق النقد المزورة، بجانب المخرجات الالكترونية المتمثلة في المحررات الإلكترونية المزورة مثل التوقيعات الإلكترونية المزورة، والملفات المعنوية التي تعبر إحدى وسائل ارتكاب الجريمة.

أ- مدى صلاحية ضبط بيانات للحاسب الآلي

لقد ظهر خلاف بين الفقهاء فيما يتعلق بتلك الكيانات، هل هي صالحة لأن تكون محلاً للضبط أم لا، ويمكن التعرض لتلك الآراء فيما يلي:

الرأي الأول: يذهب إلى أن بيانات الحاسب لا يمكن أن تعتبر محلًا للضبط، والسبب في ذلك انعدام الكيان المادي فيها، ويعني ذلك أنه لا يمكن الكشف عنها وضبطها إلى أن يتم تحويلها إلى كيان مادي ملموس. ويمكن تحقيق ذلك عن طريق تصويرها فوتوغرافياً، أو نقلها على دعامة، أو غيرها من الوسائل المادية، ويستند هذا الرأي على نصوص التشريعات المرتبطة بالضبط المادي الذي يكون محله الأشياء المادية.

الرأي الثاني: يذهب إلى أن البيانات التي يتم معالجتها إلكترونيًا تعتبر ذبذبات إلكترونية أو موجات كهرومغناطيسية، أي أنه يمكن تسجيلها وحفظها وتخزينها على كيانات مادية. وبالتالي فإنه من الممكن أن يتم نقلها واستقبالها وبثها وإنتاجها من جديد.

والمقصود بذلك أنها موجودة، وأن هذا الوجود لا يمكن إنكاره، وهذا الرأي أيضاً يستند إلى بعض النصوص التشريعية كالمادة ٧/٧٩ من قانون الإثبات الكندي التي تنص على أن عملية تفتيش وضبط السجلات المتعلقة بمؤسسة مالية لا يتجاوز تفتيش المكان والحصول على نسخة من تلك السجلات، سواء أكانت في شكلها المكتوب، أو في شكل إلكتروني (الفيل، ٢٠١١).

وكنتيجة لذلك، فقد دفع هذا الأمر المشرع في عدد من الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط لتشمل بالإضافة إلى الأشياء المادية المحسوسة والبيانات المعالجة إلكترونيًا أو إصدار تشريعات تتعلق بجرائم الحاسوب حيث تتضمن القواعد الإجرائية المناسبة لهذه الصورة من المعلومات والبيانات كما ورد في

قانون الإجراءات الفرنسي الذي جاء كمحاولة لسد الفجوة بموجب قانون الأمن الداخلي رقم ٢٣٩ لعام ٢٠٠٣م، حيث استحدث المادة (٧٦-١ فقرة)، و التي تم تعديلها بموجب المادة (٦٠-٣) من القانون رقم (٢٠١٦ -٧٣١) الصادر في (٣ جوان ٢٠١٦م).

والذي نص على أن البيانات التي يتم استخلاصها عن طريق إجراء التفتيش للنظام المعلوماتي، فلابد أن يتم نسخها على دعامات، ومن ثم تحرز في أحراز مختومة، ومن الجدير بالذكر أن فرنسا كانت ضمن الدول الأعضاء في اتفاقية "بودابست"، والتي نصت المادة (١٩) من القسم الرابع منها على: "من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزءاً منه أو المعلومات المخزنة على سلامة تلك المعلومات المخزنة".

وفي حالة عدم القدرة على تطبيق إجراء الحجز طبقًا لما ورد في المادة (٦) المذكورة سابقًا، بسبب مشكلات تقنية أو فنية، يجب على السلطة المعنية بالتفتيش أن تقوم باستخدام التقنيات الملائمة للحد من وصول البيانات التي تتضمنها المنظومة المعلوماتية، كما يمكن نسخ تلك البيانات، وبصفة خاصة الموجودة تحت تصرف الأشخاص المرخص لهم باستخدام هذه المنظومة.

ففي حالة إذا تم تحديد مكان البيانات المراد التحفظ عليها عن طريق التفتيش، فلابد من إجراء المعالجة الفنية عليها حتى يتمكن من التحفظ عليها وإثباتها، أما بالنسبة لحفظ الأدلة في شكل مخرجات كمستندات مطبوعة لا تعتبر تفتيش عن أدلة الجريمة، ولكنها تعتبر الكشف عن تلك الأدلة وضبطها.

ضبط الأدلة المتحصلة من الوسائل الإلكترونية قد تتضمنه الصعوبات الهائلة خاصة أنه مرتبط بنظام إلكتروني بشكل كامل، الأمر الذي يتطلب ضرورة التعاون الدولي الذي يساهم في تحقيق هذا الضبط دون عرقلة لسير النظام المعلوماتي.

وبالنسبة للمكونات المادية للحاسب الآلي، فلا توجد أي مشكلات فيما يتعلق بعملية ضبطها، حيث يمكن بسهولة ضبط الوحدات المعلوماتية التي تتمثل في وحدة المدخلات، وما تتضمنه من مكونات مثل لوحة المفاتيح، والشاشة، ونظام الإدخال المرئي، أو نظام الإدخال الصوتي، والفأرة، والقلم الضوئي، ونظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية وغيره من نظم إدخال الرسومات والأشكال.

أما فيما يتعلق بوحدة الذاكرة الرئيسية، سواء أكانت للقراءة فقط، أو للكتابة والقراءة معًا، فيمكن ضبطها بما تشمله من دوائر إلكترونية ومسجلات، ويمكن ضبط وحدة التحكم، وايضاً ضبط وحدة المخرجات وما تشتمل عليه من وسائل كالشاشة، الطباعة، الرسم والمصغرات الفيلمية، ويمكن ضبط معلومات مخزنة الثانوية وبما تتضمنه من الأقراص المغناطيسية بنوعيها المرن والصلب، بالإضافة إلى الأشرطة المغناطيسية.

ب– ضبط المراسلات الإلكترونية

سيتم تناول عملية ضبط المراسلات الإلكترونية التي

تتم من خلال استخدام البريد الإلكتروني، بالإضافة إلى التعرض إلى أعمال التنصت والمراقبة الإلكترونية لشبكات أجهزة الحاسوب.

ضبط مراسلات البريد الإلكتروني Electronic Mail

يقوم البريد الإلكتروني بنقل وتبادل الرسائل بالاستعانة بشبكة الإنترنت دون الحاجة إلى اللجوء إلى الوسائل التقليدية، وبالتالي أصبح البريد الإلكتروني أحد أهم وسائل الإنترنت انتشارًا واستخدامًا نظرًا لسهولة استخدامه.

ويجوز في التشريع الإماراتي والمقارن أن يتم ضبط مراسلات البريد الإلكتروني، وذلك لاعتبارها من المستندات الإلكترونية المعترف بيها في العديد من التشريعات، والمعترف بصلاحيتها لأن تكون محلًا للتزوير، وبحجيتها في إثبات الجريمة، فبالنظر إلى أن كل ما يتم تحريره يتم التعبير عنه بلغة رقمية، نجد أن تلك اللغة أصبحت تحل محل الكتابة، ومن هنا ثبتت صلاحية هذا المحرر الرقمي ليكون محلًا للتزوير (الحلي، ٢٠١١).

فإذا كان هذا المستند الإلكتروني مسطورًا ويمكن قراءته وإدراك فكرته ومعناه ومضمونه، فإنه يصبح محررًا إلكترونيًا، وبالتالي يمكن قبول الحجية القانونية بما يتفق مع هوية الفرد المنسوب إليه إصدار هذا المحرر، فضلًا عن الفرد الذي وضع عليه وتوقيعه الإلكتروني.

وفي عام ١٩٩٤م، فور إصدار قانون العقوبات الفرنسي، قام المشرع بإلغاء المادتين ٥/٤٦٢ و٦/٤٦٢ الذين أقرهما القانون رقم ٨٨/١٩ الذي تم إصداره ف ١٩٨٨/١/٥م الذي يتناول تجريم غش المعلوماتية، حيث تناولت المادة الأولى من هذا القانون تجريم تزوير المستندات المعالجة آليًا.

أما المادة الثانية فقد نصت على تجريم استخدام تلك المحررات، وقد أضيف أيضًا للمادة ٤٤١ من الكتاب الرابع لقانون العقوبات تجريم عمليات تزوير المستندات المعالجة آليًا واستخدامها، بحيث أصبحت تنص هذه المادة على أنه يعد تزويراً "كل تغيير بطريق الغش للحقيقة في مكتوب أو في أي دعامة أخرى تحتوي علي تعبير عن الفكر".

ومن هنا يمكن القول بأن جريمة التزوير في المعلوماتية قد شهدت تطورًا كبيرًا من جريمة تزوير المستندات المعالجة آليًا فقط واستخدامها، إلى جريمة تزوير المستندات المعلوماتية واستخدامها.

المطلب الثاني: الوسائل الحديثة لإثبات الجريمة الالكترونية

بالنظر إلى الطبيعة الخاصة التي تميز الجرائم الإلكترونية، نجد أنها تتطلب دائمًا وجود خبرة فنية وتقنية عالية، والتي يتفق توقيتها مع إجراءات البحث والتحري عن الجرائم الإلكترونية (التقصي)، كما أنها تستمر أثناء إجراءات التحقيق والمحاكمة وفقًا للطبيعة الفنية والتقنية المتعلقة بطريقة ارتكاب الجريمة، والطبيعة المعنوية الخاصة بمحل الجريمة (مراد، ٢٠١١).

الفرع الأول: تعريف الخبرة التقنية ومجالاتها في الجرائم الإلكترونية

١- تعريف الخبرة التقنية

يقصد بها المساعدة التي يتم تقديمها للقاضي في المجال الفني والتقني، والتي عن طريقها يستطيع القاضي تكوين عقيدته ووجدانه فيما يتعلق بالقضية المطروحة أمامه، والتي تتطلب توافر خبرة فنية، أو معرفة علمية لا يمتلكها (إبراهيم، ٢٠١٤). فيمكن القول بأنها عملية البحث والتقصي فيما يتعلق بالمشكلات المادية أو الفنية التي يعجز المحقق على تحقيق أهدافه من خلالها، بحيث لا يتمكن من جمع الأدلة الإلكترونية اللازمة بالنسبة لها من خلال اللجوء إلى طرق أخرى للإثبات.

وبديهي أن الخبراء العاملين بالتحقيق الجنائي الإلكتروني يجب أن يكونوا ذوي خبرة في لغات البرمجة، وغيرها من أنظمة حديثة للتشغيل، بالإضافة إلى تصميمات البرامج وطرق تشغيلها، والتعرف على ما هو جديد في هذا المجال، فضلًا عن ضرورة العمل على تحليل البرامج وأنظمة التشغيل، وأن يستقر بوجدانه أن هناك أفراد آخرين يمتلكون الخبرة الكافية لاختراق الشبكات (موسى، ٢٠٠٩).

٢ – مجالات الخبرة في الجرائم الإلكترونية

هناك العديد من الأنماط المختلفة والمتنوعة من العمليات الإلكترونية، والتي ترتبط ارتباطا وثيقًا باستعمال الوسائل الإلكترونية، فعلى سبيل المثال نجدها في الأعمال المصرفية، وفي التجارة الإلكترونية، حيث أنه من المتوقع أن تتنوع الجرائم طبقًا لتنوع الوسائل الإلكترونية التي يتم استخدامها، والتي يتم من خلالها استهداف تلك العمليات.

فعلى سبيل المثال نجد عمليات تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو المخرجة بعد المعالجة، أو في تعديل البيانات، والتلاعب في البرامج الأساسية أو برامج التطبيقات الملحقة بأجهزة الحاسب الآلي، فضلًا عن عمليات الغش أثناء نقل وبث البيانات، ولهذا فإن هذا النوع من الجرائم يستلزم وجود خبراء ذوي صفات خاصة ومهارات فنية وتقنية عالية.

الفرع الثاني: الضوابط القانونية لمشروعية الخبرة القضائية في الجرائم الإلكترونية

لقد أقرت المبادئ القانونية أنه لا يجوز للقاضي اللجوء إلى الخبرة الفنية إلا في الحالات التي يمكنه العلم بها أو إيضاحها، والمقصود بالخبرة الفنية هنا إمكانية المتخصص التقصي عن الموضوعات المادية أو الفنية التي لم يتمكن المحقق من الوصول إليها، وفي حالة عدم قدرته على التوصل للأدلة الضرورية لإثبات الجريمة بجميع الوسائل المتاحة المتمثلة في رفع البصمات المعثور عليها بمسرح الجريمة، أو عند الكشف عن سبب الوفاة في جرائم القتل العمد.

وحتى يتم الوصول إلى الحقائق المتعلقة بهذه الجرائم، نجد أن القانون قد شرع الاستعانة بخبراء متخصصين في هذا المجال، وفي موضوع التحقيق والفحص، كما أصبح أحد إجراءات التحقيق قيام المحقق بندب الخبير، وبالمثل عمليات

إيداع تقارير الخبرة، ومن الجدير بالذكر هنا أن توافر الخبرة لا يؤثر على التقادم نظرًا لكونها أعمالًا مادية.

ويحتاج الأمر غالباً إلى إجراءات فنية غاية في الدقة لإتاحة القدرة على الولوج إلى أنظمة الوسائل الإلكترونية عن طريق استعمال الشيفرات والأكواد السرية. إذا كان الغرض الأساسي من الخبرة هو الوقوف على الحقيقة فيما يتعلق بالمسائل العلمية والفنية والتقنية والمادية، فإنها ملازمة لمراحل الدعوي الجزائية، وبذلك لا يمكن اعتبارها مقتصرة على سلطة التحقيق، ولكن يحق للمحكمة أن تأمر بها.

أ – تعيين الخبير

لقد أجاز المشرع للمحقق الحرية التامة في الاستعانة بالخبراء المتخصصين في الجرائم جميعًا بشكل عام، وفي الجرائم الإلكترونية بوجه خاص، ويهدف ذلك إلى الوصول إلى الحقائق الكامنة خلف الغموض واللبس في هذه الجرائم، ومن الجدير بالذكر أن أجهزة الحاسوب بمختلف ملحقاته من شبكات متعددة ترتبط بالعديد من المجالات التقنية والعلمية والفنية المتقدمة.

ولذلك فإن اللجوء إلى ندب الخبراء الإلكترونين من سلطات التحقيق يحقق المصلحة القصوى للعدالة، ولذلك نجد أنه لا يتوجب على المحقق أن يستعين بالخبير كالاستجابة للجاني أو لغيره من الخصوم، والسبب في ذلك أن عمل الخبير يخضع لإشراف المحقق ويجب أن يتم في حضوره.

ب – واجبات الخبير التقني

١- حلف اليمين: يجب على الخبير أن يقوم بحلف اليمين أمام المحقق قبل أن يبدأ في ممارسة عمله، ويتضمن حلف اليمين أن يقوم الخبير على تقديم كافة التقارير المكتوبة ذات الصلة بالقضية، وأن يقوم بإبداء رأيه بأمانة وصدق.

وفي حالة عدم تأديته لليمين فيبطل عمله، ولا يجوز الأخذ بالحكم المبني على عمله، حتى في حالة أن تقرير الخبير هو الدليل الوحيد الذي يمكن الأخذ به، ويمكن أن يقوم الخبير الذي تم انتدابه بالاستعانة بخبراء آخرين حتى يقدم له يد العون في عمله، ولا يؤدوا هؤلاء الخبراء اليمين ولا يمكن أن يؤثر ذلك بأي شكل على صحة وصدق التحقيق أو الحكم (بيومي، ٢٠٠٧).

٢- تأدية مهام عمله بنفسه يجب على الخبير أن يقوم بتأدية مهام عمله بنفسه في الحدود التي أقرها أمر الندب، وألا يقوم بتخطيه أو تجاوزه.

٣- خضوع الخبير للرقابة القضائية: فالأصل يجب على الخبير أن يقوم بمزاولة عمله في حضور المحقق وتحت إشرافه وملاحظته، فضلًا عن ذلك يسمح المشرح للخبير بأن يمارس مهامه دون حضور أي من الخصوم، حيث أن المتخصص الفني يقوم بدور المعاون الفني المساعد للقاضي الجنائي، وفي بعض الأحيان يتطلب الأمر قيام الخبير بعمله تحت رقابة القاضي حتى يتم التأكد من التوصل إلى الرؤية الفنية الكاملة للجريمة المطروحة.

ويرجع السبب في ذلك أن كل من الفقه والقانون قد اتفقوا على أنه في حالة مواجهة

المحكمة لقضية فنية بحتة، فيجب أن يتم تسخير كافة الوسائل الممكنة للوقوف على الحقائق كاملة، ويجب الإشارة هنا إلى ما ورد في المادة (١٨) من اتفاقية "بودابست" على أهمية أن تقوم الدول بإصدار تشريعات يتم من خلالها إلزام مقدم الخدمات الفنية، وغيره من الأفراد القائمين بتوفير المعلومات اللازمة التي يمتلكونها أو تقع تحت سيطرتهم، والتي يتم تخزينها ضمن أنظمة الحاسب الآلي أو على دعامة.

المبحث الثالث: الدليل المتحصل من الجريمة الإلكترونية

بالنظر إلى التطور الهائل الذي يشهده مجال تكنولوجيا المعلومات في الآونة الأخيرة، والذي أدى إلى تطور وسائل الاتصال بشكل كبير في المجتمع، أسفر عن تطور في الوسائل التي يقوم الجاني باستخدامها لارتكابه للجرائم بشكل عام، وبصفة خاصة الجرائم الإلكترونية، ونتج عن ذلك عدم قدرة وسائل الإثبات التقليدية على إثبات هذا النوع من الجرائم.

ولذلك فإن الوسيلة المثلى لإثبات الجرائم الإلكترونية هي الوسائل الفنية والتقنية والعلمية، الأمر الذي تطلب العمل على تحديث وسائل الإثبات الجنائي للتصدي لهذا النوع من الجرائم، والمقصود بذلك تطوير خبرات وقدرات العاملين على مواجهة الجرائم الالكترونية، سواء أكان ذلك أثناء عملية التقصي وجمع الاستدلالات، أو في مرحلتي التحقيق والقضاء، حتى لا ينتج عن صعوبة الإثبات إفلات مرتكبي هذه الجرائم من العدالة (محكمة النقض المصرية، ١٩٨١).

وبالنظر إلى ما نصت عليه تشريعات الإثبات الجنائي، نجد أنها تنص على أنه لا يجور للقاضي أن يقوم بإصدار حكمه وفقًا لعلمه الخاص، فيجب عليه الإحاطة بجميع حقائق القضية المطروحة أمامه عن طريق ما يتم عرضه عليه من أدلة، ولذلك فإن الدليل هو المصدر الرئيسي للحقائق التي يقوم القاضي عن طريقه بالإحاطة بجميع جوانب القضية، ومن ثم يقوم بإصدار حكمه وفقًا لما تقدم له من أدلة.

وبالنسبة إلى الجرائم الإلكترونية نجد أن الدليل الإلكتروني هو الوسيلة التي يمكن من خلالها إثبات هذا النوع من الجرائم، ومن خلال ما ورد فقد تم طرح مشكلتين رئيسيتين من قبل الفقهاء، وهما (عقيلة، ٢٠١٢): الأولى: أن الدليل الإلكتروني يعد من الأدلة المستحدثة التي نتجت عن التطور العلمي الذي يشهده العالم أجمع حديثًا، كما أن له خصائص خاصة به تنبع من البيئة التي ينشأ بها والشكل الذي يتخذه، ويتمحور هذا التساؤل حول إذا ما كان يجوز الأخذ به كدليل للإثبات.

وفي هذا الصدد تم الإشارة إلى ضرورة توافر صفة المشروعية في الدليل الإلكتروني فيما يتعلق بوجوده وطريقة التوصل إليه، وتتمثل تلك المشروعة في مدى قبول المشرع للدليل ضمن أدلة الإثبات الجنائي، ويليه التعرف على إذا ما كان قبول الدليل الإلكتروني والأخذ به يتماشى مع المبادئ المتعارف عليها في التشريع الاجرائي؟

الثانية: تتعلق بمدى مصداقية الدليل

الإلكتروني في تمثيله للحقيقة، وخاصة أن هذا النوع من الأدلة من الصعب الحصول عليه، كما أنه معرض للتلاعب به وإتلافه نظرًا للتقدم التقني والتكنولوجي، الأمر الذي يجعل من الصعب إدراك ذلك لغير المتخصص، وهنا برز التساؤل الذي يتمحور حول كيفية التحقق من مصداقية الدليل الإلكتروني؟ وهل مفهوم المصداقية يتنافى مع الطبيعة الخاصة للدليل الالكتروني؟

ومن هنا يمكن القول أنه لا يمكن الاعتماد فقط على توافر دليل من شأنه إثبات الجريمة ونسبتها للجاني لإصدار حكم الإدانة، حيث يجب توافر القيمة القانونية للدليل الإلكتروني والتي تعتمد بشكل رئيسي على مسألتين أساسيتين، وهما: المشروعية والحجية، ولذلك سوف نتناول في هذا المبحث مشروعية القيمة القانونية للدليل الإلكتروني على النحو التالي:

المطلب الأول: مشروعية الدليل المستمد من الجريمة الالكترونية.

المطلب الثاني: حجية الدليل الإلكتروني امام القاضي الجزائي.

المطلب الاول: مشروعية الدليل المستمد من الجريمة الالكترونية

يسمح لمن يقومون بالتحري والبحث عن الأدلة بالتوصل للحقائق بشكل غير مطلق، حيث يعتمد تحديد الأدلة على ضوابط تتمثل في الالتزام بالشرعية الإجرائية والحفاظ على الحريات والحقوق، ولذلك سيتم في هذا المطلب تناول حرية القاضي الجنائي في أن يقبل الأدلة الالكترونية.

الفرع الأول: المقصود بمشروعية الدليل الإلكتروني

إن أحد أهم الأسس التي تعتمد عليها التشريعات الجنائية الحديثة هي قاعدة شرعية الجرائم والعقوبات، ولكنها وحدها ليست كافية للحفاظ على حرية الإنسان وحماية حقوقه، ومن ثم كان حتماً تدعيمها بقاعدة دقيقة وواضحة تقوم على تنظيم تلك الإجراءات، ويقصد بذلك ألا تتعارض تلك الإجراءات مع النصوص القانونية الثابتة في نفوس المجتمع (محمد، ٢٠٠٦).

فإذا تم التوصل إلى الدليل من خلال وسيلة غير مشروعة فلا يجوز الأخذ به، حتى في حالة الدليل الإلكتروني، مما يجعلنا نتساءل عن ماهية المعيار الذي يبين العلاقة الموجودة بين العمل الإجرائي والأعمال التي تعقبه حتى ينال منها حكم الإبطال.

وهناك العديد من المعايير التي حددها الفقه، ولكن أهم تلك المعايير يتمثل في أن ولكن أهم تلك المعايير يتمثل في العلم اللاحق الذي يرتبط بالإجراءات السابقة وكونه ضروريًا لصحة العمل الذي يلحق به، والمقصود بذلك أن مدى صحة الإجراء الأول أو بطلانه تؤثر على الإجراء الثاني (هليل، ٢٠٠٦).

ومن هنا يمكن القول بأنه يجب توافر عنصر الصدق في مضمون الدليل حتى تتوافر مشروعيته، ويتم تحقيق ذلك من خلاله التوصل إلى مضمون الدليل من خلال طرق مشروعة تتوافق مع ما أقره القانون، كما يجب أن تتصف أساليب الاستنتاج وطرق الحصول عليه بالأمانة

والنزاهة.

ويعد شرط توافر شرعية الأدلة التي يتم استخلاصها من الوسائل الإلكترونية، أصبحت من القواعد الثابتة والأساسية للأخذ به، حيث أن مضمون تلك الأدلة قد يشتمل على حقيقة علمية تتنافى في محتواها مع الحقيقة القضائية، ولذلك فإن الوصول إلى تلك الحقائق يجب أن يكون من خلال طرق مشروعة (عزت، ٢٠١٠)

وفي هذا الصدد يمكن التعرض لأحد أمثلة الطرق غير المشروعة التي يتم اللجوء إليها للتوصل إلى الأدلة الإلكترونية والرقمية، وتتمثل في الاستعانة بأساليب الإكراه المادي أو المعنوي، ومختلف وسائل التعذيب، والتي من شأنها إجبار الجاني على الاعتراف على ارتكابه للجرم والبوح بكلمة السر، أو فك الشفرة، ومن هذه الوسائل أيضًا اللجوء إلى التدليس، أو الغش، أو المكر والخديعة في الحصول على هذا النوع من الأدلة.

الفرع الثاني: حرية القاضي الجنائي في قبول الدليل الإلكتروني مرتبطة بالمشروعية

يعتبر شرط مشروعية الدليل الجنائي من أكثر الشروط التي تدخل على سلطات القاضي الجنائي التقديرية ووزن الأدلة، وذلك الشرط يشكل قمة التطور الذي وصلت إليه نظرية الإثبات في المواد الجنائية (شريف، ٢٠٠٢).

ووفقًا لمبدأ الشرعية الإجرائية لا يمكن النظر إلى الدليل الإلكتروني المستخلص من خلال الحاسب الآلي، وذلك يتمثل في عملية الإثبات إلا في حالة الاعتراف بجانبين، الأول: وجود دليل مشروع ويمكن الاعتماد عليه في تحديد الإثبات الجنائي، واتباع ضوابط مشروعية الدليل يعتبر ميزان للقاضي الجنائي في إطار قبول الدليل وتقدير ووزن كل الأدلة الممكنة والتي يمكن الوصول من خلالها للحقيقة.

كما نجد أن التطور الكبير الذي شهدته وسائل الإثبات حديثًا، قد أوجد لنا وسائل جديدة تشمل الدليل الإلكتروني أو الرقمي الذي يعمل على انتهاك حياة الناس الشخصية للبحث عن الحقائق. ورغم ذلك فإن هذا الدليل من شأنه أن يهدد الضرورات التي تلزم للحفاظ على حقوق الإنسان والأسرار التي تخصه ولها علاقة بظاهرة المعلوماتية (الطراونة، ٢٠٠٥).

وقد أجاز المشرع الإجرائي للقاضي الجنائي الاعتماد على أي دليل في إطار العقيدة والاقتناع الشخصي الخاص به، ولكن وضع المشرع بعض الشروط والاحكام الإجرائية التي تشمل ضرورة وجود مشروعية للإجراءات التي يقوم بها القاضي الجنائي للتأكد من مشروعية الدليل، ويشمل ذلك الأدلة الإلكترونية، وقد يترتب على عدم مشروعية الإجراءات التي يتخذها المشرع أن يبطل الدليل ويبطل العمل به.

ويجب أن تلتزم سلطات البحث والتحري بالأحكام الجنائية والإجراءات التي حددها المشرع في إطار تجميع الأدلة الإلكترونية، حيث أن هذا الأمر متعلق بمدى مشروعية الدليل الذي تم جمعه، بحيث يقوم القاضي بالحكم على مدى قبوله، ويعني ذلك إذا ما كان يمكن الاعتماد على الدليل الإلكتروني في عملية الإثبات الجنائي، وإذا ما كان

صالحًا لبناء الحكم النهائي سواء بإدانة المتهم أو ببراءته، أم أن هذا الدليل غير مقبول نظرًا لكونه مخالفًا لأنه للقواعد المشروعية الاجرائية.

ويجب علي القاضي الجنائي في بادئ الأمر أن يقوم بقبول الدليل للتأكد من مدى مشروعية وسيلة الحصول عليه، ويجب أن يتم ذلك قبل وزن وتقدير الأدلة والتحقق منها ومن ثبوتها، حيث أن القاضي الجنائي لا يعتمد إلا على أدلة شرعية.

ووفقًا لنظام الإثبات الحر، فالأصل في القضايا الجزائية جواز الاثبات بجميع الوسائل المشروعة، والقيد هنا وجوب أن يكون الدليل مقبولًا من الناحية القانونية، وبالتالي أصبح من الضروري أن يعترف القانون بالدليل الإلكتروني (الرقمي بشكل خاص مع ظهور أنواع جديدة لكافة الجرائم في إطار الجوانب المتغيرة اجتماعيًا وثقافيًا التي صاحبت التطور التكنولوجي في مجال المعلومات وظهور جرائم خاصة يتم ارتكابها من خلال الحاسب الآلي.

وقد اعتمد الفقه والقضاء أن القاضي الجنائي يتمتع بحرية تحديد القيمة الثبوتية للأدلة المعروضة عليه من خلال القضايا الجزائية (بيومي، ٢٠٠٧). ويقوم باعتماد المصدر الذي يقتنع به ويطمأن إليه، دون ان يلزمه المشرع باتباع طرق او وسائل محددة للوقوع على الحقائق.

وتجب الإشارة هنا إلى أن الأدلة العلمية هي المبرر الأهم الذ اعتمده القاضي الجنائي، ويتجلى دورها الفني في حالة التعارض بين الأدلة المادية والقولية، وفي تلك الحالة يعمل الدليل العلمي والفني على التخلص من التعارض عن طريق إدخال بعض الأدلة الإلكترونية، ولا توجد قيود تمنع القاضي من تكوين عقيده ووجدان، ولذلك يتجه المشرع الإجرائي في العديد من الدول إلى الاعتراف بحجية الأدلة التي يتم الحصول عليها من خلال الحاسب الآلي كدليل للإثبات.

وفي هذا الصدد نجد أن المادة (١٧٩) من قانون الإجراءات الجزائية في الإمارات العربية المتحدة لتنص على مبدأ حرية الإثبات الجنائي، وتنص المادة على: (للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوي بتقديم أي دليل تراه لازما لإظهار الحقيقة)، وقد كفل القانون للقاضي الجنائي حرية إصدار حكمه وفقًا لاقتناعه الخاص، ولكن لا يمكن للقاضي أن يقوم بإصدار حكمه إلا وفقًا لما تم طرحه عليه في المرافعات من أدلة، والتي أقيمت المناقشة فيها حضورياً أمامه.

وتأسيساً علي ذلك فإن الدليل الإلكتروني، مثله مثل غيره من الأدلة، يتم الأخذ به في الإثبات الجنائي عامة، والإثبات في مجال الجرائم الإلكترونية خاصة، ولكن يجب الرجوع أولًا إلى ضابط المشروعية في عملية جمع الأدلة، حيث أنه لا يجب اتباع وسائل وأساليب غير مشروعة على الرغم من الحرية المكفولة في نظام الاثبات الحر، حيث أن هناك ضوابط لتلك الحرية، فلا يجب اتباع أي وسائل أو أساليب مخالفة لضوابط المشروعية في الحصول على الأدلة، وإلا ترتب على هذا عدم مشروعية الدليل وبطلانه (مصطفى، ٢٠١٠).

الفرع الثالث: انتهاك الخصوصية وعدم مشروعية الدليل الإلكتروني

يجب على عملية البحث والتقصي عن الأدلة الإلكترونية أن تتم في إطار من المشروعية، ويقصد بذلك أن يستند من يقوم بالبحث على حقوق الخصوصية وحرية الحياة الخاصة للأفراد، وإلا فإنه يرتكب جريمة اختراق للخصوصية.

وفي عملية التقصي والبحث عن الدليل الإلكتروني يجب احترام الحياة الخاصة للأفراد، والمقصود بذلك احترام المعلومات الخاصة والبيانات الخاصة بالأفراد، واحترام خصوصية البريد الإلكتروني والرسائل والمكالمات الخاصة بالأفراد، فانتهاك تلك الخصوصيات يشبه انتهاك حرمة المنازل والاطلاع على الخصوصيات الخاصة بالأفراد بدون وجه حق.

ووفقًا لذلك فإن الأدلة التي يتم الكشف عنها من خلال انتهاك خصوصية الأفراد يعد دليلًا غير مشروع، ولا يمكن الاعتماد عليه في عملية إثبات الأدلة الجنائية، حيث أن التجسس على المكالمات والرسائل إلكترونيًا يتم من خلال زرع فايروس بالحاسب الآلي للتجسس على تلك الأجهزة واختراق خصوصيات الغير للوصول لبيانات خاصة بهم، والاستعانة بتلك البيانات يعد دليلًا باطلًا ولا يستطيع القاضي الأخذ به.

ويبرز التزوير المعلوماتي من خلال ما يعرف بالتسلل الإلكتروني، ويقصد به محاولة قيام الجاني بالدخول إلى النظام للتسلل إلى البيانات والمعلومات، التي تكون في أغلب الأحيان سرية. ويتم ذلك من خلال اختراق هذه المداخل والوصول إلى قاعدة البيانات، والعمل على تعديلها والعمل على تعديلها وحذفها وتقديم بيانات مزورة لاستعمالها في تنفيذ جرائم.

ويظهر ذلك في عدة اشكال، وقد ظهرت لهم العديد من الأسماء، ومثال على ذلك الفريكرز، ويقصد بهم القراصنة الذين ظهروا قبل وجود الانترنت، وتتحدد جرائمهم على قرصنة شبكات الهاتف المحلية والدولية على حد سواء (عدنان، ٢٠١٣)، بالإضافة إلى الهاكرز، وهم المبرمجين من ذوي الخبرة والكفاءة الفنية الهائلة، وتتحدد غاياتهم في قرصنة مواقع الشركات والمؤسسات الحكومية الكبيرة، فضلًا عن مواقع النظم المعلوماتية والعسكرية.

حماية الحياة الخاصة من انتهاك الخصوصية الكترونيًا في فرنسا

وفي عام ١٩٧٨م، تم إصدار قانون رقم (٧٨-١٧) المختص بمعالجة البيانات الرسمية إلكترونيًا، حيث أنه يعمل على ضمان حفظ البيانات الشخصية التي تتعلق بالحياة الخاصة للأفراد، كما حدد قانونًا العقوبات الفرنسي مجموعة من الجرائم تشمل ما يلي:

١- ناقشت المادة رقم (٢٢٦-١) من قانون العقوبات جريمة معالجة البيانات الإلكترونية الشخصية للأفراد بدون ترخيص، فقد يعمل الجاني على معالجة بيانات الأشخاص بدون حصوله على موافقات تكفلها اللجنة الوطنية للحريات والبيانات، وقد تحددت عقوبة من يقوم بارتكاب هذا الجرم بالحبس لمدة عام وغرامة ثلاثمئة يورو

بالإضافة إلى عقوبة تكميلية متمثلة في نشر الحكم وإدراج الأشخاص المعنوية جنائيًا في الجريمة وتطبيق عقوبتي الغرامة والحرمان من العمل في النشاطات التي تم استعمالها لتنفيذ الجريمة.

٢- وتضمنت المادة رقم (٢٢٦-٢٠) من قانون العقوبات جريمة حفظ البيانات بشكل غير مشروع، وتعاقب المادة على تلك الجريمة بالسجن سنة وغرامة ثلاثمئة ألف يورو لكل من يحتفظ بالبيانات دون موافقة اللجنة ودون الحصول على إخطار مسبق للاحتفاظ بالبيانات.

٣- وتنص المادة رقم (٢٢٦-٢١) من قانون العقوبات على العقوبات التي تنطبق على جريمة الانحراف عن الهدف من معالجة البيانات الاسمية، حيث يتم سجن من تثبت عليه الجريمة لمدة خمس سنوات وغرامة مليوني يورو، على أن يتم إثبات أن الجاني احتفظ ببيانات اسمية أثناء تسجيلها أو نقلها أو تصنيفها لمعالجتها، حيث أن الاحتفاظ بتلك البيانات للتلاعب بها يشكل جريمة يعاقب عليها القانون.

حماية الحياة الخاصة من انتهاك الخصوصية الكترونياً في دولة الامارات العربية المتحدة

في عام ٢٠١٢م، تم إصدار مرسوم الخاص بقانون رقم (٥) الخاص بمكافحة جرائم تقنية المعلومات، وقد جاءت المادة (٢١) من هذه القانون لتنص على تجريم اختراق الحياة الخاصة بالأفراد، حيث أنه لا يجوز استعمال الإنترنت أو أحد الأجهزة والبرامج الحديثة في انتهاك تلك الخصوصية.

وذلك يشمل جميع الحالات فيما عدا بعض الحالات التي يسمح فيها القانون باستعمال وسائل للتنصت والاعتراض والنقل والتسجيل للمجرمين، كما يسمح القانون في بعض الحالات باختراق خصوصية بعض الأفراد وتسجيل مكالمات ومحادثات وما إلى ذلك كأدلة على ارتكاب جرائم تتابعها جهات التحقيق والمراقبة.

المطلب الثاني: حجية الدليل الإلكتروني أمام القاضي الجزائي

تتسم الجرائم الإلكترونية بأنها يصعب اكتشافها، ومن ثم يصعب إثباتها، وحيث أنها تتم في بيئة مختلفة، ولا يتم فيها التعامل بأوراق والمستندات العادية، وإنها لها آثار إجرامية تتم عن طريق الحاسب الآلي، وأن الجاني قد يتمكن من التلاعب ببيانات الحاسب الآلي والبرامج الموجودة عليه، وأن ضبط الجريمة الالكترونية لا يتم إلا عن طريق خبير متخصص، وذلك بهدف التوصل للحقيقة والحصول على الدليل الالكتروني الموجود في الحاسب الآلي.

ويعلو مبدأ حرية القاضي في الاقتناع في النظرية العامة للإثبات الجنائي، الأمر الذي يعد أحد أهم عناصر الاثبات في الدعوى الجزائية، حيث يتمتع القاضي بالحرية الكاملة في تكوين عقيدته ووجدانه من خلال الدليل الذي يقتنع به (قنديل، ٢٠١١).

وبالتالي فهو يقبل بالدليل الذي يبدو له ملائمًا للتوصل إلى الحقيقة، ويتضمن ذلك أيضًا الدليل الالكتروني. وعليه فإن الوقوف على الدليل الإلكتروني وتقديمه إلى القضاء لا يعد كافيًا لإدانة

الجاني. ويرجع ذلك للطبيعة الخاصة به، وإمكانية التلاعب بمحتواه بما يطمس الحقيقة، كما نجد أن درجة الخطأ تزيد عند الكشف عن الدليل الصادق.

وقد يرجع هذا الخطأ لأخطاء قام بها مسئول التحريات، والذي قد يكون لا يمتلك الخبرة الكافية بفنيات التعامل مع الأدلة، والتي تقوم على التقصي عن طريق العديد من الإجراءات التي يقرها القانون في الوصول للأدلة، ومن المحتمل أيضًا أن يحدث خطأ عند قيام الخبير الفني برفع الأدلة، ومن هنا تبع فكرة إمكانية حدوث شك في مدى صدق الدليل الإلكتروني في الإثبات الجنائي.

وتقوم النيابة العامة بدور فحص أدلة الإدانة التي تدين المتهم، وقد ينفي المتهم هذا الدليل، وهنا يأتي دور القاضي الذي قد يصدر الحكم الذي يعبر عن الحقيقة في القضية.

الفرع الأول: مصداقية الدليل الإلكتروني

تعبر مصداقية الدليل الإلكتروني عن مدى تأكد القاضي من عدو وجود أي تغيير، أو تلاعب، أو حذف، أو تحريف إما عن طريق التعمد أو عن طريق الخطأ في الأدلة التي يتم الحصول عليها في الجرائم الإلكترونية.

ويحاول المدافع عن مرتكبي الجرائم الإلكترونية بتشكيك القاضي في مدى مصداقية تلك الأدلة من خلال المزايدة على هذه المصداقية مما يجعل القاضي يتشكك فيه مدى صحة الدليل، وقد يقوم باستبعاده نهائيًا من القضية المطروحة.

أ- التلاعب والعبث بالدليل الإلكتروني من قبل الجناة

يتميز الجناة في جرائم المعلومات بارتكاب الجرائم عن طريق الاستعانة بالوسائل الإلكترونية بالكفاءة والذكاء والحرفية في إتقان الجوانب الفنية في الجرائم التي يتم ارتكابها، مما يمكنهم من إخفاء الأعمال غير المشروعة التي قد تكشف عن شخصيتهم أثناء استخدامهم لتلك الوسائل الإلكترونية، حيث يقومون باستعمال النبضات أو الذبذبات الالكترونية غير المرئية، والتي يمكن بواسطتها تدوين البيانات.

وقد يقوم الجناة في الجرائم الإلكترونية باختراق قواعد البيانات وتعديل محتواها من أجل الحصول على الربح وإثبات الذات، وقد يقومون بإدخال معلومات وبيانات غير سليمة في نظام الحاسوب، وقد يعملون على تعديل برامجه والتغيير في البيانات المخزنة دون ترك أي دليل يشير إلى الجرم الذي تم ارتكابه (عبد المطلب، ٢٠٠٦).

ب- محو الدليل الإلكتروني

من أهم السمات التي تميز الدليل الإلكتروني هو سهولة حذفه في وقت قصير، حيث يمكن لمرتكب الجريمة أن يمحو الأدلة القائمة ضده أو يقوم بإتلافها في وقت قصير جدًا، بضغطة زر، مما يشير إلى سهولة حذف أو تدمير تلك الأدلة الأمر الذي يزيد من خطورتها.

ولا تتمكن السلطات المختصة من كشف الجرائم التي قامت بكشفها، حيث يمكن العبث بتلك البيانات والمعلومات إما بمحوها أو

تدميرها حتى لا تتمكن السلطات من إقامة الأدلة ضد الجاني وإدانته بها. ومن الملاحظ في بعض الأحيان أن المجني عليهم يشاركون أيضًا في احتمالية عدم التوصل إلى الجرائم الإلكترونية، عن طريق التراجع في الإبلاغ عن الواقعة، أو التردد في تقديم الدليل الذى يوجد لديهم بشأن تلك الجرائم.

وقد تتمثل غايهم من وراء ذلك في ضمان ثبات وضعهم الاقتصادي، أو لتفادي مخاطر التشهير بهم وبسمعتهم، وربما لرغبتهم في عدم الكشف عن الوسيلة التي استخدمها الجناة في ارتكاب جرائمهم حتى لا ينتهجها مجرمون آخرون.

وعادة المؤسسات المالية كالبنوك، قد تلجأ إلي هذا الأسلوب نظرًا لخوف من يقومون بإدارتها من انتشار أخبار تلك الجرائم، وبالتالي يفقدون ثقة عملائهم بهم، وبالتالي يخسرون تعاملاتهم، (وتمتلئ المؤسسات المالية بما يماثل تلك الوقائع والتي لا يتم الافصاح عنها)، والتي يتسبب الإعلان عنها في نظرهم في حدوث إضرار بمصالحهم وخاصة عند إبلاغهم عن الجرائم ونسبها إلى مرتكبيها وإيقاع العقاب الملائم بهم.

ويعد هذا الأمر سوء تقدير للأمور لأنه يمكن المجرم في جرائم المعلومات في متابعة أنشطته الإجرامية في أمان، كما تؤدي لزيادة طموحه في تطوير الوسائل الإجرامية التي يتبعها وخاصة بعد وصوله للنجاح وتحقيق الثراء من جراء أعماله المشبوهة.

والتراجع عن الإبلاغ عن الجرائم الإلكترونية، قد ينتج عنه نتائج خطيرة للغاية، فقد يزيد من الرقم الأسود (سرور، ٢٠٠٩)، ويمنع وضع السياسة الجنائية الصحيحة لمكافحة تلك الجرائم عن طريق المنع أو الكشف لها عن طريق اختيار الوسائل المناسبة للتصدي لها، وهنا قام البعض، وخاصة في الولايات المتحدة الأمريكية، بأن يتم إقرار عدد من النصوص القانونية فيما يتعلق بالجرائم التي يتم ارتكابها عن ريق الحاسب الآلي، بحيث يتم إقرار أن الكشف عن هذه الجرائم هي مسؤولية على الموظفين التابعين للجهة المجني عليها، فيتوجب عليهم الإبلاغ فور وقوع الجرم وإثبات وقوعها.

ج- دور الخبير في التأكيد على مصداقية الدليل الإلكتروني

يتيح ما يتمتع به المجرم في الجرائم الإلكترونية من قدرات فنية وعقلية وصوله إلى هدفه بدون ترك أي أدلة أو آثار تأخذ ضده، فهو قد يستخدم شفرة أو وضع كلمة سر حتى يتمكن من إخفاء الدليل الذي قد يدينه في القضايا المطروحة، وقد يقوم أيضًا بوضع شفرة للتعليمات عن طريق استخدام برامج متطورة لتشفير البيانات مما يؤدي لزيادة صعوبة الكشف عنه.

ومن ناحية أخرى، فقد أصبح الكشف عن الدليل الذي يدل على إثبات الجرائم عن طريق الوسائل الإلكترونية شديد الصعوبة، خاصة في الجرائم التي يتم فيها ربط جهاز الحاسوب بشبكة الاتصالات العالمية، ويرج السبب في ذلك إلى تطلب هذا الدليل لوجود خبرات فنية، وكفاءة عالية في عملية معالجة المعلومات والبيانات بشكل

يمكن من التوصل إلى الدليل وضبطه بأفضل الطرق (حسين، ٢٠١١: ٢٥).

الفرع الثاني: حرية القاضي الجنائي في تقدير الدليل الإلكتروني

بشكل عام، لا يقوم نظام الإثبات الحر أساليب محددة في عملية الإثبات، بحيث أنه يمنح لكل طرف من أطراف الدعوى الحرية في تقديم أدلة لإثبات الدعوى، وتكون مهمة القاضي الجنائي هي تقييم تلك الأدلة من أجل التوصل لقناعة بشأن الأدلة التي تم طرحها أمامه للبحث، حيث يتم إصدار الحكم النهائي له في ظل تلك القناعة التي تعبر عن كشف حقيقة الجريمة.

ونظرًا لكون الأدلة الإلكترونية أحد تطبيقات الدليل العلمي لما تتسم به من موضوعية وحيادية، فضلًا عن إمكانيتها وكفاءتها في إقناع القاضي الجنائي، وهو الأمر الذي جعل البعض يعتقد بأنه كلما تمتعت الأدلة العلمية بمساحة أكبر، ومنها الأدلة الإلكترونية بشكل خاص، كلما تقلص الدور التقديري للقاضي الجنائي (الجملي، ٢٠٠٩).

وفي مرحلة النقاش فيما يتعلق بالدليل العلمي بشكل عام، والدليل الإلكتروني بشكل خاص، يجب أن يتم التمييز بين قيمة الدليل الإلكتروني العلمية القاطعة، وبين ما يحيط بكشف الدليل من ظروف وملابسات.

في هذه الحالة نجد أن للقاضي الحق الكامل في عدم قبول هذا الدليل إذا ثبت له أن وجودة لا يتوافق بشكل منطقي مع ملابسات الجريمة، بحيث لا يتقبله عقله، كما يجوز للقاضي قبول الدليل في حالة إذا ثبت أنه ملائم لظروف وملابسات القضية، وبالتالي يمكن الأخذ به.

والخلاصة نستطيع القول أنه ليست هناك صعوبات أو مشكلات فيما يتعلق بحجية الأدلة الإلكترونية لكونها تقع تحت مظلة الأدلة العلمية، ومرجع ذلك تمتع القاضي الجزائي بالحرية الكاملة لتقدير الأدلة لإثبات الجرائم عامة ومن ضمن ذلك الجرائم الإلكترونية.

ولذلك فإن للقاضي دورًا محوريًا ذو أهمية كبيرة في حجية الأدلة الإلكترونية، والذي يمكن من فحص أي دليل وتقدير قيمته (عن طريق الاستعانة بالخبراء مع حفظ ما يمنح لمحكمة الموضوع من حرية كاملة في تقدير قوة الأدلة في تقرير الخبراء)، وأن يأخذ بالدليل الذي يشكل اقتناعه بما استقر في عقيدته ووجدانه. ومن ثم يقوم بإصدار حكمه وفقًا لاقتناعه بالقضية المطروحة، ويكون هذا الحكم إما بالإدانة أو بالبراءة، هو أهم المبادئ القضائية التي يقوم عليها الإثبات الجنائي.

الفرع الثالث: وزن الدليل الإلكتروني في الاثبات الجنائي أمام القاضي الجنائي

تعد محكمة الموضوع هي صاحبة السلطة الكاملة في الأدلة الموجودة في الدعوى المطروحة للبحث، فهي تعتبر سلطة الخبرة الأعلى في جميع ما يمكنها الفصل فيه، ويكون من سلطتها أخذ أو ترك ما تطمئن له من التقارير التي قدمها إليها الخبراء (حكم تمييز دبي بتاريخ ٢٠١٠/٢/٨ في الطعن رقم ١٣/٢٠١٠ جزاء).

ومن ثم فإنه يقصد بقيمة الدليل الإلكتروني الذي يتم الحصول عليه من الجرائم الإلكترونية وقيمته أمام القاضي الجنائي، وهو مدى الاعتراف به في القرائن أو الأدلة الموجودة في الدعوى، ومدى الأخذ به كدليل منفرد في الحكم ببراءة أو إدانة المجرم، أم أنه يتطلب وجود أدلة أخرى تعززه للأخذ بتساند الأدلة.

١- في حالة مراعاة الجوانب القانونية والفنية عند الحصول على الدليل الإلكتروني

يعد الدليل الإلكتروني الذي يتم بواسطة إجراءات مشروعة، ويتم فيه احترام كافة الجوانب الفنية، والتي تتمثل في تأكد الخبير الفني من مدى مصداقيته من الأدلة التي يتم الاعتماد عليها في الإثبات الجنائي.

ومن ثم يصبح الدليل الإلكتروني في تلك الحالة يمكن الاعتماد عليه كدليل مستقل قائم بذاته حتى في حالة كونه الدليل الوحيد في إثبات القضية، والذي يتيح إدانة أو براءة المجرم، ولكن يتوقف ذلك على مدى تأكد القاضي من سلامة الدليل الإلكتروني من الوجهة الفنية.

٢- حالة عدم مشروعية اجراءات الحصول على الدليل الإلكتروني

ويتعلق هذا الأمر بمدى اعتبار ذلك الإجراء من الأدلة الجوهرية، وبالتالي ما يترتب عليه في مخالفة البطلان، والحالات التي يعد فيها هذا الإجراء غير جوهري، وبالتالي جواز الاعتماد عليه في الإثبات الجنائي.

ويجب النظر هنا إلى الغرض التشريعي، فتقدير القاضي عدم الأخذ بالإجراء ينتج عنه تأخر الهدف المطلوب من العمل الإجرائي، كان الإجراء في تلك الحالة جوهري (بلال، ٢٠٠٩).

وإذا كان الهدف من الإجراءات التي تتعلق بالحصول على الدليل الإلكتروني هي حماية الحق في الخصوصية ومنع انتهاك الخصوصية في المعلومات، فإنه ينتج عن انتهاك تلك الإجراءات تأخر الهدف المراد تحقيقه عن طريق هذه الإجراءات، ونظرًا لأن الهدف الرئيسي منها المحافظة على المصلحة العامة من جانب، وحماية مصلحة الفرد من جانب أخر، كما تهدف هذه الإجراءات أيضًا إلى حماية حقوق وحريات الأشخاص والمحافظة عليها.

فبالنسبة إلى الإجراءات التي تقوم على التوصل للدليل الإلكتروني، فنجد أنها تعتبر من الإجراءات الجوهرية والتي تتعلق بالنظام العام مما ينتج عنه مخالفة البطلان، والبطلان المقصود هنا هو ما يتعلق بالنظام العام.

ومن الضروري قيام المحكمة باستبعاد أي دليل ينتج عنه إجراءات غير مشروعة من خلال مخالفة ما ورد في نصوص القانون، فلا يجوز أن يأخذ القاضي بدليل قد ثبت بالفعل بأنه تم الحصول عليه من خلال استخدام وسائل غير مشروعة فقط لكون المتهم لم يتمسك به.

٣- آثار بطلان الدليل الإلكتروني

هناك اختلاف ما بين الفقه والقضاء حول هذا الأمر، فقد انقسموا فيه إلى رأيين رئيسيين، وهما:

الأول: يرى أن عدم مشروعية الدليل الإلكتروني تستلزم عدم الأخذ بما يستخلص منه من أدلة، فكل ما يبنى على باطل فهو باطل، ولا يتم الاعتداد به في الإثبات الجنائي، ويجب عدم الأخذ به واللجوء للكشف عن أدلة جديدة أخرى.

الثاني: يرى أن الأخذ بعدم المشروعية في المراقبة الصوتية لا تستوجب عدم مشروعية ما ينتج عنها من أدلة، حيث ينظر أصحاب هذا الاتجاه إلى وجود اختلاف ما بين كلًا من الدليل ووسيلة التوصل إليه.

فانعدام مشروعية الإجراء لا يؤدي بدوره لعدم مشروعية الدليل، فالقاضي يتمتع بالحرية الكاملة في تكوين عقيدته ووجدانه، فعند التوصل إلى الاقتناع التام بالدليل الجنائي كدليل على صحة الواقعة وإثبات وقوعها، فإنه سوف يقضي بالإدانة دون الأخذ بطبيعة الإجراء الجنائي الذي أدى إليه، فهذا الاتجاه يذهب إلى تغليب مصلحة الدولة في العقاب على حقوق الإنسان.

الخاتمة

وبعد مناقشة الموضوع الذي تناوله البحث والذي يتميز بالأهمية والحيوية، وهو موضوع الجريمة الإلكترونية، وجد أن المشرع الإماراتي اتخذ خطوات موفقة في نظام الأخذ بالإثبات الحر في قانون الإجراءات الجزائية، حيث حصل القضاة على سلطات تقديرية في وزن وتقدير القوة التدليلية للأدلة المعروضة عليهم.

وقد أقر المشرع الإماراتي مثله في العديد من القوانين المقارنة بمبدأ يتمثل في الإثبات الحر ومكانه في القانون الجزائي، وجاء هذا الإقرار متوافقًا بشكل منطقي مع السلطات التقديرية للقضاة في مرحلة التقدير ومرحلة وزن الأدلة ومرحلة الاقتناع بالأدلة وحقيقتها والحكم في القضايا وفقًا لما تمليه عقيدة القاضي ووجدانه عليه.

ونحن نرى بعدم التعارض، مطلقًا، فيما بين كل من التطور العلمي والإقرار بالأساليب الجديدة في الإثبات الجنائي، ومنح القاضي حريات كاملة للتوصل إلى عقيدته، فالأمر في ذاته لا يتعدى إلا أن يكون توسعًا في الاستفادة من الوسائل الجديدة واستعمالها في مجال الإثبات الجنائي، وأيضًا في جانب السلطة التقديرية للقاضي إلا في إطار التقنيات الحديثة، ومن خلال استخدامه الأفضل باعتباره أحد الوسائل العلمية.

ومن خلال هذا البحث تم استخلاص عدد من النتائج والمقترحات يمكن تناولها فيما يلي:

أولاً: النتائج

١- بقى الخلاف قائمًا على المستوى الفقهي والتشريعي حول عدم الاتفاق على مصطلح واحد للجرائم التي تختص بالإنترنت والحاسب الآلي، والجرائم التي تتعلق بالاتصالات وتقنيات المعلومات. ولذلك توجد العديد من المسميات، فتم إطلاق العديد من لتلك المسميات مثل الجرائم السيبرانية والجرائم الإلكترونية.

٢- أثبتت وسائل الإثبات القديمة فشلها في التعامل مع الجرائم الإلكترونية الحديثة، وذلك نظرًا

لاستعمال وسائل علمية وفنية مبتكرة، ولذلك وجب استعمال نفس الوسائل لمجابهتها وإثباتها، ويجب على من يعملون في الإثبات الجنائي العمل على تطوير المهارات والتقنيات لمواجهة التطور السريع للجرائم الإلكترونية.

٣- تعتبر وسائل تنفيذ الجرائم الإلكترونية هي نفس وسائل الإثبات فيها، وقام المشرع باستعمال نفس الألفاظ مثل إنشاء أو إدارة موقع إلكتروني وإنتاج برامج جديدة.

٤- يجب توافر خبرات فنية عالية بجانب القدرة على معالجة البيانات والمعلومات حتى تصبح نافعة في فهم الدليل وتحديده واختبار أفضل وسائل لضبطه، وذلك يعزز الرأى الخاص بصعوبة الإثبات في الجرائم الإلكترونية.

٥- تتوافق حجية الأدلة الإلكترونية مع حرية القاضي الجنائي في تقدير الأدلة المختلفة، حيث أنها تشكل أدلة إثبات في المواد الجنائية.

٦- كفل القانون الإماراتي للقاضي الحرية الكاملة في تحديد عقيدته وتكوينها، تشمل ضمانات كثيرة، من أمثلتها مفهوم حرية المتهم في الدفاع عن نفسه، ومفهوم عدم اجبار المتهم على تقديم أدلة تدينه، واحترام حرمة الحياة الشخصية للأفراد، حيث أنه من الضروري ضمان توافرها لتحقيق اليقين لدى القاضي، وذلك مكفولًا بالعديد من الاعتبارات القانونية والدستورية التي تختص بتطبيق النظام العام.

٧- تبني آليات وطرق الإثبات في المجال الجنائي بشكل كبير على العلوم الحديثة، حيث أن له قيمة هائلة في عملية الإثبات الجنائي، وفي هذا الصدد يجب أن يتوافر مبدأين رئيسيين، المبدأ الأول: أن السلطات المعنية تتكفل بالإجراءات والأدلة المستخلصة من الوسائل التكنولوجية الحديثة وفقًا لما أقره القانون في هذا المجال، وطبقًا لما ورد في القواعد المحددة له حتى تتناسب مع النظام العام والآداب العامة.

المبدأ الثاني: يجب على وسائل الإثبات العملية أن تعتمد على أسس علمية وقوانين ونظريات علمية تم تجربتها والتأكد من صحتها، وعلى إثر ذلك يتم الوصول لنتائج قاطعة أو مرجحة، وذلك يستلزم تحديد معايير للتفرقة بين الدليل القاطع والدليل المرجح.

ثانياً: المقترحات

١- ما دامت سلطة القاضي الجنائي التقديرية قد فرضت نفسها من خلال قوتها الثبوتية في التعامل، أصبح من الضروري أن يقوم المشرع على تطوير هذه السلطة عن طريق تنشيط مراقبة التقديرات الواقعية للقاضي الجنائي، لا سيما المتابعة في تقدير القاضي للأحداث الفنية ومطابقتها للمنطق القضائي سواء في الجنح أو الجنايات، لأن المشرع حتى وإن أدرج نصوص متعلقة بالأدلة الحديثة فإنها تبقى خاضعة للسلطات التقديرية للقاضي بشكل عام.

٢- صياغة نصوص إجرائية خاصة بتنظيم خاصة فيما يختص بالتفتيش على المسرح الإلكتروني (في حالة صدور إذن تفتيش لنظام إلكتروني للحصول على أدلة يمكن تفتيش جميع الملفات في النظام عن طريق أخذ نسخة منها بدون

اللجوء للنظام، وفي تلك الحالة يمكن للمحقق عدم الافصاح عن الأدلة لمنع العبث).

٣- أما في حالة امتداد الجريمة الآليكترونية لأكثر من مكان كتفتيش سكن آخر (غير محل الاذن بالتفتيش) لا يجوز التفتيش إلا من خلال إذن تسمح به السلطات المختصة في الحالات الضرورية.

المراجع

إبراهيم، خالد ممدوح. ٢٠١٤. الجرائم المعلوماتية. الإسكندرية: دار الفكر الجامعي.

أحمد، هلالي عبد اللاه. ٢٠١١. النظرية العامة للإثبات في المواد الجنائية. القاهرة: دار النهضة العربية.

بلال، أحمد عوض. ٢٠٠٩. استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية. القاهرة: دار النهضة العربية.

بيومي، عبد الفتاح. ٢٠٠٧. الإثبات الجنائي في جرائم الكمبيوتر والإنترنت. القاهرة: دار الكتب القانوني.

الجملي، طارق محمد. ٢٠٠٩. الدليل الرقمي في مجال الاثبات الجنائي. ورقة عمل للمؤتمر الأول المغاربي الأول حول المعلوماتية، لأكاديمية الدراسات العليا، طرابلس.

حسين، سامي جلال فقي. ٢٠١١. الأدلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي. القاهرة: دار الكتب القانونية.

الحلي، خالد عياد. ٢٠١١. إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. الأردن: دار الثقافة للنشر والتوزيع.

خليل، ضياء الدين محمد. ٢٠٠٤. قواعد الإجراءات الجنائية ومبادئها في القانون المصري. القاهرة: مطبعة كلية الشرطة.

راجح، فايز محمد. ٢٠١١. الجرائم المعلوماتية في القانون الجزائري واليمني. رسالة دكتوراه. جامعة نايف للعلوم الأمنية، قسم القانون الجنائي والعلوم الجنائية، الرياض.

سرور، أحمد فتحي. ٢٠١٦. الوسيط في قانون الإجراءات الجنائية. القاهرة: دار النهضة العربية.

شريف، السيد محمد حسن. ٢٠٠٢. النظرية العامة للأثبات الجنائي. القاهرة: دار النهضة العربية.

الطراونة، حسن عوض. ٢٠٠٥. ضوابط السلطة التقديرية للقاضي الجنائي. رسالة دكتوراه. كلية الحقوق، جامعة القاهرة.

عبد المطلب، ممدوح عبد الحميد. ٢٠٠٦، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، المحلة الكبري: دار الكتب القانونية.

عدنان، سوزان. ٢٠١٣ انتهاك حرمة الحياة الخاصة عبر الانترنت. مقال منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٩، العدد الثالث.

عزت، فتحي محمد أنور. ٢٠١٠. الأدلة الإلكترونية في المسائل الجنائية

والمعاملات المدنية والتجارية. القاهرة: دار الفكر والقانون للنشر والتوزيع.

عقيلة، بن لاغة. ٢٠١٢. حجية أدلة الإثبات الجنائية الحديثة. مذكرة ماجستير في القانون الجنائي، جامعة الجزائر، كلية الحقوق، الجزائر.

الفيل، على عدنان. ٢٠١١. الإجرام الآليكتروني دراسة مقارنة. بيروت: منشورات زين الحقوقية.

قنديل، أشرف عبد القادر. ٢٠١١. النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي. الإسكندرية: دار الجامعة الجديدة.

قنديل، أشرف عبد القادر. ٢٠١٥. الإثبات الجنائي في الجريمة الآليكترونية. الإسكندرية: دار الجامعة الجديدة.

محكمة النقض المصرية، الطعن رقم ٢٧٠٣ لسنة ٥٠ ق جلسة ١٩-٤-١٩٨١.

محمد، لينا جمال. ٢٠١٦. الجرائم الإلكترونية. عمان، دار خالد اللحياني للنشر والتوزيع.

محمد، فضل زيدان. ٢٠٠٦. سلطة القاضي الجنائي في تقدير الأدلة. الأردن: دار الثقافة للنشر والتوزيع.

مراد، بلولهي. ٢٠١١. الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة. رسالة ماجستير، جامعة الحاج خضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة.

مصطفى، عائشة بن قارة. ٢٠١٠. حجية الدليل الآليكتروني في مجال الإثبات الجنائي. الإسكندرية: دار الجامعة الجديدة.

موسى، مصطفى محمد. ٢٠٠٩. التحقيق الجنائي في الجرائم الآليكترونية. القاهرة: مطابع الشرطة.

هليل، فرج علواني. ٢٠٠٦. التحقيق الجنائي والتصرف فيه والأدلة الجنائية. القاهرة: دار المطبوعات العملية.

REFERENCES

'Abd Al-Muttalib, Mamduh 'Abd Al-Hamid. 2006. *Al-Bahth Wa al-Tahqiq Al-Jina'iyy Al-Raqamiyy Fi Jara'im Al-Kumbiwtar Wa al-Internet*. Al-Mahallat Al-Kubra: Dar al-Kutub Al-Qanuniyyah.

'Adnan, Suzan. 2013 *Intihak Hurmat Al-Hayah Al-Khassah 'Abr Al-Internet*. Maqal Manshur Fi Majallah Jami'ah Dimashq Li al-'Ulum Al-Iqtisadiyyah Wa al-Qanuniyyah. Al-Mujallad 29. Al-'Adad Al-Thalith.

Ahmad, Hilaliyy 'Abdullah. 2011. *Al-Nazariyyat al-'Ammah Li al-Ithbat Fi al-Mawadd al-Jina'iyyah*. Al-Qahirah: Dar al-Nahdat al-'Arabiyyah.

'Aqilah, Bin Laghah. 2012. *Hujjyyat Adillat Al-Ithbat Al-Jina'iyyah Al-Hadithah*. Mudhakkirah Majistir Fi Al-Qanun Al-Jina'iyy. Jami'ah Al-Jaza'ir, Kulliyyat Al-Huquq, Al-Jaza'ir.

Bilal, Ahmad 'Iwad. 2009. *Istib'ad Al-Adillat Al-Mutahassilah Bi Turuq Ghayr Mashru'ah Fi Al-Ijra'at Al-Jina'iyyah*. Al-Qahirah: Dar Al-Nahdat Al-'Arabiyyah.

Bayyumiyy, 'Abd Al-Fattah. 2007. *Al-Ithbat Al-Jina'iyy Fi Jara'im Al-Kumbiwtar Wa al-Internet*. Al-Qahirah: Dar al-Kutub Al-Qanuniyy.

Thaqafah Li al-Nashr Wa al-Tawzi‘.

Murad, Balulahiyy. 2011. *Al-Hudud Al-Qanuniyyah Li Sultat Al-Qadiyy Al-Jaza’iyy Fi Taqdir Al-Adillah*. Risalah Majistir. Jami‘ah Al-Hajj Khidr, Kulliyyat Al-Huquq Wa al-‘Ulum Al-Siyasiyyah, Qism Al-Huquq, Batinah.

Mustafa, ‘A’ishah bin Qarah. 2010. *Hujjiyyat Al-Dalil Al-Iluktruniyy Fi Majal Al-Ithbat Al-Jina’iyy*. Al-Iskandariyyah: Dar Al-Jami‘at Al-Jadidah.

Musa, Mustafa Muhammad. 2009. *Al-Tahqiq Al-Jina’iyy Fi Al-Jara’im Al-Iluktruniyyah*. Al-Qahirah: Matabi‘ Al-Shurtah.

Rajih, Fayiz Muhammad. 2011. *Al-Jara’im Al-Ma‘lumatiyyah Fi Al-Qanun Al-Jaza’iriyy Wa al-Yamaniyy*. Risalah Dukturah. Jami‘ah Nayf Li al-‘Ulum Al-Amniyyah, Qism Al-Qanun Al-Jina’iyy Wa al-‘Ulum Al-Jina’iyyah, Al-Riyad.

Sharif, Al-Sayyid Muhammad Hasan. 2002. *Al-Nazariyyat Al-‘Ammah Li al-Ithbat Al-Jina’iyy*. Al-Qahirah: Dar Al-Nahdat Al-‘Arabiyyah.

Surur, Ahmad Fathiyy. 2016. *Al-Wasit Fi Qanun Al-Ijra’at Al-Jina’iyyah*. Al-Qahirah: Dar Al-Nahdat Al-‘Arabiyyah.

Al-Tarawanah, Hasan ‘Iwad. 2005, *Dawabit Al-Sultat Al-Taqdiriyyah Li al-Qadiyy Al-Jina’iyy*. Risalah Dukturah. Kulliyyat Al-Huquq, Jami‘at Al-Qahirah.

Qandil, Ashraf ‘Abd Al-Qadir. 2011. *Al-Nazariyyat Al-‘Ammah Li al-Bahth Al-Jina’iyy Wa Athruha Fi ‘Aqidat Al-Qadiyy*. Al-Iskandariyyah: Dar Al-Jami‘ah Al-Jadidah.

Qandil, Ashraf ‘Abd Al-Qadir. 2015. *Al-Ithbat Al-Jina’iyy Fi Al-Jarimat Al-Iluktruniyyah*. Al-Iskandariyyah: Dar Al-Jami‘ah Al-Jadidah.

Al-Fil, ‘Aliyy ‘Adnan. 2011. *Al-Ijram Al-Iluktruniyy Dirasah Muqaranah*. Beirut: Manshurat Zayn Al-Huquqiyyah.

Halil, Faraj ‘Ulwaniyy. 2006. *Al-Tahqiq Al-Jina’iyy Wa al-Tasarruf Fih Wa al-Adillat Al-Jina’iyyah*. Al-Qahirah: Dar Al-Matbu‘at Al-‘Amaliyyah.

Husayn, Samiyy Jalal Faqiyy. 2011. *Al-Adillat Al-Mutahassilah Min Al-Hasub Wa Hujjiyyatuha Fi Al-Ithbat Al-Jina’iyy*. Al-Qahirah: Dar al-Kutub Al-Qanuniyyah.

Al-Huliyy, Khalid ‘Iyad. 2011. *Ijra’at Al-Taharriyy Wa al-Tahqiq Fi Jara’im Al-Hasub Wa al-Internet*. Al-Urdun: Dar Al-Thaqafah Li al-Nashr Wa al-Tawzi‘.

Ibrahim, Khalid Mamduh. 2014. *Al-Jara’im Al-Ma‘lumatiyyah*. Al-Iskandariyyah: Dar al-Fikr Al-Jami‘iyy.

‘Izzat, Fathiyy Muhammad Anwar. 2010. *Al-Adillat Al-Iluktruniyyah Fi Al-Masa’il Al-Jina’iyyah Wa al-Mu‘amalat Al-Madaniyyah Wa al-Tijariyyah*. Al-Qahirah: Dar al-Fikr Wa al-Qanun Li al-Nashr Wa al-Tawzi‘.

Al-Jamaliyy, Tariq Muhammad. 2009. *Al-Dalil Al-Raqamiyy Fi Majal Al-Ithbat Al-Jina’iyy*. Waraqah ‘Amal Li al-Mu’tamar al-Awwal Al-Magharibiyy Al-Awwal Hawla Al-Ma‘lumatiyyah, Li Akadimiyyat Al-Dirasat Al-‘Ulia, Tarablus.

Khalil, Diya’ Al-Din Muhammad. 2004. *Qawa‘id Al-Ijra’at Al-Jina’iyyh Wa Mabadi’uha Fi Al-Qanun Al-Misriyy*. Al-Qahirah: Matba‘ah Kulliyyat Al-Shurtah.

Mahkamat Al-Naqd Al-Misriyyah. *Al-Ta‘n Raqam 2703 Li Sanah 50 Q Jilsah 19-4-1981*.

Muhammad, Lina Jamal. 2016. *Al-Jara’im Al-Iluktruniyyah*. ‘Amman: Dar Khalad Al-Lihyaniyy Li al-Nashr Wa al-Tawzi‘.

Muhammad, Fadl Zaydan. 2006. *Sultat Al-Qadiyy Al-Jina’iyy Fi Taqdir Al-Adillah*. Al-Urdun: Dar Al-

إنكار

الآراء الواردة في هذه المقالة هي آراء المؤلف. فردانا: المجلة العالمية في البحوث الأكاديمية لن تكون مسؤولة عن أي خسارة أوضرر أومسؤولية أخرى بسبب استخدام مضمون هذه المقالة.