"كفاية القواعد الإجرائية في ضبط الجريمة الإلكترونية بين تحديات الواقع وقيود القانون"

(دراسة مقارنة)

د. خالد علي الجنيبي

رئيس نيابة أول

النيابة العامة بدبي- الإمارات

E-mail: kjneibi@hotmail.com

"كفاية القواعد الإجرائية في ضبط الجريمة الإلكترونية بين تحديات الواقع وقيود القانون"

(دراسة مقارنة)

د. خالد علي الجنيبي
رئيس نيابة أول
النيابة العامة بدبي- الإمارات

الملخص

لقد أفرز التطور التقني نوعاً جديداً من الجرائم سُميت بالجرائم الإلكترونية، والّتي تجسدت في ظهور أنماط سلوكية غير مشروعة خرجت من رحم الاستخدام المفرط للتكنولوجيا. فقد خلقت الجريمة الإلكترونية بُعداً جديداً للجريمة وتحدياً لرجال الضابطة العدلية. فمع تزايد أعداد الجرائم الإلكترونية وتنوع طرق وأساليب ارتكابها برزت الحاجة إلى إيجاد وسائل للحد من استفحال انتشارها. ومع سعي رجال الضابطة العدلية نحو كشف وضبط الجرائم الإلكترونية تعرضت الحقوق الشخصية للمساس كحق الأفراد في الخصوصية، وما بين تعارض المصالح بين مصلحة الدولة في الكشف عن مرتكب الجريمة وبين حق الأفراد في الخصوصية برزت ورقة البحث لتسلط الضوء على هذا التعارض بين المصلحتين، فلمن تكون الغلبة والتفضيل؟ وهل نحن في حاجة إلى تعديل قوانيننا بما يتلاءم ومتطلبات التطور التقني وبما لا يمس بحقوق الافراد الشخصية؟ أم أن في مبررات سلطات الضبط والتحري وعجزها عن مواكبة سباق التطور التقني ما يشفع لها المساس بحقوق الافراد التي كفلها الدستور لهم؟ لقد خلص البحث إلى أن الجريمة الإلكترونية أضحت واقع حال وليست سحابة صيف، هذا الواقع يحتم علينا تلميم أوراقنا وإعداد عدتنا لمواجهة هذا الخطر المستفحل الذي أصاب مجتمعنا على جميع الأصعدة سواء كانت اجتماعية أو اقتصادية أو قانونية، الأمر الذي يقودنا حتماً إلى الاعتراف بضرورة تحديث التشريعات بما يتواكب والتطور التقني.

الكلمات الدالة: جرائم تقنية المعلومات، استقصاء الجرائم وجمع الأدلة، وسائل تقصي الجرائم الإلكترونية، الأدلة الالكتورنية، الخصوصية.

Adequacy of procedural rules to control Cybercrimes: Challenges of reality and limitations of law

(A comparative study)

Dr. Khaled Ali Aljneibi
Senior Chief Prosecutor
Dubai Public Prosecution- UAE

Abstract

The use of technology to support and enrich various aspects of life has spread globally. There are many positive aspects to this change; the paperless working environment in the office is increasing communication, accessibility, and accuracy. In contrast, the negative aspect of this advancement in technology is that new ways of committing crimes have been introduced. However, numerous measures have been suggested to help overcome this outbreak of cybercrime and the losses resulting from unlawful activities resulting from technology. Aside from the fact that technology has introduced a novel of crimes, electronic evidence can also play a significant role in the successful prosecution of crimes. The advent of the technological age has had a significant effect on litigation practice, none more so than in the area of evidence gathering. The demands of modern-day litigation practice have never been greater. The cybercrimes is one of the modern crimes which never has its share in studying and which size grows rapidly despite the efforts done to encounter it. This may refer to difficulties related to its investigations, getting evidence, or problems related to international cooperation against it. This article begins with a short overview of the various cybercrimes' aspects. It then moves on to discuss the nature of the cybercrimes and search and seizure process for electronic evidence. Finally, we have discussed the procedural challenges between the right of the authorities in the detection of crime and the right of privacy, to reach the article goal. The researcher utilizes the descriptive methodology analytical. The importance of this article is due to its focusing light on a modern crime, intending to understand this phenomenon in a compressive and integral scientific method. This study will benefit the officials in encountering this crime in discovering the obstacles in its investigations and the problems of the systematic international efforts in encountering it which lead to taking important decisions and instructions to minimize these obstacles and those problems for areal compact to this crime.

Keywords: Cybercrimes, Search and Seizer for Electronic Evidence, Privacy.

تمهيد وتقسيم:

لا مناص من الاعتراف بأن الثورة المعلوماتية [١] وما صاحبها من تطور في مجالات شتَّى سواء كانت اقتصادية أو اجتماعية أو ثقافية قد أوجدت بعداً انعكس إيجاباً على حياة الأفراد والمجتمعات حتى باتت الرفاهية سمة العصر الحديث. ولا مناص أيضاً من الاعتراف بأن التطور التقني ذاته أحدث ثورة أيضاً في المجال الإجرامي حيث قلبت التكنولوجيا مفهوم الجريمة ونقلتها من طور جرائم تقليدية ذات مسرح إجرامي محدد إلى مصاف جرائم اتسم مسرحها بالافتراضي، ومع الزيادة في التطور التقني تنوع شكل الجرم الإلكتروني. فمن المسلم به أن الجريمة دائماً سابقة في الوجود على القانون، لذلك اعتبرت الجريمة الإلكترونية إفرازًا من إفرازات التطور التقني الذي اوجب على المشرع القانوني التدخل تنظيماً لهذه الظاهرة الإجرامية المستحدثة. [٢] ومما لا شك فيه أن الجريمة الإلكترونية لها من المظاهر والخصائص ما يفردها عن الجريمة في مفهومها التقليدي فقد اثارت الجريمة الإلكترونية العديد من التحديات القانونية والعملية في سبيل البحث والتحري عنها وضبط مرتكبيها، مما أظهر الحاجة أيضاً إلى تطوير أساليب إثباتها واستخدام وسائل تتماشى والتطور التقني المستخدم في ارتكابها وما تفرزه من أدلة. فقد بات الدليل الإلكتروني[٣] محل اهتمام المشرع لما يمثله من أهمية بالغة في الكشف عن مرتكب الجريمة؛ إلا انه وفي الوقت ذاته خلق تحديات قانونية عديدة في سبيل الحصول عليه، لما له من خصاص استمدها من البيئة الافتراضية للجريمة الإلكترونية ومن طبيعته المتغيرة. وما بين مصلحة المجتمع في الكشف عن الحقيقة وضبط مرتكب الجريمة وبين مصلحة الأفراد وحقهم في حماية وكفاية حقوقهم القانونية الإجرائية وخاصة حينما يتعلق الامر بالبحث والتحري عن الدليل الإلكتروني، برز سؤال البحث وهو: مدى كفاية القواعد الإجرائية في ضبط الجريمة الإلكترونية دونما مساس بحقوق الأفراد الشخصية.

(١) يعد المفكر الأمريكي/ ألفن توفلر أول من أطلق مصطلح عصر المعلومات أو الثورة المعلوماتية، حيث يعد أحد أهم رواد علم المستقبل في العصر الحديث. وعلم المستقبل هو أحد العلوم الحديثة التي تعتمد على التنبؤ بالأوضاع الاقتصادية والاجتماعية والسياسية في المستقبل ويعد عالم الاجتماع الأمريكي / جيلفيلان أول عالم استخدم مصطلح علم المستقبل في أطروحة دكتوراه قدمت إلى جامعة كولومبيا بالولايات المتحدة الامريكية في عام ١٩٢٠م.

للمزيد من الاطلاع حول عصر المعلومات انظر: ألفن توفلر، وعود المستقبل، ترجمة غازي غصون، دار الروح، لبنان، ١٩٨٥م.

وللمزيد من الاطلاع حول علم المستقبل انظر: عبد الحي وليد، مدخل إلى الدراسات المستقبلية في العلوم السياسية، المركز العالمي للدراسات السياسية، الأردن، ٢٠٠٨م.

(٢) تعد اتفاقية بودابست الموقعة بتاريخ ٢٠٠١/١١/٢٣م والمتعلقة بالجرائم المعلوماتية خير مثال على سعي الاتحاد الأوروبي نحو التصدي للاستخدام غير المشروع للأجهزة الإلكترونية وشبكات المعلومات، تتكون هذه الاتفاقية من (٤٨) مادة تتناول الإجراءات الواجب اتخاذها على المستوى القومي ودراسة التعاون الدولي ودور السلطات المحلية في البيئة الرقمية.

(٣) حسب ما أطلق علية المشرع الاوروبي من أن الدليل الإلكتروني هو: الأثر الإلكتروني الذي تخلفه الجريمة الإلكترونية أو غيرها، سواء كان هذا الأثر الإلكتروني ناتجًا عن جهاز الكمبيوتر أو هاتف محمول أو أي آلة إلكترونية حاسبة من شأنها أن تخلف دليلاً يبين نسبة الجريمة إلى مقترفيها.

التعريف بالجريمة الإلكترونية

شاع مصطلح الجريمة الإلكترونية في الآونة الاخيرة مع شيوع استخدام التكنولوجيا؛ فتعددت صيغ اصطلاحها تعدداً حمل ثراء التنوع والاتساع فعمد البعض إلى تعريفها بالجريمة المعلوماتية وعرفها البعض الآخر بجرائم تقنية المعلومات وذهب آخرون إلى إطلاق وصف جرائم الحاسب الآلي عليها. ما يهمنا هنا هو ليس مناقشة الوصف الاصح وإنما التعريف بالجريمة الإلكترونية وبيانها فقط.

من أهم التعريفات التي قيلت تعريفاً للجريمة الإلكترونية تعريف منظمة التعاون الاقتصادي والتنمية (OCDE)؛ إذْ عَرَّفت الجريمة الإلكترونية في اجتماع باريس عام (١٩٨٣م) بأنها: (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآليّة للبيانات أو نقلها).[٤]

وفي الإطار العربي جاء تعريف الجريمة الإلكترونية حينما أقامت الجامعة العربية الندوة العربية في ١٩٩٨/٢/١م في إطار تعريف الجريمة المنظمة حيث عرفت الجريمة المنظمة بأنها:(كل سلوك إجرامي ترتكبه مجموعة من الأشخاص يحترفون الإجرام بشكل مستمر لتحقيق أهدافهم ضمن نطاق أكثر من دولة)، فدار رحى تعريف الجريمة الالكترونية في فلك تعريف الجريمة المنظمة.

و في الجانب التشريعي نجد أن البعض عمد إلى تعريف الجريمة الإلكترونية في نصوص القوانين التشريعية كما هي الحال في القانون السعودي حيث عَرَّف نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم م/ ١٧ المؤرخ في: ١٤٢٨/٣/٨هـ بناءً على قرار مجلس الوزراء رقم: (٧٩) المؤرخ في: ١٤٢٨/٣/٧هـ الجريمة الإلكترونية بأنها:(أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام).[٥] وكما هيالحال أيضاً حينما عرف القانون رقم (٦٣) لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات الكويتي الجريمة الإلكترونية بانها: (كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون).[٦]

بينما نحا البعض الآخر إلى مجرد الإشارة إلى أنماط الجريمة الإلكترونية دون تعريفها كما فعل المشرع الإماراتي حين بين المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات (كما جاء في صياغة نصوصه) الجريمة الإلكترونية بأنها: (كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الشبكة المعلوماتية أو وسيلة من وسائل تقنية معلومات)[٧] وكما فعل المشرع العماني أيضاً حينما نص في المادة الأولى من المرسوم السلطاني رقم (١٢)

(٤) انظر: www.oecd.org.

(٥) انظر: المادة رقم (١) من نظام مكافحة الجرائم المعلوماتية السعودي.

(٦) انظر: المادة رقم (١) من القانون رقم (٦٣) لسنة ٢٠١٥ م في شأن مكافحة جرائم تقنية المعلومات الكويتي.

(٧) المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ م في شأن مكافحة جرائم تقنية المعلومات جاء استبدالاً للقانون الاتحادي رقم (٦) لسنة ٢٠٠٦م.

لسنة ٢٠١١م بإصدار قانون مكافحة جرائم تقنية المعلومات من أن جرائم تقنية المعلومات:(هي الجرائم المنصوص عليها في هذا القانون) [٨] دون أن يضع تعريفاً محدداً للجريمة. والحال كذلك بالنسبة إلى مملكة البحرين حينما خلا القانون رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات من تعريف صريح للجريمة الإلكترونية.

وفي الجانب الفقهي ذهب "ميروي MERWE" إلى تعريف الجريمة الإلكترونية بأنها: الفعل غير المشروع الذي يرتكب باستخدام الحاسب الآلي كأداة رئيسية فيه أو باستخدام المعالجة الآلية للبيانات.[٩] بينما ذهب البعض الاخر إلى تعريف الجريمة الإلكترونية بأنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية.[١٠] وفي السياق ذاته ذهب البعض الآخر إلى تعريف الجريمة الإلكترونية بأنها: سلوك غير مشروع معاقب علية قانوناً، صادر عن إرادة جرمية، محله معطيات الحاسوب.[١١] بينما اكتفى البعض الاخر بتعريفها على أنها أشكال السلوك الغير المشروع المرتكب عن طريق الحاسب الآلي.[١٢]

وإزاء التعدد في تعريف الجريمة الإلكترونية والذي نتج عنه أن جاءت هذه التعريفات قاصرة عن الإحاطة بمفهوم الجريمة الإلكترونية، حيث ركَز البعض على الوسيلة المستخدمة في ارتكاب الجريمة واعتمد البعض الآخر على النتيجة الإجرامية بينما ذهب البعض إلى اعتماد موضوع الجريمة. وعليه ذهبت فئة من الباحثين في شأن الجريمة الإلكترونية إلى وضع عدد من الاعتبارات حتى يمكن القبول بتعريف الجريمة الإلكترونية وهي:

- القبول الدولي للتعريف، بمعنى أن يكون هذا التعريف مقبولاً لدى الدول الأخرى.
- مراعاة التطور التكنولوجي والتقني المتسارع.
- تحديد دور الكمبيوتر في النشاط الإجرامي.[١٣]

خلاصة القول إن تعريف الجريمة الإلكترونية يكتنفه كثير من الصعوبات في تحديده تحديداً جامعاً مانعاً يمكن من خلاله التميز بينه وبين الجريمة في مفهومها التقليدي. ونرى هنا أنه من

---

(٨) انظر المادة رقم (١) من المرسوم السلطاني رقم (١٢) لسنة ٢٠١١ م في شأن اصدار قانون مكافحة جرائم تقنية المعلومات.
(9) Vander Merwe, Computer Crimes and other crimes against information Technology in South Africa, (1993) , p554.

(١٠) د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، دار النهضة العربية، مصر، ٢٠٠٩م، ص٦.

(١١) عمر محمد بن يونس، الإجراءات الجزائية عبر الانترنت في القانون الأمريكي، دار النهضة العربية، مصر، ٢٠٠٥م. انظر أيضا: د. محمد عبابنه، جرائم الحاسوب وابعادها الدولية، دار الثقافة، الأردن، ٢٠٠٥م، ص ١٧.

(١٢) د. هشام رستم، جرائم الحاسب الآلي المستحدثة، دار الكتب القانونية، مصر، الطبعة الاولي، ١٩٩٩م، ص ١١٠.

(١٣) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ٢٠١٩م، ص ٧٥.

الأسلم عدم وضع تعريف للجريمة الإلكترونية فصور الجرائم الإلكترونية لا حصر لها خاصة مع التطور التقني المتسارع، فما يمكن أن نطلق علية اليوم بأنه صورة من صور الجريمة الإلكترونية قد لا يكون كذلك في المستقبل. وعوضاً عن ذلك يمكن وضع مبادىء استرشاديه فقط يمكن من خلالها التميز بين الجريمة الإلكترونية والجريمة التقليدية.[١٤]

خصائص الجريمة الإلكترونية

من الأهمية بمكان وبعد تعريف الجريمة الإلكترونية أن نبين بعضاً من خصائص الجريمة الإلكترونية ونميزها عن الجريمة في مفهومها التقليدي المتعارف علية؛ فمعرفة الفارق بين الجريمتين قد يكون سبيل النجاح لرجال البحث والتحري في الوصول إلى كشف غموض الجريمة الإلكترونية وبالتالي إلى تحديد شخص فاعلها. وحتى تكتمل الصورة الذهنية للجريمة الإلكترونية في ذهن القارئ قبل الخوض في تفاصيل قد تكون أكثر عمقاً حين استعراض نقاط البحث فكان لازماً بيان تلك الخصائص.

إذا ما طرح سؤال: هل يمكنك التمييز بين الجريمة في مفهومها التقليدي والجريمة الإلكترونية؟ فإن الإجابة قد تكون وللوهلة الاولى بسيطة يسيرة: (نعم) يوجد فرق ولكن مع تعمق الإجابة نجد أن الأمر يحتاج إلى شروح وتفسير قد يصعب على المتلقي ذي الثقافة القانونية البسيطة فهمها. فالجريمة الإلكترونية إذ ما كانت تشترك مع الجريمة التقليدية في أركانها المتعارف عليها قانوناً من ركن مادي ومعنوي وعلاقة سببية بين الفعل والنتيجة، إلا أنها تختلف باختلاف طرق ارتكابها وأدلتها والتي يصعب على رجال القانون فهمها. فالجريمة الإلكترونية ذات مسرح افتراضي لا حدود جغرافية له ، تتعامل مع رموز ومعطيات إلكترونية غير مادية وغير ملموسة ، فالاختلاف مثلاً بين الدليل في الجريمة التقليدية والدليل في الجريمة الإلكترونية هو الدعامة التي يكون عليها كل منهما ، فالأدلة التقليدية دعامتها أشياء مادية ملموسة ، بعكس الأدلة الإلكترونية ، فإن دعامتها رموز وإشارات، واعتماداً على هذا الفارق في التكوين، والوجود، يرى البعض أن الدليل الإلكتروني ، لا يكتسب صفة الدوام والاستقرار والثبات، إذ إنه قابل للمحو والتعديل والاتلاف، كما أنه غير قابل للقراءة أو المشاهدة البصرية وإنما هو نتاج تحاليل مختبرات لها شروطها الخاصة[١٥]

كما أنّهُ وعلى النقيض من الأدلة التقليدية فإن الدليل الإلكتروني دليل قابل للنسخ والتكرار.[١٦]

(١٤) ذهب د. رؤف عبيد إلى القول: " لا ريب أن مفهوم الجريمة مفهوم متطور من زمن إلى آخر، ومن مجتمع إلى آخر، فبينما نجد أن الفقه يُعنى بالجريمة بوصفها خروجاً شكلياً على قاعده آمره أو ناهيه. نجد أن علم الإجرام يُعنى بالجريمة بوصفها ظاهرة سلوكية تتضمن خروجاً شاذاً على أي وضع اجتماعي مستقر بما يلحق ضرراً بهذا الوضع". راجع في ذلك د. رؤف عبيد، أصول علم الاجرام والعقاب، دار الفكر العربي، القاهرة، مصر، الطبعة الخامسة، ١٩٨١م، ص ٢٧.

(15) Stephen Moson, Electronic Evidence, (3rd ed, LexisNexis Butterworths 2012) ,p28.

(16) Ross Anderson, Security Engineering, (2nd edn, Wiley Publishing Inc. 2008) p78.

فالدليل الإلكتروني يمكن نسخة وإعادة إرساله إلى شريحة كبيرة من الناس فعن طريق البريد الإلكتروني أو الأجهزة التقنية الاخرى يمكن نقل الأدلة الإلكترونية بين الأفراد و الأقطار مما يثير مشكلة تتبع الدليل الإلكتروني والحصول عليه وقد تثير هذه الخاصية للجريمة الإلكترونية مشاكل عدة منها إشكاليات الاختصاص القضائي وإجراءات الملاحقة والضبط. وعلى النقيض أيضاً من الأدلة التقليدية نجد أن الدليل الإلكتروني يوفر معلومات ومعطيات تفصيلية أكثر منها في الدليل التقليدي، فغالباً الأدلة الإلكترونية تبوح بمكان وزمان ارتكاب الفعل المجرم على وجه أكثر دقة وتفصيل من الأدلة الأخرى التي تثير الجانب الاحتمالي في التحديد. فعند تدوين إقرار مكتوب مثلاً فلا سبيل لمعرفة تاريخ الإقرار ومكانة إلا من خلال البيان المدون بالإقرار والذي قد يخالف حقيقة الواقعة بينما الأدلة الإلكترونية وباستخدام أجهزة خاصة يمكن تحديد زمان ومكان الفعل على وجه الدقة لا التخمين وبالتالي تكون الأدلة الإلكترونية أكثر غنى معرفيًا عن سائر أدلة الإثبات الأخرى.[١٧]

أهمية موضوع البحث

يعد موضوع مدى كفاية القواعد الإجرائية في ضبط الجريمة الإلكترونية ومدى تأثير إجراءات البحث والتحري عن الجريمة الإلكترونية على حرمة الحياة الخاصة للأفراد من الموضوعات التي برزت على الساحة في الآونة الأخيرة خاصة مع التطور التقني المتسارع وعجز القواعد القانونية عن الوفاء بمتطلبات الشرعية الإجرائية، فتصارعت التيارات بين منادٍ بحقوق الأفراد وحمايتها من أي تدخل قد يمس الخصوصية وبين تيار ينادي بالعدالة القضائية ووجوب ضبط تسارع الجريمة الإلكترونية فكان للبحث أهميته.

الفائدة النظرية للبحث

من الناحية النظرية: فإن البحث سيعالج مدى كفاية النصوص القانونية الإجرائية في ضبط الجريمة الإلكترونية والتي قد يؤدي عدم التقيد بالقواعد الإجرائية فيها إلى المساس بسلامة الدليل وشرعيته. كما أن مثل هذه الدراسات توفر أرضاً خصبة لتسليط الضوء على معوقات التطبيق سواء كانت قانونية أو حتى فنية ومنها يمكن وضع الحلول لتذليل تلك المعوقات أو التوصية لوضع تعديلات تشريعية. وقد يكون من خلال مثل هذه المساهمات البحثية أن تبصر الباحثين عن موضوعات أكثر حداثة يمكن التطرق إليها في بحوث تكون أكثر عمقاً كبحوث الرسائل العلمية كالماجستير والدكتوراه.

(17) Amanda Ngomane, The Use of Electronic Evidence in Forensic Investigation, (DPhil thesis, University of South Africa 2010) p34.

الفائدة العملية للبحث

من الناحية العملية التطبيقية: فالواقع يؤكد تزايد أعداد وحجم الخسائر جراء انتشار الجرائم الالكترونية [١٨]؛ فمستخدمو التقنية يزدادون بعشرات الملايين وقد تضاعفت هذه الزيادة مع انتشار استخدام الأجهزة الإلكترونية واستغلالها في تسهيل وارتكاب الجرائم.[١٩] ومما يؤكد أهمية هذا الموضوع أيضاً تلك المصلحة القومية والاجتماعية التي تستحق من المشرع التدخل تنظيماً لظرف الحصول على الأدلة الخاصة بالجرائم الإلكترونية بطريقة تكفل للأفراد أيضاً خصوصيتهم دون تعسف في استعمال السلطة.

إشكالية البحث

يتناول هذا البحث مشكلة قانونية بدأ بزوغ فجرها مع الاستخدام المفرط للتكنولوجيا وانتشارها في جميع مناحي الحياة. فمع شيوع استخدام الأجهزة الإلكترونية وتطورها الكبير والمتسارع وتطويعها في ارتكاب الجرائم بات من السهل كسر الحواجز الأمنية والوصول بمنتهي اليسر إلى شريحة كبيرة من الضحايا الذين يتم استهدافهم كمجني عليهم، فتفشت بالتالي رقعة انتشار الجريمة الإلكترونية. وفي سعي محمود سارعت العديد من الدول إلى كبح جماح الجريمة الإلكترونية بإصدار قوانين عقابية مشددة تجرم من خلالها أنماط السلوك الاجرامي وتحمي من خلاله الأفراد والمجتمعات من الآثار السلبية للجريمة الإلكترونية. إلا أنه وعلى الجانب الاخر وجدَت هذه الدول أن مجرد وجود القوانين العقابية قد لا يكون كافياً لمحاربة الجريمة الإلكترونية وبسط الحماية القانونية للأفراد والمجتمعات من مغبة الجريمة الإلكترونية بسبب قصور في التشريع الإجرائي الذي مكن العديد من مرتكبي الجرائم الإلكترونية من الإفلات من العقاب. الأمر الذي دفع افراد الضابطة العدلية[٢٠] إلى تجاوز حقوق كفلها الدستور بالحماية للأفراد حين سعيهم لضبط جريمة الإلكترونية. من هنا ظهرت إشكالية البحث: حيث سنحاول معالجة أبعاد التعرض لخصوصية الأفراد حين البحث عن الأدلة المتعلقة بجريمة ما ومدى كفاية القواعد الإجرائية المنصوص عليها في القوانين الإجرائية بالوفاء بمتطلبات الشرعية حين البحث عن الدليل الإلكتروني المتعلق بالجريمة الإلكترونية. فالتقنية أحياناً ما تكون غريبة على القانونيين

---

(١٨) أظهرت شركة نورتن العالمية المتخصصة في مجال أمن المعلومات ان عدد الأشخاص الذين تعرضوا إلى مخاطر وجرائم الكترونية بعام ٢٠١٧م بلغ ٩٧٨ مليون شخص حول العالم وإن حجم الخسائر المالية الناتجة عن ذلك بلغت ١٧٢ بليون دولار امريكي. لمزيد من المعلومات انظر التقرير : https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. اخر مشاهدة: ٢٠١٨/١٢/٢٤م.

(١٩) أظهر تقرير منظمة مكافحة الاحتيال العالمية أن مجموع الخسائر المالية لجرائم الاحتيال بصورة عامه والاحتيال الإلكتروني بلغت في عام ٢٠١٩م ٧ بليون دولار امريكي بمتوسط خسائر ١٣٠٠٠٠ دولار أمريكي للقضية الواحدة. لمزيد من المعلومات انظر التقرير: https://www.acfe.com/report-to-the-nations/٢٠٢٠/. اخر مشاهدة: ٢٠٢٠/١٠/١٣م.

(٢٠) يطلق على مصطلح الضابطة العدلية في دولة الإمارات وبعض الدول الأخرى الضبطية القضائية.

ورجال الضابطة العدلية لعدم فهم طريقة عملها وعدم استيعابها بالسرعة اللازمة مما ينتج عنه بطء في تنظيمها وطريقة معالجتها والتعامل معها خاصة إذا ما حاولنا تنظيم هذه التقنية وفق أطر قانونية محددة. إن هوة التسارع بين المجالين القانوني والتقني لا يمكن قياسه إذا ما سلمنا بواقع الحال وهو أن التقنية مجال متسارع حيث تطالعنا التقنية في كل يوم بما هو جديد في عالم الأجهزة والأدوات الإلكترونية وفي المقابل نجد أن تعديل القوانين بما يتواكب مع هذا التطور التقني يحتاج إلى سنوات وعمل شاق؛ فما يتم مناقشته من تعديلات للقوانين قطعاً سوف تصبح عديمة الفائدة حين إقرارها بعد مضي فترة زمنية طويلة. وخروجاً على ذلك قد يلجأ رجال الضابطة العدلية إلى طرق وأساليب لكشف الجريمة الإلكترونية بطريقة قد تمس الحقوق المكتسبة للأفراد بموجب الدساتير الوطنية ومنها الحق في الخصوصية فكان لازماً منا تسليط الضوء ولو بجزء يسير على هذه المشكلة القانونية. فهل تكفي القواعد الإجرائية المنصوص عليها في القوانين الإجرائية في مكافحة الجريمة الإلكترونية دون مساس بحقوق الأفراد الشخصية ومنها الحق في الخصوصية؟ أم يلزم إجراء تعديلات تشريعية خاصة في القوانين تكون متناسبة وطبيعة الجريمة الإلكترونية؟

خطة البحث

وعلى ضوء التعارض بين المصلحتين العامة والخاصة (مصلحة المجتمع في الكشف عن الحقيقة وضبط مرتكب الجريمة وبين مصلحة الأفراد وحقهم في حماية حقوقهم القانونية الإجرائية) ستناقش هذه الورقة الإشكالية الإجرائية التي تثيرها الجريمة الإلكترونية في سبيل البحث عن مرتكب الجريمة وخاصة حق الأفراد في الخصوصية انطلاقاً من فرضية مفادها أن القواعد الإجرائية المنصوص عليها في القوانين الإجرائية الجزائية لم تعد قادرة على ضبط الجريمة الإلكترونية والحد منها. وللوقوف على ذلك سنعمد إلى تقسيم الورقة إلى مبحثين رئيسين:

المبحث الاول: استقصاء الجرائم وجمع الأدلة.

المبحث الثاني: تأثير إجراءات البحث والتحري عن الجريمة الالكترونية على حرمة الحياة الخاصة للأفراد.

المبحث الاول

استقصاء الجرائم وجمع الأدلة

إن كانت القاعدة في الدعاوى الجزائية هي جواز الإثبات بكافة طرق الإثبات القانونية، والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي قد يعترف بالدليل ذي الطبيعة الإلكترونية[٢١]، إلا أن هذا الاعتراف قد يكون مشروطاً بقناعة القاضي

(٢١) ذهب البعض إلى أن الأدلة الإلكترونية هي أدلة ثانوية يمكن الأخذ بها على أساس أنها الدليل الأفضل ، بينما اشترط البعض الاخر للأخذ بالأدلة الالكترونية أن تكون بناء على تقرير معد من قبل خبير.

واطمئنانه للدليل، إلا أن هذا الأمر لم يَخْلُ من نقاش فقهي أثارته طبيعية الجريمة الإلكترونية حول كفاية القواعد الإجرائية في ضبط الجريمة وتتبع مرتكبيها وهو ما سوف نحاول عرضة في هذا المبحث.

فمن المسلم به أن القواعد الإجرائية الخاصة بالبحث والتحري عن الجرائم والمنصوص عليها في قواعد ونصوص القوانين الإجرائية جاءت قواعد عامة لا تخص جريمة معينة دون غيرها وإن كان للجريمة الإلكترونية طبيعة خاصة بها تفردها عن الجرائم الأخرى إلا أن المشرع وفي كثير من الدول لم يميزها بإجراءات خاصة[٢٢]، وعلية تخضع إجراءات البحث والتحري عن الجريمة الإلكترونية إلى ذات القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية. هذا الأمر كان مثار نقاش بين الفقه؛ فقد ذهب البعض إلى أن إجراءات البحث والتحري عن الجريمة الإلكترونية تمر بذات المراحل التي تمر بها الجريمة التقليدية وبالتالي تكون القواعد العامة صالحة في مجال البحث عن الجريمة الإلكترونية[٢٣]، وأضاف رأي مؤيد آخر إلى أن الأمر يحتاج فقط إلى تطوير لبعض المفاهيم القانونية. بينما ذهب البعض الاخر إلى أن الجريمة الإلكترونية ذات طبيعة خاصة وعليه لا تنسجم القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية مع هذا النوع من الجرائم[٢٤]، فقد ذهب أصحاب هذا الرأي إلى أن تطبيق هذه القواعد قد يؤدي إلى المساس بحقوق وحريات الأفراد حين القيام بالبحث والتحري عن الجريمة الإلكترونية.[٢٥] وقد تفرد المرشد الفيدرالي الأمريكي بوضع قواعد خاصة حين البحث والتحري عن الأدلة الإلكترونية يجب الاسترشاد بها حيث نص على عدد من الإجراءات الواجب مراعاتها واتخاذها في سبيل التفتيش والحصول على أدلة إثبات الجريمة الإلكترونية.[٢٦] وهو الأمر ذاته الذي اتخذته بريطانيا حينما وضعت قواعد استرشاديه يجب الأخذ بها حينما يتعلق الأمر بالبحث والتحري عن الدليل الإلكتروني.[٢٧] وفي هذا السياق ذهبت الصين إلى تعديل قانون الإجراءات الجزائية حينما نصت على قواعد إجرائية خاصة معنية بالبحث عن الأدلة الإلكترونية [٢٨]، كما عمدت بريطانيا إلى تضمين بعض القواعد الاجرائية الخاصة في قوانينها حينما يتعلق الامر بالبحث والتحري عن

---

(٢٢) نص القانون رقم (١٤) لسنة ٢٠١٤م القطري والخاص بمكافحة الجرائم الإلكترونية على قواعد إجرائية خاصة في الباب الثالث والرابع من القانون، وفي هذا تفرد عن باقي القوانين العقابية الأخرى والخاصة بدول منطقة الخليج العربي. وقد سار على هذا النهج المشرع البحريني أيضاً بإصدار القانون رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات.

(٢٣) مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة-القاهرة، الطبعة الأولى ٢٠٠٨ م، ص١٧.

(24) See; Sharon Nelson, Bruce Olson and John Simek, The Electronic Evidence and Discovery Handbook: Form, Checklists And Guidelines(New York: American Bar Association 2006)1-2.

(٢٥) عبد الفتاح بيومي حجازي ، الإثبات في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية-القاهرة، طبعة ٢٠٠٧ م، ص١٣٧.

(٢٦) انظر في ذلك: The US Secret Services' Pocket Guide for First Responders

(٢٧) انظر في ذلك: ACPO (Association of Chief Police Officers)

(٢٨) انظر في ذلك: The Chinese Criminal Procedure Law. Articles 10 and 16

الدليل الإلكتروني.[٢٩] وهو ما سارت علية مملكة البحرين فقد بين الفصل الثاني من القانون رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات عدداً من الإجراءات الخاصة المتبعة حين البحث والتحري وضبط الأدلة الخاصة بجرائم تقنية المعلومات.[٣٠]

وعلية وقبل الخوض في استعراض بعض من الإجراءات الخاصة بتتبع وضبط الجرائم فإنه من الواجب علينا أن نعرف أولاً الأدلة ونبين أهمية الأخذ بها في إثبات الجرائم المستحدثة في مطلب أول لنعرج بعدها في مطلب ثانٍ لبيان بعض وسائل تقصي الجرائم.

المطلب الأول

تعريف الأدلة وبيان أهميتها وأحكامها

الفرع الأول

الأدلة

الدليل هو مفرد كلمة أدلة وهو ما يستدل به، فالدليل هو المرشد والكاشف.[٣١] واصطلاحاً عرف الدليل بأنه العلم الذي يلزم للعلم بشيء آخر.[٣٢] أما في الفقه فقد تم تعريف الدليل بأنه «الرهان و الحجة التي يستدل من خلالها على صحة الدعوى»،[٣٣] وعرفه البعض بأنه «الواقعة التي يستمد منها القاضي اقتناعه على ثبوت الاتهام ويبني عليها حكمه في الدعوى».[٣٤] أما البعض الآخر فقد عرف الدليل بأنه تلك الوسيلة التي يستعين بها القاضي للوصول إلى حقيقة الدعوى[٣٥] مما سبق يتبين لنا أن الدليل هو وسيلة رجال الشرطة التي يسعون من خلالها إلى إثبات وقوع جريمة في المقام الأول ونسبتها إلى فاعل محدد ومن ثم يتم التحقيق مع المشتبه به وموازنة الأمر من قبل النيابة العامة تمهيداً لإحالة المتهم إلى المحاكمة في حال ما إذا تم ترجيح أدلة الإدانة على أدلة البراءة ويفصل في الدليل بعد ذلك قاضي الموضوع متى ما اقتنع بالدليل وصحته ونسبته إلى شخص المتهم.

---

(٢٩) انظر في ذلك: UK Criminal Procedure and Investigations Act 1996, see also; Investigation of Protected Electronic Information Code of Practice 2007, Paragraph 3.12.

(٣٠) انظر في ذلك الفصل الثاني من القانون البحريني رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات.

(٣١) أحمد محمد الفيومي، المصباح المنير في غريب الشرح الكبير، لبنان، بيروت، المكتبة العلمية، الجزء الاول ، طبعة ٢٠١٠، ص ١٩٨.

(٣٢) علي بن محمد الشريف الجرجاني، التعريفات ، لبنان، بيروت، دار الكتب العلمية ، طبعة ١٩٨٣، ص ١٠٤.

(٣٣) أحمد ابو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص ، الجزء الأول، المركز العربي للدراسات الامنية والتدريب، ٢٠٠٦، ص١٨٠.

(٣٤) د. مأمون سلامة، الإجراءات الجزائية في التشريع المصري ، مصر، دار النهضة العربية للنشر والتوزيع، الجزء الاول، طبعة ٢٠٠٨، ص ٧٦٤.

(٣٥) د. احمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، مصر، دار النهضة العربية للنشر والتوزيع، الطبعة العاشرة ، ٢٠١٦، ص ٧٣.

الفرع الثاني

أهمية الأدلة في إثبات الجرائم المستحدثة

مما لا شك فيه أن الحياة في تطور مستمر ناتج عن التطور في جميع مناحي الحياة دون استثناء، هذا التطور لم يكن مقتصراً على رفاهية الحياة المدنية للأشخاص بل طوعه المجرمون في تطوير وتسهيل أساليب ارتكابهم للجريمة ، فأصبحت الوسائل الحديثة المتطورة أداة المجرمين في ارتكاب الجرائم وفي المقابل وجدت أجهزة إنفاذ القانون من رجال الشرطة والنيابة العامة والقضاة أنفسهم في مواجهة أشخاص هجروا الوسائل التقليدية في ارتكاب الجرائم إلى أساليب أكثر حداثة ومن ثم برز الجانب السلبي لاستخدام الأجهزة والأدوات الحديثة فكان لازماً مواجهة هذا الإجرام المنظم بطرق وأساليب تتناسب وطرق ارتكاب الجرائم الحديثة. فلجأت الدول إلى استخدام الأجهزة الخاصة في تتبع الأدلة الإلكترونية وتسجيل المكالمات الهاتفية والولوج إلى الأجهزة الالكترونية عن بعد لاستخدامها في إثبات الجرائم ونسبة مرتكبيها وقد كان لهذا التوجه في استخدام الأجهزة محاذيره في إمكانية انتهاكه لحقوق الأشخاص وخاصة حق الخصوصية. فغلبت مصلحة الدولة في الحفاظ على أمن واستقرار المجتمع وشعور أفراده بالأمن والأمان على مصلحة الشخص في حماية حقوقه الشخصية من الانتهاك. فقد سعت الدول إلى استخدام الأجهزة الحديثة في إثبات الجرائم لما لها من أهمية كبيرة في تسهيل الوصول إلى معرفة شخص مرتكب الجريمة بدقة وحرفية تفوق الأدوات القديمة المتعارف عليها، فإذ ما قارنا استخدام الأجهزة التقنية في تفريغ تسجيل مرئي وإثبات مدى تطابق الصور المستخرجة من التسجيل بصورة المشتبه به فإنه قطعاً سيؤدي إلى نتائج أكثر دقة من التي سوف نحصل عليها لو ما تمت المقارنة بالمشاهدة البصرية فقط من قبل رجال الشرطة. وعليه يكون للأدلة الالكترونية أهميتها العملية في إثبات الجرائم ما يبيح للدول التغاضي عن تلك المطالبات التي تنادي بحماية حقوق الأشخاص من الانتهاك.

الفرع الثالث

الاحكام الخاصة بإجراءات البحث والتحري عن الأدلة

إن الهدف الأسمى من إجراءات البحث والتحري عن الأدلة هي معرفة الحقيقة. فهي السبيل إلى إنفاذ القانون وإقرار العدالة، فمن غير الحقيقة لن تقوم الحياة السوية بين الأفراد ولن ينعم العدل بينهم، وبدون العدالة لن يتوفر الأمن والأمان ولن يحفظ النظام وتتطور الدول. فمهمة البحث عن الأدلة الخاصة بالجرائم هي مهمة شاقة عسيرة تستهدف كشف الجرائم ونسبة مرتكبها إلى شخص معين. وعليه رتب القانون الأعمال المنوطة بالسلطات الإدارية في سعي منه إلى تنظيم عمليات البحث والتحري عن مرتكب الجريمة. وتنظيماً لهذا الأمر أقرت الدول النصوص التشريعية المنظمة، حيث عبر المشرع الإماراتي في نص المادة (٣٥) من قانون الإجراءات الجزائية

الإماراتي على"يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم في شأن الجرائم ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على الإيضاحات وإجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة". وحتى يباشر افراد الضابطة العدلية إجراءات البحث والتحري بحثاً عن الأدلة يجب أن يتوافر عددٌ من الأحكام العامة وهي:

- أن يهدف الإجراء إلى البحث عن أدلة الجريمة
- إن الغرض من إجراءات البحث والتحري هي البحث عن الأدلة الخاصة بجريمة معينة. ويجب أن تكون هذه الأدلة أدلة مادية كأدوات الجريمة أو البصمات الخاصة بالمتهم أو أي أثر مادي يمكن من خلاله التوصل إلى تحديد شخص المتهم ويقتنع به القاضي، وقد تكون هذه الأدلة قولية كاعتراف المتهم أو شهادة شهود الواقعة.
- يجب أن يقوم بالإجراء شخصٌ مخولٌ قانوناً بذلك
- يجب أن يكون الشخص القائم بإجراءات البحث والتحري عن الأدلة شخصاً مخولاً قانوناً بالقيام بالإجراء، فلا يجوز لأي فرد القيام بإجراءات التفتيش أو المعاينة أو الانتقال ما لم يكن مخولاً بالقيام بالإجراء، ويكون ذلك بناء على تكليف رسمي صادر من النيابة العامة وهذا ما عَبَّرت عنه صراحة المادة (٥٣) من قانون الإجراءات الجزائية الإماراتي حينما نصت على» لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبساً بها وتتوفر أمارات قوية على أن المتهم يخفي في منزله أشياء أو أوراقا تفيد كشف الحقيقة".
- يجب أن تكون الأدلة ناشئة عن جريمة ارتكبت فعلاً

لا يتم البدء في إجراءات البحث والتحري بحثاً عن الأدلة إلا عن جريمة وقعت فعلاً، فلا يصح القيام بإجراءات البحث والتحري والاستقصاء عن جريمة مستقبلية، ولوقامت التحريات والدلائل عن أنها سوف تقع. ولا يكفي وقوع الجريمة أيضاً لوحدها للقيام بإجراءات البحث والتحري إذ يجب أن تكون الجريمة التي وقعت أيضاً معاقباً عليها قانوناً. [٣٦]

من ذلك يلاحظ إن جميع إجراءات البحث والتحري عن الجرائم تكون وفق أطر قانونية منظمة منصوص عليها قانوناً، فلا يجوز انتهاك حق أي شخص باتخاذ أي إجراء في مواجهته إلا بموجب أمر مسبب يصدر من قبل الجهة المختصة بالإجراء، ويكون وفق ما ينص علية القانون.

---

(٣٦) انظر في ذلك: د. حسن صادق المرصفاوى، أصول الإجراءات الجنائية، منشأة المعارف، الاسكندرية ، مصر، ١٩٨٢، ص ٣١١.

المطلب الثاني

وسائل تقصي الجرائم

سيستعرض هذا المطلب الإجراءات التي تباشرها جهة التحقيق في جمع الأدلة المادية على ارتكاب الجريمة، مع أهمية بيان أن هذه الإجراءات لَم تَرِدْ في القانون حصراً حيث يجوز لجهة التحقيق إجراء أي إجراء إضافي يكون مفيداً في الكشف عن الجريمة طالما كان مشروعاً؛ كمقارنة البصمات مثلاً أو العرض القانوني للاستعراف على الشخص. وسنقصر حديثنا هنا في هذا المطلب على ثلاثة إجراءات فقط هي الانتقال والمعاينة والتفتيش وضبط الأشياء دون مناقشة باقي الإجراءات الأخرى كسماع الشهود وندب الخبراء والاستجواب والمواجهة فلا مجال لها في موضوع البحث.

الفرع الأول

الانتقال والمعاينة

الانتقال والمعاينة هما من الإجراءات أو الوسائل التي يلجأ اليها المحقق والتي تعني انتقاله إلى مكان محدد لكشف جريمة ارتكبت بغرض معاينة مكان الجريمة وجمع الاثار المتعلقة بها وتحديد وقت ارتكابها أو طريقة ارتكابها.[٣٧] وللانتقال والمعاينة أهميتهما في استجلاء الحقيقة وضبط الأدلة المادية التي استخدمت في ارتكاب الجريمة كما أنها تساعد في رسم تصور في ذهن المحقق بطريقة ارتكابها. الانتقال أو المعاينة كإجراء فانه غير ملزم لسلطة التحقيق وإنما متروك لسلطة تقديرية للمحقق فله أن يقوم به أو أن يتركه إلا في الحالة التي أوجب فيها القانون ذلك كما جاء بنص المادة (٤٣) من قانون الإجراءات الجزائية الاتحادي الإماراتي حيث نصت المادة : «على مأمور الضبط القضائي في حالة التلبس بجريمة أن ينتقل فوراً لمحل الواقعة ويعاين الآثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ويسمع أقوال من كان حاضرا أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبيها ، وعليه إخطار النيابة العامة فوراً بانتقاله. وعلى النيابة العامة الانتقال فوراً إلى محل الواقعة بمجرد إخطارها بجناية متلبس بها».

وبذلك أوجبت المادة المحقق الانتقال والمعاينة في حالة كانت الجريمة متلبساً بها، فيجب على المحقق الانتقال لمحل الواقعة ومعاينة الآثار المادية للجريمة لإثبات حالة المكان والأشخاص. ولن يثير هذا الإجراء أي مشاكل إجرائية طالما كان مكان الانتقال والمعاينة محدداً ولكنَّ احتمالاً قد يثير العديد من المشاكل والصعوبات الإجرائية إذ ما افترضنا أن المعاينة أو الانتقال للبحث في

(٣٧) د. ياسر حسين بهنس، الوسيط في شرح نظام الإجراءات الجزائية السعودي الجديد، مصر، مركز الدراسات العربية للنشر والتوزيع، الطبعة الاولي، ٢٠١٨م، ص ١٧٥.

الخوادم الإلكترونية أو الرقمية التي لا حدود لها أو التي قد تكون متصلة بأنظمة أو اشخاص آخرين والتي تستلزم لبحثها أو معاينتها إجراء العديد من عمليات التتبع والاستيضاح، وبالتالي قد يكون هناك خروج عن حدود المكان الواقعي للجريمة إلى مكان آخر غير محدد وهذا الإجراء قد يكون مدخلاً لانتهاك خصوصية الأفراد والتعرض لحقوق مكتسبة لهم بموجب الدساتير الوطنية أو حتى الاتفاقيات والمعاهدات الدولية.

الانتقال لمسرح الجريمة الإلكترونية

ينبغي أن لا يغفل عن البال عند الانتقال والمعاينة وجمع الأدلة من مسرح الجريمة الإلكترونية أن يعي القائم بالبحث أنه يتعامل مع مسرحين:

- مسرح تقليدي: يقع خارج البيئة الرقمية ويتمثل في الأجهزة والمكونات المادية لها. والتي قد يترك بها الجاني آثاراً وأدلة، كالبصمات والمتعلقات الشخصية وغيرها من الأشياء التي يمكن من خلالها الاستدلال لتحديد هوية الجاني. وهنا يتعامل الخبير حسب اختصاصه مع تلك الأدلة بما يتناسب معها من أساليب علمية في ضبطها وتحريزها.
- مسرح افتراضي: يقع داخل البيئة الرقمية ويتمثل في البيانات والمعلومات غير المحسوسة التي توجد بداخل شرائط الكترونية أو أقراص أو في خوادم. وهنا يجب أن يتعامل مع هذا النوع من الأدلة خبير متخصص في المعالجة الآلية للبيانات خشية ضياعها أو تدميرها.

- معاينة مسرح الجريمة الالكترونية

من المسلم به أن للمعاينة أهمية في كشف غموض كثير من الجرائم التقليدية، إلا أنَّ أهميتها هذه قد لا ترقى ان تكون بذات الأهمية في كشف الجريمة الإلكترونية. وقد يرجع سبب ذلك إلى:

عدم وجود آثار مادية في معظم الجرائم الإلكترونية. فالجرائم الإلكترونية من النادر أن تترك آثارًا ماديةً يمكن من خلال معاينتها الاسترشاد إلى تحديد شخص مرتكب الجريمة.

طمس الأدلة بمرور الزمن بين وقت ارتكاب الجريمة الإلكترونية ووقت اكتشافها. فمن المسلم به أن الأدلة الإلكترونية الخاصة بالجريمة الإلكترونية أدلة متغيرة غير ثابتة على حال وبالتالي تتغير وتطمس بسرعة نتيجة أي فعل أو نشاط يمكن أن يمسها ولو كان عرضياً غير مقصودٍ.

قلة عدد الخبراء في مجال الجرائم الإلكترونية. حيث يتطلب وجود عدد من الخبراء المتخصصين في مجال الجرائم الإلكترونية الذين يمكن الاستعانة بهم في الانتقال ومعاينة مسرح الجريمة الإلكترونية، فغالباً ما يتم الانتقال لمعاينة مسرح جريمة الكترونية من قبل رجال التحريات والبحث الجنائي والذين لا يتمتع معظمهم بالخبرة والاطلاع الكافي في مجال البحث عن الأدلة الإلكترونية.

وحتى تكون للمعاينة أهميتها في مجال الجرائم الإلكترونية لابد من وجود قواعد استرشاديه خاصة بكيفية التعامل مع مسرح الجريمة الإلكترونية. كما يجب أن تؤكل هذه المهمة إلى أشخاص مؤهلين بذلك. ففي فرنسا على سبيل المثال، هناك فريق مكون من ثلاثة عشر فرداً مختصاً كلاً في مجاله حين يستلزم الحال الانتقال والمعاينة لمسرح جريمة الكترونية يقوم كل فرد منهم بمهام متخصصة تلقى تدريباً متخصصاً عنها، وذلك في سبيل إعداد تقرير فني خاصة يقدم للنيابة العامة.

الفرع الثاني

التفتيش

يسعي رجال البحث والتحري من وراء تفتيش الأجهزة والمعدات والأماكن والأشخاص إلى ضبط أدوات الجريمة لنسبتها بعد ذلك إلى مرتكبيها.[٣٨] حيث يعد التفتيش وسيلة لإثبات واقعة مادية، وقد يكون موضوع التفتيش مكاناً أو شخصاً، ففي حالة كان موضوع التفتيش مكاناً فيقصد به البحث عن الأدلة المستخدمة في ارتكاب جريمة معينة ونسبة صلتها لشخص معين ويتم تنفيذ التفتيش في مكان محدد كمسكن أو مكتب أو مركبة أو أي مكان يثبت صلة المشتبه به. أما إذا كان موضوع التفتيش شخصاً فيقصد به هنا البحث المادي في جسم المشتبه به أو الملابس التي يرتديها من أجل إثبات صلته بالجريمة المرتكبة.[٣٩] ويعد التفتيش من أخطر الإجراءات الجزائية التي تمس حياة الافراد، فهو إجراء يمس مستودع أسرارهم. لذلك حرصت الدول أن تضمن أحكام الدساتير الوطنية ما يكفل للأفراد حمايتهم من هذا الإجراء وذلك بموجب ضوابط قانونية محددة. [٤٠] فقد ذهب الدستور الأردني في المادة (١٠) إلى النص على:"للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المبينة في القانون، وبالكيفية المنصوص عليها فيه". كما نصت المادة (٢٥) من دستور مملكة البحرين على:» للمسكن حرمة، فلا يجوز دخولها أو تفتيشها بغير إذن أهلها إلا استثناءً في حالات الضرورة القصوى التي يعينها القانون، وبالكيفية المنصوص عليها فيه". كما نصت المادة (٢٦) من دستور مملكة البحرين على: "حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقاً للإجراءات والضمانات المنصوص عليها فيه". كما نص الفصل التاسع من دستور الجمهورية التونسية على: "حرمة المسكن وسرية المراسلة وحماية المعطيات الشخصية مضمونة إلا في الحالات الاستثنائية التي يضبطها القانون". وذهبت المادة (٤٣) من دستور جمهورية السودان

(٣٨) انظر في ذلك: د. مأمون سلامة، قانون العقوبات، القسم العام ، دار النهضة العربية، القاهرة، ١٩٩٠م، ص٥.
(٣٩) انظر في ذلك: د. آمال عثمان، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ١٩٧٥م، ص٥.
(٤٠) انظر في ذلك: د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجزائية ، دار النهضة العربية، القاهرة، مصر، ٢٠٠٢، ص٤٣٥.

الديمقراطية إلى: "للمساكن حرمة فلا يجوز دخولها دون إذن ساكنيها أو تفتيشها إلا في الأحوال وبالطرق المبينة في القانون". ونصت المادة (٣١) من دستور الجمهورية العربية السورية على:» المساكن مصونة لا يجوز دخولها أو تفتيشها إلا في الأحوال المبينة في القانون». وذهبت المادة (٢٢) من دستور الجمهورية العراقية إلى النص على: "٠٠٠ ب- لا يجوز القبض على أحد أو توقيفه أو حبسه أو تفتيشه إلا وفق أحكام القانون. ج- للمنازل حرمة، لا يجوز دخولها أو تفتيشها، إلا وفق الأصول المحددة بالقانون". المادة (١٢) من دستور دولة قطر نصت على:» تكفل للناس حرمة المساكن فلا يجوز دخولها بغير إذن أهلها، إلا في الأحوال التي يعينها القانون وبالكيفية المنصوص عليها فيه». المادة (٣٨) من دستور دولة الكويت نصت على:» للمسكن حرمة، فلا يجوز دخولها بغير إذن أهلها، إلا في الأحوال التي يعينها القانون وبالكيفية المنصوص عليها فيه». ونصت المادة (٤٤) من دستور جمهورية مصر العربية على:» للمساكن حرمة فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائي مسبب وفقاً لأحكام القانون». وقد نصت المادة (٢٦) من الدستور الاتحادي لدولة الإمارات العربية المتحدة على: «الحرية الشخصية مكفولة لجميع المواطنين، ولا يجوز القبض على أحد أو تفتيشه أو حجزه أو حبسه إلا وفق أحكام القانون». كما نصت المادة (٣٦) من دستور دولة الامارات على «للمساكن حرمة فلا يجوز دخولها بغير إذن أهلها إلا وفق أحكام القانون وفي الأحوال المحددة فيه».

وفي هذا الصدد يجب الإشارة إلى قاعدة عامة أقرتها أيضاً المادة (٥١) من قانون الإجراءات الجزائية الاتحادي الإماراتي حيث قضت «لمأمور الضبط القضائي أن يفتش المتهم في الأحوال التي يجوز فيها قانوناً القبض عليه ويجرى تفتيش المتهم بالبحث عما يكون بجسمه أو ملابسه أو أمتعته من آثار أو أشياء تتعلق بالجريمة أو تكون لازمة للتحقيق فيها». وعليه يلاحظ أنه يكفي وجود أمر بالقبض على الشخص حتى يجوز تفتيشه. كما يجب التنويه هنا أيضاً إلى أن إجراء التفتيش يكون للبحث عن الأشياء المتعلقة بالجريمة التي وجدت دلائل كافية على ارتكابها وليس مجرد إجراء وقائي فقط.[٤١]

كما نصت المادة (٥٣) من قانون الاجراءات الجزائية الاتحادي الإماراتي على «لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبساً بها وتتوفر أمارات قوية على أن المتهم يخفي في منزله أشياء أو أوراقا تفيد كشف الحقيقة ويتم تفتيش منزل المتهم وضبط الأشياء والأوراق على النحو المبين بهذا القانون. كما يتم البحث عن الأشياء والأوراق المطلوب ضبطها في جميع أجزاء المنزل وملحقاته ومحتوياته». وعليه نجد أن المشرع الإماراتي انتبه إلى أن التفتيش يمس حقوق الفرد سواء حريته الشخصية أو حرمة مسكنه

(٤١) د. جودة جهاد، الوجيز في شرح قانون الإجراءات الجزائية لدولة الإمارات العربية، الجزء الأول، الدعاوى الناشئة عن الجريمة - الإجراءات التحضيرية للدعوى الجزائية-، الطبعة الاولي، مطابع البيان، ١٩٩٤م، ص٢٩٤.

لذلك وضع من الضمانات ما كفل للأفراد حقوقهم وحرياتهم فلا يجوز تفتيش الشخص أو مسكنه إلا بأذن كتابي من النيابة العامة،[٤٢] وحينما تكون هناك ضرورة تقتضي التفتيش ففي غير هذه الأحوال لا يجوز التفتيش ويعد الإجراء باطلاً. كما وضع المشرع عددً من الضوابط التي تكفل للفرد حريته وحرمة مسكنه حيث نصت المادة (٥٥) من قانون الإجراءات الجزائية الاتحادي الإماراتي على أنه لا يجوز تفتيش منزل المتهم إلا للبحث عن الأشياء الخاصة بالجريمة التي يجري جمع الأدلة أو التحقيق بشأنها، ونصت المادة (٥٨) من ذات القانون على أنه إذا وجدمن يتولى التفتيش بمنزل المتهم أوراقاً مختومة أو مغلقة بأي طريقة فلا يجوز لمأمور الضبط القضائي أن يفضها. كما اقرت المادة (٧٧) من القانون المشار إليه أعلاه حقاً لعضو النيابة العامة وبعد موافقة النائب العام ان يضبط لدى مكتب البريد جميع المكاتبات أو الرسائل أو المطبوعات ويستثني من ذلك ما يتم ضبطه لدي مكاتب المحامي أو الطرود ولعضو النيابة بعد موافقة النائب العام بموجب المادة (٧٥) من ذات القانون أن يراقب المحادثات السلكية واللاسلكية. كل هذه النصوص وضعت ضماناً للأفراد من اتخاذ أي إجراء في حقهم قد يؤدي إلى انتهاك خصوصيتهم.

وفي هذا الشأن ذهبت الاتفاقية الأوروبية إلى أن مفهوم المراسلات التي نصت عليها المادة(٨) من الاتفاقية الأوروبية لحقوق الانسان الصادرة عام ١٩٥٠م يشمل المكالمات الهاتفية أيضا بجانب المراسلات الكتابية.[٤٣] وفي ذلك احترام لحقوق الانسان وحماية لمراسلاته واتصالاته. وهو ما أكدت عليه المحكمة الأوروبية لحقوق الانسان أيضاً حيث عدت التنصت على المكالمات الشخصية عملاً غير مشروعً ويعد تدخلاً وانتهاكاً للحياة الخاصة للأفراد.

هذا الأمر قد لا يثير أي إشكالية إجرائية طالما أن الإجراءات اتبعت وفق القواعد المنصوص عليها في القوانين المنظمة، إلا أن الجريمة الالكترونية وما تثيره عطفاً على طبيعتها الخاصة من إشكالية إجرائية خاصة في مجال ضبط الكيانات المعنوية غير المحسوسة وتتبع الأدلة جعلت من القواعد التقليدية عاجزه عن ضبط الأدلة دون وجود شبهة خرق للقوانين الإجرائية أو اعتداء على خصوصية الأشخاص وحقوقهم المكفولة قانوناً، ويجب الإشارة هنا إلى أن الاتفاقيات الدولية ومنها الاتفاقية الأوروبية أجازت انتهاك حقوق الأفراد وحرمة مراسلاتهم ومكالماتهم حينما يتعلق الأمر بجريمة إرهابية وذلك حمايةً لسلامة الناس ولحفظ النظام العام ولمنع الجريمة حفاظاً على الأمن القومي للدول، ففي هذ الشأن قضت المحكمة الأوروبية في حكم صادر عنها سنة ١٩٧٨م بالنص على منح التشريعات الوطنية سلطات استثنائية في مراقبة الاتصالات والمراسلات في الحالات الخاصة بالتجسس والإرهاب حيث عدت ذلك الأمر من مقتضيات المحافظة على الأمن

(٤٢) استثناء من ذلك حينما تكون الجريمة متلبسًا بها (المادة ٥٣ من قانون الإجراءات الجزائية الاتحادي).

(٤٣) للمزيد حول هذه الاتفاقية انظر: د. محمد الميداني، النظام الأوروبي لحماية حقوق الانسان، ، لبنان ، منشورات الحلبي الحقوقية، الطبعة الثالثة، ٢٠٠٩م، ص١٠٥.

القومي ولمنع الجريمة. [٤٤] ولا يختلف الأمر هنا من وجه نظرنا بين الجريمة الإرهابية أو الجريمة الإلكترونية والتي تكون في بعض الأحيان أشد وطأه وخطورة من الجريمة الإرهابية من ناحية الخسائر المالية للأفراد أو المجتمعية أو حتى مساسها بالسلم العام والأمن القومي للدول. ولكن الأمر هنا يجب ألا يترك على مصراعيه وإنما يجب أن تكون هناك ضوابط ونظم يجب مراعاتها والأخذ بها، فلا يجوز انتهاك خصوصية شخص دون أن يكون هناك مبررٌ مقنعٌ لذلك فعلى سبيل المثال حينما يعجز رجال الضابطة العدلية عن الوصول إلى شيء مادي لازم تفتيشه ولن يتأتى ذلك إلا من خلال تعاون المشتبه به مع رجال الضابطة العدلية في الوصول إليه ففي حالة الرفض هنا نرى أن لرجال الضابطة العدلية الحق في اتخاذ أي إجراء يكون لازماً لكشف الجريمة طالما أن هذا الأمر ضروري وسيؤدي إلى كشف الحقيقة وإيصال الحق إلى طالبه. هذا الأمر وإن كان يثير بين طياته معارضة أنصار الحقوق القانونية كحق الأفراد في الصمت وعدم جواز تقديم الشخص دليلاً ضد نفسه، إلا أنه يلاحظ مؤخراً قد صدور عدة أحكام بالمخالفة لهذه المبادئ ومنها على سبيل المثال أحكام المحكمة الأوروبية لحقوق الإنسان والتي ألزمت الشخص على تقديم الأرقام السرية الخاصة بفك التشفير حيث أن هذا الامر لا يتعلق بحقوق الأشخاص في عدم تقديم دليل ضد نفسه وإنما الأمر يتعلق بالأمن القومي.[٤٥] وفي هذا السياق ذهبت أيضا المملكة المتحدة حين نظر دعوى Stott v Brown حيث ذكرت بأن حق الشخص في عدم تقديم دليل ضد نفسه ليست من الحقوق المطلقة وإنما من حق الدولة حماية المجتمع من الخطر وبالتالي يمكن إجبار الشخص على تقديم معلومات أو فك الشفرات إذا ما تعلق الأمر بالجوانب الفنية التي تعجز السلطات عن الوصول إليها بدون مساعدة المتهم.[٤٦] وباستقراء نصوص المرسوم بقانون رقم (٥) لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات الإماراتي نجده جاء خلواً من النص على أي إجراء يجب مراعاته حين قيام رجال البحث والتحري بتفتيش الأجهزة أو الأنظمة المعلوماتية الخاصة بتتبع أو ضبط أدلة الجريمة الإلكترونية تاركاً الامر لقانون الإجراءات الجزائية الاتحادي الاماراتي، وعلى الرغم من تعديل القانون بالمرسوم بقانون رقم (١٧) لسنة ٢٠١٨م وما سبقة من تعديلات بعامي ٢٠٠٥م و٢٠٠٦م إلا أنه لم يشر إلى أي إجراءات خاصة حينما يتعلق الأمر بتفتيش الأجهزة أو الأنظمة المعلوماتية ولم يلزم الشخص أيضاً بتقديم أي تسهيلات إذا ما طلبت منه من قبل رجال الضابطة العدلية حينما يعجز أفرادها عن الوصول إلى الدليل المطلوب الكشف عنه. في المقابل نجد قانون تنظيم الصلاحيات التحقيقية لسنة ٢٠٠٠م البريطاني يمنح الشرطة الصلاحية لإجبار المشتبه بهم بتقديم كلمات المرور الخاصة بأجهزتهم الخاصة الخاضعة للتفتيش. ونجد

(٤٤) انظر في ذلك: Klass and others v Germany, European Court of Human Rights.
(٤٥) انظر في ذلك: European Court of Human Rights, 1997/ 23 EHRR 313 & EWCA 2008/ 2177 .
(٤٦) انظر في ذلك: 2003/Stott v Brown, WLR 817.

أيضاً القانون البحريني رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات قد وضع فصلاً مستقلا خاصاً بالإجراءات الخاصة بجرائم تقنية المعلومات ففي مجال التفتيش نصت المادة (١٥) من القانون المشار إليه على:

١- للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي وتفتيشه:

أ - نظام تقنية المعلومات المتصل بالجريمة أو زي جزء منه وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب - أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

٢- إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند) أ (من الفقرة (١) من هذه المادة أمارات قوية بأن البيانات المتصلة بالجريمة مخزنة في نظام تقنية المعلومات آخر أو في جزء منه، وكانت هذه البيانات قابلة لأن يتم الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإن للنيابة العامة أن تصدر أمراً مسبباً بمد الدخول والتفتيش إلى النظام الآخر".

يلاحظ على المادة السابقة أنها وضعت عدداً من الضوابط الإجرائية الخاصة بتفتيش أنظمة المعلومات والبحث عن الأدلة المتصلة بالجرائم الإلكترونية ولم تترك الأمر للقواعد الإجرائية العامة. والرأي هنا أنه يجب على المشرع الإماراتي النظر مَرَّةً أخرى في نصوص المرسوم بقانون رقم (٥) لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات حمايةً للحق وضماناً لسلامة الإجراءات الخاصة بالبحث عن الأدلة خاصة وأن الواقع العملي أفرز العديد من الصعوبات الإجرائية التي حالت دون الوصول إلى الدليل وبالتالي إثبات الجريمة الإلكترونية.

تفتيش المكونات الإلكترونية

في مَا سبق ما للتفتيش من أهمية في الكشف عن الجرائم وتتبع مرتكبيها، واستعرضنا النصوص القانونية المنظمة لعمليه التفتيش والضوابط الخاصة به؛ فكان حَريًّا بنا هنا أن نوضح أيضا طريقة التفتيش عن الأدلة في البيئة الرقمية. يكون التفتيش للنظم الإلكترونية من خلال البحث عن الأدلة في الوعاء الذي يحوي هذه النظم ويقصد به هنا الجهاز الإلكتروني. فالجهاز الإلكتروني يحتوي على مكونات مادية ومكونات منطقية، كما أن له شبكات اتصال سلكية ولا سلكية. هذا الجهاز الإلكتروني قد يعمل بمفردة أو من خلال شبكة اتصالات يتم من خلالها اتصال جهازين أو أكثر بشبكة اتصالات سلكية أو لاسلكية، وقد تكون هذه الأجهزة موجودة في موقع واحد أو أكثر من موقع ويتم ربطها عن طريق خطوط الهاتف.[٤٧]

(٤٧) انظر في ذلك : د. هلالي عبد الإله احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دار النهضة العربية ،

وهنا يثار تساؤل هام عن: مدى إمكانية خضوع الجهاز الإلكتروني للتفتيش؟ إن الإجابة عن هذا السؤال تقتضي منا توضيح ثلاث صور:

اولاً: تفتيش المكونات المادية للجهاز الإلكتروني

لا وجود لخلاف فقهي في خضوع المكونات المادية للأجهزة الإلكترونية لعملية التفتيش طالما كانت وفقاً للقواعد القانونية المنصوص عليها والمقررة في القوانين الإجرائية، والقيد هنا فقط فيما إذا كانت تلك المكونات في مكان خاص أو في مكان عام. ولتوضيح الأمر:

إذا كانت المكونات المادية للجهاز الإلكتروني المراد تفتيشه في مكان خاص

كأن يكون الجهاز الإلكتروني في مسكن المشتبه به أو مركبته، فيأخذ بذلك حكم تفتيش المسكن من إجراءات أو ضمانات مقرره قانوناً. ويجب هنا مراعاة ما إذا كان الجهاز متصلاً بجهاز آخر ويوجد في مكان خلاف مسكن المشتبه به، وعليه لا يجوز بسط نفاذ أمر التفتيش ليشمل المكان الآخر فتجاوز هذا الأمر يعرض الدليل للبطلان وعدم الأخذ به أمام المحكمة. حيث يعد الدليل المتحصل علية دليلاً متحصلا عليه بالمخالفة للقانون ولا يمكن الاعتداء به كدليل إثبات في مواجهة المتهم.

إذا كانت المكونات المادية للجهاز الإلكتروني المراد تفتيشه في مكان عام

كأن يكون الجهاز في مكان عام كالمقاهي أو المطاعم أو الحدائق، فيجب هنا مراعاة القواعد الخاص بتفتيش الأشخاص. كما يجب أن يكون الشخص حائزاً فعلا للجهاز ومسيطراً عليه. وبذلك تُعمل القواعد الإجرائية المنصوص عليها في القوانين الإجرائية. وخروجاً على ذلك نجد أن بعض الدول نصت صراحة على تفتيش مكونات الأجهزة الإلكترونية كالقانون الإنجليزي والذي ينص صراحة على تفتيش مكونات الحاسب الآلي.[٤٨] وفي الجانب الآخر نصت دول أخرى على عدم جواز تفتيش الأجهزة الإلكترونية كالقانون الأمريكي ، حيث منع تفتيش مكونات الحاسب الآلي إلا بإذن خاص بذلك. فقد عبر الدستور الأمريكي على:» حق الناس في أن يكونوا آمنين في شخوصهم ومنازلهم وأوراقهم وممتلكاتهم ضد التفتيش إلا على أساس سبب معقول ومدعوم بقَسم وإفادة، موصوف فيها بدقة المكان المقصود تفتيشه والأفراد والأشياء المراد ضبطها». وفي هذا الخصوص ذهبت أيضاً المحكمة العليا الأمريكية حيث أوجبت شرطين للخروج من قيود التفتيش المنصوص علية في الدستور: ١- أن لا يكون هناك انتهاك لخصوصية الافراد.٢- أن يكون التفتيش مبرراً ومقبولاً.[٤٩]

القاهرة، مصر، ٢٠٠٠م، ٧٣ ص وما بعدها.

(٤٨) انظر في ذلك: Computer Misuse Act 1990.

(٤٩) للمزيد من الايضاح انظر في ذلك : د. عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت (في القانون الامريكي)، دار النهضة العربية ، القاهرة، مصر، ٢٠٠٤م، ٥٥ ص.

ثانياً: تفتيش المكونات المعنوية للجهاز الإلكتروني

على النقيض من الصورة الأولي والمتمثلة في تفتيش المكونات المادية للأجهزة الإلكترونية، أثارت الصورة الثانية العديد من وجهات النظر. فقد ذهب البعض إلى خضوع المكونات المعنوية من بيانات ومعلومات للقيود الخاصة بتفتيش الأجهزة المادية على اعتبار أن المكونات المعنوية هي امتداد للمكونات المادية، بينما ذهب البعض الآخر إلى أن المكونات المعنوية تحتاج إلى إذن خاص بها وتعامل معاملة مستقلة عن أمر التفتيش الخاص بتفتيش المكون المادي للجهاز الإلكتروني.(٥٠)

ثالثاً: تفتيش الشبكات الخاصة بالأجهزة الإلكترونية

هنا يجب حين إجراء عمليات التفتيش والبحث أن يراعي القائم بالإجراء عددًا من الفرضيات:

اتصال الجهاز الإلكتروني بجهاز أخر داخل الدولة

كأن يكون الجهاز في منزل المشتبه به ومتصلاً بجهاز آخر في مكان آخر خلاف منزل المشتبه به، ويقع الجهازان داخل نطاق دولة واحدة. ذهبت بعض الدول كألمانيا إلى امتداد أمر التفتيش ليشمل المكان الآخر المتصل بالجهاز الموجود بمنزل المشتبه به.(٥١) بينما ذهبت غالبية الدول إلى عدم امتداد أمر التفتيش إلى أي مكان آخر خلاف ما ورد بأمر التفتيش فلا يجوز الامتداد.

اتصال الجهاز الإلكتروني بجهاز آخر خارج الدولة

تثور هذه الفرضية إذا ما كان الجهاز الآخر المتصل بالجهاز المراد تفتيشه يتواجد خارج الدولة. فقد ذهبت جلَ الدول إلى عدم جواز امتداد أمر التفتيش ليشمل الجهاز المتواجد خارج الدولة، ومنها ألمانيا حيث اعتبرت أن ذلك الأمر يعد خرقاً لسيادة الدول ففي غياب وجود أي اتفاق خاص بين الدول ينص على جواز القيام بهذا الإجراء يعد الإجراء باطلاً. وعلى النقيض من ذلك ذهبت هولندا مثلا إلى جواز الإجراء وامتداد أمر التفتيش ليشمل الجهاز الموجود خارج الدولة متى ما كان الإجراء ضرورياً لكشف الجريمة.(٥٢)

مما سبق يتضح جلياً أن تفتيش الأجهزة الإلكترونية ليس بالأمر اليسير، وإنما يتطلب الأمر إجراءات خاصة ومراعاة جوانب عديدة. كما يحتاج أمر تفتيش الأجهزة الإلكترونية لكوادر فنية مختصة تجيد التعامل مع الأجهزة الإلكترونية. فخطأ بسيط قد يغير من مجرى الأمور ويؤدي إلى إفلات المتهم من العقاب. لذا وجب أن تحاط الجريمة الإلكترونية بعناية تختلف عما تحضى به الجريمة التقليدية.

---

(٥٠) د. هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، دار النهضة العربية ، القاهرة، مصر، ٢٠٠٠م، ٧٧ ص.

(٥١) انظر نص المادة (١٠٣) من قانون الإجراءات الجنائية الألماني .

(٥٢) انظر نص المادة (١٢٥) من قانون الإجراءات الجنائية الهولندي.

الفرع الثالث

ضبط الأشياء

إن الغاية التي يسعى إليها المحقق من إجراء التفتيش هي ضبط جميع الأشياء المتعلقة بالجريمة والتي يؤدي ضبطها الكشف عن الجريمة والوصول إلى تحديد شخص مرتكبها. وحتى يكون هذا الإجراء متصوراً فإن محل الضبط يجب أن يكون شيئاً مادياً ، وهنا قد تثور مشكلة إجرائية أيضاً إذ ما كانت الأشياء المراد ضبطها أشياء غير مادية وغير محسوسة وهي من الأمور المتصورة والتي قد تحدث حين البحث عن الأدلة الالكترونية حيث أن من طبيعة الأدلة الالكترونية أن تكون أدلة غير مادية وغير محسوسة وغير مرئية.[٥٣] وبالتالي تثور هنا احتمالية انتهاك خصوصية الأشخاص حينما يتتبع رجال الضابطة العدلية دليلاً معيناً فيبحثون في أمور قد لا تكون متصلة بالجريمة المراد ضبطها ولكنها لازمة لكشف الحقيقة وبالتالي تنتهك خصوصية الأفراد. كل ذلك يجب ان يكون من وجهة نظرنا وفق أطر وضوابط معينة لا تغلب فيها مصلحة على مصلحة أخرى ويراعى فيها حقوق كل طرف، فكشف الجريمة مطلب جوهري لحماية المجتمع وأفراده وضمانة للسلم العام والخاص وفي المقابل يجب أن يشعر الأفراد أن حقوقهم مصونَةً بموجب القانون ولا يجب أن تنتهك جزافاً. هذا الأمر لن يتأتى إلا بالنص عليه صراحة في قواعد إجرائية، وبالنظر إلى القواعد والأنظمة المرعية قانوناً في دولة الامارات العربية المتحدة نجدها جاءت خلواً من النص على هذه القواعد الإجرائية الخاصة حينما يتعلق الأمر بضبط الأشياء غير المادية أو غير المحسوسة حيث تناولت القواعد الإجرائية ضبط الأشياء المادية المحسوسة فقط حيث يتضح ذلك جلياً بالنظر إلى نص المادة (٦١) من قانون الإجراءات الجزائية الاتحادي رقم (٣٥) لسنة ١٩٩٢م وتعديلاته لغاية المرسوم بقانون رقم (١٧) لسنة ٢٠١٨م حيث ذكرت:» لمأموري الضبط القضائي أن يضبطوا الأشياء التي يحتمل أن تكون قد استعملت في ارتكاب الجريمة أو نتجت عن ارتكابها أو يحتمل أن تكون قد وقعت عليها الجريمة وكذلك كل ما يفيد في كشف الحقيقة وتوصف هذه الأشياء وتعرض على المتهم ، ويطلب منه إبداء ملاحظاته عليها ويحرر بذلك محضر يوقعه المتهم أو يذكر فيه امتناعه عن التوقيع٠٠٠٠».

فمن صياغ المادة يتضح أن الضَبط يكون للأشياء المادية كالأوراق أو الأدوات التي استخدمت في ارتكاب الجريمة ذات الطبيعة المادية فقط، ولم يتم النص على الأشياء ذات الطبيعة غير المادية على الرغم من تعديل قانون الإجراءات الجزائية الاتحادي لثلاث مرات أعوام ٢٠٠٥م و٢٠٠٦م و٢٠١٨م. وبالمقارنة بالقوانين الأخرى بالمنطقة نجد أن القانون البحريني رقم (٦٠) لسنة ٢٠١٤م نص على عدد من الإجراءات الخاصة التي يجب اتباعها حينما يتعلق الأمر بضبط كيانات غير

(٥٣) انظر في ذلك: Stephen Mason,(n11) p28.

مادية ، فقد نصت المادة (١٣) من القانون على:» ١- للنيابة العامة أن تأمر أي شخص يكون حائزاً أو تحت سيطرته بيانات معينة لوسيلة تقنية المعلومات بتقديمها على وجه السرعة بما في ذلك البيانات المخزنة داخل نظام تقنية معلومات أو أية وسيلة تقنية المعلومات.

٢- للنيابة العامة أن تأمر أي مزود خدمة بتقديم أية معلومات تكون في حيازته أو تحت سيطرته عن أي مشترك في خدماته أو مستخدم لها، سواء كانت هذه المعلومات في صورة بيانات وسيلة تقنية المعلومات أو في أية صورة أخرى ولا يدخل في ذلك بيانات خط السير والمحتوى.

وذلك كله متى رأت النيابة العامة الحاجة إلى ذلك لإظهار الحقيقة في الجريمة». كما نصت المادة (١٤) من ذات القانون على:» لقاضي المحكمة الصغرى، بناء على طلب النيابة العامة، وبعد اطلاعه على الأوراق أن يأمر بما يلي:

أ- القيام على وجه السرعة بالحفاظ على بيانات خط السير المتصلة بالجريمة سواء كان الإرسال قد تم بثه من خلال مزود خدمة واحد أو أكثر.

ب- الكشف عن قدر كاف من بيانات خط السير لتمكين النيابة العامة من تحديد مزود الخدمة والمسار الذي تم إرسال هذه البيانات من خلاله، متى كان ذلك يساهم في إظهار الحقيقة في جريمة معاقب عليها بموجب هذا القانون أو أي قانون آخر. ويصدر القاضي أمره في هذه الحالة مسبباً». ونصت المادة (١٦) من ذات القانون على:» للنيابة العامة سلطة الضبط والتحفظ على بيانات وسيلة تقنية المعلومات التي يتم الدخول إليها استناداً إلى أحكام المادة (١٥) من هذا القانون، ويشمل ذلك ما يلي:

أ- الضبط والتحفظ على نظام تقنية المعلومات، أو أي جزء منه، أو أي من وسائط تخزين بيانات وسيلة تقنية المعلومات.

ب- استنساخ بيانات وسيلة تقنية المعلومات والاحتفاظ بالنسخة.

ج- المحافظة على سلامة بيانات وسيلة تقنية المعلومات.

د- رفع بيانات وسيلة تقنية المعلومات من نظام تقنية المعلومات الذي تم الدخول إليه أو جعل الدخول إليها غير متاح». ونصت المادة (١٨) من ذات القانون المشار الية على:» مع مراعاة الضوابط المنصوص عليها في البند (ب) من المادة (١٤) من هذا القانون، يجوز للنيابة العامة بعد الحصول على إذن من قاضي المحكمة الصغرى القيام بما يلي:

أ- تكليف أي شخص مختص بالقيام بجمع وتسجيل بيانات خط السير وبيانات المحتوى، أو أي منهما، المتعلقة باتصالات محددة يتم إرسالها بواسطة نظام تقنية المعلومات، وذلك حين حدوث هذه الاتصالات.

ب- تكليف أي مزود خدمة، بالقيام بالأعمال المشار إليها في البند (أ) أو تقديم المساعدة اللازمة لمن كلفته النيابة العامة القيام بهذه الأعمال.

ج- تكليف أي شخص مختص للقيام بحجب بيانات محتوى أية وسيلة تقنية المعلومات أو أي جزء منها ارتكبت بواسطتها أي من جرائم تقنية المعلومات». وحماية لخصوصية الأشخاص وكفالة حقوقهم نصت المادة (٢/١٨) من القانون المشار إليه على:"يحظر على من تم تكليفه وفقاً لأحكام الفقرة (١) من هذه المادة الكشف دون مسوغ في القانون لأي شخص آخر عن هذا التكليف أو بأية معلومات ذات صلة به أو الانتفاع بها بأية طريقة». وباستقراء جميع النصوص الأخرى نجد أن المشرع البحريني وضع ضماناً آخر لتلك الحقوق حينما ترك تقدير جميع تلك القرارات بيد القاضي المختص. وعلية نجد ان من الأجدر بالمشرع الإماراتي أن يحذو حذو المشرع البحريني بالنص على بعض الإجراءات الخاصة بضبط الكيانات غير المادية بما يكفل للأفراد شبهة أي انتهاك قد يتعرضون له.

المبحث الثاني

تأثير إجراءات البحث والتحري عن الجريمة الإلكترونية على حرمة الحياة الخاصة للأفراد

ميزنا الجريمة الإلكترونية فيما سبق ببعض المميزات عن الجريمة في مفهومها التقليدي وأشرنا إلى أن الجريمة الإلكترونية ترتكب في مسرح الكتروني أو في فضاء افتراضي مفرغ يختلف كلياً عن المسرح الذي ترتكب فيه الجريمة التقليدية حيث يتم الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الاستدلال والتحقيق ، فهي إجراءات صيغت لضبط وإثبات جرائم ترتكب في عالم ملموس مادياً ، يلعب فيه السلوك المادي الدور الأكبر و الأهم؛ ونحن هنا لسنا في مستعرض بيان المشاكل الإجرائية الناجمة عن ضبط الجريمة الإلكترونية حينما تتعدى الحدود الإقليمية ومدى فاعلية الاتفاقيات الدولية والمساعدات القضائية في الحصول على الأدلة لكشف غموض الجريمة الإلكترونية فهو مسعى تناوله الفقهاء في كثير من الدراسات والبحوث، وإنما نحن هنا لإلقاء الضوء على مشكلة إجرائية بدأ بزوغ فجرها مع الاستخدام المفرط لوسائل التواصل الاجتماعي وبرامجها وما صاحبه من استغلال لميزة أتاحتها الشركات التجارية ألا وهي ميزة حماية بيانات المستخدمين من الإفشاء للغير بما فيها سلطات الضابطة العدلية فاستغل ضعفاء النفوس هذه الميزة في التخفي عن عيون سلطات الضبط، الأمر الذي أدى إلى عجز السلطات عن تحديد شخص المتهمين. هنا تجلى سؤال البحث عن مدى كفاية النصوص القانونية في ضبط الجريمة الإلكترونية دونما مساس بحقوق الأفراد الشخصية؟ إن الاجابة عن سؤال البحث يتطلب

منا التطرق أولاً إلى بيان الخصوصية في مطلب أول قبل التطرق إلى مناقشة النصوص القانونية في مطلب ثان.

المطلب الاول

بيان الخصوصية

إن الخصوصية حقٌ كفله الله عزَ وجلَ قبل أن تكفله القوانين الوضعية فقد ذكر المولى في كتابه الكريم:(«يا أيها الذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأنسوا وتسلموا على أهلها»[٥٤] وذكر عزَ وجلَ أيضاً في محكم كتابة :(«ولا تجسّسوا ولا يغتب بعضكم بعضا»).[٥٥]

وكما كان للدين الإسلامي كانت للشرائع الأخرى كالشرائع اليونانية والصينية القديمة أشارات للحق في الخصوصية. وفي الجانب التشريعي فقد أقرت العديد من الدول ومنذ مئات السنين جوانب الحق في الخصوصية ففي عام ١٣٦١م تم سن قانون في بريطانيا (The Justices of the Peace Act) يمنع اختلاس النظر واستراق السمع ويعاقب عليهما بالحبس.

وبعد هذا التاريخ وضعت العديد من الدول تشريعات منظمة لحماية الحق في الخصوصية ومنها على سبيل المثال ما وضعه البرلمان السويدي عام ١٧٧٦م من قانون الوصول إلى السجلات العامة والذي ألزم كافة الجهات الحكومية التي لديها معلومات أن تستخدمها لأهداف مشروعة. وفي عام ١٨٥٨م منعت فرنسا نشر الحقائق الخاصة وفرضت عقاباً على المخالفين، أما قانون العقوبات النرويجي فقد منع في عام ١٨٨٩م نشر المعلومات التي تتعلق بالشخصية والأوضاع الخاصة.

وكان ظهور الحق في بيان الخصوصية في الإعلان العالمي لحقوق الانسان (٤) لعام ١٩٤٨م والذي كفل حماية الأماكن والاتصالات إعلان لمولد مفهوم الحق في الخصوصية في العصر الحديث حيث عبرت المادة (١٢) من الإعلان على عدم جواز تعريض أي شخص لأي تدخل تعسفي في حياته الخاصة أو شؤون اسرته أو مراسلاته. كما كان لاتفاقيات حقوق الانسان العالمية كالعهد الدولي للحقوق المدنية والسياسية (ICCPR) واتفاقية الأمم المتحدة للعمال المهجرين واتفاقية الأمم المتحدة لحماية الطفولة وغيرها من الاتفاقيات دور التأكيد على هذا الحق وحمايته. وكما كان على المستوى الدولي كان لحماية لحق في الخصوصية على المستوى الإقليمي فهناك العديد من الاتفاقيات والتي اعترفت بالحق في الخصوصية ونظمت قواعد حمايته كما هي الحال في الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية (روما لعام ١٩٥٠م) وغيرها من الاتفاقيات والمواثيق، فقد عبرت هذه الاتفاقية على احترام الحياة الخاصة للأفراد ومراسلاتهم. وبعام ٢٠٠٠م عبر الميثاق الأوروبي للحقوق الأساسية على ضرورة التزام الدول بحماية الحياة

(٥٤) الآية ٢٧ من سورة النور.
(٥٥) الآية ١٢من سورة الحجرات.

الخاصة للأشخاص وأفراد عائلتهم. وعلى الصعيد العربي أصدرت القمة العربية المنعقدة بتونس عام ٢٠٠٤م إعلاناً لميثاق حقوق الأفراد في حماية حياتهم الشخصية. ومع التطور التقني واتساع استخدام الأجهزة برزت دعوة حماية الأشخاص وكفالة حقوقهم الشخصية من الانتهاك الإلكتروني والتي عبرت عنه كلٌ من ألمانيا والبرازيل حينما عرضتا مشروع حماية الخصوصية الرقمية للأشخاص عام ٢٠١٣م أثناء انعقاد الجمعية العمومية للأمم المتحدة وهو ما اعتمدته بعد ذلك الجمعية في سنة ٢٠١٤م بالنص عليه بموجب ميثاق صدر حمل رقم ٦٩/١٦٦ لسنة ٢٠١٤م.

من المسلم به أن وضع تعريف جامع مانع للخصوصية أو الحق في الحياة الخاصة أصبح من ضروب الخيال فكلٌ يورد المعنى الذي يتسق وتعريفة الشخصي للحق، ولهذا تعددت التعريفات التي صيغت تعريفاً للخصوصية أو الحق في الحياة الخاصة كما يسميها البعض وتباينت، ليس بين النظم القانونية المختلفة فحسب، وإنما في إطار النظم القانونية المتماثلة. فللفقه تعريفاته وللقضاء تعريفاته [٥٦]، أما التشريعات فقد سلكت موقفاً صامتاً ولم تورد تعريفاً قانونياً للخصوصية تاركة الأمر للفقه والقضاء لتفسيره ، واكتفت بوضع نصوص تكفل حماية الحق وعددت صور الاعتداء عليه. إن تعريف الحق في الخصوصية يرتبط في الحقيقة بمنظومة من التقاليد والثقافات والقيم الدينية السائدة لكل مجتمع. وأمام صعوبة وضع تعريف للحق في الخصوصية، اتجه جانب من الفقه إلى وضع تعريفاً سلبياً، يحدد المقصود بالخصوصية بكل ما لا يعد من حياة الأفراد العامة، غير أن هذا المسلك شابَهُ الاعتراض والانتقاد من وجوه عده؛ أهمها صعوبة التمييز بين ما يندرج ضمن مفهوم الحياة العامة وذلك الذي يقع ضمن نطاق الحياة الخاصة. مثال ذلك الحياة المهنية التي تعد لدى البعض مما يدخل في نطاق الحياة العامة تكون لدى آخرين مما يعد من صميم الحياة الخاصة. وأمام هذا وذاك؛ برزت فكرة جديده قسمت مفهوم الخصوصية إلى عدد من الأقسام جاءت كالتالي:

١- الخصوصية المعلوماتية (Information Privacy): والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المحل الذي يتصل عادة بمفهوم حماية البيانات (Data protection)[٥٧].

٢- الخصوصية الجسدية أو المادية (Bodily Privacy): والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كالفحوصات الجينية (GENETIC

(٥٦) ذهبت محكمة التميز بدبي في الحكم الصادر في الطعن رقم (٥٣) لسنة ٢٠١٦م بتاريخ ٢٠١٦/٠٢/٠٨م إلى تعريف الخصوصية بأنها السياج الذي يحول دون اطلاع الاخرين على الحياة الخاصة للأفراد سواء عن طريق السمع أو النظر أو التقاط الصور.

(57) See; Daniel J. Solove and Paul M.Schwartz, Information Privacy Law Aspen Cacebook, (4rd edn, Wolters Kluwer, 2011) USA.

TESTS)، والفحوص المخبرية كفحص المخدرات وغيره من الفحوص الطبية والمخبرية.[٥٨]

٣- خصوصية الاتصالات (Telecommunications Privacy): والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الالكتروني وغيرها من الاتصالات.[٥٩]

٤- الخصوصية الإقليمية: (نسبة إلى الأقليم المكاني) والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية.

وبذلك يتضح لنا أن للشخص حيزه الخاص به والذي يتفاعل من خلاله مع غيره من الأشخاص فيسمح لهم بالمشاركة وقد لا يسمح. فللشخص الحق أن يشاركه غيره معلوماته أو بياناته وقد يجيز لهم استغلالها تجاريا أيضا، وكما له حيزه الخاص له أيضا حيزٌ عامٌّ كنشاطه ومهنته والتي يتشارك من خلالها مع أشخاص آخرين. ويرتبط الحق في الخصوصية أيضاً بالشخص نفسه وما إذا كان مشهوراً أو بالمكان الذي حدثت به الواقعة فإذا ما كان مكاناً عاماً مطروقاً للجميع لم يعد للشخص حقٌّ في حماية خصوصيته.[٦٠]

وأمام هذه الأنواع من الخصوصية ظهرت على الساحة الفقهية والقانونية تناقضات تمثلت في حق الأفراد في الخصوصية وموجبات الاطلاع عليها. وإذا كانت الجهود التنظيمية، الإدارية والتشريعية، سعت إلى إقامة التوازن بين هذه الحقوق المتعارضة فإن جمع ومعالجة البيانات الشخصية، قد خلق واقعا صعباً هدد التوازن بين حق الخصوصية وحق السلطات في الاطلاع على البيانات والمعلومات الشخصية. لذلك نجد أن بعض الدول قد سعت إلى وضع الأطر القانونية المنظمة لهذا الامر، ومثال ذلك فرنسا حينما وضعت القانون رقم (١٧) لسنة ١٩٧٨م والخاص بالمعالجة الالية للبيانات. حيث تضمن القانون باباً خاصاً كفل من خلاله عدم الاعتداء على بيانات الأشخاص، كما نص القانون على إنشاء لجنة وطنية يجب استشارتها قبل معالجة أية بيانات شخصية يمكن أن تمس حقوق الأشخاص مع إقرار استثناء من أنه وفي حالة البحث عن جريمة فلا يلزم أخذ رأى اللجنة.[٦١] وهو الحال كذلك في الولايات المتحدة الأمريكية بإقرار قانون خصوصية الاتصالات والصادر عام ١٩٨٦م.

(58) See; Ruth A. Miller, The Limits of Bodily Integrity, Ashgate Adultery, and Rape legislation in Comparative Perspective (Ashgate Publishing Limited, 2007) USA.

(59) See; Blarca Rodriquez, Privacy in Telecommunication, (Martinus Nijhoff Publishers, 1997) USA.

(٦٠) انظر في ذلك: ساره رمال، الحق في الخصوصية في العصر الرقمي، منشورات الحلبي الحقوقية، بيروت، ٢٠١٧م ،ص١٢-١٤.

(٦١) انظر الباب الأول من القانون الفرنسي رقم (١٧) لسنة ١٩٧٨م في شأن المعالجة الآلية للبيانات الشخصية.

المطلب الثاني

ضوابط إجراءات البحث والتحري عن الجريمة الإلكترونية

لا خلاف في أن الوصول إلى الحقيقة هي غاية إجراءات البحث والتحري، بيد أن هذه الغاية لا يكون الوصول إليها إلا من خلال نظم وضوابط محددة، فالغاية لا تبرر الوسيلة. وانما يجب أن تكون هناك ضوابط وأطر يعمل من خلالها من يود الوصول إلى إثبات الحقيقة القضائية، حتى لا يضل أو يتعسف في سبيل سعيه نحو اكتشاف الجريمة. من هذا المنطلق ارتكزت المواثيق الدولية في الإعلان عن مجموعة من القيم الأساسية التي يجب مراعاتها والأخذ بها حين يتم القيام بأي إجراء في مواجهة الافراد.[٦٢]

إن المواءمة بين سعي السلطات نحو اكتشاف الجرائم وتتبع مرتكبيها وبين الحفاظ على حقوق الأفراد الشخصية استلزمت عدداً من الضمانات والتي عبرت عنها المواثيق الدولية كالمادة الثامنة من الاتفاقية على حماية الحق في حرمة الحياة الخاصة حيث عبرت:» لكل شخص الحق في احترام حياته الخاصة والعائلية ...». كما عبرت الفقرة الثانية من المادة المشار إليها إلى: لا يجوز للسلطة العامة التدخل في مباشرة هذا الحق، إلا إذا كان هذا التدخل ضرورياً، .... لحماية النظام أو لمنع الجرائم». وبذلك نجد أن هناك قيدين:

- أن يكون هناك نصٌ قانونيٌّ يجيز الاجراء.
- أن يكون الاجراء ضرورياً لمنع ارتكاب الجرائم أو حمايةً للمجتمع. [٦٣]

وفي نطاق إقامة التوازن بين حق المجتمع في حفظ النظام وإنفاذ القانون وبين حق الأفراد في حماية حقوقهم الشخصية يجب أن يلتزم رجال الضابطة العدلية الموكول إليهم مباشرة إجراءات البحث والتحري عن الجرائم بمجموعة من الضوابط والنظم والتي أرستها المواثيق الدولية أو النصوص القانونية والتي يمكن سرد بعضها في النقاط التالية:

أن يكون هناك واقعة لجريمة إلكترونية وقعت بالفعل قرر لها المشرع عقوبة محددة.

اتهام شخص أو أشخاص بارتكاب الجريمة الإلكترونية أو المشاركة في ارتكابها. بمعنى أن يتم تحديد شخص بوصفة فاعلاً أو شريكاً ويستوجب عقابه عن فعله.

توافر أمارات قوية أو قرائن تفيد عن وجود أدلة يمكن من خلالها اكتشاف الجريمة وتحديد

---

(٦٢) تقضي المادة الثانية من ميثاق الأمم المتحدة على أن من أغراض إنشاء المنظمة تطوير وتشجيع احترام حقوق الإنسان وحرياته الأساسية. انظر أيضاً الاتفاقية الأوروبية لحقوق الإنسان.

(٦٣) للمزيد انظر في ذلك: د. مفيد محمود شهاب، (مشروع الميثاق العربي لحقوق الإنسان في ضوء العهد الدولي للحقوق الاقتصادية والاجتماعية والثقافية)، دار العلم للملايين، بيروت، لبنان، المجلد الثاني، ١٩٨٩، ص٤١١.

شخص فاعلها. هذا الضابط يتطلب أن تكون هناك تحريات جديه قد تم إجراؤها وتم التوصل من خلالها إلى وجود أمارات عن وجود أدلة يمكن من خلالها الوصول إلى اكتشاف الجريمة. (٦٤)

المطلب الثالث

التحديات الإجرائية في الكشف عن الأدلة الإلكترونية

وحق الأفراد في حماية خصوصيتهم

تأسَّست نظريّات الإثبات على حقيقة أساسيّة - كان للرومان قصب السبق في التعبير عنها - وهي أنَّ الحق المجرَّد عن الدليل لا وجود له، ويُعد عَدمًا عند حصول المنازعة. وأمَّا الإثبات الجنائي، فهو: نشاط إجرائي مُوجَّه مباشرةً للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتّهام للتأكيد أو للنفي، يتوقَّف عليه الإجراء القضائي. وبمعنًى آخر، هو: إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين. والهدف من الإثبات، هو: بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة؛ فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات فوسيلة الإثبات، هي: كل ما يستخدم في إثبات الحقيقة - فهي نشاط يُبذَل في سبيل اكتشاف حالة أو مسألة أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة - أي: الأدلة - ونقلها إلى المجال الواقعي الملموس وصولا إلى اقتناع القاضي الجزائي بها. (٦٥)

إن الوصول إلى الحقيقة قد لا يكون بالأمر اليسير على رجال البحث والتحري حينما يتعلق الأمر بالأدلة الإلكترونية لما يميزها عن الأدلة الأخرى بمميزات تجعل من فرضية اختراق رجال البحث والتحري للقواعد والنصوص الإجرائية أمرًا لا مفر منه وبالتالي تثور مسألة شرعية الدليل المتحصل عن الإجراء غير المشروع من عدمه.

ان المبادئ والنظم القانونية والتي كفلت حق الخصوصية للأفراد كحق من حقوق الشخصية للأفراد اصطدمت بحقوق أخرى كحق سلطات الدولة في البحث والتحري عن المشتبه بهم خاصة مع الازدياد السريع في استخدام التكنولوجيا والبرامج التقنية في ارتكاب الجرائم وما صاحبها من منع الشركات التجارية الحاضنة لبيانات المستخدمين من البوح أو الإفصاح عن بيانات المستخدمين بذريعة حماية الخصوصية. وبفعل هذه الميزة غدا استخدام البرامج التي تتيحها الشركات التجارية أرضاً خصبة لارتكاب الجرائم الإلكترونية فثار بذلك تساؤل هام؛ عن مدى إمكانية ترجيح متطلبات العدالة على فكرة شرعية الحصول على الأدلة الإلكترونية؟

(٦٤) ذهبت المحكمة الاتحادية العليا في الإمارات إلى أن : "جدية التحريات وكفايتها لإصدار الإذن بالقبض والتفتيش من المسائل الموضوعية التي يوكل فيها الأمر إلى سلطة التحقيق، تحت رقابة محكمة الموضوع" - انظر القضية رقم (١١٣) لسنة ٣٣ قضائية (أمن دولة) - المحكمة الاتحادية العليا ، جلسة ٢٠٠٥/٦/٦م / ص ٢١٣.

(٦٥) للمزيد حول نظرية الحق انظر في ذلك: د. علي هادي العبيدي، المدخل لدراسة القانون (نظرية القانون ونظرية الحق)، الآفاق المشرقة، الشارقة، الإمارات العربية المتحدة، ٢٠١٤م.

فمن المسلم به أن شرعية الإجراء المتخذ في الحصول على الدليل بصفة عامة تستمد من القواعد القانونية العامة ومن الاتفاقيات الدولية واجتهادات القضاة والتي تستبعد أي دليل متحصل عليه بطريقة غير شرعية؛ إلا أنَّ الأمر قد يكون سببا رئيساً في عدم الحصول على الدليل وبالتالي عدم الوصول إلى الحقيقية. هذا الأمر دفع بالعديد من رجال الفقه والقضاة للبحث عن الحقيقة باعتبارها مقصد المشرع من إقرار القوانين العقابية والإثباتية ، وإن الأدلة التي لا تؤدي إلى الوصول إلى الحقيقة لا قيمة لها ولا تتماشى وإرادة المشرع في الكشف عن الحقيقة.[٦٦]

مسألة الشرعية كانت مثار شد وجذب بين فريق ينادي بالتمسك بالشرعية في الحصول على الدليل على أساس أن الإثبات يقتصر على إثبات الوقائع ولا يسعى إلى بيان مقصد المشرع أو وجهة نظره ، وعليه يجب الحصول على الأدلة بطريقة شرعية ويبقي القضاة فيصل الحكم عليها، وفريق يرى أن تحقيق العدالة يبرر اتخاذ أي وسيلة تؤدي للوصول إلى الحقيقة باعتبارها مقصد المشرع من إقرار القوانين ومسعاه حيث يسعى المشرع من وضع القوانين إلى الوصول إلى حقيقة الامر ولا تثريب اذا ما تم الحصول على الدليل بطريقة غير مشروعة طالما كان قادراً على إثبات الواقعة ونسبتها إلى الفاعل الأصلي.

وهذا ما يلاحظ على توجه القضاء الفرنسي الحالي، فمن المعلوم أن القوانين اللاتينية تأخذ بمبدأ شرعية الأدلة فأي دليل متحصل بطريقة غير مشروعة يتم استبعاده من أدلة الإثبات، إلا أن توجه القضاة الفرنسي الحديث ذهب إلى الأخذ بهذا النوع من الأدلة والتي قد تكون متحصلة من إجراء غير مشروع. فقد ذهبت محكمة النقض الفرنسية في حكمها الصادر بتاريخ ٢٠١٢/٠١/٣١م إلى أن التسجيلات المتحصل عليها بالمخالفة لأحكام المادة (١٧٠) من قانون الإجراءات الجزائية الفرنسي يمكن الاخذ بها ومناقشتها أمام المحكمة.[٦٧] وفي هذا إشارة إلى الخروج عن المبادئ المستقر عليها في القضاء الفرنسي. إن هذا التوجه يعبر عن حقيقة لا بد من الاعتراف بها وهي أن القواعد الإجرائية المرتبطة بمبدأ الشرعية غدت غير قادرة في إثبات بعض الجرائم وخاصة الإلكترونية منها. وعلى هدى من ذلك؛ عمدت بعض الدول إلى تعديل القواعد الإجرائية في البحث عن الدليل خاصة وإذا ما دعت الحاجة إلى الإسراع في الحصول عليه خشية ضياعه وهو ما عمدت آلية أستراليا [٦٨] والولايات المتحدة الأمريكية [٦٩] حينما عدلت قوانينها بما يتلاءم ومتطلبات الحصول على الدليل.

ومن هذا المنطلق ثارت فرضية ترجيح فكرة تقديم حق الدولة في الكشف عن الجرائم وتعقب

(66) See; Mission De Recherche, droit et justice, La preuve pénale internationalisation et nouvelles technologies, la documentation française, paris, 2007, p15 .
(67) Cass.crim.,31janv.2012, n 11-85.464.
(68) The Australian Crimes Act 1941, s4k.
(69) The USA Patriot Act Section 213.

مرتكبيها على فكرة شرعية الإجراء المتخذ في سبيل الحصول على الدليل خاصة مع التطور السريع في طرق ووسائل ارتكاب الجرائم وعدم مواكبة التعديلات في النصوص التشريعية لأنماط السلوك المرتكب.

وعلى هدى مما سبق، يمكننا القول إنه لا خلاف في أن البرامج والأجهزة الإلكترونية التي تقدمها الشركات التجارية بمختلف أنواعها أداة ممتازة لجمع المعلومات؛ لأنها تتضمن معلومات مهمة عن المستخدمين، وبالتالي يمكن لمأموري الضابطة العدلية استخدامها في جمع الاستدلال عن جرائم تقنية المعلومات ، حيث توفر الجهد والمال وعن طريقها يمكن التوصل إلى المعلومات الشخصية بنوعيها الحقيقي والافتراضي للمستخدمين ، فمن خلال تحليل شبكات الفيسبوك مثلا أو برنامج الواتس آب يمكن تحديد العلاقة بين المشتبه فيهم والجرائم الناشئة عن الشبكات الاجتماعية؛ إلا أنه ينبغي على السلطات إذا ما رغبت في البحث عن المعلومات أو البيانات أن تراعي التوازن فيما بين الحق في الخصوصية والحفاظ على سرية المعلومات من ناحية ، ومصلحة العدالة الجنائية في الوصول إلى المعلومات التي تسهم في كشف الحقيقة عن الجرائم المعلوماتية من ناحية أخرى. وباستقراء النصوص القانونية المنظمة نجد أنها خلت من إلزام الشركات التجارية بمساعدة سلطات الضابطة العدلية في جمع البيانات حيث تحكم الشركات التجارية نظمها الداخلية والتي تمنع اطلاع الغير على البيانات أو المعلومات الشخصية للمستخدمين المطلوبة الأمر الذي بلا شك يعوق سلطة جمع الاستدلال من الوصل الي بيانات المستخدمين وبالتالي الكشف عن الجرائم وتعقب مرتكبيها.[٧٠] فعلى سبيل المثال نجد أن شركة مايكروسفت وضعت عدد من الحالات حصراً والتي يمكن من خلالها الكشف عن بيانات المستخدمين وهي الحالات التي تمثل خطراً على الحياة أو في حالات الطوارئ فقط [٧١] وفيما عدا ذلك لا يجوز الكشف عن البيانات أو إعطاء أي معلومات خاصة بالمستخدمين حتى ولو كانت الجهة الطالبة جهة قضائية، ومن ثم تقف سلطات جمع الاستدلال عاجزة عن الوصول إلى بيانات المستخدمين. وتوضيحاً لذلك إذا ما استخدم أحد الاشخاص البريد الإلكتروني لشركة مايكروسفت مثلاً في الاحتيال على عدد من الأشخاص ووقعوا ضحايا لفعل الاحتيال ورغبت سلطات جمع الاستدلال الحصول على بيانات ذلك المستخدم أو حتى تحديد العنوان البروتوكولي للشبكة المعلوماتية [٧٢] فإن الشركة تمتنع عن تزويد السلطات

(٧٠) من أشهر المطالب في هذا الخصوص حينما رفضت شركة أبل في عام ٢٠١٦م أمرا قضائيا يطلب اختراق هاتف مهاجم سان برناردينو ، حيث رفضت شركة أبل أمرا قضائيا أصدرته محكمة أمريكية يطلب منها مساعدة محققي مكتب التحقيقات الفيدرالي في اختراق بيانات محتفظ بها على هاتف متهم، ولم تستطع المحكمة إجبار الشركة على تقديم تلك المساعدة.

(٧١) هذه الحالات الطارئة محددة حصراً في حالة خطر الوفاة أو الإصابة المادية الجسيمة لشخص فقط ، ويجب تقديم طلب كتبي بذلك موقع من جهة قضائية يتضمن مختصر عن الحالة الطارئة وشرح لكيف يمكن ان يؤدي الإفصاح عن المعلومات المطلوبة المساعدة في الحالة الطارئة ووفق شروط إجرائية أخرى محددة ايضاً.

(٧٢) عرف المرسوم بقانون رقم(٥) لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات الاتحادي في المادة الأولى منه العنوان البروتوكولي بانه " معرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات ويتم استخدامه لأغراض الاتصال ".

بهذه البيانات بذريعة حماية الخصوصية ودون أن يكون لسلطة الضابطة العدلية الحق في مطالبة أو إلزام الشركة بتقديم البيانات التي بحوزتها أو حتى مساءلتها جزائياً عن فعل الامتناع. هذا القصور التشريعي فسح المجال بلا شك لاتساع رقعة ارتكاب الجرائم الإلكترونية وساهم في تخفي الجناة عن أعين رجال الضبط وزاد عناءهم حين البحث عن مرتكبي هذا النوع من الجرائم. ومن هنا ظهرت الحاجة إلى إجراء مراجعة تشريعية شمولية لنصوص تجريم جرائم تقنية المعلومات وطرق جمع أدلتها، فمن أجل الوصول إلى غاية محاربة ومكافحة الجريمة الإلكترونية يجب أن تكون هناك نصوصٌ عقابية ناجعة ومتكاملة مع نصوص اجرائية تتناسب وطبيعة الجرائم الإلكترونية مع ضرورة وجود تضافر وتعاون وتنسيق دولي؛ فمن خلال هذا التكامل يمكن الوصول الي غاية المشرع من التشريع وحماية المجتمع من خطر استفحال جرائم تقنية المعلومات والحد من الآثار الاجتماعية والاقتصادية الناجمة عن هذا النوع من الجرائم. فالتقنية بحد ذاتها لا تنتهك الخصوصية بل الأفراد هم من ينتهكون الخصوصية عن طريق استخدام التقنية ومن أجل ضمان حسن الاستخدام لابد للمشرع من أن يضع الإطار القانوني الذي من خلاله تستخدم التقنية.

الخاتمة

ختاماً، قد لا تكون هذه الورقة أوفت الموضوع حقة من ناحية العرض والتحليل فهناك دائماً مبررات للاختصار. ما نود الوصول آلية من خلال العرض السابق أن الجريمة الإلكترونية أصبحت واقع حال وليست سحابة صيف، هذا الواقع يحتم علينا تلميم أوراقنا وإعداد عدتنا لمواجهة هذا الخطر المستفحل الذي أصاب مجتمعنا اجتماعياً واقتصادياً وقانونياً. إن التعديل التشريعي أصبح حاجة لا غنى عنها، فالتطور التقني متسارع فمع إشراقة شمس كل يوم جديد تطالعنا الشركات التجارية بما هو متطور ومستحدث، هذا التطور استغله ضعفاء النفوس في تسهيل ارتكاب الجريمة فكان التطور التقني خدمة يسرت وسهلت على الجناة ارتكاب جرائمهم؛ وعلى الجانب الآخر أضحت النصوص التشريعية بعيدة كل البعد عن مواكبة هذا التطور وهي حقيقة يجب الاقرار بها، ذلك أن التعديلات التشريعية لم توازِ التطور التقني ولَم تَفِ بالإحاطة بأنماط السلوك الممارس عن طريق تقنية المعلومات. وعلى الرغم من ذلك فالأمر يستوجب ان تكون هناك رؤيا واضحة وجهود تسعى لتجسير الهوه الفاصلة بين القصور التشريعي والتطور التقني بشكل يمنع أو يحد من استغلال الجناة للتكنولوجيا لتحقيق مآرب غير مشروعة. ومن خلال هذه الورقة سعينا جاهدين قدر المستطاع لبيان مدى خطورة جرائم تقنية المعلومات واستظهار النقص والقصور التشريعي المتمثل في عدم كفاية النصوص القانونية في الحد من استفحال الجريمة الإلكترونية؛ وختاماً يمكن ان نضع بعضاً من التوصيات التي يمكن الاسترشاد بها:

١- التوصية بتعديل القوانين العقابية الخاصة بالجريمة الإلكترونية بحيث تشمل قواعد إجرائية منظمة لطرق جمع الاستدلال تتناسب وطبيعة تلك الجرائم مع الاعتراف بحجية البيانات والمعلومات المستخلصة من الوسائل الإلكترونية في مجال الاثبات الجنائي. مع الإشارة إلى إمكانية النظر في القانون البحريني رقم (٦٠) لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات كمثال يمكن الاسترشاد به.

٢- التوصية بتعديل القوانين العقابية الخاصة بالجريمة الإلكترونية من خلال وضع التزامات على مقدمي الخدمة التقنية تتمثل في الزامهم بجعل البيانات والمعلومات الخاصة بالمستخدمين متاحة لسلطات الضابطة العدلية متى ما كانت موضع جمع استدلال عن جريمة قد ارتكبت وفق شروط محددة.

٣- ضرورة النص على المسؤولية الجزائية لمزودي خدمات الاستضافة عن المحتوى، إذا ما توافر لديها العلم الفعلي بطبيعته غير المشروعة، ولم يتصرف فوراً لإزالة البيانات، أو جعل الوصول إليها مستحيلاً، أو لم يُبقِ على البيانات التي يمكن من خلالها التعرف على الشخص الذي أسهم في إنشاء المحتوى الإلكتروني. وعلى أن تحدد فترة زمنية معينة يجب عليهم الاحتفاظ خلالها بالبيانات أو المعلومات.

٤- التوصية بالإنضمام إلى الاتفاقيات الدولية القضائية في شأن المساعدات القضائية وتبادل المعلومات بين الدولة وباقي الدول الأخرى الأعضاء بالأمم المتحدة.

٥- التوصية بوضع ضوابط وشروط لاستخدام مواقع وبرامج التواصل الاجتماعي وغيرها من البرامج المشابهة؛ إذ يجب على المستخدمين استكمال تسجيلهم في هذه المواقع ببياناتهم الحقيقية، وإلزام مزودي الخدمة بتحديد شروط مسبقة لاستخدام هذه المواقع. فحجم المعلومات الشخصية المخزنة ببرامج التواصل الاجتماعي يجعل منها مصدراً غنياً بالمعلومات والبيانات التي يمكن الاستعانة بها عند البحث عن مرتكبي الجرائم.

قائمة المراجع

أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزء الأول، المملكة العربية السعودية، الرياض، المركز العربي للدراسات الأمنية والتدريب، ٢٠٠٦.

أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مصر، دار النهضة العربية للنشر والتوزيع، الطبعة العاشرة، ٢٠١٦.

أحمد محمد الفيومي، المصباح المنير في غريب الشرح الكبير، لبنان، بيروت، المكتبة العلمية، الجزء الاول، طبعة ٢٠١٠.

ألفن توفلر، وعود المستقبل، ترجمة غازي غصون، دار الروح، لبنان، ١٩٨٥م.

آمال عثمان، شرح قانون الإجراءات الجنائية، مصر، القاهرة، دار النهضة العربية، ١٩٧٥م.

جودة جهاد، الوجيز في شرح قانون الإجراءات الجزائية لدولة الإمارات العربية، الجزء الأول، الدعاوى الناشئة عن الجريمة - الإجراءات التحضيرية للدعوى الجزائية-، الطبعة الاولي، الإمارات العربية المتحدة، دبي، مطابع البيان، ١٩٩٤م.

حسن صادق المرصفاوى، أصول الإجراءات الجنائية، منشأة المعارف، الاسكندرية، مصر، ١٩٨٢م.

خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، مصر، ٢٠١٩م.

رؤوف عبيد – أصول علم الإجرام والعقاب-، دار الفكر العربي، القاهرة، مصر، الطبعة الخامسة، ١٩٨١م.

ساره رمال، الحق في الخصوصية في العصر الرقمي، منشورات الحلبي الحقوقية، لبنان، بيروت، ٢٠١٧م.

عبد الحي وليد، مدخل إلى الدراسات المستقبلية في العلوم السياسية، المركز العالمي للدراسات السياسية، الأردن، ٢٠٠٨م

عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجزائية، دار النهضة العربية، القاهرة، مصر، ٢٠٠٢م.

عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنيت، مصر، القاهرة، دار الكتب القانونية، طبعة ٢٠٠٧ م.

عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت في التشريعات العربية، مصر، القاهرة، دار النهضة العربية، ٢٠٠٩م.

علي بن محمد الشريف الجرجاني، التعريفات، لبنان، بيروت، دار الكتب العلمية، طبعة ١٩٨٣.

علي هادي العبيدي، المدخل لدراسة القانون (نظرية القانون ونظرية الحق)، الافاق المشرقة، الشارقة، الامارات العربية المتحدة، ٢٠١٤م.

عمر محمد بن يونس، الإجراءات الجزائية عبر الانترنت في القانون الأمريكي، مصر، القاهرة، دار النهضة العربية، ٢٠٠٥م.

مأمون سلامة، الإجراءات الجزائية في التشريع المصري، مصر، القاهرة، دار النهضة العربية للنشر والتوزيع، الجزء الاول، طبعة ٢٠٠٨.

مأمون سلامة، قانون العقوبات، القسم العام، مصر، القاهرة دار النهضة العربية، ١٩٩٠م.

محمد الميداني، النظام الأوروبي لحماية حقوق الإنسان، لبنان، بيروت، منشورات الحلبي الحقوقية، الطبعة الثالثة، ٢٠٠٩م.

محمد عبابنه، جرائم الحاسوب وأبعادها الدولية، الأردن، درا الثقافة، ٢٠٠٥م.

مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الالكترونية، مصر، مطابع الشرطة- القاهرة، الطبعة الأولي ٢٠٠٨م.

هشام رستم، جرائم الحاسب الآلي المستحدثة، مصر، دار الكتب القانونية، الطبعة الاولي، ١٩٩٩م.

هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، مصر، ٢٠٠٠م.

ياسر حسين بهنس، الوسيط في شرح نظام الإجراءات الجزائية السعودي الجديد، مصر، القاهرة، مركز الدراسات العربية للنشر والتوزيع، الطبعة الاولي، ٢٠١٨م.

Amanda Ngomane, The Use of Electronic Evidence in Forensic Investigation, (DPhil thesis, University of South Africa 2010).

Blarca Rodriquez, Privacy in Telecommunication, (Martinus Nijhoff Publishers, 1997) USA.

Daniel J. Solove and Paul M.Schwartz, Information Privacy Law Aspen Cacebook, (4rd edn, Wolters Kluwer, 2011) USA.

Mission De Recherche, droit et justice, La preuve pénale internationalisation et nouvelles technologies, la documentation française, Paris, 2007.

Ross Anderson, Security Engineering, (2nd edn, Wiley Publishing Inc. 2008).

Ruth A. Miller, The Limits of Bodily Integrity, Ashgate Adultery, and Rape legislation in Comparative Perspective (Ashgate Publishing Limited, 2007) USA.

Sharon Nelson, Bruce Olson and John Simek, The Electronic Evidence and Discovery Handbook: Form, Checklists And Guidelines (New York: American Bar Association 2006).

Stephen Moson, Electronic Evidence, (3rd end, LexisNexis Butterworths 2012).