الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني
(دراسة مقارنة)

دكتور
أحمد لطفي السيد مرعي
كلية الحقوق – جامعة المنصورة
قسم القانون الجنائي

بسم الله الرحمن الرحيم

﴿فَبَدَأَ بِأَوْعِيَتِهِمْ قَبْلَ وِعَاءِ أَخِيهِ ثُمَّ اسْتَخْرَجَهَا مِن وِعَاءِ أَخِيهِ ۚ كَذَٰلِكَ كِدْنَا لِيُوسُفَ ۖ مَا كَانَ لِيَأْخُذَ أَخَاهُ فِي دِينِ الْمَلِكِ إِلَّا أَن يَشَاءَ اللَّهُ ۚ نَرْفَعُ دَرَجَاتٍ مَّن نَّشَاءُ ۗ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ﴾

صدق الله العظيم

(سورة يوسف – آية 76)

ملخص البحث باللغة العربية

مع بدء الألف الثالثة دخلت الإنسانية مرحلة جديدة من تطور الفكر الإنساني على إثر الثورة المعلوماتية، فنشأ ما يسمى بالدليل الرقمي وما يرتبط بالإجرام المعلوماتي أو الالكتروني. وهو نمط حديث من الجرائم الذي مثل مأزقًا للسياسة الجنائية المعاصرة.

والحقيقة أنه لا تقتصر الإشكاليات التي تطرحها ظاهرة جرائم تقنية المعلومات والإجرام الالكتروني على الجوانب الجنائية الموضوعية، بغية البحث عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الإجرام، بل طالت أيضًا الجوانب الجنائية الإجرائية. ولعل الذي حدانا إلى اختيار الجانب الجنائي الإجرائي لجرائم تقنية المعلومات ليكون محور بحثنا هذا هو تركيز جل الدراسات القانونية في باب جرائم المعلوماتية على العناية بالجانب الموضوعي لتلك الجرائم. ولقد أزاد صدور القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات من أهمية هذا البحث إذ يمكننا من طرح رؤية تقييمية لآليات المكافحة المصرية لهذه الجرائم على نحو ما وردت في ها القانون، خاصة في شقها الإجرائي الذي حواه الباب الثاني من القانون المعنون: "الأحكام والقواعد الإجرائية".

وعلى ذلك تبرز الإشكالية الرئيسة لهذا البحث في طرح التساؤل حول مدى إمكانية الاعتماد على إجراءات التحقيق التقليدية في الكشف عن الجرائم الإلكترونية، وما إذا كانت الإجراءات الجنائية التقليدية المتعلقة بالتفتيش الإلكتروني قادرة على احتواء خصوصيات هذا الإجرام، دون المساس بمتطلبات الشرعية الإجرائية (المبحث الأول). أم الجزء الثاني من هذا البحث فقد خصصناه لمعالجة إشكالية طبيعة وحجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني (المبحث الثاني).

الملخص باللغة الإنجليزية

"Digital Evidence Obtained From Electronic Criminal Inspection, A Comparative Study"

With the beginning of the third millennium, humanity entered a new stage of the development of human thought following the information revolution, so the so-called digital evidence and what is related to information or electronic crime emerged. It is a modern type of crime that has represented a dilemma for contemporary criminal policy.

In fact, the problems raised by the phenomenon of information technology crimes and cybercrime are not limited to objective criminal aspects, in order to search for the possibility of applying its traditional texts to this new type of crime, but also to the criminal procedural aspects. Perhaps what prompted us to choose the criminal and procedural aspect of IT crimes as the focus of our research is the focus of most legal studies on information crimes, on taking care of the objective aspects of those crimes.

The issuance of Law No. 175 of 2018 in the matter of combating information technology crimes has increased the importance of this research, as it enables us to present an evaluation view of the Egyptian combating mechanisms for these crimes as stipulated in this law, especially in its procedural aspect contained in Chapter Two of the Law entitled: Provisions and Rules of Procedure. "

Accordingly, the main problem of this research emerges when it raises the question about the extent of reliance on traditional investigation procedures in detecting electronic crimes, and whether the traditional criminal procedures related to electronic searches are able to contain the specifics of this crime, without prejudice to the requirements of procedural legitimacy (Chapter I). Or the second part of this research, we have devoted it to addressing the problematic nature and authenticity of the digital evidence obtained from electronic inspection (Chapter II).

مقدمة

أولاً: إشكالية البحث:

مع بدء الألف الثالثة من ميلاد السيد المسيح عليه السلام، دخلت الإنسانية مرحلة جديدة من تطور الفكر الإنساني على إثر الثورة المعلوماتية، التي أعملت تأثيرها في كافة مناحي الحياة، وقاربت بين الشعوب زماناً ومكاناً، وكشفت عن حجم هائل من البيانات والمعلومات المعالجة والتي يتم تبادلها على نطاق محلي وعابر للحدود[1]، فنشأ ما يسمى بالدليل الرقمي*L'Evidence numérique*، والإجرام المعلوماتي أو الالكتروني *Criminalité informatique ou électronique* (ما يتصل بالحاسب الآلي)، والسيبراني *Cybercriminalité* (ما يتعلق بشبكة المعلومات)، وجرى الحديث عن ثورة تضاهي الثورة الصناعية الأولى أواخر القرن التاسع عشر، والتي أحلت الآلة محل الجهد البدني، هدفها – أي هدف الثانية تلك – إحلال الآلة محل النشاط الذهني للإنسان، الأمر الذي كثف الإقبال على الحواسب الآلية[2] والاشتراك في الشبكات المعلوماتية، سواء من قبل القطاعات العامة أو الخاصة، إلى الدرجة التي أضحى معها من العسير على تلك القطاعات أن تؤدي نشاطها بدون اللجوء إلى تقنية المعلومات.

وقد رفعت الزيادة في استعمال هذه التقنيات الرقمية من معدلات المخاطر المرتبطة بسوء استخدامها، حتى عظم الحديث عما يسمى جرائم تقنية المعلومات، أو الجرائم الإلكترونية[3]، وهو نمط حديث من الجرائم الذي مثل مأزقًا للسياسة الجنائية المعاصرة، لاسيما إذا اقترنت بالجريمة المنظمة والعابرة للحدود والجرائم الإرهابية، وذلك بالنظر إلى ذاتية أركانها وحداثة أساليب ارتكابها، والبيئة التي ترد عليها، وخصوصية مرتكبيها[4]، ووسائل كشفها، وتنوع الغاية من ارتكابها[5]، والتي تعرف وفق معايير مختلفة منها: محل الجريمة، أو وسيلة ارتكابها، أو قدرة الجاني على التحكم في تكنولوجيا المعلومات[6]، وتتنوع بين الاختراق، والتلاعب ببيانات وبرامج الحاسب الآلي، والاحتيال والتزوير

---

[1] في عام 2013 قدرت شركة *IBM* حجم البيانات المتداولة عالمياً في السنة بنحو 2.5 تريليون بايت، 90% منها أنتج في عامين سابقين فقط على هذا التاريخ. ذكرت هذه الإحصائية بواسطة:

J. Bourguignon, La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat, in Société Française pour le Droit International, Colloque de Rouen sur "Internet et droit international", du 30 Mai au 1er juin 2013, éd. Pedone, Paris, 2014, note 1, p.357.

[2] يعرف الحاسب الآلي بأنه: "مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلية طبقًا لبرنامج تم وضعه مسبقًا للحصول على نتائج معينة. راجع، هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص6، محمد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر، عمان، 2002، ص5. وقد عرفته المادة الأولى من القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات بأنه: "الحاسب: كل جهاز أو معدة تقنية تكون قادرة على التخزين، أو أداء عمليات– منطقية، أو حسابية، وتستخدم لتسجيل بيانات أو معلومات، أو تخزينها، أو تحويلها، أو تخليقها، أو استرجاعها، أو ترتيبها، أو معالجتها، أو تطويرها، أو تبادلها، أو تحليلها، أو للاتصالات".

[3] *K. Tiedemann, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, RDPC., n°7, Bruxelles, 1984, p.61.*

[4] *P. Glineur, Droit et Ethique de l'Informatique, Story Scientia, Bruxelles, 1991, p.180 ; D. B. Parker, Figting Computer Crime "A new Framework for Protecting Information", Joh Wiley and sons, 1998, p.136 ; D. Martin, et F. P Martin, Cybercrime, Paris, PUF., 2001, p.75.*

[5] *P. Lacoste, Les métiers de l'intelligence économique, Défense Nationale, Paris, 2006, p.144.*

د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 1992، ص17 وما بعدها، د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص5 وما بعدها، ص50 وما بعدها،، خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008، ص 6 وما بعدها، جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، جامعة مولود معمري، تيزي وزو، 2018، ص2، عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائي والمقارن، رسالة ماجستير، جامعة العقيد الحاج لخضر، باتنة، الجزائر، 2011-2012، ص12.

[6] يمكن تعريف الجريمة الإلكترونية بأنها: "عبارة عن كل اعتداء يطال معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات. راجع لمزيد من التفصيل حول تعريف الجريمة الإلكترونية:

المعلوماتي، وسرقة الهوية، وإساءة استعمال البريد الالكتروني، والاحتيال في استخدم بطاقات الائتمان، وانتهاك حرمة الحياة الخاصة...الخ.

ولقد جعل الخبير الاسكتلندي من الإجرام المعلوماتي والقرصنة عبر الإنترنت *Colin Rose* الجريمة الإلكترونية ثالث تهديد خطير يواجه القوى العظمى، بعد خطر الأسلحة الكيماوية والبكتريولوجي والأسلحة النووية[7]؛ فجرائم تقنية المعلومات تتسم بسهولة ارتكابها في فضاء افتراضي متخوم بالأجهزة الآلية، وشبكات الاتصال غير المرئية، والتي يصعب السيطرة عليها حيث يتجاوز السلوك الإجرامي فيها أحيانًا كثيرة الحدود المكانية بالمعنى التقليدي[8]، فضلاً عن كونها لا تخلف أية آثار محسوسة، ويمتاز مرتكبيها بأوصاف عدة، أهما الذكاء الإجرامي، لما يملكوه من كم المعارف التقنية المرتبطة بمعالجة البيانات[9].

وتشير بعض تقديرات منظمة التعاون الاقتصادي والتنمية *OCDE.* إلى أن حجم المبادلات الإلكترونية عبر شبكة المعلومات الدولية قد بلغ 400 مليا في عام 2000، وهو عشرة أضعاف ما تم في عام 1998، وقد قفر المبلغ إلى 8500 مليار في عام 2005[10].

D. Wall, Crime and the Internet, Routledge, N.Y, 2001, p.3 ; M. Alexander, Computer crime, Computer World, vol. XXIV, n°11,1990, p.104 ; A. Lucas et J. Deveze, Le droit de l'informatique et de l'internet, PUF. Paris, 2001, p.496 ; D. B. Parker, Combattre la criminalité informatique, OROS., Paris, 1985, p.18 ; D. B. Parker, Figting Computer Crime "A new Framework for Protecting Information", Joh Wiley and sons, 1998, p.112 ; M. Wasik, Crime and The Computer, Oxford University Press, 1991, p.2 ; D. Thompson, Current trends, in Computer control crime, Computer Quarterly, vol. 9, n°1, 1991, p.2. ; K. Tiedemann, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, RDPC., n°7, Bruxelles, 1984, p.61 ; R. Totty & A. Hardcastle, Computer-Related Crime in Information Technology and the Law, Macmilla Publishers, U.K. 1986, p.26.

د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص5، د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، 1997، ص2، محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص16، د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1994، ص29 وما بعدها، د. يونس عرب، جرائم الكمبيوتر والانترنت، اتحاد المصارف، 2001، ص19، نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، 2008، ص59.

[7] *M. Chawki, Essai sur la notion de cybercriminalité, IEHE, Lyon, 2006, p .2 ; D. WALL, Crime and the Internet, Routledge, N.Y, 2001, p. 3.*

وراجع:

C. Rose, Discours prononcé lors de l'ouverture du G-8 sur la cybercriminalité, Paris, 2000.

مشار إليه لدى:

R. Boos, La lutte contre la cybercriminalité au regard de l'action des Etats, th. Lorraine, 2016, p. (avant-propos) ; D. B. Parker, Figting Computer Crime, op. cit., p.112.

[8] *U. Sieber, The international Handbook on Computer Crime "Computer related Economic Crime and the Infringements of Privacy", John Wiley and Sons, 1986, p. 83.*

[9] *Y. Masuada, The Information Technology Revolution, Oxford Blackwell, Oxford, 1985, p.620 ; A. Lucas et J. Deveze, op. cit., p.496 ; D. B. Parker, op. cit., p.10 ; M. Alexander, op. cit., p.9.*

[10] وراجع حول إحصاءات أخرى، عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائي والمقارن، رسالة ماجستير، جامعة العقيد الحاج لخضر، باتنة، الجزائر، 2011-2012، ص1، ص11.

D. B. Parker, op. cit., p.112.

وقد كشفت جوانب الخصوصية تلك للجرائم الإلكترونية عن مأزق التعامل مع أنشطتها الإجرامية، سواء من حيث تكييف السلوك الإجرامي المرتكب ووضعه تحت مظلة النصوص التجريمية التقليدية، وتعريض مبدأ شرعية التجريم والعقاب لخطر المساس به، وما يرتبط به من مبادئ التفسير الضيق للنصوص العقابية، وحظر القياس، الأمر الذي أوجب على المشرع الجنائي سن نصوص جنائية جديدة تتوافق مع هذه الأنشطة الإجرامية المستحدثة، وتتيح لمرفق العدالة الجنائية قدر من الفاعلية بغية تطوير آليات ووسائل مكافحة الجرائم التي ولدتها تكنولوجيا الإعلام والاتصال، والاستفادة من معطيات هذه التكنولوجيا الحديثة في الكشف عن الجرائم وإثباتها وملاحقة مرتكبيها للدفع بهم بين يد العدالة[11].

والحقيقة أنه لا تقتصر الإشكاليات التي تطرحها ظاهرة جرائم تقنية المعلومات والإجرام الالكتروني على الجوانب الجنائية الموضوعية[12]، بغية البحث عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الإجرام، بل طالت أيضًا الجوانب الجنائية الإجرائية[13]. فبينما صيغت النصوص الجنائية الإجرائية التقليدية – المنضوية بين طيات قانون الإجراءات الجنائية عادة – لمواجهة جرائم كلاسيكية، لا توجد ثمة عوائق كبيرة في باب إثباتها أو التحقيق في وقائعها وجمع الأدلة القولية أو المادية بشأنها، ويهيمن عليها مبدأ الاثبات الحر، والاقتناع الذاتي للقاضي الجنائي، وحق القاضي في اتخاذ أي إجراء مشروع يمكن من خلاله الوصول إلى الحقيقية بشأن الجريمة ومرتكبيها[14]، تقف هذه النصوص عاجزة عن أن تتلاءم مع المشكلات الإجرائية التي تثيرها عملية البحث والتنقيب في مجال الجرائم الإلكترونية، لاسيما إثبات هذه الجرائم، التي ترتكب في عالم افتراضي غير ملموس، لا تعتاد عليه سلطات الاستدلال والتحقيق، كما هو الحال في باب الجرائم التقليدية من قتل أو سرقة أو تزوير أو تزييف...الخ، حيث يلعب السلوك المادي الدور الأكبر في مجال إثباتها والتحري والبحث فيها، باعتبار تعدد العناصر المادية والآثار الملموسة المتخلفة عنها على مسرح الجريمة، خلافًا للجريمة الإلكترونية، التي تتدفق على مسرح افتراضي

---

[11] د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص3.

[12] راجع لمزيد من التفصيل حول هذه الجوانب، د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 1992، د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، دار النهضة العربية، 1998، د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)، ط1، دار النهضة العربية، 2006، محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، 2004، د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ط1، دار النهضة العربية، 2004، أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت . دراسة تحليلية مقارنة، ط1، دار وائل للنشر . عمان، 2000، موسى مسعود أرحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مجلة دراسات قانونية، جامعة قاريونس، ع17، ص80.

[13] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة . أسيوط، 1994، د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي . دراسة مقارنة، ط1، دار النهضة العربية، 1997، د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002، نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات . دراسة مقارنة، دار الفكر الجامعي، 2013، د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، 2002، د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية"، ط1، 2004 . 2005، د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)، ط1، دار النهضة العربية، 2006، موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا . طرابلس، الفترة 28 . 2009/10/29، د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، جامعة مولود معمري، تيزي وزو، 2018.

[14] في هذا المعنى، د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص3.

غير مادي *Immatériel*، لا ينجم عنها آثار مدركة بالوسائل المعتادة، الأمر الذي يمكن من سرعة اقترافها، ويسر محو آثارها وإخفاء أدلتها.

ولعل الأمر يزداد صعوبة حالما ترتكب هذه الجرائم على نطاق إقليمي عابر للحدود، حيث تصبح إشكالية ملاحقتها وتتبعها وجمع أدلتها من قبل السلطات الوطنية في إقليم دولة أخرى، وما يرتبط بذلك من مفاهيم السيادة والولاية القضائية والتعاون الدولي على المحك، وهو الأمر الذي عظم من الاهتمام الحكومي والهيئات الدولية بفكرة الأمن السيبراني والحماية التقنية للنظم وبرامج الحاسب الآلي وشبكات المعلوماتية، للدرجة التي أصبحت معها هذه الموضوعات تأخذ موضع الصدارة في النقاشات العلمية في مجال تكنولوجيا تقنية المعلومات.

ولم يكن الفقه الجنائي ليغفل عن هذا الاهتمام، فأخذ على عاتقه إبراز أوجه القصور التي تعترى تطبيق النصوص الإجرائية التقليدية على جرائم تقنية المعلومات، وكشف عن ضرورة تدارك أوجه القصور باستحداث نصوص جنائية إجرائية تمكن رجال العدالة الجنائية من البحث والتحقيق واستنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم، مع مراعاة احترام الحق في الخصوصية الفردية، أي العناية بتحقيق التوازن بين حق المجتمع في الحماية من انعكاسات تقنية المعلومات وأخطارها وبين الضرورة الملحة في العصر الرقمي من الاستفادة من إمكانيات هذه التقنية وفوائدها الفردية والمجتمعية.

ولعل الذي حدانا إلى اختيار الجانب الجنائي الإجرائي لجرائم تقنية المعلومات ليكون محور بحثنا هذا هو تركيز جل الدراسات القانونية في باب جرائم المعلوماتية على العناية بالجانب الموضوعي لتلك الجرائم، فضلاً عن قلة المراجع التي طرحت على بساط البحث الإشكاليات المرتبطة بآليات التحقيق فيها، وبيان العقبات الإجرائية التي تصطدم بها سلطات الاستدلال والتحقيق في التعامل معها، بغية اقتراح السبل الفعالة لتجاوز هذه العقبات. ولقد أزاد صدور القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات من أهمية هذا البحث إذ يمكننا من طرح رؤية تقييمية لآليات المكافحة المصرية لهذه الجرائم على نحو ما وردت في ها القانون، خاصة في شقها الإجرائي الذي احتواه الباب الثاني من القانون المعنون: "الأحكام والقواعد الإجرائية" (المواد 5 إلى 11).

وعلى ذلك تبرز الإشكالية الرئيسة لهذا البحث في طرح التساؤل حول مدى إمكانية الاعتماد على إجراءات التحقيق التقليدية في الكشف عن الجرائم الإلكترونية، وما إذا كانت الإجراءات الجنائية التقليدية قادرة على احتواء خصوصيات هذا الإجرام، دون المساس بمتطلبات الشرعية الإجرائية.

ثانيًا: جهود رسم السياسة الجنائية لمكافحة الإجرام المعلوماتي:

الحق أنه قد تعددت الجهود التي أرادت تشكيل مساراً للسياسة الجنائية في مواجهة الإجرام المعلوماتي ؛ فعلى الصعيد الدولي عقدت الأمم المتحدة العديد من المؤتمرات لمواجهة الجرائم الإلكترونية منها المؤتمر السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين والذي ألمح إلى ضرورة الاهتمام بجرائم الحاسب الآلي باعتبارها

صنف من الجرائم العابرة للحدود. وفي أغسطس عام 1995 عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا وكانت الجريمة الإلكترونية والاهتمام بمكافحتها وملاحقتها أحد الموضوعات التي تم بحثها من خلال حلقة نقاشية متخصصة.

أما على مستوى المنظمات الإقليمية، فقد تجلى الاهتمام بالأمر على المستوى الأوروبي من خلال إبرام اتفاقية بودابست الموقعة في 23 نوفمبر عام 2001 المتعلقة بالإجرام المعلوماتي، إيمانا من الدول الأعضاء في المجلس والدول الموقعة عليها بالتغييرات الجذرية التي حدثت بسبب الرقمنة والعولمة المستمرة للشبكات المعلوماتية[15].

واستجابة على المستوى الوطني لضرورات مواجهة هذا النوع الحديث من الإجرام عبر ترسانة تشريعية فعالة، قامت فرنسا بإصدار قانون 6 يناير 1978 الخاص بالمعالجة الإلكترونية للبيانات الرسمية، وبينما كان مطروحا للنظر أمام مجلس الشيوخ مشروع قانون أعد لتعديل قانون حرية الاتصالات الصادر 1986 ليتفق مع التوجيهات الأوروبية الجديدة، تقدمت الحكومة الفرنسية بتعديل لهذا المشروع يتعلق بإضافة مواد جديدة للقانون المذكور بشأن الإذاعة والتليفزيون مستهدفة الحكومة من هذا التعديل تعريف القائم على تقديم خدمة الإنترنت، وشروط التقدم لممارسة هذه الخدمة التي منها ضرورة الحصول على موافقة مسبقة كغيره ممن يقومون بتوفير خدمات الاتصالات السمعية والبصرية من المجلس الأعلى للإذاعة والتليفزيون.

وقد اعتبر جانب من الفقه أن المشروع عندما قام بتعريف الاتصالات السمعية والبصرية قد وسع في التعريف بحيث شمل خدمات الإنترنت من بين وسائل الاتصال، وعندما عرض المشروع على المجلس الدستوري قرر عدم دستورية الفقرتين 2 و3 من المادة 43 من المشروع استنادًا إلى أن نص هاتين الفقرتين يخل ويقيد حرية الاتصال وتبادل الأفكار والآراء التي تعدّ من أسمى حقوق الإنسان الذي من حقه أن يتكلم ويكتب ويطبع بحرية طالما لم يسئ استخدام هذه الحرية التي حددها القانون، وكانت مآخذ المجلس الدستوري على المشروع أنه لم يضع ضوابط يتم بمقتضاها إصدار الموجهات العامة والقرارات التي تصدر بناء عليها وخصوصا أنه قد يترتب عليها قيام المسؤولية الجنائية[16].

---

[15] في مجلس أوروبا وضعها الجريمة الإلكترونية، بودابست بشأن محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، 2006، ص120. واتفاقية المتحدة والولايات أفريقيا واليابان، وجنوب من كندا، كل أوروبا، مجلس في الأعضاء الدول مراقب بالإضافة إلى بصفة الاتفاقية بشأن المفاوضات في ستراسبورج وشارك دول من وعدد والصين روسيا الموقعة غير دولة، وأبرز الدول وثلاثون ست الآن حتى عليها صادقت فيما دولة، وأربعون حتى الآن سبعة المعاهدة على الأمريكية. ووقعت المرتكبة وكراهية الأجانب العنصرية الطبيعة ذات الأعمال يتعلق بتجريم إضافي على بروتوكول تشتمل فصول. كما أربعة في مادة 48 من وتتكون الاتفاقية اللاتينية، أمريكا عبر الإنترنت.

[16] مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، بحث مقدم إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد بين 23-2012/9/25، ص7.

ورغبة من المشرع الفرنسي في تنظيم استعمال الإنترنت، صدر القانون رقم 19 لسنة 1988 المتعلق ببعض جرائم المعلوماتية، والذي عدل في سنة 1992[17]، ثم صدر القانون رقم 230 لسنة 2000 في شأن الإثبات والمتعلق بالتوقيع الإلكتروني[18].

وفي الولايات المتحدة الأمريكية صدر في 8 فبراير 1996 قانون بشأن الاتصالات يستهدف تقييد حرية القصر في الاطلاع على الصور والمواد المخلة بالآداب أو التي يكون الأولاد القصر طرفا فيها ويمكن الاطلاع عليها من خلال التعامل مع الإنترنت، ورغم أن هذا القانون لم يقم إلا بمد نطاق العقوبات الجنائية السارية بشأن الأعمال الفاضحة التي تتمٍ باستخدام اتصال هاتفي ليشمل أي اتصال يتم بأية وسيلة من وسائل الاتصالات، وجعل من سوء النية ركنا في تلك الجرائم واستحقاق العقاب عنها حينما قرر المشرع عدم مسؤولية المستعمل أو من يقوم بتوفير خدمات الإنترنت إذا وقع منه بحسن نية، إلا أن بعض الجماعات المدافعة عن الحقوق المدنية اعتبرت أحكام هذا القانون تخالف التعديل الأول للدستور الأمريكي الذي يكفل حرية التعبير عن الرأي وطالبت هذه الجماعات من القضاء وقف العمل بهذا القانون لحين الفصل في عدم دستوريته.

وفي 12 يونيو 1996، وبناء على دعوى أخرى بوقف العمل بذلك القانون، صدر حكم من محكمة فيلادلفيا الاتحادية ليؤكد أن جماعات الحقوق المدنية أثبتت أن النصوص الخاصة بقانون آداب الاتصال تخالف التعديل الأول للدستور الأمريكي؛ وبتاريخ 26 يونيو 1997 أصدرت المحكمة العليا الأمريكية حكمها القاضي بعدم دستورية بعض نصوص قانون آداب الاتصالات، وعولت هذه المحكمة في حيثيات حكمها على أنه لا يجوز ترتيب المسؤولية الجنائية على توجيهات أو قرارات عامة لم توضح الأسباب التي تقوم عليها، أو عبارات نصوص عامة غير محددة الألفاظ من شأنها أن تقيد حرية التعبير عن الرأي التي يكفلها الدستور[19].

وهكذا، وعلى الرغم من أخفاق المشرعين الفرنسي والأمريكي في وضع ضوابط وتنظيم استعمال الإنترنت، إلا أن النصوص القائمة كانت في أغلبها صالحة كثيرًا للانطباق على الجرائم التي تقع عبر الإنترنت، كتلك النصوص الخاصة بحماية حرية الحياة الخاصة، والنصوص المتعلقة بتجريم القذف والسب، والنصوص التي تحمي الصغار من الاستغلال الجنسي[20].

---

[17] وعلى مستوى مكافحة الجرائم من الناحية الشرطية تم إنشاء إدارة خاصة كما في فرنسا وكندا، وتخصص عدد من رجال المباحث الجنائية في جرائم الحاسب الآلي، وكذلك أنشئت أجهزة مركزية لمتابعة هذا النوع من الجرائم. وقد تم في فرنسا إعداد مركز لمكافحة الجرائم المرتبطة بالمعلومات والاتصالات في وزارة الداخلية، ويدخل ضمن اختصاص ذلك النوع المتخصص من مأموري الضبط القضائي أن يقوم بالتفتيش وضبط المستندات الإلكترونية المزورة والمقلدة.

[18] وعرفت دول أخرى هذا النوع من القوانين مثل ألمانيا منذ عام 1986، والنمسا والنرويج واليابان منذ عام 1987، واليونان منذ 1988، والدانمرك ولكسمبورج وايطاليا منذ 1993، وسويسرا منذ 1994، وإسبانيا وكندا وفنلندا منذ عام 1995.

[19] مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، 2000، ص17 وما بعدها.

[20] مفتاح بوبكر المطردي، المرجع السابق، ص8.

وفي المملكة المتحدة جرت تحقيقات أولية على يد لجنة القانون الاسكتلندي ضمنتها مذكرة استشارية مسببة نشرت عام 1982، وفى عام 1988 تم ذات الأمر من خلال ورقة عمل قامت بوضعها لجنة القانون التي وضعت تقريرها النهائي في عام 1989، وقد أسفر كل ذلك عن قانون أطلق عليه إساءة استخدام الحاسب الآلي، الذي تمت الموافقة عليه في يونيو من عام 1990، ودخل حيز النفاذ في أغسطس من ذات العام.

ويبدو أن هذه الجهود والمبادرات لموجهة الجرائم الإلكترونية كانت متأخرة بمنظور الزمن، وذلك على خلفية أن أول جريمة إليكترونية وقعت في الولايات المتحدة الأمريكية كانت عام 1956، وأن أول جريمة وقعت في البلاد الإسكندنافية كانت في فنلندا عام 1968 متعلقة بتقليد برامج الحاسب الآلي، في حين أن المبادرة الأولى بإصدار تشريع يتعلق بمعلومات الحاسب الآلي كانت من السويد التي أصدرت قانونا بشأن حماية المعلومات الشخصية الخاصة المخزنة في الحاسب الآلي والانترنت عام 1973، وعدلت تشريعاتها في سنة 1982، وتلتها الولايات المتحدة الأمريكية التي أصدرت في عام 1976 قانونا خاصا بحماية الحاسب الآلي، وفي عام 1984 تبنى الكونجرس قانونا متعلقا بالتحليل المعلوماتي، عدل بالقانون رقم 1213–1986 لمواجهة جرائم الحاسب الآلي، ومنذ عام 1993 وقد أصبح لدى جميع الولايات الأمريكية تشريعات خاصة بجرائم الحاسب الآلي، وأخيرا صدر في 14 فبراير 2002 قانون للمعاملات التجارية الرقمية.

أما على مستوى الدول العربية، فقد بدأ الإدراك بأهمية الموضوع يتزايد في بعض التشريعات العربية مثل التشريع التونسي الذي كان له فضل السبق بين الدول العربية في سن قانون خاص بالتجارة الإلكترونية، وهو القانون رقم 83 لسنة 2000 الصادر في أغسطس سنة 2000 في شأن المبادلات والتجارة الإلكترونية، وفي المملكة الأردنية الهاشمية صدر القانون رقم 85 لسنة 2001 بشأن قانون المعاملات الإلكترونية، وكان قانونًا مؤقتًا، إلا أنه أصبح نهائيًا بقانون جرائم أنظمة المعلومات. ذات الأمر نلاحظه في الجزائر من خلال المرسوم التنفيذي رقم 256 لسنة 1998 بشأن البريد والمواصلات، والمرسوم التنفيذي رقم 307 لسنة 2000 بشأن وضع ضوابط وشروط وكيفية إقامة خدمات الإنترنت واستغلالها، وفي دبي صدر القانون رقم 2 لسنة 2002 بخصوص المعاملات والتجارة الإلكترونية، وفي البحرين صدر المرسوم بقانون رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية، المعدل بالقانون رقم 13 لسنة 2006، وفي مصر اعتمد القانون رقم 15 لسنة 2004 بشأن المعاملات الإلكترونية، ثم القانون 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

وفي دولة الإمارات العربية المتحدة جاء القانون رقم 2 لسنة 2006 متعلقًا بمكافحة جرائم تقنية المعلومات، وفي اليمن صدر القانون رقم 40 لسنة 2006 في خصوص أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وفي المغرب ظهير شريف رقم 129–07–1 صادر في 19 من ذي القعدة 1428 (30 نوفمبر 2007 ف) بتنفيذ القانون رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، وفي سلطنة عمان صدر المرسوم السلطاني رقم 69 لسنة 2008 بإصدار قانون المعاملات الإلكترونية، وفي قطر سن المرسوم بقانون رقم 16 لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية.

ثالثًا: منهج البحث:

لقد انتهجنا من أجل بحث الإشكالية التي سطرنا لها هذه الأوراق منهجًا وصفيًا تحليليًا، أما كونه وصفي فذلك لأنه سيبرز المفاهيم الكلية ذات الصلة بالإجراءات المتبعة في الاستدلال والتحقيق في جرائم تقنية المعلومات، لاستخلاص الدليل والعقبات التي تعتري اتخاذ هذه الإجراءات. أما كونه منهجًا تحليليًا فذلك لأنه يطرح بأسلوب تفصيلي جزئيات الإشكالات القانونية التي تثيرها المواجهة الإجرائية للجريمة الإلكترونية، وتقييم الحلول التي طرحها الفقه والتشريع والقضاء المقارن في مجال المكافحة الإجرائية لجرائم تقنية المعلومات.

رابعًا: خطة البحث:

من أجل طرح رؤية وصفية تحليلية لإشكالية البحث، سوف نقسم خطة هذا الأخير إلى مبحثين رئيسيين: أولهما يهدف إلى بيان قصور قواعد التفتيش التقليدية في مجال جرائم تقنية المعلومات، وتحليل صعوبات تنفيذ التفتيش الإلكتروني **(المبحث الأول)**. أما الضلع الثاني من هذا البحث فقد خصصناه لمعالجة إشكالية طبيعة وحجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني، إذ من الضروري البحث عن قيمة ومشروعية هذا الدليل الفني في الإثبات أمام القضاء الجنائي بالنظر إلى سهولة تعرضه للتلاعب والتحريف، فضلاً عن ضرورة البحث في مدى خضوع هذا الدليل ذو الطابع العلمي لمبدأ الاقتناع الذاتي للقاضي الجنائي، وما يخوله من سلطة تقديرية لهذا الأخير **(المبحث الثاني)**.

المبحث الأول
جرائم تقنية المعلومات: إشكالية قصور قواعد التفتيش التقليدية

تمهيد وتقسيم:

مما أضحى مسلمًا به أن الدراسات القانونية لا يمكنها أن تسهم في تيسير الاستفادة من التقدم التكنولوجي إلا حالما تتوافق وتتجاوب النصوص القانونية مع الواقع الذي تطبق فيه، الأمر الذي يوجب تطويرها بذات السرعة التي يتطور بها المحل الخاضع لحكم هذه النصوص.

ولما كانت ثورة الاتصالات قد كشفت عن جملة من الجرائم ذات الطبيعة الخاصة من حيث وسائل ارتكابها أو المحل الذي تقع عليه، وطبيعة جناتها الذين يجمعون بين ذكاءين، أحدهما بشري وآخر اصطناعي، فإن صعوبة مواجهتها جنائيًا لم يعد محلاً للشك، بحيث انكشف أمام الفقه الجنائي عجز قانون الإجراءات الجنائية عن استيعاب الجرائم المستحدثة التي ترتكب بوسائل تقنية المعلومات، التي عادة لا تتقيد بحيز مكاني محدود، ولا تنصب على محل مادي

ملموس، ولا تترك آثارًا يمكن معاينتها بالوسائل التقليدية، حتى ظل هذا الباب يعاني من حالة فراغ تشريعي لفترات طوال[21].

وإزاء هذا القصور في النصوص الإجرائية ومنعًا من إفلات الجناة لجأ الفقه والقضاء إلى الاجتهاد في تفسير تلك النصوص الإجرائية التقليدية – لاسيما القواعد الحاكمة للتفتيش – لمواجهة جرائم تقنية المعلومات. غير أن هذه المحاولات قد اكتنفتها صعوبات جمة بالنظر إلى الطبيعة التقنية والعلمية لهذه الجرائم، وهو الأمر الي أوجب تدخل المشرع لتكريس قواعد إجرائية خاصة تمكن أجهزة التحقيق من استخلاص الدليل الفني المناسب من ذات البيئة الرقمية بحسبانها مسرحًا للجريمة المعلوماتية، وإزالة العقبات التي تقف حائلاً دون تنفيذ التفتيش الإلكتروني[22].

وعليه فسوف نقسم هذا المبحث إلى مطلبين: نعالج في أولهما مدى مقبولية إجراءات التحقيق التقليدية في مجال جرائم تقنية المعلومات، وفي ثانيهما نتناول صعوبات تنفيذ التفتيش الإلكتروني.

المطلب الأول
التفتيش التقليدي: مدى المقبولية في مجال جرائم تقنية المعلومات

تقسيم:

أصبح الحديث عن الإجراءات الجنائية في مجال تقنية المعلومات ضرورة ملحة مع القصور المتكشف للإجراءات الكلاسيكية التي وضعت لتناسب عالم الماديات المحسوس على خلاف المسرح الإلكتروني الافتراضي، فهناك محدودية لسريان الإجراءات التقليدية للتفتيش بشأن الكيانات المنطقية للحاسب (فرع أول)، ومع الإقرار بذلك فإن تساؤلاً يثار بشأن تفتيش شبكات المعلومات (فرع ثان).

الفرع الأول
تفتيش الكيانات المنطقية للحاسب

مما هو شائع من حيث في الواقع أن يرتهن التحقيق بضرورة تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء التي تفيد في كشف الحقيقة بشأن جريمة قد وقعت بالفعل. وهو أجراء تقوم به سلطة التحقيق في الأصل (قاضي التحقيق أو النيابة العامة باختلاف الدول في ذلك)[23]، أو مأمور الضبط القضائي في أحوال استثنائية تقتصر في جل التشريعات على الندب وأحوال التلبس.

---

[21] راجع حول القصور على المستوى الموضوعي، د. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والإنترنت، الإمارات، مايو 2000، ص5 وما بعدها.

[22] محمد قدري حسن عبد الرحمن، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، ع79، مركز بحوث الشرطة، الشارقة، أكتوبر 2011، ص 159.

[23] د. محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، ج2، التفتيش والضبط، 1978، د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1998، ص538 وما بعدها، د. عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2019-2020، ص636 وما بعدها، د. سامي الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، عين شمس، 1972.

والتفتيش إجراء من اجراءات التحقيق تباشره سلطة مختصة بهدف البحث في مستودع سر فرد معين عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونًا[24].

وعلى أساس هذا التعريف فإنه التفتيش في أصله وضع ليصبح طريق وأداة للإثبات المادي، بغية ضبط الأدلة ذات الطابع المادي، مما يجعله يجافي مع الطبيعة غير الملموسة للبرمجيات وبيانات الحاسب الآلي، ومواقع شبكة الإنترنت[25].

وعلى هذه تظهر صعوبة محل التفتيش الإلكتروني، فمحل التفتيش تقليديًا هو كل مستودع يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته، وتكون بالتالي تبعًا لذلك له حرمة، كالمسكن أو سيارة أو الرسائل. أما المستودع في الجرائم الإلكترونية فهو حاسب آلي يتضمن وحدات، منها وحدات المعالجة المركزية *Hardware* ووحدات وحدات التخزين أو ما يسمى بوحدة التحكم، فضلاً عن البرامج التطبيقية، والبيانات *Software* ومكونات أخرى للمعالجة الآلية، متصل كل ذلك بشبكات اتصالات سلكية ولاسلكية محلية ودولية *Networks Telecommunication*[26].

ولا مشكلة تثار بشأن تفتيش المكونات المادية للحاسب – كالشاشة والطباعة والكيبورد...الخ – باعتبار ذلك تسري عليه الإجراءات الجنائية التقليدية، وسلامة الإجراءات عادة تتوقف هنا على المكان الذي توجد فيه هذه المكونات المادية، عامًا كان أم خاصًا، وتسري عليها ذات الشروط والضمانات المتعلقة بالتفتيش وفق قواعده العامة[27].

ويبدأ الأمر في التعقيد بشأن تفتيش الكيانات المنطقية للحاسب، والتي تعرف بأنها: "مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات"[28]، والتي يثار بشأنها التساؤل حول صلاحيتها لأن تكون

---

[24] راجع في تعريف التفتيش، د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1998، ص539، د. عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2019-2020، ص636. وراجع بشأن التفتيش في الجرائم الإلكترونية، علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ط1، البحرين، بدون دار نشر، 2010، ص20.

[25] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006، ص192، د. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010، ص76 وما بعدها.

[26] على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، 26 إلى 28 أبريل 2003، ص135، رشيدة بوكر، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، 2012، ص395، باسل أحمد عبد المحسن محمد لطفي، دور القاضي المستعجل في وقف الاعتداءات الجنائية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، 2010، ص130.

[27] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009، ص195، فايز محمد أرجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، رسالة دكتوراه، جامعة الجزائر 1، 2011، ص309، عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد 22، ع86، مركز بحوث الشرطة، الشارقة، 2013، ص260.

محلاً للتفتيش، لضبط دليل من خلالها. فهناك شكوك حول إمكانية اعتبار البحث عن أدلة الجريمة الإلكترونية في نظم وبرامج الحاسب نوعًا من التفتيش، باعتبار أن البيانات الإلكترونية أو البرامج في حدّ ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، وهو ما يخرج عن غرض التفتيش وهو البحث وضبط دليل مادي، الذي لا يعدو إلا أن يكون الدليل الذي ينبعث من عناصر مادية ناطقة بنفسها ويؤثر في اقتناع القاضي بطريقة مباشرة[29].

وقد حاول الفقه المقارن إزالة عدم التوافق بين مفاهيم التفتيش التقليدية وبين جرائم تقنية المعلومات بالقول بأنه وإن كانت هذه النظم والبرامج الحاسوبية عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط ودعامات مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا إخضاعها لقواعد التفتيش التقليدية؛ فالفقه الكندي قد وسع من تفسيره لمعنى التفتيش المنصوص عليه في المادة 487 من قانون العقوبات ليشمل تفتيش المكونات المنطقية للحاسب، والأمر نفسه فيما يخص قانون إساءة استخدام الحاسوب الإنجليزي لعام 1990 الذي نص على إمكانية تفتيش المكونات المادية والمعنوية للكمبيوتر[30].

وقد أخذ القضاء اليوناني بهذا التوجه الفقهي، وفسر عبارة " أي شيء" الواردة في المادة 251 من قانون الإجراءات الجنائية – التي تنص على أنه: "يجوز لسلطات التحقيق القيام بأي شيء يكون ضروريًا لجمع الدليل" – بأنها تشمل البحث وضبط البيانات والمعطيات المعالجة إلكترونيًا والمخزنة داخل الأوعية الإلكترونية الرقمية أو حاملات البيانات المادية أو في الذاكرة الداخلية للحاسب[31].

بينما نحى جانب آخر من الفقه إلى القول بعد إمكانية هذا التوافق مع قواعد التفتيش التقليدية لكونها هذه الأخيرة إنما في وقت لم يعرف الدليل المادي بأنه الدليل الذي ينبعث من عناصر مادية ناطقة بنفسها ويؤثر في اقتناع القاضي بطريقة مباشرة[32]، كما لم تكن نظم المعالجة الآلية والكمبيوتر قد عرفت بعد، الأمر الذي يستدعي سن قواعد خاصة، أو التعديل فيما هو قائم من قواعد تقليدية[33].

---

[28] عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط2، منشورات الحلبي القانونية، 2007، ص61.

[29] أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه، عين شمس، 1982، ص374.

[30] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، 1994، ص66 وما بعدها، هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دارسة مقارنة، دار النهضة العربية، 2006، ص201، علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، 26 إلى 28 أبريل 2003، ص81.

[31] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص96، أحمد بن أزيد جوهر الحسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، جامعة القاهرة، 2009، ص145، نبيلة هبة هروال، المرجع السابق، ص225، خالد ممدوح إبراهيم، المرجع السابق، ص 197.

[32] أحمد ضياء الدين محمد خليل، المرجع السابق، ص374.

[33] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص380، موسى مسعود أرحومة، الإشكاليات، المرجع السابق، ص8.

وبالتالي فإنه لا يمكن إخضاع المكونات المعنوية للحاسوب من برامج وبيانات لعملية التفتيش والضبط التقليدية[34]، وهو ما تأثر به المشرع الألماني، إذ نص في المادة 94 من قانون الإجراءات الجنائية صراحة على أن التفتيش والضبط يرد فقط على الأشياء المادية المحسوسة المتعلقة بالجريمة دون غيرها. ومن هنا، ارتأى الفقه الألماني أن البيانات والمعلومات الإلكترونية لا يمكن ضبطها إلا بعد تفريغها في كيان مادي محسوس مثل طبع هذه البيانات على الورق، أو تخزينها في دعامة مادية مثل الأقراص المغناطيسية، أو تصويرها على الشاشة أو نقلها على حافظة بيانات، فالمهم هو نقل هذه البيانات إلى وسط مادي محسوس لكي يتم إخضاعها للتفتيش. وهو ذات التوجه الذي اعتمده الفقه في معظم دول أمريكا الجنوبية والياباني والروماني حين اعتبر البيانات والبرامج والسجلات المغناطيسية مجرد مكونات غير مرئية في حد ذاتها، كونها نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية غير محسوسة ماديًا لا يرد عليها تفتيش أو ضبط، إلا بعد تحويلها إلى كيان مادي[35].

ويبدو أن التشريعات المعاصرة قد فضلت حل الخصوصية التشريعية، بدءًا من المشرع الأمريكي حين أتى بنصوص جديدة تخص تفتيش الحاسب الآلي في القسم رقم 2000 من القانون الإجرائي الاتحادي الخاص بجرائم الحاسب[36]، لتنص على السماح بتفتيش أجهزة الحاسب الآلي والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي[37]. وجاء من بعده المشرع الإنجليزي بنصه في قانون إساءة استخدام الحاسب الآلي لعام 1990 على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي، وتبعه المشرع الفرنسي الذي قام بتعديل نصوص التفتيش التقليدية لتواكب التكنولوجيات الحديثة، إذ أضاف بموجب المادة 42 من القانون رقم 545-2004 المتعلق بالثقة في الاقتصاد الرقمي عبارة "المعطيات المعلوماتية" مشيراً إلى المادة 94 من قانون الإجراءات الجنائية، لتصبح هذه المادة على النحو التالي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيداً لإظهار الحقيقة"[38].

وفي إطار التشريعات العربية، نجد أن قانون التجارة البحريني نص في المادة (23) منه على أنه" في حالة وجود دلائل كافية على استغلال أي محل في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، فإنه يجوز إجراء تفتيش لهذا المحل وللمشتبه فيهم من الموجودين فيه، وضبط الأشياء الموجودة فيه والتي يشتبه في صلتها بالجريمة، وكل ما يفيد في كشف الحقيقة طبقاً للإجراءات والشروط المنصوص عليها في قانون أصول المحاكمات الجزائية لعام 1966 وتعديلاته"، بما يدل على أن المشرع البحريني قد أحال إلى قانون الإجراءات الجزائية في هذا الصدد، فضلاً

---

[34] هلالي عبد اللاه أحمد، المرجع السابق، ص89، على محمود على حمودة، المرجع السابق، ص14.

[35] *A. Georgo, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Roumanie, RIDP., 1993, p.551.*

رشاد خالد عمر، المشاكل القانونية الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، 2013، ص146.

[36] نبيلة هبة هروال، المرجع السابق، ص226.

[37] عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، 2005، ص373.

[38] *F. Fourment, Procédure pénale, la perquisition du disque d'un ordinateur à chaud, CPU., Paris, 2004, p.5.*

عن أنه يجوز الاستعانة أثناء التفتيش والضبط بموظفي وزارة التجارة والصناعة المختصين ، للاستفادة بخبرتهم الفنية في هذا الشأن.

أما في سلطنة عمان فقد نصت المادة (26) من المرسوم السلطاني رقم (69 /2008) بإصدار قانون المعاملات الإلكترونية على أنه "للسلطة المختصة اتخاذ الإجراءات التي تراها مناسبة للمراقبة والإشراف على مدى التزام مقدمي خدمات التصديق بأحكام هذا القانون، ولهذه السلطة أن تصل إلى أي نظام حاسب آلي أو أي جهاز أو بيانات أو أية مواد أخرى متصلة بذلك النظام، بغرض إجراء التفتيش والمراقبة، ولها أن تصدر أمراً لأي شخص مختص بأن يوفر لها المساعدة الفنية المعقولة وغيرها من المساعدات حسبما تراه ضرورياً".

وفي شأن القانون المصري، ففي خطوة أولى نصت المادة (64) من القانون رقم 10 لسنة 2003، بإصدار قانون تنظيم الاتصالات على أنه: "يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسرى ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أو يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلاؤهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة ".

وحسنًا فعل المشرع المصري عند إصداره القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات – وكخطوة حاسمة – أن خصص المادة السادسة منه لسن أحكام خاصة تسمح بتفتيش الكيانات المنطقية للحاسب والتي أدرجت تحت عنوان الأوامر القضائية المؤقتة، وجاء نصها على النحو التالي: "لجهة التحقيق المختصة – بحسب الأحوال– أن تصدر أمراً مسبباً، لمأموري الضبط القضائي المختصين، لمدة لا تزيد على 30 يوماً قابلة للتجديد لمرة واحدة، متي كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضي أحكام هذا القانون بواحد أو أكثر مما يلي: 1– ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو انظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لها مقتضي. 2– البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط".

والحقيقة أنه تفضل صياغة المادة السادسة في القانون المصري وضماناتها غيرها من التشريعات العربية ؛ فمثلا نصت المادة 14 من القانون القطري رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية على أن للنيابة

العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة. ويجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة. فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

ولا ننسى أن نشير إلى الاتفاقية الأوروبية حول الإجرام المعلوماتي والتي نصت صراحة على حق الدول الأعضاء في تفتيش النظم المعلوماتية وحثتها على تجسيد هذا الحق بكل وضوح في قوانينها الإجرائية لتفادي أي إشكال يمكن أن يثار حول الموضوع، وذلك من خلال المادة 1/19 التي نصت على أن لكل طرف الحق في سن القوانين مما هو ضروري لتمكين السلطات المختصة من تفتيش أو الدخول إلى نظام الحاسب أو جزء منه أو المعلومات المخزنة فيه، والوسائط التي يتم تخزين معلومات الحاسب بها ما دامت مخزنة في إقليمها.

الفرع الثاني
تفتيش شبكة المعلومات (التفتيش عن بعد)

عادة ما يكون الحاسب الآلي متصلاً بشبكة معلومات محلية أو دولية، والتي تعني اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالاً سلكيًا أو لاسلكيًا أو بواسطة الأقمار الصناعية، وقد تكون هذه الأجهزة مرتبطة بعضها البعض في موقع واحد فيطلق عليها الشبكة المحلية، أو موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف أو المجال المغناطيسي فتسمى الشبكة الممتدة أو شبكة الإنترنت[39].

وهنا يثار التساؤل حول مكنة تفتيش شبكة المعلومات تلك، وهو أمر من المؤكد تحوطه صعوبات تقنية جمة بالنظر لطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تمامًا عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى، فهل يمكن الحديث عن امتداد الاختصاص بالتفتيش في تلك الأحول ليشمل صلاحية المأذون له بالتفتيش إلى المعلومات التي توجد خارج اختصاصه الجنائي أو في نظام معلوماتي آخر خلاف المأذون الدخول إليه أو تفتيشه، وهو ما يمكن تسميه بالتفتيش عن بعد؟

إن الأمر المطروح ليس سهلاً الإجابة عليه ؛ فالأمر لا يتعلق فقط بتجاوز الاختصاص المكاني، بل قد ينال من حق الغير في الخصوصية. ويلزم التفرقة بين عدة فروض[40]:

[39] عرفت المادة الأولى من القانون 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات الشبكة المعلوماتية بأنها: " مجموعة من الأجهزة أو نظم المعلومات مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية؛ والتطبيقات المستخدمة عليها".

[40] راجع لمزيد من التفصيل، محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، 2017، ص211 وما بعدها.

أما في حال كان الأمر يتعلق بنطاق دولة واحدة، فالحقيقة أن التشريعات أضحت حاسمة بالسماح بامتداد الاختصاص، فها هو التشريع الألماني قد نص في القسم 103 من قانون الإجراءات الجنائية على مكنه امتداد التفتيش إلى السجلات والبيانات الموجودة في مكان آخر غير المكان الجاري التفتيش فيه دون الحاجة إلى إذن يخص هذا التمديد كلما دعت ضرورة التحقيق إلى ذلك، وهو ما اتبعه المشرع البلجيكي الذي نص في المادة 88 من قانون تحقيق الجنايات على أنه إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء فإن هذا البحث يمكن أن يمتد إلى نظام آخر يوجد في مكان آخر غير مكان البحث الأصلي، بشرط أن يكون ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث، وتكون هناك مخاطر تتعلق بضياع الأدلة بالنظر لسهولة محو أو إتلاف أو نقل البيانات محل البحث[41].

ذات الأمر نلاحظه بالنسبة لقانون جرائم المعلوماتية الأسترالي لعام 2001، الذي رخص بعمليات التفتيش على وجه السرعة للبيانات خارج المواقع التي تم اختراقها عن بعد بواسطة الحواسيب الجاري تفتيشها، وذلك دون اشتراط الحصول على موافقة مسبقة من السلطات المختصة الأخرى[42].

أما بشأن المشرع الفرنسي فلم يتوان عن اتباع ذات الأمر وهو في معرض تعديله لقانون الإجراءات الجنائية بموجب القانون رقم (239-2003 المتعلق بالأمن الداخلي الصادر في 18 مارس عام 2003، والذي سمح بموجب المادة 1/17 لسلطات الضبط القضائي الدخول من الجهاز الرئيسي إلى المعلومات التي تهم البحث والتحري المخزنة في أنظمة معلوماتية أخرى وضبطها بناء على أمر بالتفتيش واحد كلما كان ذلك ممكنا[43]. كما سمحت الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية الموقعة في بودابست في 23 نوفمبر عام 2001 بموجب المادة 2/19 منها الدول الأعضاء بمد نطاق التفتيش الذي كان محله جهاز حاسب معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال، إذا كان يوجد بها معلومات أو بيانات مهمة للتحقيق يمكن الدخول إليها من خلال الجهاز محل التفتيش دون أن يشكل ذلك تجاوزًا للاختصاص الإقليمي.

ورغم أن المشرع المصري لم يكن بذات الحسم في إجابته على التساؤل المطروح آنفًا، إلا أن المادة السادسة قد أوردت بين طياتها عبارة قد يستشف منها السماح بامتداد الاختصاص طالما وقع الأمر داخل جمهورية مصر العربية. فالمادة السادسة قد سمحت لجهة التحقيق المختصة – بحسب الأحوال– أن تصدر أمراً مسبباً، لمأموري

---

[41] *C. Meunier, La loi du 28 novembre 2000 relative à la criminalité informatique, Formation Permanente, CUP., février 2001, n°103.*

د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2001، ص 113

[42] نورة طرشي، مكافحة الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر 1، 2011، ص 110.

[43] *l'art 17/1: «Les officiers de polices judicaire ou, sous leur responsabilité, les agent de police judicaire peuvent, et au cours d'une perquisition effectuée dans les condition prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition a des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès que ces données sont accessibles à partir du système initial ou disponible pour le système initial». Cf. M. Quener et J. Ferry, Cybercriminalité, défi mondial, 2ème éd. Economica, Paris, 2009, p.2.*

الضبط القضائي المختصين، لمدة لا تزيد على 30 يوماً قابلة للتجديد لمرة واحدة، متي كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضي أحكام هذا القانون بواحد أو أكثر مما يلي:

1- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو انظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه ...

2- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.

وعبارة "**تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه**"، دال على تبني المشرع وسماحه بامتداد الاختصاص بشأن جرائم تقنية المعلومات الواقعة داخل مصر، دون أن يكون الاختصاص المحلي عائقًا دون الملاحقة.

كما ننوه إلى أنه من المتفق عليه فقهًا وقضاءً في القانون المصري أن للمحقق أن يمد اختصاصه بالتفتيش وفقاً لنظرية الضرورة الإجرائية خارج دائرة اختصاصه إذا ظهر من ظروف التحقيق ما يستوجب امتداد هذا الاختصاص إلى خارج تلك الدائرة[44].

وتحوطًا فإن لسلطة التحقيق أن تأمر مقدم الخدمة بتسليم ما لدية من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني، وفي كل الاحوال يحب أن يكون أمر جهة التحقيق المختصة مسببًا (البند 3 من المادة السادسة).

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة في المواعيد، ووفقًا للإجراءات الجنائية.

ولم تتأخر بعض التشريعات عن النص صراحة على ذلك في مجال جرائم تقنية المعلومات، فها هو المشرع الجزائري ينص المشرع الجزائري عن التشريعات المذكورة أعلاه، إذ نص في المادة 2/5 من القانون رقم 4-9 لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخ زنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

[44] نقض 8 مارس 1990، مجموعة أحكام النقض، س41، ص482، رقم 82. في ذات المعنى، نقض 1 يناير 1998، مجموعة أحكام النقض، س49، ص11، رقم 1.

وكان المشرع البحريني بذات الحسم حين نص في المادة 15 من القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات على أن للنيابة العامة أن تصدر أمراً مسبباً بالدخول وتفتيش نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه. وكذلك أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

وإذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند (أ) من الفقرة (1) 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.

وقد يحدث أن يتصل حاسب المتهم بحاسب آخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية، ويقوم بتخزين بيانات أو معلومات تفيد إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج إقليم الدولة التي يقيم فيها، عن طريق شبكة الإنترنت بهدف عرقلة سلطات البحث من الوصول إلى الدليل ؛ فهل يمتد الاختصاص أيضًا في تلك الحالة إلى المنظومة المعلوماتية الموجود في دولة أخرى في إطار ما يسمى بالتفتيش العابر للحدود؟[45]

إن الأمر في الحقيقة بحاجة إلى أن تعقد الدولة اتفاقيات ثنائية أو تنضم إلى اتفاقيات جماعية تسمح بذلك، إذ ليس من المنطقي أن تسمح دولة لنفسها بهذا الامتداد في إقليم دولة أخرى عدوانا على سيادة تلك الأخير, كما يمكن للدول تخفيفًا من هذه الصعوبات أن تلجأ لأسلوب الإنابة القضائية، بأن تنيب الدولة سلطات دولة أخرى في اتخاذ الإجراء الذي ترغب فيه تجاه المتهم، متى كان يقع في اختصاص تلك الأخرى[46].

وفى هذا الشأن قضت إحدى المحاكم الألمانية في جريمة غش ارتكبت في ألمانيا، بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية، وفى واقعة نشر فيروس *Love bug* عام 2000 الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي، فعندما اكتشف الخبراء الأمريكيون بان هذا الفيروس أرسل من الفليبين فإن تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفليبينية والحصول على إذن من قاضي التحقيق بالفليبين[47].

---

[45] راجع لمزيد من التفصيل، حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، جامعة عين شمس، 2005، ص376.

[46] *Y. Padova, Un aperçu de la lutte contre la cybercriminalité en France, RSC., n°4, octobre-décembre, 2002, p.765.*

[47] مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، بحث مقدم إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد بين 23-25/ 9/2012، ص44.

ولذلك حرصت المادة الرابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على صون السيادة بقولها في البند الثاني منها: "2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي".

بيد أن بعض الدول وبقصد التحسب لنقل المعلومات المتعلقة بوقائع إجرامية إلى خارج البلاد وتهريبها للخارج بقصد تخزينها وإخفائها وما يستدعيه ذلك من الاستعجال في تعقبها وملاحقتا لاستعمالها كدليل إثبات، وسعت بعض التشريعات المقارنة من صلاحيات سلطات التحقيق للقيام بتفتيش الأنظمة المتصلة حتى لو كانت متواجدة في خارج إقليمها الوطني، وقيدت ذلك بتوافر حالة الضرورة. ويمكن أن نمثل لذلك بالمادة 125 من قانون جرائم الحاسب الآلي الهولندي التي نصت على أنه يجوز لجهات الاستدلال والتحقيق مباشرة التفتيش داخل الأماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في إقليم دولة أخرى، بشرط أن يكون هذا التدخل ضروريًا ومؤقتًا ومفيدا في كشف الحقيقة[48].

وقد تبنى قانون الأمن الداخلي الفرنسي ذات التوجه حين نص في الفقرة الثانية من المادة 57 من قانون الأمن الداخلي رقم 239-2003 لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المعلوماتية المتصلة المتواجدة في خارج الإقليم الوطني كلما كان ذلك ممكنا، فنصت على أنه: "إذا تبين مسبقًا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني، ويمكن الدخول إليها أو أنها متاحة انطلاقا من النظام الرئيسي، فانه يمكن الحصول عليها من طرف ضابط الشرطة القضائية على وجه السرعة كلما دعت ضرورة التحقيق لذلك، على أن يتم إبلاغ السلطات المختصة في الدولة التي تتواجد هذه المعطيات على إقليمها فيما بعد وفقاً للضوابط المنصوص عليها في المعاهدات الدولية"[49].

وقد أجاز المجلس الأوروبي من خلال توصيته رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات مد التفتيش الالكتروني للحاسب إلى الشبكة المتصلة به ولو كانت تلك الشبكة واقعة في إقليم دولة أخرى، وأكد على أنّه "يجوز لسلطة التحقيق والاستدلال بمناسبة التفتيش الإلكتروني بسط مجال تفتيش حاسب معين يدخل في دائرة اختصاصها إلى غيرها من الأجهزة الإلكترونية المرتبطة به بواسطة شبكة الإنترنت بما فيها المتواجدة خارج الاختصاص الوطني وضبط المعطيات المتواجدة فيها، كلما كان التدخل الفوري للقيام بذلك ضروريًا"[50].

---

[48] *P. Verguchet, La répression des délits informatiques dans un perspective internationale, op. cit., p.374.*

[49] *C. Meier Marsella, L'effectivité du processus répressif dans le traitement de la cybercriminalité, enquête sur le système juridique français, th. Paris II, 2005, p.259 et s.*

[50] *M. Quemener, Conseil de l'Europe et lutte contre la cybercriminalité, Revue Expertises des systèmes d'information, n°347, mai 2010, p.170 ; A. Diop, Procédures pénales et TIC., p.25, sur le site : http ;//196.1.99.9/moodle/mod/book/print.php?id=106 ; J. Bourguignon, La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat, article présenté au Colloque de Rouen sur «Internet et droit international, organisé par La Société Française pour le Droit International du 30 mai au 1 juin 2013, Pedone, Paris, 2014, p.368.*

وإدراكًا منها لأهمية التفتيش العابر للحدود في مواجهة الجرائم الإلكترونية وما يتطلبه من سرعة التدخل لضبط الأدلة الرقمية السهلة التلف والضياع، اقترحت لجنة الدول الأطراف في الاتفاقية الأوروبية للجرائم الإلكترونية خلال المناقشات التي أجرتها في عام 2009 فضلاً عن حالة إذا كانت المعلومات متاحة للجمهور أي كان المكان الجغرافي لتلك البيانات، أو حالة تلقي سلطات التحقيق في دولة طرف على إقليمها عبر نظام إلكتروني المعلومات من قبل شخص مرخص له بتداولها بالوسائل الإلكترونية موجود في دولة طرف أخرى (المادة 32 من الاتفاقية)[51] حالات أخرى ترى من المفيد السماح فيها بالتفتيش عن بعد في أجهزة أو شبكات تابعة لدول أخرى دون الحصول على إذن منها، وهذه الحالات هي كالتالي:

- حالة التفتيش عن بعد بحسن النية: وتتوافر هذه الحالة عندما تقوم سلطات التحقيق بالولوج في أجهزة أو شبكات تابعة لدولة أجنبية دون قصد، كأن يجد المحقق نفسه يبحث في برنامج حاسب متواجد في دولة أجنبية صدفة أو خطئاً، أو عندما يصعب عليه التحديد يقينًا موقع البيانات المبحوث عنها.
- حالات الاستعجال القصوى أو الحالات الاستثنائية: والملاحظ هنا أن اللجنة لم تحصر حالات الاستعجال والاستثنائية التي يمكن لهيئات التحقيق اللجوء فيها الى التفتيش عن بعد دون الحصول على إذن من الدولة المعنية، إنما اكتفت بتقديم بعض الأمثلة عنها، كوجود خطر ضياع الأدلة الرقمية عن طريق الإتلاف أو التلاعب فيها بالتعديل، ووجود خطر إفلات المشتبه فيه.

وقد صمت المشرع المصري في قانون مكافحة تقنية المعلومات عن الأخذ بتلك الحلول ملتزمًا تمامًا بمبدأ احترام سيادة الدول الأخرى، الذي حرصت الاتفاقية العربية على حث الأطراف على عدم انتهاكه.

وهذا لا يمنع السلطات المصرية من اللجوء إلى المساعدة القضائية المتبادلة وفي نطاق الاتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام المعلوماتي. كما أن للسلطات المصرية أن تتبع حكم المادة 40 من الاتفاقية العربية التي رخصت لسلطات الدول الأطراف من الوصول إلى معلومات تقنية المعلومات عبر الحدود وبدون الحصول على تفويض من دولة طرف أخرى أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات، وأن تصل أو تستقبل – من خلال تقنية المعلومات في إقليمها – معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

المطلب الثاني
صعوبات تنفيذ التفتيش الإلكتروني

[51] *Art. 32: "... une partie peut, sans l'autorisation d'une autre partie ; a- accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou b- accéder a, ou recevoir au moyen d'un system informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyens de ce système informatique".*

تقسيم:

على الرغم مما بذلته الدول من أجل رسم سياسة جنائية على المستوى التشريعي موضوعيًا وإجرائيًا لمواجهة الإجرام المعلوماتي إلا أن التفتيش الإلكتروني مازال يواجه على نحو خاص عدد من العقبات كطريق من طرق جمع الأدلة الرقمية، بعضها قد يكون فنيًا **(الصعوبات الفنية للبحث عن الدليل الرقمي) (أولاً)**، وبعضها الآخر قد يكون قانونيًا **(الصعوبات القانونية للبحث عن الدليل الرقمي) (ثانيًا)**.

أولاً: الصعوبات الفنية للبحث عن الدليل الرقمي:

يواجه اكتشاف الجريمة الإلكترونية صعوبات عدة ترجع بالأساس إلى غياب الآثار المادية للجريمة، فهي الجريمة الهادئة، فضلاً عن سهولة إخفاء ومحو الدليل ؛ فارتكاب هذا الصنف من الجرائم لا يتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح لحدوث اختراق معلومات وسجلات مخزنة في الحاسب الآلي ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها دون أن تخلف أية آثار خارجية مرئية، فلا شهود غالبًا يمكن الاستعانة بأقوالهم في التحقيق، ولا بصمات يمكن تحليلها أو أدلة مادية يمكن فحصها. هذا فضلاً عن صعوبة نسبة الدليل الرقمي إلى متهم معين، بل قد تعوق عدد من المسائل الفنية فرصة الوصول للدليل[52]. وجملة تلك الصعوبات هو ما نفصل فيه على النحو التالي.

1- سهولة طمس الدليل الرقمي:

تتميز آثار الجريمة المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر بالثراء الشديد من حيث المعلومات، والتي قد تشمل صفحات المواقع المختلفة *Web Pages*، والبريد الإلكتروني *E-mail* ، والفيديو الرقمي *Video digital*، والصوت الرقمي *Audio Digital* ، وغرف الدردشة والمحادثة *Chat Sessions*، والملفات المخزنة في الكمبيوتر الشخصي، والصور المرئية *Images Digitized*.

ويسهل – نظرًا للمعرفة التقنية التي يتميز بها المجرم المعلوماتي – أن يتمكن مرتكبو الجرائم الإلكترونية نتيجة ضعف الأنظمة الرقابية من التسلل والعبث في النبضات والذبذبات الإلكترونية التي تسجل عن طريقها المعلومات والبيانات تلك بغرض إحداث تغيرات في البيانات والمعلومات والتلاعب في منظومة الحاسب الآلي ومحتوياته، أو دس برامج خاصة ضمن برنامجه فلا يشعر بها القائمون بالتشغيل، ومن ثم إخفاء ما قاموا به أو محو الدليل عليه، بحيث يتعذر إعادة عرض أعمال التسلل والدخول.

وهكذا يستطيع الجناة في الجرائم الإلكترونية إخفاء جرائمهم وطمس آثارها في وقت قياسي وقبل أن تصل إليها سلطة التحقيق، الأمر الذي يؤدي إلى صعوبات تعيق إجراءات التحقيق الرامية إلى الوصول إلى دليل، ومن أمثلة سهولة محو الدليل المعلوماتي في وقت قصير، أنه أثناء إجراء المحاكمة للمسؤولين عن أحد المشروعات بألمانيا طلبت

[52] د. جميل عبد الباقي الصغير، المرجع السابق، ص6 وما بعدها.

سلطات التحقيق المساعدة القضائية من السلطات السويسرية من أجل ضبط البيانات التي توجد في النظام المعلوماتي لإحدى الشركات السويسرية، وأثناء سير الإجراءات تمكن الجناة من محو البيانات التي كانت من الممكن أن تستخدم كدليل، ولكن لحسن الحظ بعد ضبط الدعامات والأقراص الصلبة وأسطوانات الليزر، تمكن الخبراء بطرق فنية من استعادة البيانات التي كانت مسجلة عليها.

ومن قبيل ذلك أيضًا، أن كان مكتب التحقيقات الفيدرالية بالولايات المتحدة الأمريكية قد تمكن من ضبط المدير التنفيذي السابق لشركة *Massachusetts Sudbury* التي تعمل في مجال الإلكترونيات، وذلك لقيامه باستئجار القراصنة، لتنزيل وتحميل مفاتيح فك الشفرات الخاصة بالتليفزيون المدفوع مقدمًا، ولأنه كان قد تسبب في خسارة للشركات صاحبة الحق في استغلال التليفزيونات المدفوعة مقدما، بلغت ما يقرب من سبعة ملايين دولار، وقدم المتهم للمحاكمة، إلا أن هيئة الحلفين بالمحكمة الاتحادية العليا برأت ساحته، لعدم وجود دليل يصلح لأدانته، لكونه قد تمكن من إزالة، ومحو أي دليل يفيد ارتكابه للواقعة، وهذه الحقائق تثير مشكلات متعددة في إجراءات المحاكمة، منها المعايير المقبولة للضبط المعلوماتي، ومعايير التحريز[53].

2- صعوبة نسبة الدليل الرقمي إلى متهم معين:

تختلف الجريمة الإلكترونية عن الجريمة التقليدية، بأن الجريمة الأولى لا تحتاج لارتكابها لأي نوع من العنف، وإنما تقع بواسطة إدخال بيانات لمعلومات خاطئة أو محظورة ضمن البرامج، أو تحريف أو تعديل البيانات والمعلومات المخزنة أصلا في الحاسب الآلي، أو إرسال برامج تخريبية أو التجسس على البيانات والمعلومات المخزنة ونسخها ... الخ. وإذا ما صادف واكتشفت هذه الأفعال وجمعت الأدلة على وقوعها، فإن هذه الأدلة قد لا تفصح عن صلة شخص معين بالجريمة المرتكبة، نظرا لأن معظم نظم الحاسب الآلي لا تسمح للمراجعين والفنيين بالتتابع العكسي لمسار مخرجاتها، علاوة على صعوبة تتبع الآثار الإلكترونية ومراجعة وفحص الكم الهائل من البيانات والمعلومات المدرجة بالأنظمة، وتعمد الجناة إلى إخفاء هويتهم.

ويمكننا أن نمثل على الصعوبات التي تشكلها ضخامة كم البيانات والمعلومات وتأثيرها السلبي على جمع الأدلة بشان الجريمة المعلوماتية وملاحقة المجرمين بالواقعة التي شاهدتها ألمانيا الاتحادية عام 1971 حيث اكتشفت شركة طلبيات بريدية (*Order–fimmail*) سرقة أشرطة ممغنطة تحتوي على (*300,000*) عنوانا لعملائها واستصدرت من المحكمة أمرا يسمى وقف الإعمال، وذلك باستعادة كل هذه العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من الذين ارتكبوا السرقة، وتنفيذا لذلك سمحت الشركة المنافسة لمساعد مأمور التنفيذ، أن يدخل مقر الحاسب الآلي الخاص بها، وذلك للحصول على تلك العناوين، ووجد نفسه وسط كم هائل من الأشرطة والأقراص الممغنطة التي لا يدري عنها شيئا، ولا يمكن فحص محتوياتها أو لديه القدرة على ذلك فغادر مقر الشركة دون أية

[53] باسل أحمد عبد المحسن محمد لطفي، دور القاضي المستعجل في وقف الاعتداءات الجنائية، المرجع السابق، ص136.

معلومات، إلا أن الشركة المنافسة قامت من تلقاء نفسها بعد أيام، بتسليم بيانات العناوين إلى الشركة المعتدى عليها، وإن كان ذلك لا يمنع من نسخ هذه الشرائط قبل تسليمها، الأمر الذي يفرغ أمر المحكمة من مضمونه[54].

واكتشاف هوية الجناة تتعذر في الجرائم الإلكترونية بالنظر إلي صعوبة تحديد عنوان المجرم الإلكتروني، وتعيين مكان تواجد جهاز الحاسب الآلي مصدر النشاط الإجرامي، والأمر يحتاج إلى جهود تقنية عالية ونظام فحص إلكتروني يسمى بعلم البصمات المعاصر، مكن في فترة ما من التعرف على هوية مبتكر فيروس "ميليسا" ومبتكر موقع خدمات بولمبروج لأخبار المال الاحتيالي الذي يرفع الأسهم عن طريق الخداع والذي يتم من خلاله تتبع الحركة العكسية لمسار الإنترنت، أو الحركة التراسلية للنشاط الممارس عبر الإنترنت إلى غاية الوصول إلى عنوان رقمي للجهاز يسمى *Adresse internet*، وهذا العنوان هو عبارة عن بروتوكول لعنونة البيانات والمواقع في شبكة المعلومات . [55] *Protocole IP*.

وإذا كانت الاستعانة بالمعلومات والعناوين والمصادر التي يحتويها نظام يساعد في كشف هوية مرتكب جريمة إلكترونية ما إلا أن هذه النتيجة ليست دائما صحيحة، لأن ما يتم التوصل إليه من خلال التقنية السابقة هو عنوان رقمي للحاسب فقط وهذا لا يكفي وحده لإسناد الفعل الإجرامي إلى صاحب الحاسب المذكور، فقد لا يكون له صلة بالجريمة على الإطلاق، كأجهزة الحاسب المستأجرة مثلاً في مقاهي الإنترنت، أو كان الحاسب مسروقًا أو تم التحايل للوصول للعنوان الرقمي وإساءة استخدامه ... وهكذا[56].

وقد أكد القضاء الفرنسي هذا الأمر في قضية فوريسيون، حين نشرت رسالة إلكترونية عنصرية ضد الصهيونية تحمل اسم الفرنسي *Robert Faurission*، وحين اكتشفت على الموقع *Aaargh*، الذي تم إيوائه في الولايات المتحدة الأمريكية، حركت دعوى قضائية ضد هذا الشخص، إلا أن المحكمة لم تستطع إقامة الدليل على أن المتهم هو الناشر الحقيقي للرسالة المؤثمة، وعليه قضت بأن وجود اسم المتهم في ذيل الرسالة لا يثبت بأنه مصدرها الحقيقي ولا يكفي أن يكون دليل إدانة، لان هذا الاسم يمكن لأي شخص أن يكتبه إمعانا في التمويه، الأمر الذي يقتضي إلزام متعهد الوصول بتحديد شخصية المشترك وعدم توصيل الأسماء المجهولة[57].

---

[54] هشام مُحَّد فريد رستم، المرجع السابق، هامش 1، ص19.

[55] جمال براهيمي، المرجع السابق، ص201.

[56] جمال براهيمي، المرجع السابق، ص203، أرسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، بحث مقدم إلى الندوة الإقليمية حول: الجرائم المتصلة بالكمبيوتر، المملكة المغربية، في 19-20 يونيو 2007، ص113 وما بعدها.

[57] *TGI. 8 nov. 1998, sur le site :http://www.legalis.jnet.decision/illicite-divers/correct-Paris-1998-htm*.

يضاف إلى ذلك أن برتوكول الإنترنت *TCP/ IP* الذي يكشف عن الحاسب المستخدم في ارتكاب الجريمة الإلكترونية ليس موحدًا على المستوى العالمي وليس لصيقًا به بصفة دائمة، بل هو قابل للتغيير مع كل اتصال بشكة الإنترنت[58].

وقد انتهى بعض المشاركون في مؤتمر جرائم الحاسب المنعقد في أوسلو بين 29 -31 مايو عام 2000، إلى أن تحديد هوية مرتكب الجريمة الحقيقي أمر نسبي، إذ لا يوجد تجهيل بالمعني الكلي لشبكة المعلومات، حيث يترك الفاعل في كل الأحوال آثار أثناء تنقله في شبكة المعلومات تسمح للمحقق بالوصول إليه، وبالتالي يمكن للمحقق استجواب صاحب هذا الحاسب المشتبه فيه عما إذ كان قد سمح لشخص آخر استعمال جهازه، وتاريخ ومدة استعماله، ثم يقارن كل هذه المعلومات مع معلومات الجريمة وتتبع الآثار عبر الإنترنت *La traçabilité* لتحديد هوية المستخدمين والوصول للشخص المسئول جنائيًا[59].

وحسنًا فعل المشرع المصري ضمن قانون مكافحة جرائم تقنية المعلومات حين ألزم بموجب المادة الثانية أولاً/1/أ مقدم الخدمة بحفظ وتخزين سجل النظام المعلوماتى أو أي وسيلة لتقنية المعلومات لمدة 180 يوما متصلة، ومن بين البيانات الواجب حفظها وتخزينها البيانات التي تمكن من التعرف على مستخدم الخدمة.

3- مكنة إعاقة الوصول إلى الدليل الرقمي:

يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمته وضبط أدلتها باستخدام تقنيات التشفير[60] أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها[61]، والأمر يحتاج من المحقق إلمام وافي بعدد من العلوم الإحصائية والخوارزميات وعلم تحليل الشفرات، أو ما يعرف بعلم استرجاع النص الواضح بعبارة معينة بدون معرفة المفاتيح، الأمر الذي يقف عقبة أمام تنفيذ التفتيش.

هذا وقد أثبتت التحقيقات في بعض الجرائم الإلكترونية بألمانيا وجود صعوبات تواجه البعض من هذه التحقيقات نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم.

---

[58] *M. A. Habhab, Le droit pénal libanais à l'épreuve de la cybercriminalité, th : Montpellier I, 2009, p.115 et s.*

د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، 2013، ص220، د. عمر محمد بن يونس، المرجع السابق، ص811، د. جمال براهيمي، المرجع السابق، ص204.

[59] د. جمال براهيمي، المرجع السابق، ص205.

[60] يقصد بالتشفير جملة مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن لشخص ثالث قراءتها.

[61] د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002، ص115، إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، 2000، ص11، ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، 2000، ص24 وما بعدها.

ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير، كوسيلة لمنع ضبطه والإيقاع به، واقعة حدثت في الولايات المتحدة عام 1996، إذ كان المشتبه به مشغلا للوحة إعلانات *BBS*، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الإلكترونية، حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به، فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب، وقاموا بكتابة برنامج يحاول تشغيل النسخة الاحتياطية، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهوله إلى أسماء المستفيدين وأرقامهم، ولكن لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به، خاصة وأنها كانت مشفرة، ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة، ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها، ولكن التشفير حال دون ذلك.

وللوصول إلى كلمة المرور قام المحققون بإنشاء رقمين جديدين من أرقام المستفيدين، لهم أسماء مختلفة، ولكن لهم نفس كلمة المرور، وبهذه الطريقة وبتتبع كلمتي المرور المتشابهتين أمكن العثور على مكان وجود كلمات المرور على القرص الصلب، ووضع المحققون يدهم على كلمة المرور الخاصة بالمتهم في ملف المستفيدين، ثم قاموا بإحلال كلمة المرور السابق استخدامها مع المستفيدين الوهميين مكان كلمة المرور الخاصة بالمشغل (وهي مشفرة كما هي)، وبذلك أمكن الدخول إلى الحاسب باستخدام اسم المشغل مع كلمة المرور الخاصة بالمستفيد الوهمي[62].
ويثار التساؤل حول ما إذا كان يمكن إجبار أحد الأشخاص العاملين على شبكة المعلوماتية بفك الشفرة للحصول على الدليل الرقمي[63]. هنا يذهب اتجاه إلى أنه ليس من واجب الشاهد وفقًا للالتزامات التقليدية للشاهد أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور، أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الفقه الألماني، حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب، لأن الالتزام بأداء الشهادة لا يتضمن هذا الواجب. بينما يذهب البعض الآخر من الفقه الفرنسي إلى أن من بين الالتزامات التي يتحمل بها الشاهد، طبع ملفات البيانات أو الإفصاح عن كلمات المرور وشفرات الخاصة بالبرامج المختلفة، لأن القواعد العامة في مجال الإجراءات، تحتفظ بسلطانها في مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم المواد (62)، (109)، (138) من قانون الإجراءات الجنائية الفرنسية، مع الأخذ في الاعتبار أن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيًا إلا في مرحلتي التحقيق والمحاكمة.

وفي هولندا يتيح مشروع قانون الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه، والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب، وكانت مصلحة التحقيق تقتضي الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحلها. كذلك الأمر في اليونان، إذ يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للولوج إلى نظام المعلومات، كما يمكن أيضاً الحصول منه على

[62] حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2000، ص233 وما بعدها.

[63] راجع، باسل أحمد عبد المحسن مُحَمَّد لطفي، دور القاضي المستعجل في وقف الاعتداءات الجنائية، المرجع السابق، ص115-116.

بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب الآلي، وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل، وليس الكشف عن معلومات جديدة وفقا لنص الفقرة الأولى من المادة (223) من قانون الإجراءات الجنائية اليوناني.

وعادة ما يستعين المجرم بأساليب أمنية وتدابير حماية فنية أخرى من أجل إعاقة سلطات التحقيق من الوصول إلى الدليل، ومن ذلك تحميل برنامج للفيروسات داخل حاسبه على شكل برامج غير مرئية، كفيروس حصان طروادة والدودة أو برامج القنابل المنطقية أو الزمنية، وجعل وظيفة هذه الفيروسات هي حماية الحاسوب وما يحتويه من بيانات وبرامج وملفات من خطر الدخول والنسخ غير المرخص. وغالبًا ما يبرمج المجرم المعلوماتي بداية نشاط هذه الفيروسات بمجرد محاولة اختراق الحاسب أو النسخ لتقوم مباشرة بتخريب نظام تشغيل الجهاز محل التفتيش وإتلاف كلي للبيانات والملفات المخزنة داخل ذاكرته، مما يجعلها غير قابلة الاسترجاع وبالتالي استحالة قيام المحقق بمهمة التفتيش حول البيانات والمعلومات داخل الحاسب[64].

وكذلك قد يستعين المجرم – رغبة في إعاقة تفتيش الحاسب استخدام تقنية إخفاء المعلومات *Steganography* ، وذلك بوضع بيانات مهمة داخل بيانات أخرى قد تكون على شكل ملفات مصورة أو صوتية أو فيلمية أو على شكل بيانات تنفيذية لبرامج الحاسب، أو يقوم بإخفاء هذه المعلومات في مساحة معينة من القرص الصلب مخصصة فقط لتخزين ملفات أنظمة التشغيل دون غيرها، الأمر الذي يشدد من مهمة رجال التحقيق في هذا النوع من الجرائم من الوصول إلى أدلة مادية مستمدة من التفتيش[65].

ثانيًا: الصعوبات القانونية للبحث عن الدليل الرقمي:

1- تنازع الاختصاص بالتفتيش في الجرائم الإلكترونية عبر الوطنية:

سبق القول أن ظاهرة الإجرام الالكتروني تثير العديد من المشكلات في نطاق القانون الجنائي الإجرائي، إذ أن نصوصه وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد ثمة صعوبات كثيرة في إثباتها أو التحقيق وجمع الأدلة فيها، مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولاً إلى الحقيقة الموضوعية بشأن الجريمة المرتكبة وجناتها.

---

[64] د. محمد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص496، جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص208.

[65] حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 410، محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، ط 3، كلية الشريعة والقانون، جامعة الإمارات، الفترة من 1 إلى 3 مايو 2004، ص1070، د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 115.

وتبدأ المشكلات الإجرائية للتفتيش الإلكتروني في التصاعد ما أن يتصل الأمر ببيانات معالجة آليًا وكيانات منطقية غير محسوسة، تنفذ الجرائم المتصلة بها بسرعة وبذكاء عال، مع القدرة على إخفاء آثارها وإتلاف الأدلة التي تخلفها عقب التنفيذ مباشرة، فضلا عن إمكانية لجوء مرتكبي هذه الجرائم إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية محمية بشفرات أو رموز سرية بغية إخفائها عن سلطات التحقيق المعنية.

ومما يزيد الأمر صعوبة أن الجريمة الإلكترونية قد ترتكب بشكل عبر وطني بحيث تتوزع أركانها على أكثر من دولة، فيصبح الولوج إلى الأنظمة والشبكات الإكترونية الموجودة في دولة أخرى يصطدم بعقبة السيادة، فإذا أضفنا إلى كل ذلك تباين نظرة التشريعات الإجرائية الدولية إلى الجريمة الإلكترونية، بالإضافة إلى ضعف وهشاشة وسائل التعاون الدولي لمواجهة الإجرام المعلوماتي، فإنه يصبح تنفيذ التفتيش الإلكتروني جد عسير[66].

ومما يقف في البدء من الناحية القانونية صداً لتنفيذ التفتيش الإلكتروني أن الجرائم من هذا النوع ترتكب في أغلب صورها بشكل خفي ومستتر في غفلة من المجني عليه، نظراً لطبيعة البيئة الافتراضية غير المحسوسة، فهي جرائم تخلو من العنف، ولا تحتاج إلى جهد كبير في ارتكابها، إذ يكفيها حاسوبً متصلاً بشبكة المعلومات الدولية وجملة معارف تقنية تعبر عن ذكاء مكتسبها ومستخدمها[67].

ثم تأتي مشكلة تنازع الاختصاص بالتفتيش في الجرائم الإلكترونية العابرة للحدود الوطنية، فقد يحدث أن ترتكب جريمة من الجرائم الإلكترونية من طرف أجنبي على إقليم دولة معينة، فيؤول الاختصاص في هذه الحالة إلى الدولة التي ارتكبت الجريمة على إقليمها استنادا إلى مبدأ الإقليمية، والى الدولة التي يحمل الجاني جنسيتها استناداً إلى مبدأ الشخصية الجنائية الإيجابية، وقد تشكل هذه الجريمة تهديدًا لأمن وسلامة دولة أخرى أو تمس بمصالحها الجوهرية والخاصة فتدخل في اختصاصها استنادا إلى مبدأ العينية، وهو ما يترتب عليه تنازع الاختصاص بين هذه الدول[68].

ولا شك أن تحديد مكان وقوع الجريمة تتوزع بشأنه المعايير وتتعدد بين الدول، بين قائل بأنه مكان ارتكاب النشاط الإجرامي، وبين آخر يأخذ بمعيار مكان وقوع النتيجة الإجرامية، وثالث يأخذ بأي من الضابطين إذا تحقق على الإقليم الوطني[69]. ومثال هذا التنازع أن يرسل المتهم برنامج من برامج الفيروسات من جهاز الكتروني متواجد في دولة معينة إلى جهاز آخر يقع في دولة ثانية مرورًا بجهاز ثالث، ورابع في دول أخرى، وهكذا[70].

---

[66] قريب من هذا المعنى، د. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، المرجع السابق، ص7.

[67] *M. Chawki, Combattre la cybercriminalité, éd. de Saint-Amans, Paris, 2008, p.318.*

[68] عبده مُحَمَّد بحر، معوقات التحقيق في جرائم الإنترنت، رسالة ماجستير، قسم العلوم الشرطية، كلية الدارسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999، ص26.

[69] راجع، د. أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، بدون تاريخ، ص73 وما بعدها. وتنص بعض التشريعات على ذلك، منها قانون الإجراءات الجنائية الجزائري في المادة 586 التي جاء فيها أنه: "تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها قد تم في الجزائر".

[70] *A. Diop, op. cit., p.14.*

والحقيقة أنه يتعين الأخذ بمفهوم موسع لمبدأ الإقليمية بشأن تحديد مكان وقوع الجريمة الإلكترونية بعيدًا عن الفعل المادي أو أحد عناصره، بالنظر لارتباط هذه الجرائم بعالم افتراضي لا تترك فيه آثار ملموسة.

وقد أقر القضاء الفرنسي هذا المفهوم الجديد لمبدأ الإقليمية، مؤكداً على اختصاصه على سند من أنه على الرغم من تواجد مركز " *Yahoo* " خارج الإقليم الفرنسي، إلا أن الرسائل التي يقوم ببثها هذا الجهاز تظهر في فرنسا ويمكن للجمهور الفرنسي الاطلاع عليها، لذلك اعتبر أن الجريمة مرتكبة في كل مكان تظهر فيه هذه الرسائل غير المشروعة محل البث[71].

بل نجد مثلاً أن القضاء الأمريكي وسع اختصاصه ليشمل كل الجرائم التي يمتد آثارها إلى الإقليم ولو كانت عناصر الركن المادي قد اجتمعت في دولة أخرى. وهكذا قضي بأنه إذا تم إدخال بيانات من إقليم دولة معينة تتضمن جريمة معلوماتية، وكانت هذه البيانات مقروءة في دولة أخرى وتمس بمصالحها أو تعرضها للخطر أو يمكن أن تمتد آثارها إلى إقليمها، فان محاكم هذه الدولة تكون مختصة. ومثال ذلك أن يضع الجاني صورًا مؤثرة على جهاز وكان الخادم يتواجد في بريطانيا وكانت هذه الصور متاح الاطلاع عليها في الولايات المتحدة الأمريكية، ففي هذه الحالة يكون القضاء الأمريكي مختصًا في التحقيق والفصل في هذه الوقائع، لا لأن أحد عناصر هذه الجريمة وقع في الإقليم الأمريكي، بالنظر لامتداد آثار الجريمة[72].

وهذا ما قضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة، وقضت به كذلك محكمة *Minnesota* في قضية جرانتي جات ريسورت بشأن بث موقع لألعاب القمار عبر الإنترنت من لاس فيجاس بولاية نيفادا، الذي وصل إلى ولاية مينيسوتا التي يحظر قانونها مثل هذه الألعاب. وتكرس هذا الاتجاه القضائي أيضًا فيما انتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الإنترنت. وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (*PGP.*) على الإنترنت بمثابة تصدير لها، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الاختصاص، بصرف النظر عن مكان وضع البرمجية[73].

وقد لجأت بعض الدول في صراحة تامة في تنظيم مشكلة تنازع الاختصاص في الجرائم الإلكترونية بنصوص واضحة في اتفاقيات دولية ثنائية ومتعددة الأطراف، يتم من خلالها تحديد الضوابط التي بموجبها توزع الولاية القضائية بين الأطراف المتعاقدة، ومن ذلك ما نصت عليه المادة 15 من اتفاقية منظمة الأمم المتحدة لمكافحة

---

[71] *P. Vergucht, op. cit., pp.347-348 ; A. Diop, op. cit., p.15. J.-P. Mignard, Cybercriminalité et cyber répression entre désordre et harmonisation mondiale, th. Paris 1, 2004, p.603 et s.*

[72] لمزيد من التفصيل، د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004، ص908 وما بعدها.

[73] لمزيد من التفصيل، د. عمر محمد بن يونس، المرجع السابق، الموضع السابق. وراجع، باسل أحمد عبد المحسن محمد لطفي، دور القاضي المستعجل في وقف الاعتداءات الجنائية، المرجع السابق، ص143.

M. Chawki, op cit., pp.323-324.

الجريمة المنظمة على أنه يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

– حينما ترتكب الجريمة في إقليم تلك الدولة.

– حينما ترتكب الجريمة ضد أحد مواطني تلك الدولة.

– حينما ترتكب الجريمة من طرف أحد مواطني تلك الدولة أو من طرف شخص عديم الجنسية اتخذ مكان إقامته المعتاد في إقليمها.

ثم أضافت هذه المادة، أنه إذا بلغت الدولة التي تمارس ولايتها القضائية عن سلوك إجرامي ما بموجب المعايير السالفة الذكر أو علمت بطريقة أخرى أن دولة واحدة أو أكثر باشرت إجراءات التحقيق والمتابعة القضائية في السلوك ذاته، فعلى السلطات المختصة في هذه الدول أن تتشاور فيما بينها لغرض تنسيق ما تتخذه من التدابير.

وبالمثل جاءت اتفاقية مجلس أوروبا لمكافحة الجريمة الإلكترونية[74] فنظمت بدورها مسألة الاختصاص من خلال المادة 22، والتي نصت على أنه يلتزم كل طرف بوضع ما يلزم من تدابير تشريعية لإقرار الاختصاص بشأن أي جريمة إلكترونية وذلك عندما ترتكب الجريمة على إقليمه، أو عندما ترتكب الجريمة من طرف أحد مواطنيه إذا كانت الجريمة معاقبًا عليها بموجب القانون الجنائي لمكان ارتكابها. أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة[75].

هذا، وقد حثت هذه الاتفاقية الأطراف المتعاقدة في حالة وجود تنازع الاختصاص بين أكثر من طرف بشأن أية جريمة الكترونية تقررها هذه الاتفاقية، باللجوء متى كان ذلك ممكنا إلى التشاور فيما بينها لغرض تحديد الاختصاص القضائي الأكثر ملائمة لمتابعة هذه الجريمة (الفقرة 5 من المادة 22).

وبخصوص القانون المصري لمكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، فإننا نلحظ أنه قد حدد في المادة الثالثة منه نطاق تطبيقه مكانيًا قائلاً: "مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متي كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في أي من الأحوال الاتية:

1– إذا ارتكبت الجريمة على متن أيه وسيله من وسائل النقل الجوي أو البري أو المائي وكانت مسجله لدي جمهورية مصر العربية أو تحمل علمها.

---

[74] *Conseil de L'Europe, La criminalité informatique, Recommandation n°R(89) sur la criminalité en relation avec l'ordinateur et rapport final du comité Européen pour les problèmes criminels, Strasbourg, Conseil de l'Europe, 1990, pp.94-96 ; M. Quemener, Conseil de l'Europe et lutte contre la cybercriminalité, Revue Expertises des systèmes d'information, n°347, mai 2010, p.170.*

[75] *M. Quemener, Conseil de l'Europe, op. cit., Ibid.*

2- إذا كان المجني عليهم أو أحدهم مصريًا.
3- إذا تم الاعداد للجريمة أو التخطيط أو التوجيه أو الاشراف عليها أو تمويلها في جمهورية مصر العربية.
4- إذا ارتكبت الجريمة بواسطة جماعة إجرامية تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية
5- إذا كان من شأن الجريمة إلحاق ضرر بأي من موطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها في الداخل أو الخارج.
6- إذا وُجد مرتكب جريمة في جمهورية مصر العربية بعد ارتكابها ولم يتم تسليمة.

وهكذا وسع المشرع المصري من اختصاصه المكاني ومن مفهوم مبدأ الإقليمة، إلى الحد الذي اعتمد فيه مبدأ الولاية الجنائية العالمية، وذلك بالاكتفاء بمنح السلطات المصرية الاختصاص لمجرد القبض على المتهم في مصر، ما لم تقم السلطات بتسليمه لدولة أخرى، وهو ما يعرف بمبدأ التسليم أو المحاكمة، دون اشتراط وقوع الجريمة في مصر، أو امتداد آثارها إلى الإقليم المصري، ولو لم يكن الجاني أو المجني عليه من مواطني جمهورية مصر العربية.

ومن أجل الدفع بمزيد من التعاون الدولي في مكافحة جرائم تقنية المعلومات، والحد من فرص تنازع الاختصاص والإفلات من العقاب نصت المادة الرابعة الموسومة بمجال التعاون الدولي لمكافحة جرائم تقنية المعلومات على أن تعمل السلطات المصرية المختصة على تيسير التعاون بالبلاد الاجنبية في إطار الاتفاقيات الدولية والاقليمية والثنائية المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات.

2- قعود الضحايا عن التبليغ عن الجرائم الإلكترونية:

من المعتاد في شأن الجرائم الإلكترونية أن يتكتم عليها المجني عليه ولا يقم بتبليغ السلطات المختصة عن وقوعها بعد تكشفها له، خاصة إذا اتصلت الجريمة الإلكترونية بمؤسسات تجارية ومالية ذات سمعة وثقة لدى المتعاملين معها؛ فالسمعة أمر لا يقلب التفريط اقتصاديًا، كما تخشى الشركات إذا أبلغت عن جريمة إلكترونية أن يتم الحجز على أجهزة الحاسب لديها أو تعطيل شبكة معلوماتها بغرض التفتيش وضبط وجمع الأدلة، وهو ما قد يمس بسرية معاملاتها، ويعرضها لخسائر جمة، ربما أشد مما أحدثته الجريمة الإلكترونية من أضرار[76].

وهكذا كشفت إحدى الدارسات الإحصائية التي أجراها المعهد الوطني للقضاء التابع لوزارة العدل الأمريكية بأن أكثر من 70% من الجرائم الإلكترونية التي يتم اكتشافها لا تبلغ عنها إلى سلطات الأمن. وهي النتيجة نفسها التي أكدتها الدراسة التي أعدها معهد أمن الحاسب بمشاركة مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية[77].

[76] *P. Vergucht, La répression des délits informatiques, op. cit., p.323 et s.*
د. هشام محمد فريد رستم " الجرائم المعلوماتية، المرجع السابق، ص435 وما بعدها.
[77] حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص19 وما بعدها.

ورغبة في تجاوز هذه العقبة في التحقيق الجنائي الإلكتروني، ولاسيما التفتيش، اقترح البعض فرض التزام وجوبي بالإبلاغ عن الجرائم الإلكترونية بمجرد علمهم بها تحت طائلة الجزاء الجنائي عند الإخلال بهذا الالتزام[78].

وأمام تعرض هذا الاقتراح للنقد، ذهب البعض إلى ضرورة الإبلاغ عن الجرائم الإلكترونية مع جعله يُقَدم إلى جهة معلوماتية إشرافية بعيدة عن الأمن، وهو الحل الذي لجأ إليه المشرع الأمريكي في قانون حماية البنوك حين الزم كل موظفي البنوك بالإفصاح أو التبليغ عن كل ضياع أو نقص غير مبرر لمبلغ يفوق ألف دولار إلى جهاز المراقبة المالية، الذي يقوم بمراجعة الأمر وإخطار الجهات الأمنية إذا كان هناك ما يستدعي ذلك[79].

والأفضل بالقطع هو تحفيز الضحايا نحو الإبلاغ عن كل جريمة إلكترونية عن طريق اتخاذ الدولة جملة من التدابير الإدارية، كاشتراط الإبلاغ لاستفادة المجني عليه من بعض الحقوق والمزايا، كالحصول على تعويضات من شركات التأمين مثلاً[80].

فإذا أضفنا إلى كل ما سبق أنه قد تصبح الحماية التي تكفلها القوانين والمواثيق الدولية[81] للحق في حرمة الحياة الخاصة، أو الحق في الخصوصية، عقبة أمام سلطات التحقيق عند تنفيذ التفتيش الإلكتروني لأن المحقق الذي يقوم بالتفتيش على نظم الحاسب الآلي وقواعد بياناته أو على شبكات الإنترنت غالبا ما يتجاوز النظام المعلوماتي للمشتبه فيه إلى أنظمة أخرى مرتبطة به، بسبب شيوع التشبيك بين أجهزة الحاسب وانتشار الشبكات الداخلية على مستوى المنشآت، والشبكات المحلية والدولية، وهو ما سيسمح عند بالاطلاع على ملفات سرية وبيانات خاصة بأشخاص قد لا يكون لهم علاقة بالجريمة.

المبحث الثاني

[78] د. هشام محمد فريد رستم، الجرائم المعلوماتية، المرجع السابق، ص438

[79] *P. Vergucht, op.cit. p.327 et s.*

[80] *M. Linglet, Délinquance informatique, sur le front de la nouvelle criminalité, une parade concerné, RIPC., mai 1995, p.182.*

[81] ويمكن أن نذكر من هذه المواثيق: المواد 1، 5، 12 من الإعلان العالمي لحقوق الإنسان لعام 1948، والمادة (17/ف 1، 2) من العهد الدولي للحقوق المدنية والسياسية لعام 1966، والمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لعام 1950، والمادة 11 من الاتفاقية الأمريكية لحماية حقوق الإنسان لعام 1969، والمادة 17 من الميثاق العربي لحقوق الإنسان لعام 2004.

تقسيم:

تستهدف إجراءات التحقيق تحصيل دليل مشروع يثبت الجريمة وينسبها إلى جناتها فاعلين كانوا أو شركاء، فالتحقيق والإثبات قرناء لا ينفصلان، أحدهما يتصل بالوسلية، والآخر يرتبط بالغاية منها. وكما أعملت ثورة المعلوماتية أثرها في الوسائل المتعلقة بالتحقيق، فإنها قد نالت كذلك من طرق الإثبات الجنائي، إذ لم تعد الطرق التقليدية قادرة مع التكيف مع العالم الافتراضي المتصل بتقنية المعلومات[82]. وهكذا اتسع نطاق الدليل الالكتروني، إذ أصبحت الأجهزة الإلكترونية من حواسب، وهواتف ذكية، وكاميرات، وشبكات الاتصالات الرقمية تشكل مستودعا مهما للمعلومات والبيانات التي من شانها أن تدعم جهود تحقيق العدالة الجنائية. وهكذا كان لازمًا طرح التساؤل حول الطبيعة القانونية ونطاق الأدلة الرقمية **(المطلب الأول)**، قبل البحث في حجية هذه الأدلة أمام القاضي الجنائي **(المطلب الثاني)**.

المطلب الأول
الطبيعة القانونية للدليل الرقمي

تقسيم:

المعلوم أن طبيعة الدليل تتشكل وتتحدد من طبيعة الجريمة التي تولد منها؛ فالدليل في الجريمة الإلكترونية يثبت بأدلة رقمية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها الجريمة. فما ماهية الدليل الرقمي؟ **(أولاً)**، وما الأدلة الرقمية المقبولة في الإثبات الجنائي؟ **(ثانيًا)**.

أولاً: ماهية الدليل الرقمي:

يرتبط الدليل الرقمي الناشئ عن البيئة الافتراضية الإلكترونية بتكنولوجيا وسائل الاتصال وشبكات الربط الحديثة وتداول المعلومات، فانه من الضروري أن يكون أي تعريف لهذا النمط من الأدلة متسما بالمرونة بما يسمح باستيعابه وتواكبه مع سائر جرائم تقنية المعلومات.

ولم يتفق الفقه الجنائي على تعريف موحد للدليل الرقمي[83]، فقيل أنه: "ذلك الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية أو كهربائية يمكن جمعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل علمي يمكن اعتماده أمام القضاء الجنائي"[84].

والملاحظ على هذا التعريف أنه يلحق مفهوم الدليل الالكتروني بمفهوم البرنامج رغم وجود فرق كبير في الوظيفة التي يؤديها كل عنصر، فبرنامج الحاسب الآلي له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية،

---

[82] قريب من هذا المعنى، د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، ط1، دار النهضة العربية، 1999، ص95 وما بعدها، د. أمير يوسف فرج، الجرائم المعلوماتية على شبكة الإنترنت، ط1، دار المطبوعات الجامعية، 2008، ص47 وما بعدها.

[83] راجع لمزيد من التفصيل، حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، 2017، 8 وما بعدها.

[84] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، 2006، ص88.

أما الدليل الالكتروني فيكمن دوره الأساسي في معرفة كيفية حدوث جرائم الاعتداء على نظم المعالجة الآلية، بهدف إثباتها ونسبتها إلى مرتكبيها[85].

أو أنه: "يشمل المعطيات الرقمية المشتقة من أو بواسطة النظم والمعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الإعلام الآلي أو شبكات الاتصالات وفق إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميًا وترجمتها الى نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة للمتهم طبقً لها"[86].

ويؤخذ على هذا التعريف كذلك هو حصره الأدلة الإلكترونية في تلك التي "تستخرج من أجهزة الإعلام الآلي وملحقاتها، دون سواها من الوسائل التقنية الإلكترونية الأخرى التي تعتمد المعالجة الآلية للمعلومات كالهواتف النقالة والبطاقات الذكية والتي يمكن أن تكون مصدرًا مهما للأدلة الإلكترونية، وهو ما يعد تضييقًا لدائرة هذه الأخيرة[87].

ومما قيل أيضًا في تعريف الدليل الرقمي أنه: "طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى إحدى الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب والرسائل الإلكترونية المخزنة أو المنقولة رقميًا"[88].

وعرف الدليل الالكتروني كذلك بأنه: "مجموعة البيانات والمعطيات المأخوذة من العالم الافتراضي التي يمكن إعدادها وتجميعها وتخزينها وتحليلها إلكترونيًا باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور او تسجيلات صوتية أو مرئية"[89]. وما يؤخذ على هذا التعريف هو إضفاؤه صفة الدليل الالكتروني على تلك الأدلة المستخلصة من وسطها الافتراضي المأخوذة من الحاسب مما يعني بمفهوم المخالفة بأن تلك المعطيات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية التي لم تفصل عن الحاسب الآلي لا تصلح لأن توصف بالدليل الالكتروني، وهذا أمر تعوزه الدقة[90].

---

[85] د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص121-122.

[86] خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الرابط التالي:
http://Kenanaonline.com/users/KhaledMamdouh/posts/79345

[87] د. جمال براهيمي، المرجع السابق، ص122.

[88] *M. Clément-Fontaine, Définition et cadre juridique de la preuve numérique, in, Colloque sur La preuve numérique à l'épreuve du litige, Les acteurs de litige à la preuve numérique, organisé par la Compagnie Nationale des Experts de Justice en Informatique et Associées, le 13-04-2010, sur le site :www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf.*

[89] طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا بطرابلس، 28-29 أكتوبر 2009، ص6.

[90] د. جمال براهيمي، المرجع السابق، ص123.

وارتأى البعض أنه: "معلومات يقبلها المنطق والعقل ويصدقها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أية مرحلة من مراحل الدعوى الجنائية لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة"[91].

وعرفه أخيرًا المشرع المصري في المادة الأولى من القانون 175 لسنة 2018 بأنه: "أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

ونستطيع من جانبنا تبني تعريف شامل للدليل الرقمي ليصبح: "كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات إلكترونية او ذبذبات كهربائية او نبضات مغناطيسية، يتم استخلاصها وجمعها وتحليلها وفق إجراءات قانونية وعلمية، وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم، ويمكن استخدامها في أية مرحلة من مراحل الدعوى الجنائية لإثبات الجريمة وتقرير البراءة أو الإدانة "، وهو مقارب للتعريف الذي تبنته المنظمة العالمية للدليل الكمبيوتر *IOCE* في تقريرها الصادر في أكتوبر عام 2001[92].

وفي اعتقاد البعض أن الأدلة الجنائية الرقمية مجرد مرحلة متقدمة من الأدلة المادية التقليدية المدركة بالحواس الإنسانية المعتادة[93]، وهو أمر يتنافى مع حقيقة الدليل الرقمي المرتبط ببيئة افتراضية لا سابق مماثل لها ؛ فهذا الأخير دليل علمي يتكون من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي، ويجب أن يحكم الدليل الإلكتروني طبيعته العلمية، بحيث يكون متجاوبًا مع حقائق العلم ولا يخالف نظرياته الرقمية، وإلا تعين إهداره كدليل[94].

كما أن الدليل الرقمي ذا طابع تقني، ومن ثم يرتبط فقط بالبيئة التقنية التي يتواجد فيها، والتي تشمل مختلف الأجهزة التكنولوجية حواسب وخوادم ومضيفات وهواتف وشبكات ؛ فكل ما يخرج عن تلك الأمور لا يسمى دليلاً إلكترونيًا رقميًا[95]. وهو بهذه الصفة قابل للاستنساخ بشكل يطابق الأصل وله نفس القيمة العلمية، بما يخالف منطق الأدلة المادية التقليدية. وهذا الميزة تمكن من الحفاظ على الدليل الرقمي من التلف أو الفقد أو أي شكل من أشكال التلاعب، وذلك لإمكانية مقارنة النسخ مع الأصل باستخدام برمجيات متخصصة. هذا فضلاً عن قدرة الدليل الرقمي

---

[91] محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، بحث مقدم إلى الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، دبي، من 15 إلى 2008/11/19، ص25.

[92] مصطفي محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، 2009، ص213.

[93] عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، جامعة الدول العربية، الفترة من 26-27 أبريل 2008، ص7، علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المرجع السابق، ص77.

[94] د. علي محمود علي حمودة، المرجع السابق، ص 77.

[95] د. عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، المرجع السابق ص17، د. جمال براهيمي، المرجع السابق، ص125.

على رصد معلومات متتالية عن الجاني وجريمته وتحليلها آليًا وهو ما يرفع من قدرات منظومة البحث الجنائي، إلى جانب قابلية الدليل الرقمي على التطور بقدر ما تتطور العلوم الرقمية[96].

ومما نختتم به، هي ميزة صعوبة التخلص من الدليل الإلكتروني خلافًا للدليل المادي التقليدي، إذ تتصف الأدلة الرقمية بمكنة استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، وذلك باستخدام أدوات وبرمجيات خاصة، كما يعد محو الدليل الرقمي قرينة إذناب في مواجهة المتهم[97].

ثانيًا: الأدلة الرقمية المقبولة في الإثبات الجنائي:

يمكن تصنيف الدليل الرقمي كأصل عام إلى صنفين هما: الدليل الرقمي الأصلي، ويتمثل في المحررات الإلكترونية المكونة من بيانات ومعطيات يدخلها المزود ويرسلها عن طريق وسيط الكتروني فيترجمها الوسيط وفق برنامج معين ويمررها إلى المتلقي الذي يمكنه استخراجها بالاستعانة بوسيط إلكتروني آخر وقراءتها بالبرنامج وإظهارها على شكل صورة الإدخال[98].

وهناك أيضًا الدليل الرقمي المكرر، وهي الصورة طبق الأصل المأخوذة عن الدليل الإلكتروني الأصلي أو استنساخ رقمي دقيق لجميع المعلومات والبيانات التي يتضمنها المحرر الأصلي والمستقلة عنه.

وتحت هاذين التقسيمين ترد عدة تقسيمات فرعية، فهناك من حيث هيئة الدليل الرقمي أدلة مكتوبة وأدلة العرض المرئي وأخرى صوتية أو سمعية[99]. وهناك من ينوع الدليل تنويعًا مغايرًا[100] فيجعل هناك أدلة الكترونية خاصة بأجهزة الحاسب الآلي وملحقاته. ثم أدلة إلكترونية خاصة بالشبكة العالمية للمعلومات ومختلف نهاياتها الطرفية. وأخيرًا أدلة إلكترونية خاصة ببروتوكولات *TCP/IP* تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

أما من حيث قيمة الدليل في الإثبات، فهناك الدليل المعد سلفًا للإثبات وتتضمن السجلات التي تم أنشاؤها بواسطة الجهاز الالكتروني تلقائيًا، وتعتبر هذه السجلات من مخرجات الجهاز التي لم يسهم الإنسان في إنشائها، مثل سجلات الهاتف، وفواتير أجهزة الحاسب الآلي. وكذلك السجلات التي جزء منها تم حفظه بالإدخال وجزءها الأخر تم

---

[96] د. عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، بحث مقدم إلى ندوة الدليل الرقمي، جامعة الدول العربية، القاهرة، من 5 إلى 8 مارس 2006، ص17، رشيدة بوكر، المرجع السابق، ص388.

[97] د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص126، محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، المرجع السابق، ص26-27، د. عمر محمد بن يونس، المرجع السابق، ص982، أحمد سعد محمد الحسيني، المرجع السابق، ص157.

[98] د. جمال براهيمي، المرجع السابق، ص128.

[99] القاهرة، 2013، ص720. القانونية، الكتب دار الالكتروني، التوقيع على الاعتداء جرائم على مقارنة حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية

[100] د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، 2003، ص20 وما بعدها، سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار كتب القانونية، 2011، ص59، ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005، ص9.

إنشاؤه بواسطة الجهاز ومن أمثلة ذلك، البيانات التي يتم إدخالها إلى جهاز الحاسب وتتمُّ معالجتها من خلال برنامج خاص[101].

أما الأدلة التي لم تُعد أساسًا للإثبات، فتشمل كل ما نشأ دون إرادة المستخدم الشخص، فتخص كل أثر يتركه الجاني دون أن يكون رغبًا وجوده، وتسمى بالبصمة الرقمية، أو الآثار المعلوماتية الرقمية، وهى تتجسد في المخلفات التي يتركها مستعمل شبكة الإنترنت كالمواقع التي تصفحها والملفات التي زارها والتواريخ المرتبطة بهذه الزيارات، والتي تسجل على الذاكرة المخفية للقرص الصلب بجهاز المستخدم داخل فهرس خاص للنظام، وكذا ملفات البريد الالكتروني *E-Mail* التي تحمل مختلف الرسائل المرسلة منه أو التي استقبلها الموجودة أو المحذوفة وكافة العمليات والاتصالات التي تمت من خلال النظام المعلوماتي أو شبكة المعلومات العالمية[102].

ولا شك أن النوع الثاني قيمته الاستدلالية أكبر وأكثر أهمية في الإثبات الجنائي حيث يمكن ضبطها بواسطة تقنيات التتبع والاسترداد ولو بعد فترة من إنشائها لكونها نشأت رغمًا عن إرادة مستخدم الحاسب. أما النوع الأول فهو عرضة للفقد، فلا يؤمل فيه ولا يحتج به كثيرًا في إثبات جرائم تقنية المعلومات بالمعنى الفني الدقيق التي يكون النظام المعلوماتي هو بذاته محلاً للاعتداء، أو حتى غيرها من الجرائم الإلكترونية التي ترتكب عبر الحاسب كالاحتيال وغسل الأموال الاستيلاء على أرقام بطاقات ائتمان...الخ[103].

المطلب الثاني
حجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني

أولاً: الدليل الرقمي واتصاله بنظام الإثبات الجنائي:

يبدي الفقه والقضاء الجنائيين عادة قلقًا كبيرًا حيال الاثبات باستخدام الأدلة الرقمية خشية عدم تعبيرها عن الحقيقة بالنظر لكم التزييف والتحريف الذي يمكن أن يقع على هذا النوع من الأدلة، الأمر الذي يطعن في مشروعية الدليل كشرط أساسي لمقبوليته في الإثبات وفق الأصول العامة[104].

---

[101] أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، 2015، ص21.

[102] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص22-28.

[103] أحمد يوسف الطحطاوي، المرجع السابق، ص22، مصطفى محمد موسى، أساليب إجرامية للتقنية الرقمية (ماهيتها ومكافحتها)، دار الكتب القانونية، 2005، ص 56، يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، 2011، ص76، د. جمال براهيمي، المرجع السابق، ص132 وما بعدها.

[104] راجع لمزيد من التفصيل، د. عبد الرءوف مهدي المرجع السابق، ص1671 وما بعدها، د. أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، 1993-1994، د. أحمد ضياء الدين خليل، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه، عين شمس، 1982، د. رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997.

ولا تتفلت الأدلة الرقمية من غطاء المشروعية كباقي الأدلة، بغية تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة[105]. وتتسع وتضيق سلطة القاضي في قبول الدليل في الإثبات بحسب النظام الذي ينتمي إليه القاضي، هل يتبع نظام الأدلة القانونية، أم نظام حرية الإثبات[106].

وعليه تختلف طريقة الاعتراف بالدليل الرقمي في الإثبات من دولة لأخرى بحسب طبيعة نظام الإثبات السائد فيها[107]، ففي نظام الإثبات المقيد يحدد المشرع الأدلة المقبولة ويحدد شروط قبولها وقوتها الإقناعية، فليس للقاضي من دور في تقدير الدليل، سوى مجرد التحقق من الشروط التي تطلبها المشرع[108]، وهو الأمر الذي يفقد القاضي عمله الرئيس وهو الحكم بناءً على الاقتناع وفقًا لضميره، وهو ما تسبب في تراجع العمل به حتى في دولته المؤسسة له – أي بريطانيا – واصبح للقاضي أي يستخلص الحقيقة من اي دليل ولو لم يكن منصوصًا عليه قانونًا وفق قاعدة الإدانة دون أدنى شك، وهو ما اتبعه كذلك القضاء الأمريكي وفق قاعدة الدليل الأفضل[109]، التي تعطي للقاضي سلطة تقديرية في قبول نسخ أو صور الدليل الأصلي في حالة عدم توافر هذا الأخير (أي الدليل الأصلي) أو فقدانه.

وهكذا ساد وتوسع – لاسيما في جل التشريعات الأوروبية والعربية – نظام الاثبات الحر، القائم على ألا يحدد المشرع طرقًا معينة للإثبات ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجنائي، صاحب الدور الإيجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب قناعته الذاتية[110]، ويقتصر دور المشرع على بيان الشروط القانونية المتطلبة في الدليل، منعًا للشطط في قبول الأدلة[111]، مع الأخذ أحيانًا وفي نطاق محدود بنظام الأدلة القانونية، ليصير النظام نظامًا مختلطًا في الإثبات الجنائي، وهو وضع القانون المصري والياباني والشيلي[112].

وهكذا لم يعد يقيد قبول الأدلة الرقمية في الإثبات الجنائي سوى أن تكون حصلت بطرق مشروعة وفق الأصول القانونية[113]، مع خضوع الدليل لمبدأ الاقتناع الذاتي للقاضي الجنائي.

---

[105] د. هلالي عبد اللاه أحمد، حجية المخرجات الكومبيوترية في المواد الجنائية، المرجع السابق، ص 104.

[106] *R. Merle et A. Vitu, Traité de droit criminel, T. II, Procédure pénale, 1979, n°925 et s.*

د. عبد الرءوف مهدي المرجع السابق، ص*1649* وما بعدها.

[107] د. رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، 1997، ص85، سامي جلال فقي 2011، ص81. القانونية، كتب دار الإثبات، في وحجيتها الحاسب من المتحصلة حسين، الأدلة

[108] د. هلالي عبد اللاه أحمد، حجية المخرجات الكومبيوترية في المواد الجنائية، المرجع السابق، ص 91، سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب، المرجع السابق، ص82.

[109] *J. Stephen et autre, La preuve en procédure pénale comparée, Rapport de synthèse pour les pays de Common Law, AIDP., 1992, p 33.*

سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، المرجع السابق، ص303.

[110] د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، المرجع السابق، ص373-379.

[111] أحمد يوسف الطحطاوي، المرجع السابق، ص 195، سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب، المرجع السابق، ص 93.

[112] د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص143 وما بعدها.

[113] *J.-R. Demarchi, La loyauté de la preuve en procédure pénale, outil transnational de protection du justiciable, Recueil Dalloz, 2007, p.2012.*

د. رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، 2004، ص154.

وعليه، لا يجوز للقاضي قبول دليل رقمي دون مراعاة الشروط الشكلية والموضوعية للإذن بالتفتيش الإلكتروني مثلاً، أو كان قد تحصل بإكراه المتهم المعلوماتي على فك شفرة أو الإفصاح عن كلمة السر اللازمة للدخول إلى الملفات المخزنة داخل النظم المعلوماتية، أو القيام بإجراء التصنت أو المراقبة الإلكترونية عن بعد دون مسوغ قانوني[114].

ثانيًا: حجية الدليل الرقمي أمام القاضي الجنائي:

يثار التساؤل حول القوة التدليلية للدليل الرقمي في الدعاوى الجنائية، أي ما قوته في كشف الحقيقة، ومدى صدقيته على نسبة الفعل للمتهم[115].

ومسألة تقييم الدليل هي مسألة موضوعية محضة تدخل في صميم سلطة القاضي التقديرية بحثا عن الحقيقة. والسائد بالنسبة للأدلة التقليدية من اعتراف أو شهادة شهود أو قرائن...الخ أن سلطة القاضي الجنائي في تقدير الدليل يحكمها مبدأ حرية القاضي في تكوين عقيدته، فهل ينطبق ذلك على الدليل الرقمي؟[116].

من المؤكد والمشاهد هو ضعف القاضي الجنائي من حيث الكفاءة الفنية والمعرفة في المجال المعلوماتي، لاسيما وأنه مجال تتطور فيه التقنية بشكل متسارع، وأمام ذلك يتعذر على القاضي الجنائي إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، فضلا عن تمتع هذا الدليل في قوته التدليلية بقيمة في الإثبات قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، إلى جانب الطبيعة الفنية الخاصة بالدليل الرقمي والتي تمكن من العبث بمضمونه بسهولة على نحو يقبل تغيير حقيقته، دون أن يدرك ذلك سوى ذوي الخبرة الفنية[117].

وهنا يطرح التساؤل، ما سلطة القاضي الجنائي تجاه الدليل الرقمي؟، وهل له من دور في تقدير صدقيته وقياس قوته التدليلية؟، وهل له حق رفضه بحكم عدم قناعته به؟[118]

إن الإجابة على هذا التساؤل يوجب على القاضي في البدء التيقن من توافر الشروط التي تمنح باجتماعها الدليل الرقمي حجية في الإثبات الجنائي، وأهمها على الإطلاق شرط اليقينية.

إذ يلزم أن يتحقق القاضي المطروح أمامه الدليل الرقمي من أنه غير قابل للشك وليس دليلًا مرجوحًا عندما يتجه إلى هدم مبدأ أصل البراءة، فهذا الأخير لا يهدمه إلا إدانة جازمة مبنية على أدلة لا يتسرب إليها الظن والاحتمال.

والمبدأ إذا هو افتراض أصالة الدليل الرقمي ومن ثم القناعة اليقينية به، تلك القناعة المدركة بالحواس وفق التصورات الإنسانية والخبرة التي تتشكل في وجدان وعقل القاضي عبر سنوات عمله بالمحاكم المختلفة، وهو الأمر المعتمد في

---

[114] علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، 2009، ص4. بحث منشور على الرابط: *www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc*

[115] ياسر محمد الكومي محمود أبو حطب، المرجع السابق. ص303.

[116] د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص13.

[117] د. جمال براهيمي، المرجع السابق، ص151، أحمد يوسف الطحطاوي، المرجع السابق، ص233.

[118] لمزيد من التفصيل، د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية، المرجع السابق، ص135 وما بعدها، محمد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، الكويت، ع2، س36، يونيو 2012، ص552 وما بعدها.

القضاء الأمريكي وفقًا لقانون الحاسب الآلي لولاية أيوا الصادر في عام 1984 وقانون الإثبات لولاية كاليفورنيا لعام في 1983، حيث تعتبر النسخ المستخرجة من البيانات التي يحتويها الحاسب من أفضل الأدلة المتاحة للإثبات وأكثرها يقينية[119]. وعليه أكدت المحكمة العليا الأمريكية في قضية*United States v. Russo* في عام 1974 حينما قضت أنه مع افتراض استخدام حاسب يؤدي وظائفه بشكل سليم، ومع توافر الثقة فيه وإمكانية التعويل عليه، فان مخرجاته يجب أن تكون مقبولة كدليل على المعاملات التي أدخلت فيه[120].

كذلك نص قانون الإثبات الأمريكي في المادة 3/1001 على أنه إذا كانت البيانات مخزنة في حاسب أو آلة مشابهة فان أية مخرجات طابعة منها أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقًا للبيانات تعد بيانات أصلية. وتضيف المادة 5/1500 من قانون الإثبات لولاية كاليفورنيا لعام 1983 بأن المعلومات المسجلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيهما، يجب ألا توصف أو تعامل على أنها غير مقبولة بمقتضى قاعدة فضل دليل[121].

وعلى ذات المنوال سار المشرع ين الإنجليزي والياباني بقبولهما ضمن أدلة الإثبات مخرجات الحاسب الآلي التي تم تحويلها إلى صور مرئية، سواء أكانت هي الأصل أم كانت نسخًا مستخرجة عن هذا الأصل[122]. أما المشرع الألماني فقد جعل من خلال المادة (224) فقرة ثانية من قانون الإجراءات الجنائية مخرجات الحاسب الآلي بأنواعها المختلفة من بيانات أو مطبوعات أو نسخ من قبيل المصادر التي يجب على المحكمة تقبلها في الإثبات .وهو الشيء نفسه الذي تبناه المشرع اليوناني في المادة 364 من قانون الإجراءات الجنائية.

ولا يعود هذا القبول للدليل الرقمي والإقرار بحجيته إلا للتسليم بمنطق افتراض الأصالة في الدليل الرقمي، والناشئة عن الطابع العلمي لهذا النوع من الأدلة، والذي يبقيه في مكانه الذي تم استخلاصه منه رغم حذفه من النظام المعلوماتي بالحاسب الآلي أو شبكة المعلومات.

وللقاضي المزود ببعض المعارف التقنية أن يلجأ إلى استخدام عدة وسائل للتحقق من سلامة الدليل الرقمي وعدم تغييره أو تحريف، ومن ثم النيل من أصالته ويقينيته، منها[123]:

---

[119] ياسر محمد الكومي محمود أبو حطب، المرجع السابق، ص305، رشيدة بوكر، المرجع السابق، ص497.

[120] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص182.

[121] د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، 1999، الطبعة الأولى، ص1.

[122] *B. Amory et Y. Poullet, Le droit de la preuve face à l'informatique et la télématique, RIDC., n°2, Avril 1985, p.339.*

[123] *D. Ammar, Preuve et vraisemblance, contribution à l'étude de la preuve technologique, RTD. Civ, juillet-septembre, 1993, p.499.*

د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص27، ممدوح عبد الحميد عبد المطلب وزبيدة محمد قاسم عبد العزيز، الله عبد وعبد جاسم محمد، المرجع السابق، ص2246-2247، رشيدة بوكر، المرجع السابق، ص501، أحمد يوسف الطحطاوي، المرجع السابق، ص238، جمال براهيمي، المرجع السابق، ص154.

- **تقنية التحليل التناظري الرقمي:** وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم الحكم على النسخ المستخرجة.
- **استخدام عمليات حسابية خاصة تسمى بالخوارزميات:** ويتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الالكتروني أو في حالة ما إذا كان هناك شك في أن العبث قد مسّ النسخة الأصلية.
- **استخدام الدليل المحايد:** وهو نوع من الأدلة الرقمية المخزنة في البيئة الافتراضية ولا علاقة له بموضوع الجريمة، ولكنه يساهم في التحقق من مدى سلامة الدليل وعدم تحريفه.
- **إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لعدة تجارب** بغية التأكد من أنها عرضت كل المعطيات المتعلقة بالدليل الالكتروني وأنها لم تضف إليه نتائج جديدة.

على أنه من المهم التأكيد على أن يقينية الدليل الرقمي وخضوعه لما يخضع له الدليل العلمي لا تعني عدم قابلية سلامته عند التحصل عليه للخطأ، ومثال ذلك الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل، كالخلل في الشفرة المستخدمة، أو استعمال معلومات ومواصفات خاطئة. وإما بسبب الخطأ في استخدام أداة تقل نسبة صوابها 100%، مثل ما يحدث غالبا في وسائل اختزال المعطيات أو معالجتها بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها بها.

ولهذا تنص المادة 69 من قانون الشرطة والإثبات الجنائي البريطاني على أنه لا يكون البيان المتضمن في مستند صادر عن طريق الحاسب مقبولا كدليل على أية واقعة واردة فيه إلا إذا تبين : 1- عدم وجود أسس معقولة لاعتقاد بأن البيان يفتقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب. 2- أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فأي جزء لم يكن يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته[124].

أما عن القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 فقد مال إلى هذا التوجه حين نص في المادة الحادية عشرة من القانون المعنونة: "في الأدلة الرقمية" هذه الحجية حين أكدت على أنه يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الاثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية.

ولكن لم يجب على المشرع المصري على تساؤلنا حول سلطة القاضي الجنائي تجاه الأدلة الرقمية، هل تخضع لما تخضع له الأدلة الجنائية المادية من حيث مبدأ حرية القاضي الجنائي في تكوين عقيديته؟

[124] *J.-F. Casile, Plaidoyer en faveur d'aménagement de la preuve de l'infraction informatique, RSC., 2004, p.76 et s ; D. Ammar, op.cit., p.500.*

إن الإجابة على هذا التساؤل نراها ترتبط بالطابع العلمي للدليل الرقمي ؛ فهذا الطابع يجب أن يلعب دورًا حاسمًا في الحد من حرية القاضي الجنائي في تكوين عقيدته، فقد أصبح هذا النوع من الأدلة جزءاً من نتاج العلم الموثوق في نظرياته ونتائجه، وهو ما يحتم على القاضي الجنائي قبوله والإقرار بحجته في الإثبات رغم عدم إلمامه بمعارف تقنية المعلومات، دون إعمال للمفاهيم التقليدية لنظامي حرية الإثبات والإثبات المختلط، وهو ما استقر في التطبيق القضائي في أغلب الدولة العملاقة في مجال تقنية المعلومات، كأمريكا وبريطانيا وكندا[125]، وليصبح المعتمد بشأن الدليل الرقمي هو مبدأ الإثبات القانوني المقيد، كحالة جديدة من الحالات المقررة في التشريع المصري، بمقتضاها لا يجب أن ينازع القاضي في قيمة ما يتمتع به الدليل الرقمي من قوة تدليلية تأكدت بقوة العلم، طالما توافرت في الدليل الشروط التي يتطلبها القانون لتحصيله وكان مشروعًا[126].

خاتمة

طفنا خلال صفحات هذا البحث بين جملة من الإشكاليات، فكان البدء ببيان عدم ملائمة القواعد التقليدية للتفتيش مع مستجدات جرائم تقنية المعلومات، فضلاً عن استعراض الصعوبات التي تواجه تنفيذ التفتيش الإلكتروني. ثم عرجنا من بعد على تحليل طبيعة وحجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني، وذلك بهدف بحث حجية هذا النوع من الأدلة في الإثبات الجنائي، وبيان حدود السلطة التي يتمتع بها القاضي حياله، وما إذا كان يخضع شأنه شأن باقي الأدلة الجنائية المادية لمبدا حرية اقتناع القاضي الجنائي في تكوين عقيدته.

---

[125] د. هلالي عبد الإله أحمد، حجية المخرجات، المرجع السابق، ص95.

[126] رشيدة بوكر، المرجع السابق، ص507. وراجع عكس هذا الرأي، علي حسن الطوالبة، مشروعية الدليل المستمد من التفتيش الجنائي، المرجع السابق، ص13. وقد مالت محكمة النقض الفرنسية إلى ترك الحرية كاملة للقاضي الجنائي في تكوين عقيدته بشأن الدليل الرقمي، فقضت بأنه إذا اطمأنت محكمة الموضوع وفقًا لاقتناعها الذاتي والقواعد العامة إلى ما استندت إليه النيابة العامة من قرائن بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة، وقد ثبت ذلك من خلال جهاز آلي التقط صورة السيارة المتجاوزة للسرعة، ودون أن يكون السائق قد سئل فإنها لا تكون ملزمة بتحديد ما استندت إليه من عناصر الواقعة في تبرير اقتناعها. راجع، محمد عبد الشافي إسماعيل، المرجع السابق، ص 166. وراجع في تأييد موقف محكمة النقض الفرنسية، د. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص165-166.

ولقد أحسن المشرع المصري صنعًا حين عجل بإصدار قانون مكافحة جرائم تقنية المعلومات الصادر بالقانون 175 لسنة 2018 بغية تقوية البنية التشريعية في مواجهة هذا النمط الجديد من الإجرام الذي يتلون يومًا بعد يوم، ويتخذ أنماطًا وأشكالاً غاية في الخطورة على المستوى الوطني والدولي، لا سيما وأنه قد استبان لنا خلال هذا البحث صعوبة موائمة النصوص الإجرائية التقليدية مع طبيعة جرائم تقنية المعلومات.

ولقد كان المشرع موفقاً في عدة نقاط في هذا القانون، منها:

- أنه ضَمّن صدر القانون – وفق بنيان أنجلوسكسوني في صياغة التشريعات – تعريفًا لأهم المصطلحات التي يستلزمها التعامل القانوني مع البيئة المعلوماتية (م.1)، وكذلك تحديده لأهم الالتزامات التي تقع على مقدمي الخدمة (م.2) وتحديد المسؤولية الجنائية الواقعة عليهم (الفصل الخامس من القانون م.30–م.33)، وتوسعته للنطاق المكاني الخاص بسريان القانون (م.3)، الأمر الذي يتلاءم بحق مع طبيعة جرائم المعلوماتية، وتصديره القانون بإلزام السلطات المصرية بالتعاون الدولي من تبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات والمساعدة على التحقيق فيها وتتبع مرتكبيها (م.4). وكذلك معالجته لبعض الإشكاليات الإجرائية كتلك المرتبطة بأوامر حجب المواقع الإلكترونية (م.7، م.8)، وأوامر المنع من السفر (م.9)، الذي جعل التظلم من كلا النوعين من الأوامر من اختصاص القضاء الجنائي، ممثلاً في محكمة الجنايات المختصة. ومن ذلك أيضًا إيلاء المشرع اهتمامًا بمسألة الخبرة الفنية التي تحتاجها الكشف عن جرائم تقنية المعلومات وجمع الأدلة عنها وضبط مرتكبيها (م.10).

- حرص المشرع المصري على التضيق على الدليل الرقمي ومنع خروج الدعائم المادية التي تحمله خارج البلاد من خلال إيراده معالجة في المادة التاسعة من القانون للأمر بالمنع من السفر كتدبير تحفظي – وهو أمر يحتاج مراجعة شاملة في القوانين المصرية – قد يمكن سطات التحقيق من ضبط الدليل الرقمي على الإقليم المصري. وهكذا نص المشرع على أنه يجوز للنائب العام أو من يفوضه من المحامين العامين الأول بنيابات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام في ارتكاب أو الشروع في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، أن يأمر بمنع المتهم من السفر خارج البلاد أو بوضع اسمه على قوائم ترقب الوصول بأمر مسبب لمدة محددة. كما أجاز المشرع لمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال خمسة عشر يومًا من تاريخ علمه به، فإذا رفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم. وفى جميع الأحوال ينتهى المنع من السفر بمرور سنه من تاريخ صدور الأمر، أو بصدور قرار بأن لا وجه لإقامة الدعوى الجنائية أو بصدور قرار نهائي فيها بالبراءة أيهما أقرب.

يضاف إلى ذلك أنه كان يحدونا الأمل في مزيد من الفاعلية في مواجهة هذه الجرائم من خلال أن يُضَمن المشرع هذا القانون بعض الأحكام، والتي من بينها على الأخص:

1. كان يفضل أن يكون امتداد الاختصاص المنصوص عليه ضمنًا في المادة السادسة من قانون مكافحة جرائم تقنية المعلومات مقيداً بوجود أمارات قوية، أو توافر حالة ضرورة، على أن البيانات المتصلة بالجريمة مخزنة في نظام تقنية معلومات 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، كي يسمح بمد الدخول والتفتيش إلى النظام الآخر، على نحو ما جاءت صيغة المادة 15 من القانون البحريني رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات.
2. كان يحسن ألا تأتي صياغة الفقرة الأولى من المادة السابعة من القانون 175 لسنة 2018 الواردة في شأن الإجراءات والقرارات الصادرة بشأن حجب المواقع، بما يجعل صدور قرار سلطة التحقيق بهذا الحجب رهنًا بارتكاب ما يعد جريمة من الجرائم المنصوص عليها في القانون إلى جانب أن تشكل الجريمة المرتكبة تهديدًا للأمن القومي أو تعريض أمن البلاد أو اقتصادها القومي للخطر. وهذا الربط لاشك من شأنه أن يعطل جهود سلطات التحقيق في مواجهة جرائم تقنية المعلومات. ولهذا فمن الأفضل حذف عبارة: "وتشكل تهديداً للأمن القومي أو تعرض أمن البلاد أو اقتصادها القومي للخطر"، بحيث تصبح سلطة التحقيق في سعة وأن يكون لها أن تأمر بحجب أي موقع إلكتروني توافرت أدلة على بثه أي عبارات أو أرقام أو صور أو أفلام أو أية مواد دعائية، أو ما في حكمها مما يعد جريمة من الجرائم المنصوص عليها بالقانون، ولو لم تكن الجريمة المرتكبة تشكل تهديداً للأمن القومي أو تعرض أمن البلاد أو اقتصادها القومي للخطر. فقد يصعب ربط بث موقع للعبة قتالية نبه الخبراء إلى خطورتها في رفع مستوى العدوانية عند الشباب بأي من الأمور المذكورة في الفقرة محل هذا النقد.
3. وفي ذات السياق، كان من الأفضل ألا يجعل المشرع قرار سلطة التحقيق بالحجب رهنًا بأن يكون ذلك ممكناً فنيًا (الفقرة الأولى من المادة السابعة أيضًا)، ففضلاً عن أن تحديد القدرة الفنية لهذا الأمر قد يأخذ وقتًا، الأمر الذي يضعف من سرعة المواجهة، فإن الأمر الصادر بالحجب ولو لم يكن تنفيذه ممكنًا فنيًا من شأنه أن يرفع مستوى الوقاية لدى الجمهور تحول بين فئة وبين انخراطهم في التعامل مع الموقع المقصود بالحجب، الأمر الذي من شأنه أن يسهم في تحقيق الردع العام والردع الخاص معًا.
4. كان لزامًا جعل الأمر بحجب المواقع مرهوناً بتوافر أدلة تتسم بالكفاية على جدية الاتهام – لا مطلق الأدلة كما هي الصياغة الحالية للفقرة الأولى من المادة السابعة – وذلك مثلماً فعل المشرع – وحسنًا فعل –بشأن الأمر بالمنع من السفر (م.9)، نظرًا لخطورة هذا الأمر ومساسه بالحق الدستوري المقرر للإنسان في حرية التعبير عن الرأي بكافة الوسائل (م.65 من دستور 2014) وحقه في تداول المعلومات عبر وسائط الإعلام الرقمي (م.70 من الدستور).
5. ضرورة الاعتراف الوجوبي بالمسؤولية الجنائية المباشرة للشخص الاعتباري، وإخضاعه لعقوبات ذات طبيعة جنائية، وبخاصة الغرامات الجنائية، في كل مرة ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون باسم ولحساب هذا الشخص. ذلك أن المشرع جعل مسؤولية الشخص الاعتباري جوازية، وأقرب إلى أن تكون تابعة لمسؤولية المسؤول عن الإدارة الفعلية للشخص الاعتباري إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقاً لمصلحة له أو لغيره، وليس من بين العقوبات الجائز توقيعها الغرامات، إذ قصر الأمر على

السماح للمحكمة – وفق سلطتها التقديرية – أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، كما أن لها في حاله العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري (م.36).

6. يتعين أن يقر المشرع مبدأ أصالة الدليل الرقمي الناشئ عن طابعه العلمي، ومن ثم يقينية هذا النوع من الأدلة بحيث تحد حرية القاضي الجنائي في تكوين عقيدية إزاءها، وليصبح الأمر حيالها أقرب لنظام الإثبات القانوني المقيد، ولتنحصر سلطة القاضي إذا ما عرض عليه دليل رقمي فقط في التحقق من استخلاصه بطرق مشروعة، وهو ما يستوجب تعديل المادة 11 من القانون.
7. أنه كان من المرجوح جعل الإبلاغ عن الجرائم الإلكترونية وجوبيًا مع فرضة غرامة جنائية عند الإخلال بهذا الالتزام، والأفضل الاستعانة بالتدابير الإدارية في هذا الشأن لتحفيز الضحايا على الإبلاغ عن الجرائم الإلكترونية.

وفي الختام نقول، إن فاعلية قانون مكافحة جرائم تقنية المعلومات ليس رهنًا فقط بسلامته التشريعية في بنيانه، بل في الحقيقة بإنفاذ أحكامه على أرض الواقع، وهو ما يوجب رفع كفاءة أعضاء سلطات الضبط والتحقيق المنخرطين في مهمة مكافحة هذا النوع من الجرائم. هذا بالإضافة إلى تيسير سبل تواصل ضحايا الإجرام المعلوماتي مع الأجهزة المختصة، من خلال النشر الكافي على الجمهور لخطوات الإبلاغ والوقاية من الجرائم من هذا النوع.

قائمة المراجع

(ذكرت الأسماء مع حفظ الألقاب)

أولاً: المراجع باللغة العربية:

- **أحمد بن أزيد جوهر الحسن المهندي، تفتيش الحاسب الآلي وضمانات المتهم، رسالة ماجستير، جامعة القاهرة، 2009.**
- **أحمد سعد مُحَمَّد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، 2012.**
- **أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، بدون تاريخ.**
- **أحمد ضياء الدين مُحَمَّد خليل، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه، عين شمس، 1982.**
- **أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، 2015.**
- **أرسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، في 19–20 يونيو 2007، ص113.**
- **أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت ـ دراسة تحليلية مقارنة، ط1، دار وائل للنشر ـ عمان، 2000.**
- **إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، 2000، ص11.**
- **أمير يوسف فرج، الجرائم المعلوماتية على شبكة الإنترنت، ط1، دار المطبوعات الجامعية، 2008.**
- **باسل أحمد عبد المحسن مُحَمَّد لطفي، دور القاضي المستعجل في وقف الاعتداءات الجنائية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، 2010.**

- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، 2011.
- جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2018.
- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 1992.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002.
- حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، 2017.
- حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013، ص720.
- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2000.
- حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، جامعة عين الشمس، 2005.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009.
- خالد ممدوح إبراهيم، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور على الرابط التالي:
http://Kenanaonline.com/users/KhaledMamdouh/posts/79345
- رشاد خالد عمر، المشاكل القانونية الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، 2013.
- رشيدة بوكر، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، 2012.
- رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، القاهرة، 2004.
- رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، 1997.
- سامي الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، عين شمس، 1972.
- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار كتب القانونية، 2011.
- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، ط1، دار النهضة العربية، 1999.
- طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا بطرابلس، 28-29 أكتوبر 2009.
- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد 22، ع86، مركز بحوث الشرطة، الشارقة، 2013.
- عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، 2019-2020.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، 2002.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006.
- عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائي والمقارن، رسالة ماجستير، جامعة العقيد الحاج لخضر، باتنة، الجزائر، 2011-2012.
- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، 2005.

- عبده مُحَمَّد بحر، معوقات التحقيق في جرائم الإنترنت، رسالة ماجستير، قسم العلوم الشرطية، كلية الدارسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999.
- عفيفي كمال عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط2، منشورات الحلبي القانونية، 2007.
- علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، 2009، ص4. بحث منشور على الرابط: ***www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc***
- علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، ط1، البحرين، بدون دار نشر، 2010.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، 1997.
- على محمود على حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، 26 الى 28 أبريل 2003.
- عمر مُحَمَّد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ط1، دار النهضة العربية، 2004.
- عمر مُحَمَّد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، ط1، 2004 . 2005.
- عمر مُحَمَّد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت، بحث مقدم إلى ندوة الدليل الرقمي، جامعة الدول العربية، القاهرة، من 5 إلى 8 مارس 2006.
- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، جامعة الدول العربية، الفترة من 26–27 أبريل 2008.
- غنام مُحَمَّد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والإنترنت، الإمارات، مايو 2000.
- غنام مُحَمَّد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، 2013.
- فايز مُحَمَّد أرجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، رسالة دكتوراه، جامعة الجزائر 1، 2011.
- مُحَمَّد أحمد المنشاوي، سلطة القاضي الجنائي في تقدير الدليل الإلكتروني، مجلة الحقوق، الكويت، ع2، س36، يونيو 2012.
- مُحَمَّد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، ط 3، كلية الشريعة والقانون، جامعة الإمارات، الفترة من 1 إلى 3 مايو 2004.
- مُحَمَّد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت، بحث مقدم إلى الحلقة العلمية "الانترنت والإرهاب"، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، دبي، من 15 إلى 19 نوفمبر 2008.
- مُحَمَّد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، 2004.
- مُحَمَّد حسام محمود لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.
- مُحَمَّد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة ، ط1 ، دار وائل للنشر، عمان، 2002.
- مُحَمَّد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، دار النهضة العربية، 1998.
- مُحَمَّد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، 2006.
- مُحَمَّد قدري حسن عبد الرحمن، جرائم الاحتيال الإلكتروني، مجلة الفكر الشرطي، ع79، مركز بحوث الشرطة، الشارقة، أكتوبر 2011.

- محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، 2017.
- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005.
- محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، ج2، التفتيش والضبط، 1978.
- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1998.
- مصطفى محمد موسى، أساليب إجرامية للتقنية الرقمية، ماهيتها ومكافحتها، دار الكتب القانونية، 2005.
- مصطفي محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، 2009.
- مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، بحث مقدم إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد بين 23-2012/9/25.
- ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، 2000.
- ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، 2006.
- ممدوح عبد الحميد عبد المطلب وزبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، دبي، من 10-12 مايو *2003*.
- موسى مسعود أرحومة، السياسة الجنائية في مواجهة جرائم الإنترنت، مجلة دراسات قانونية، جامعة قاريونس، ع17، ص80.
- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا ـ طرابلس، الفترة 28 ـ 2009/10/29.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات ـ دراسة مقارنة، دار الفكر الجامعي، 2013.
- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، 2008.
- نورة طرشي، مكافحة الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر 1، 2011.
- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، 1994.
- هشام محمد فريد رستم، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني – واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، كلية الشريعة والقانون، ط3، المجلد الثاني، 3 مايو 2000، ص435.
- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ـ دراسة مقارنة، ط1، دار النهضة العربية، 1997، ط.2006.
- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، 2003.
- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)، ط1، دار النهضة العربية، 2006.
- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)، ط1، دار النهضة العربية، 2006.
- يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، 2011.

- يونس عرب، جرائم الكمبيوتر والإنترنت، اتحاد المصارف، 2001.

ثانيًا: المراجع باللغة الأجنبية:

- ***M. Alexander, Computer Crime, Computer World, vol. XXIV, n°11,1990, p.104.***
- ***D. Ammar, Preuve et vraisemblance, contribution à l'étude de la preuve technologique, RTD. Civ, juillet-septembre, 1993, p.499.***
- ***B. Amory et Y. Poullet, Le droit de la preuve face à l'informatique et la télématique, RIDC., n°2, Avril 1985, p.335.***
- ***R. Boos, La lutte contre la cybercriminalité au regard de l'action des Etats, th. Lorraine, 2016.***
- ***J. Bossan, Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC., n°2, 2013, pp. 295-319.***
- ***J. Bourguignon, La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat, article présenté au Colloque de Rouen sur «Internet et droit international», organisé par La Société Française pour le Droit International du 30 mai au 1 juin 2013, Pedone, Paris, 2014, p.368.***
- ***J.-F. Casile, Plaidoyer en faveur d'aménagement de la preuve de l'infraction informatique, RSC., 2004, p.76.***
- ***M. Chawki, Essai sur la notion de cybercriminalité, IEHE, Lyon, 2006.***
- ***M. Chawki, Combattre la cybercriminalité, éd. de Saint-Amans, Paris, 2008.***
- ***M. Clément-Fontaine, Définition et cadre juridique de la preuve numérique, in, Colloque sur La preuve numérique à l'épreuve du litige, Les acteurs de litige à la preuve numérique, organisée par la Compagnie Nationale des Experts de Justice en Informatique et Associées, le 13-04-2010, sur le site : www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf.***
- ***Conseil de L'Europe, La criminalité informatique, Recommandation n°R(89) sur la criminalité en relation avec l'ordinateur et rapport final du comité Européen pour les problèmes criminels, Strasbourg, Conseil de l'Europe, 1990, pp.94-96.***
- ***J.-R. Demarchi, La loyauté de la preuve en procédure pénale, outil transnational de protection du justiciable, Recueil Dalloz, 2007.***
- ***A. Diop, Procédures pénales et TIC., p.25, sur le site : http ://196.1.99.9/moodle/mod/book/print.php?id=106***
- ***F. Fourment, Procédure pénale, la perquisition du disque d'un ordinateur à chaud, CPU., Paris, 2004.***
- ***A. Georgo, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Roumanie, RIDP., 1993, p.551.***
- ***P. Glineur, Droit et Ethique de l'Informatique, Story Scientia, Bruxelles, 1991.***
- ***P. Lacoste, Les métiers de l'intelligence économique, Défense Nationale, Paris, 2006, p.144.***
- ***M. Linglet, Délinquance informatique, sur le front de la nouvelle criminalité, une parade concerné, RIPC., mai 1995, p.182.***
- ***A. Lucas et J. Deveze, Le droit de l'informatique et de l'internet, PUF. Paris, 2001.***
- ***D. Martin, et F. P Martin, Cybercrime , Paris, PUF., 2001, p.75.***

- *Y. Masuada, The Information Technology Revolution, Oxford Blackwell, Oxford, 1985.*
- *C. Meier Marsella, L'effectivité du processus répressif dans le traitement de la cybercriminalité, enquête sur le système juridique français, th. Paris II, 2005.*
- *J.-P. Mignard, Cybercriminalité et cyber répression entre désordre et harmonisation mondiale, th. Paris 1, 2004.*
- *R. Merle et A. Vitu, Traité de droit criminel, T. II, Procédure pénale, 1979.*
- *C. Meunier, La loi du 28 novembre 2000 relative à la criminalité informatique, Formation Permanente CUP, février 2001, n°103.*
- *Y. Padova, Un aperçu de la lutte contre la cybercriminalité en France, RSC., n°4, octobre-décembre, 2002, p.765.*
- *D. B. Parker, Combattre la criminalité informatique, OROS., Paris, 1985.*
- *D. B. Parker, Figting Computer Crime, ''A new Framework for Protecting Information'', Joh Wiley and sons, 1998.*
- *M. Quemener, Conseil de l'Europe et lutte contre la cybercriminalité, Revue Expertises des systèmes d'information, n°347, mai 2010, p.170.*
- *M. Quemener et F. Dalle, L'accès à la preuve numérique, enjeu majeur de toute enquête pénale: pratique et perspectives, Dalloz IP/IT, n°7-8, 2018, pp. 418-424.*
- *M. Quener et J. Ferry, Cybercriminalité, défi mondial, 2ème éd. Economica, Paris, 2009.*
- *U. Sieber, The international Handbook on Computer Crime ''Computer related Economic Crime and the infringements of privacy'', John Wiley and Sons, 1986*
- *J. Stephen et autre, La preuve en procédure pénale comparée, Rapport de synthèse pour les pays de Common Law, AIDP., 1992.*
- *K. Tiedemann, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, RDPC., n°7, Bruxelles, 1984, p.61.*
- *D. Thompson, Current trends, in Computer control crime, Computer Quarterly, vol. 9, n°1, 1991, p.2.*
- *R. Totty & A. Hardcastle, Computer-Related Crime in Information Technology and the Law, Macmilla Publishers, U.K. 1986, p.26.*
- *P. Vergucht, La répression des délits informatiques dans une perspective internationale, th. Montpellier 1, 1996.*
- *D. Wall, Crime and the Internet, Routledge, N.Y, 2001.*
- *M. Wasik, Crime and The Computer, Oxford University Press, 1991.*

فهرست الموضوعات

طبيعة وحجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني

تقسيم: .....

المطلب الأول
الطبيعة القانونية للدليل الرقمي

تقسيم: .....
أولاً: ماهية الدليل الرقمي:.....
ثانيًا: الأدلة الرقمية المقبولة في الإثبات الجنائي: .....

المطلب الثاني
حجية الدليل الرقمي المتحصل عن التفتيش الإلكتروني

أولاً: الدليل الرقمي واتصاله بنظام الإثبات الجنائي: .....
ثانيًا: حجية الدليل الرقمي أمام القاضي الجنائي: .....
- خاتمة: .....
- قائمة المراجع: .....
- فهرست الموضوعات: .....

"اللهم اجعل هذا العمل خالصًا لوجهك الكريم"