ذاتية الضوابط الإجرائية للأدلة الجنائية الرقمية في الأنظمة القانونية ذات الأصل اللاتيني والأنجلوأمريكي

الدكتورة

ميادة مصطفى محمد المحروقي

مدرس القانون الجنائي

المعهد العالي للعلوم التجارية بالمحلة الكبرى

أستاذ مساعد بكليات الشرق بالمملكة العربية السعودية (سابقاً)

2019 م

المقدمة

موضوع البحث:

أسفرت التطورات السريعة في مجال تكنولوجيا المعلومات عن تغيرات اقتصادية واجتماعية لم يسبق لها مثيل في مختلف فئات وقطاعات المجتمع، بل وأدت سهولة الولوج إلى المعلومات والبيانات واستخدام إمكانات غير محدودة في تبادلها، إلى حدوث نمو هائل في حجم المعلومات المتبادلة والعابرة لكافة الحدود الجغرافية. في المقابل صاحبت تلك التطورات انعكاسات سلبية لا حد لها جراء سوء استخدام البيئة التقنية، وهو ما نتج عنه استحداث أنواع جديدة من الجرائم التي تنبئ عن خطورة مرتكبيها، ألا وهي جرائم تقنية المعلومات.[1]

لذا كان الإهتمام بمكافحة جرائم تقنية المعلومات ضرورياً، كون الواقع الذي نلمسه اليوم في ظل ثورة المعلومات الهائلة يحتم علينا أن نعمل سوياً للحاق بهذه الثورة العلمية، وأن نكون على استعداد لمواجهتها بشتى الطرق. ولعل أبرز دور في مكافحة تلك الجرائم، هو تطور تقنيات الأدلة الجنائية الرقمية، فعن طريق تلك التقنيات يستطيع الباحثون اكتشاف خيوط الأدلة لمعرفة هذه الجرائم وتتبع مرتكبيها؛ حيث يبرز دور الأدلة الرقمية وحجيتها عندما تقف الأدلة التقليدية عاجزة عن إثبات الجرائم الإلكترونية ذات الطبيعة الخاصة والتي تعتمد في أغلبها على التضليل والخداع ولا تترك أثراً مادياً ملموساً يمكن التعامل معه.

وتتحدى المفاهيم القانونية القائمة وتتسارع في مواكبة التطورات التكنولوجية التي باتت تهدد المصالح المشروعة وتنتج العديد من الجرائم المعقدة. ومع ذلك تثير جرائم التقنية العديد من الإشكاليات في نطاق قوانين الإجراءات الجنائية التي وضعت نصوصه لتحكم الإجراءات المتعلقة بالجرائم التقليدية سواء في مرحلة الاستدلالات أو التحقيق أو الإثبات

---

[1] عرف وزارة العدل الأمريكية جرائم الكمبيوتر بأنها "مخالفة القانون الجنائي التي تتضمن معرفة بتقنية الكمبيوتر في ارتكابها أو في التحقيق فيها أو الاتهام بها". انظر:

- Alex Cameron, Fundamentals of Electronic Evidence and Discovery (Lexisnexis, forthcoming April 2010).
- See also: Alexander Galicki; Drew Havens; Alden Pelker, Computer Crimes, 51 Am. Crim. L. Rev. 875 (2014), p. 883.

أمام المحكمة والتي باتت تتباين مع الجرائم التي ترتكب في العالم الافتراضي، الأمر الذي يشكل تحدياً دائماً سواء فيما يتعلق بصلاحية الإجراءات الجنائية التقليدية في إثبات جريمة ارتكبت في بيئة تقنية افتراضية، أو فيما يتعلق بالتزام تلك الإجراءات بمتطلبات الشرعية في سبيل إثبات جرائم التقنية الحديثة.

أهمية البحث:

أثبتت وسائل الاتصالات الرقمية جدارتها في تسهيل مهام الحياة بشكل كبير، وفي المقابل قد يتم إساءة استخدامها بخلاف الغاية المبتغاه منها، وينتج عنها أدلة قد تكون ذات علاقة بالمحاكمات الجنائية. فالاهتمام الذي يحظى به الدليل الرقمي مقارنة بغيره من الأدلة الأخرى؛ مرده انتشار استخدام وسائل تقنية المعلومات، والتي تعاظم دورها في ظل الاتجاه نحو العصر الرقمي. وهذا لا يعني أن الدليل الرقمي ترتبط أهميته بإثبات الجرائم الإلكترونية فحسب، بل تمتد أهميته ودوره في إثبات الجرائم التقليدية كالسرقة أو النصب أو التزوير باستخدام آداة إلكترونية كالحاسب الآلي أو جهاز الهاتف الخلوي. وعلى النقيض فالجرائم المعلوماتية يمكن إثباتها بوسائل الإثبات التقليدية كالشهادة أو الاعتراف.

وفي ظل هذه المعطيات تتجلى أهمية البحث من خلال تسليط الضوء على بيان ذاتية الأدلة الجنائية الرقمية المصاحبة للجرائم المعلوماتية في ظل ما تشهده الساحة المعلوماتية من زيادة مضطردة في تلك الجرائم التي تخلف ورائها أثاراً لا حد لها، إضافة إلى دراسة مدى مواءمة التدابير الإجرائية ومشروعيتها في البيئة التكنولوجية، والتحديات التى تواجهها تلك الإجراءات للحفاظ على الدليل الرقمي كدليل إثبات في الجرائم الجنائية. وكون تلك التحديات تتوافق ومتطلبات إنفاذ القانون مع حماية حقوق الإنسان والحريات.

إشكاليات البحث وتساؤلاته:

نظراً للطبيعة الخاصة التي تفرضها البيئة الإلكترونية وما ينتج عنها من جرائم، لاسيما وأنها أفرزت تحديات هامة للقوانين الوضعية واصطدامها مع مبدأ الشرعية الجنائية. ولكون الدليل الرقمي يتمتع بصفة الحداثة كونه ذا طبيعة خاصة من حيث الوسط الذي ينتج عنه والطبيعة التي يبدو عليها، الأمر الذي يثير العديد من التساؤلات التي تتعلق بمشروعية الأخذ به والاستناد إليه في الإثبات الجنائي، فمشروعية الدليل دائماً ترتبط بوجوده وطريقة الحصول عليه. ولعل هذا ما يثير الأمر أهمية، حيث أن مشروعية وجوده تستلزم أن يكون

المشرع قد قبله ضمن أدلة الإثبات الجنائي، أما مشروعية الحصول عليه فتقتضي أن يتم الحصول عليه وفق إجراءات قانونية مشروعة، وإذا ما نظرنا إلى طبيعة الدليل الرقمي والوسط المستمد منه، لوجدنا العديد من الإشكاليات التي تتعلق بالوسط الافتراضي الذي يتم فيه البحث والتفتيش عن الدليل وضبطه بما يتفق مع الأصول المقررة في القانون، كذلك صفة الشخص المخول له سلطة تفتيش وضبط الدليل.

يضاف إلى ذلك مدى قبول الدليل الرقمي في الإثبات ومدي يقينية تلك الأدلة في تأثيرها على اقتناع القاضي، لاسيما مع توقع العبث بتلك الأدلة وتخريبها مما يجعلها مخالفة للحقيقة. وبناء على ذلك فتكمن إشكالية البحث في الإجابة على عدة تساؤلات رئيسة من بينها، ما الدليل الرقمي وكيف تنوعت أشكاله التي باتت في زيادة مضطرده؟ كيف يمكن استخلاص الدليل الرقمي من أماكن تواجده وتحليله جنائياً؟ ولماذا تميزت الضوابط الإجرائية المتعلقة بالكشف عن الدليل الرقمي بذاتية وخصوصية عن غيرها من الضوابط العامة في نظم الإجراءات الجنائية؟ وهل تراعي تلك الضوابط الخاصة مبدأ الشرعية الجنائية الإجرائية بما يتوافق مع متطلبات الحفاظ على حقوق وحريات الأفراد؟ وما المعايير التي يعتمدها القاضي في سبيل بناء قناعته بالدليل المقدم للمحكمة؟ وهل للدليل الرقمي حجية في الإثبات أمام القاضي في جميع الأحوال؟ وهل يمكن استبعاد تلك الأدلة، وفي حال كانت الإجابة بنعم فما الحالات التي يمكن استبعاد الأدلة الرقمية بشأنها؟

في ضوء ما تقدم تصبو الدراسة إلى الإجابة على التساؤلات محل إشكاليات البحث، كذلك التساؤلات الدقيقة التي يمكن أن تتفرع عنها، في محاولة للوصول إلى حلول مهنية وعلمية تدعم إجراءات العدالة الجنائية في ظل المتغيرات العلمية وتحديات العصر الرقمي.

منهج البحث:

يعتمد البحث على المنهج التأصيلي التحليلي إضافة إلى المنهج المقارن، حيث تركزت الدراسة على تناول ماهية الأدلة الجنائية الرقمية وأماكن وجودها إضافة إلى كيفية التعامل معها واستخلاصها مع عرض وتحليل أهم وأحدث القضايا التي أثيرت بشأنها.

ولأن قانون تقنية المعلومات المصري حديث العهد ولم نجد تطبيقات قضائية خاصة بالإشكاليات التي يثيرها البحث، فقد تمت معالجة موضوع الدراسة بالاستعانة بقوانين مقارنة، على الأخص القانون الأمريكي الذي تناول أغلب الإشكاليات التي أثارها الدليل الرقمي وقام

بالتصدي لها، وهو ما سيتيح لنا الاطلاع على القوانين المقارنة والاجتهادات القضائية فرصة التطرق للسبل التي تبنتها تلك التشريعات في محاولة للاستفادة منها ومعرفة الأسس القانونية التي استندت إليها.

تقسيم البحث:

تحقيقاً للأهداف المنشودة من الدراسة، ولبحث أهم الإشكاليات القانونية التي يثيرها الدليل الرقمي وعلاقته بالإثبات الجنائي، فقد تم تقسيم البحث على النحو التالي:

المبحث التمهيدي: ماهية الدليل الرقمي وطرق تحليله جنائياً.

المطلب الأول: مفهوم الدليل الرقمي وأنواعه

المطلب الثاني: البحث عن الدليل الرقمي تمهيداً لتحليله جنائياً

الفصل الأول: ذاتية البحث عن الدليل الرقمي في مرحلة جمع الاستدلالات

المبحث الأول: مجالات الاستدلالات من جانب مأمور الضبط القضائي لضبط الدليل الرقمي من شبكة الإنترنت.

المبحث الثاني: دور مقدم الخدمة في مرحلة جمع الاستدلالات

المبحث الثالث: الحق في الخصوصية المعلوماتية وعلاقتها بجمع الاستدلالات

الفصل الثاني: الطبيعة الخاصة لمرحلة التفتيش والضبط بحثاً عن الدليل الرقمي

المبحث الأول: التفتيش في جرائم تقنية المعلومات

المبحث الثاني: الضبط والتحفظ على الأدلة المتحصلة من الأجهزة الرقمية

الفصل الثالث: ذاتية الأدلة الجنائية الرقمية في مرحلة المحاكمة

المبحث الأول: إلزام مزودي الخدمات والغير بتقديم الدليل الإلكتروني

المبحث الثاني: حجية الدليل الرقمي في الإثبات الجنائي

المبحث الثالث:استبعاد الأدلة الجنائية الرقمية على سند من بطلانها

الخاتمة. قائمة المصادر والمراجع

المبحث التمهيدي

ماهية الدليل الرقمي وطرق تحليله جنائياً

لوحظ أن الأدلة الجنائية سابقاً كانت تقتصر على أدلة مادية ملموسة أو مرئية أو مسموعة للرجل العادي أن يتعامل معها، إلا أنه مع ظهور جرائم التقنية، أدى إلى وجود طبيعة معلوماتية غير ملموسة. بناء على ذلك سوف نتناول خلال هذا المبحث مفهوم الدليل الرقمي مع بيان أنواعه، إضافة إلى أماكن تواجد الدليل الرقمي في مختلف الأجهزة الرقمية، وكيفية استخلاصه عن طريق مختصي المعمل الجنائي الرقمي وتقديمه كدليل أمام المحكمة. وذلك من خلال المطالب التالية:

المطلب الأول

مفهوم الدليل الرقمي وأنواعه

أولاً: مفهوم الدليل الرقمي Digital evidence

الدليل لغة: ما يستدل به، ويقال الدَّال، وقد دله على الطريق يدله دَلالَةً وَدِلالَه ودُلُولَة. وفي حديث علي رضي الله عنه في صفة الصحابة" ويخرجون من عنده أدلة" وهي جمع دليل، أي بما قد علموا، فيدلون عليه الناس، بمعنى يخرجون من عنده فقاء، فجعلهم أنفسهم أدلة مبالغة. ودللت بهذا الطريق أي عرفته ودللت به أي أَدُل دلالة، وأدللت بالطريق إدلالاً.[2]

ويقال أن الدليل ما يلزم من العلم به، العلم بشئ آخر، فإذا قدم المدعي حجته للقاضي واقتنع الأخير بتلك الحجة لزم عليه الحكم للمدعي فيما ادعاه.[3]

أما الدليل اصطلاحاً: فيعرف بأنه معلومة يقبلها المنطق والعقل، يتم الحصول عليها بإجراءات قانونية ووسائل فنية أو مادية أو قولية، ويمكن استخدامها في أي مرحلة من

---

[2] ابن منظور، أبو الفضل جمال الدين محمد بن مكرم "لسان العرب". بيروت. دار إحياء التراث العربي. 1983م، ص 1414.

[3] ابن قيم الجوزية، محمد بن أبي بكر بن أيوب بن سعد شمس الدين"إعلام الموقعين عن رب العالمين"، الطبعة الأولى، تحقيق محمد عبدالسلام إبراهيم، بيروت، دار الكتب العلمية. الجزء الأول، سنة 1411هـ-1991م، ص 410.

مراحل التحقيق أو المحاكمة، لإثبات حقيقة فعل أو شيء أوشخص له علاقة بجريمة أو جاني أو مجني عليه".[4]

والدليل الرقمي مصطلح يشير إلى المعلومات الإثباتية التي يتم نقلها أو تخزينها في صيغة رقمية، والتي يمكن استخدامها بعد ذلك في المحاكمة، ويشترط قبل قبولها كأدلة من قبل المحكمة تحديد ما إذا كانت صحيحة وذات علاقة بالقضية من عدمها.[5]

واتجه رأي إلى تعريف الدليل الرقمي بأنه "الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء"[6]. وفي رأينا أن هذا التعريف قصر مفهوم الدليل الرقمي على الأدلة المستمدة من الحاسب الآلي، ففيه تضييق لنطاق دائرة الأجهزة الرقمية المستمد منها الدليل الرقمي، كما أنه ربط الدليل بمصدر استخلاصه، فإذا سلمنا بذلك لوجدنا أن المجالات المغناطيسية أو الكهربائية إذا تم فصلها عن مصدرها لا تصلح لأن توصف بكونها دليل رقمي.

وثمة رأي يعرف الدليل الرقمي بأنه الأدلة التي تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت، أو تثبت وجود علاقة بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها.[7] أما المنظمة الدولية لأدلة الحاسوب IOCE فتعرف الدليل الرقمي بأنه"جميع المعلومات المخزنة أو المتنقلة في شكل ثنائي، والتي يمكن أن تعتمد عليها المحكمة".[8]

---

[4] محمد الأمين البشري "التحقيق في الجرائم المستحدثة" جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2004، ص 230.

[5] Stephen Manson, "**Expert in Cyber Security**". PDF, Retrieved Aug 20, 2018. http://www.stephenmason.eu/articles/electronic-evidence.html.

[6] ممدوح عبدالحميد "البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت" دار الكتب القانونية، مصر، 2006م، ص52.

[7] Eoghan Casey, "**Digital Evidence and Computer Crime",** 3rd Edition, London, Academic Press, 2011, P 33.

[8] مشار إليه: عمر محمد يونس " الجرائم الناشئة عن استخدام الإنترنت" القاهرة، دار النهضة العربية، 2004م.

وقد عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، الدليل الرقمى بأنه أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

ويمكننا تعريف الأدلة الرقمية بأنها جميع البيانات التي يتم تخرينها في شكل رقمي، عن طريق استخدام إحدى الوسائل أو الأجهزة الرقمية، ويختص باستخلاصها ذوي الخبرة الفنية باستخدام برامج ووسائل تقنية، والتي تفيد في كشف حقيقة جريمة معينة ويمكن تقديمها كدليل أمام المحكمة.

ثانياً: أنواع الدليل الرقمي

أضحت الأدلة الرقمية التي تستند إليها المحاكم في زيادة مستمرة كالصور الرقمية ورسائل البريد الإلكتروني وسجلات المعاملات ATM ومستندات معالجة النصوص، وتواريخ من برامج المراسلة الفورية وجداول البيانات وتاريخ المتصفح والحساب، وقواعد البيانات ومحتويات ذاكرة الكمبيوتر والنسخ الإحتياطية للكمبيوتر وتتبع GPS والملفات الصوتية ومقاطع الفيديو الرقمية.[9]

ويمكننا تصنيف الدليل الرقمي على النحو التالي:

أ)بحسب المصدر: أي مصدر الدليل (الحاسب، الهاتف الخلوي، الشبكة)

ب) بحسب طبيعة البيانات: بمعنى هل هي ملفات محذوفة تم استرجاعها أم ملفات موجودة بالفعل.

ج) بحسب نوع الدليل: صور أو فيديوهات أو علامات مرجعية Book marks أو معرفات الجلسة Cookies أو سجلات المخُدّم Server logs.

وفيما يتعلق بأنواع الأدلة الرقمية المعتمدة من المحاكم فتتمثل في الأتي:[10]

1- الأقراص الصلبة 2- سجلات النظام System Logs 3 - الهاتف الخلوي

---

[9] Stephen Manson, "**Expert in Cyber Security**". Ibid.

[10] ممدوح عبد الحميد عبدالمطلب "أدلة الصور الرقمية في الجرائم عبر الكمبيوتر" مركز شرطة دبي، سنة 2005م، ص 9،10.

4- وسائط التخزين الخارجية USB 5- سجلات الموجه Router Logs
6- رسائل البريد الإلكتروني 7- سجلات المحادثات 8- شريحة الهاتف SIM
9- سجلات أجهزة الحماية (الجدار الناري Fire wall أو أجهزة كشف الاختراق ISD)
10- سجلات قواعد البيانات.

ثالثاً: أماكن وجود الدليل الرقمي

تنقسم الأجهزة الرقمية إلى نوعين الأول أجهزة إدخال وإخراج، أما الثاني فوسائل لتخرين المعلومات. والتي تعد مرتبطة بعضها البعض حيث تقوم أجهزة الإدخال أو الإخراج بدور الوسيط بين مستعمل الجهاز ووسائل تخزين المعلومات، ويعد من أمثلة ذلك محتوى التخزين المتحرك مثل وحدة تخزين القرص المضغوط CD، أو الذاكرة الفلاشية USB flash.[11] وتكمن أهم أماكن البحث عن الدليل الرقمي فيما يلي:

أ)جهاز الحاسب وملحقاته: ومن خلاله يتم استخراج تاريخ تصفح الإنترنت أو الملفات المحذوفة أو مفاتيح سجلات النظام في نظام Windows أو السجلات Logs. وكذلك الملحقات المرتبطة بسجلات log files والتي تحتوى على كمية هائلة من المعلومات والخاصة بالاستخدام الشخصي للحاسب فتحتوي على عناوين IP كما ترتبط تلك السجلات مع برامج حماية Firewalls وبرامج تحديد المسارات Routers والتي تسجل غالباً تحركات الدخول والخروج مع بروتوكولات TCP/IP. [12]

ب) كذلك الملحقات بالحاسوب ذات الصلة بالجريمة كالطابعات والماسحات الضوئية والكاميرات الرقمية.

ت) قواعد البيانات: مثل. SQL Server or Oracle

ج) الشبكة: البيانات عبر الشبكة والتي يمكن تحليلها باستخدام برنامج مثل Wire shark.

---

[11] خالد مصطفى الجسمي "الإثبات الجنائي بالأدلة الرقمية" دار السلام للطباعة والنشر، مجلة القانون المغربي، العدد 34، سنة 2017م، ص 26.

[12] محمد حسن السراء "الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية" مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد الحادي والعشرون، إبريل العدد 81، سنة 2012م، ص 49.

د) جهاز الهاتف الخلوي: ويمكن البحث عن الدليل في سجل المكالمات والرسائل أو التطبيقات.

رابعاً: كيفية التعامل مع الدليل الرقمي

يعتبر الدليل الرقمي من قبيل الأدلة العلمية غير الملموسة، والتي تختلف عن الأدلة المادية الملموسة، فهو عبارة عن مجالات مغناطيسية أو كهربائية، ومن ثم فجمع وترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أنه بذلك أصبح دليل، بل أن التجميع والتوثيق لا يعدو كونه عملية نقل لتلك المجالات من طبيعتها الرقمية إلى معلومات يمكن الاستناد إليها في الإثبات.[13]

واعتمد المؤتمر الدولي المعني بجرائم التكنولوجيا عام 1999 المبادئ التوجيهية التالية للحفاظ على مقبولية الأدلة الرقمية والتي تتمثل في الآتي:

1. عند اتخاذ إجراء للحصول على الأدلة الرقمية ، لا ينبغي أن يغير الإجراء تلك الأدلة.
2. عندما يكون من الضروري أن يحصل الشخص على أدلة رقمية أصلية، يجب أن يكون ذلك الشخص مكلفًا من جهة قضائية أو معاونيها وفقاً للقانون.
3. يجب توثيق جميع الأنشطة المتعلقة بمصادرة الأدلة الرقمية أو الوصول إليها أو تخزينها أو نقلها توثيقاً كاملاً وحفظها وإتاحتها للمراجعة.
4. كل فرد مسؤول عن جميع الإجراءات المتخذة فيما يتعلق بالأدلة الرقمية أثناء وجود الأدلة الرقمية. وكذلك أي جهة مسؤولة عن الحصول على الأدلة الرقمية أو الوصول إليها أو تخزينها أو نقلها هي المسؤولة عن الامتثال لهذه المبادئ.

وحفاظاً على الدليل الرقمي فيجب على الخبير المختص إنشاء صورة طبق الأصل من الدليل المتحصل عليه، فعلى سبيل المثال فالقرص الصلب والذي يكون الدليل الرقمي غالباً به، كونه يقوم بتخزين البيانات على أساس نظام العد الثنائي Binary System الذي يحتوي على عنصرين فقط هما الصفر 0 والواحد 1، فيقوم الحاسب بالتعامل معها في شكل

---

[13] علي محمود علي حمودة "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي" المؤتمر العلمي الأول "الجوانب القانونية والأمنية للعمليات الإلكترونية" أكاديمية شرطة دبي، في الفترة من 26-28 إبريل 2003م.

Bits والخانة التي تحتوي على نبضة كهربائية تمثل الرقم واحد والتي لا تحتوي على نبضة كهربائية تمثل الرقم صفر، وذلك بحسب حالة القرص الصلب، وكل سلسلة معينة من الأصفار والواحدات يفهمها نظام التشغيل على أنها حرف معين أو تعليمة معينة. وعليه فيجب حفظ القرص الصلب في مكان بعيد عن الحقول المغناطيسية لحمايته من التخريب، على أن تتم عملية التحليل الجنائي على الصورة المأخوذة من القرص الصلب وليس على الجهاز الأصلي.[14]

ويتم النسخ عن طريق نسخ كافة البيانات المخزنة من الجهاز الرقمي محل الجريمة إلى جهاز آخر بالمعمل الجنائي، ثم البدء في مرحلة التحليل على ما سنرى لاحقاً.[15]

المطلب الثاني

البحث عن الدليل الرقمي تمهيداً لتحليله جنائياً

أولاً: علم التحليل الجنائي الرقمي

هو علم استخدام تقنيات العلم والتكنولوجيا في عمليات التحقيق الجنائي، ومن خلاله يتم فحص الأجهزة الرقمية أو المنظومة المعلوماتية، وتحليل العمليات واسترجاع البيانات والملفات بهدف الحصول على دليل رقمي، وتتم هذه العملية وفق ضوابط ومعايير معينة، كي يتم المحافظة على الأدلة الرقمية في شكلها الأصلي دون تعديل أو تخريب.

ويعتمد التحليل الجنائي على فرضيات يتم فحص كل فرضية ويتم تسجيل النتيجة. والفرضية عبارة عن سؤال يتم الإجابة عليه، فإذا فرضنا أن المتهم حذف ملف معين، فيتم

---

[14] جميل حسين طويلة "التحليل الجنائي الرقمي– دليل عملي لطرق التحليل الجنائي الرقمي في الجرائم المعلوماتية"، ص 57 كتاب منشور عبر موقع https://arabcyberwarrior استرجاع بتاريخ 2019/1/25م.

[15] ممدوح عبدالحميد عبدالمطلب " استخدام أدوات التحليل التناظري الرقمي في بحث وتحقيق جرائم الحاسب الآلي"مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد 11، العدد 4، سنة 2003م، ص 81.

التحقق من هذه الفرضية من خلال استعادة الملفات المحذوفة باستخدام أدوات معينة من قبل الخبير الرقمي.[16]

ثانياً: التحليل الجنائي الرقمي للأدلة المستمدة من الأجهزة الرقمية مع الحفاظ على قوتها الثبوتية.

(أ) البحث عن الدليل الإلكتروني في نظام الكمبيوتر

عرفت المادة الأولى من اتفاقية بودابست 2001 في الفقرة أ **نظام الكمبيوتر** بأنه جهاز يتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية، ويمكن أن يشمل المدخلات والمخرجات ومرافق التخزين، ويمكن أن يعمل وحده أو أن يكون متصلاً بشبكة مع غيره من الأجهزة المماثلة. ويقصد **بمعالجة البيانات** أن البيانات في نظام الكمبيوتر يتم تشغيلها عن طريق تنفيذ برنامج الكمبيوتر، **وبرنامج الكمبيوتر** هو مجموعة من التعليمات التي يمكن تنفيذها من خلال الكمبيوتر لتحقيق النتيجة المرجوة.[17]

أما فيما يتعلق ببيانات الكمبيوتر فقد استندت الاتفاقية في فقرة ب إلى تعريف المنظمة الدولية للمواصفات لمصطلح البيانات، والذي ينص على أن يتم وضع البيانات في شكل يسمح بمعالجتها مباشرة من خلال نظام الكمبيوتر، مع ملاحظة أن تلك البيانات يقصد بها البيانات الإلكترونية أو في شكل آخر قابل للمعالجة التلقائية**[18]**.

ويعرف جهاز الكمبيوتر أو الحاسب الآلي بأنه جهاز إلكتروني يقوم بآداء العمليات الحسابية ومنطقية للتعليمات المعطاه له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، كما أن له القدرة على التعامل مع مجموعة كبيرة من البيانات مع إمكانية تخزين هذه البيانات واسترجاعها عند الحاجة إليها.[19] ونظرًا لأن أجهزة الكمبيوتر باتت أصغر حجماً وأكثر تطوراً، فأصبحت مدمجة داخل الأنظمة الأكبر الأخرى

---

[16] جميل حسين طويلة، مرجع سابق، ص60.

[17] المادة الأولى، فقرة أ، اتفاقية الجريمة الإلكترونية (بودابست 2001).

[18] للمزيد راجع: دليل ورشة عمل "الدليل الرقمي وحجيته في الإثبات الجنائي" جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، الرياض، في الفترة من 9-10 أكتوبر 2018م.

[19] طاهر الشيخ، "نظم تشغيل المعلومات" معهد إدارة الحاسب، مصر، سنة 1991، ص 1.

بطرق لا تكون دائماً واضحة وتسمح بإنشاء المعلومات وتخزينها ومعالجتها؛ لذلك يمكن أن تنشأ الأدلة الرقمية في أماكن وأشكال غير متوقعة.

ولعل أهم وسائط التخرين في أجهزة الحاسب هي القرص الصلب Hard Driver، ففيه يتم تخزين البيانات على شكل إشارات مغناطيسية ويترجمها الحاسب على أنها bits والقرص الصلب عبارة عن طبقات دائرية فوق بعضها البعض، وهي مصنوعة من الزجاج أو الألمنيوم ومصقولة بمادة مغناطسية على سطحها. وبعد تحديد مكان البيانات من خلال فحص هذه الطبقات تبدأ عملية نقل البيانات من القرص الصلب إلى الذاكرة RAM. وفي حالة حذف بعض البيانات فلن يتم حذفها من القرص الصلب، بل ستبقى فيه إلى أن يتم استخدام المساحة المخصصة لهذه البيانات من قبل بيانات أخرى.[20]لذا فمن المهم الحفاظ على القرص الصلب من أي عوامل قد تؤدي إلى تخريبه أو محو البيانات المخزنه عليه.

(ب) البحث عن الدليل الإلكتروني في قواعد البيانات

تعد قواعد البيانات من أحدث الأساليب المعاصرة في معالجة المعلومات من تخرين واسترجاع، فهي عبارة عن قائمة مرتبة من البيانات تستطيع توفير طريقة وصول منهجية وسريعة وسهلة للحصول على المعلومات بناءً على نقطة مرجعية مختارة. وترجع أهميتها في تخزين أكبر كميات من البيانات التي تتجاوز الإمكانات البشرية مع اختلاف المعلومات التي يتم تخرينها، وكذلك إمكانية استخدام عمليات التشفير التي تساعد على سرية المعلومات المخزنة بحيث لا تمّكن أي شخص من الدخول إلى قاعدة البيانات أو الإطلاع عليها.[21] ولعل أشهر أنظمة إدارة قواعد البيانات هي Oracle– Microsoft Access .

وعادة ما يتم حفظ قواعد البيانات في مُخدّم خاص بها، ولعل أفضل مكان للبحث عن الدليل الرقمي في قواعد البيانات هو سجل العمليات Transaction فهذا السجل يحتوي على كل عملية إدخال أو حذف أو اختيار أو تحديث لقاعدة البيانات. كذلك من المهم البحث عن حسابات المستخدمين في قاعدة البيانات. وتقوم أنظمة إدارة قواعد البيانات عادة

---

[20] جميل حسين طويلة، مرجع سابق، ص 77.

[21] سامر الغدا، " مفهوم قواعد البيانات" دراسة منشورة عبر موقع http://qu.edu.iq، استرجاع بتاريخ 2019/2/7م. انظر كذلك: خالد مصطفى الجسمي، مرجع سابق، ص 28.

بعمل نسخ احتياطية بشكل دوري، من خلال هذه النسخ يتم الحصول على المعلومات التي قد يتم حذفها من قاعدة البيانات الحالية.[22]

(ج) البحث عن الدليل الإلكتروني في البريد الإلكتروني (E-mail)

ترتكب العديد من الجرائم عبر البريد الإلكتروني سواء المعلوماتية أو التقليدية، وفيها يقوم المرسل بكتابة الرسالة باستخدام برنامج Outlook مثلاً أو من خلال موقع مُخدّم البريد الإلكتروني، وتصل الرسالة إلى مخدم الإرسال Sender email server والذي يقوم بدوره بإرسال هذه الرسالة إلى مخدم الإستقبال Recipient's email server وعندما يقوم الشخص المستقبل بالدخول إلى نظام البريد الإلكتروني سوف يقوم باسترداد الرسالة من المخدم.

لذا فالدليل الرقمي من الممكن وجوده في أي من الأماكن السابقة، سواء في جهاز المرسل أو في الجهاز المستقبل أو في مخدم الإرسال أو مخدم الاستقبال. وفي هذه الحالة ومن أجل إجراء عملية بحث عن دليل رقمي في البريد الإلكتروني، يجب الحصول على سجلات الرسائل من الشركة المزودة للإنترنت (مقدم أو مزود الخدمة).

وعند اعتبار رسالة إلكترونية دليل رقمي فيجب أن يتضمن الدليل نص الرسالة والمرفقات إن وجدت وترويسة الرسالة، والترويسة هي التي تحوي المعلومات الكاملة عن الرحلة التي مرت بها الرسالة عبر الشبكة ويتم فحص عنوان IP address الموجود في ترويسة الرسالة لتحديد هوية أو مكان المرسل.[23]

(د) البحث عن الدليل الإلكتروني في الهاتف الخلوي- الموبايل (Mobil)

تقسم أجزاء الهاتف الخلوي إلى ما يلي:

---

[22] جميل حسين طويلة، مرجع سابق، ص111. راجع كذلك: أمير فرج يوسف "الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، دراسة مقارنة للتشريعات العربية والأجنبية" مكتبة الوفاء القانونية، مصر، سنة 2016م، ص 39 وما بعدها.

[23] جميل حسين طويلة، مرجع سابق، ص 200.

- **الشريحة SIM (Subscriber Identity Module)** : وهي أهم جزء في جهاز الهاتف الخلوي[24]، فمن خلالها يتم تحديد الرقم الخاص بالمستخدم، كذلك معرفة معلومات عن الشبكة.

ثانياً: **أنظمة التشغيل الخاصة بجهاز الهاتف الخلوي**[25]، وتتنوع إلى :

1- **نظام IOS:** وهو نظام التشغيل الخاص بأجهزة IPhone- iPod and iPad والخاصة بشركةApple والمبني على نظام التشغيل OS for Macintosh وعند البحث عن الدليل يكون غالباً في دليل الهاتف أو الأسماء أو بعض البيانات المخفية في مجلد iPod control.

2- **نظام Android:** وهو نظام التشغيل الأكثر استخداماً حول العالم وفيه يتم تنصيب البرامج من أي متجر عبر الإنترنت بعكس iPhone الذي يسمح بتنصيب البرامج من متجر iTunes store، ولعل من سلبيات هذا الأمر انتشار البرمجيات الخبيثة الخاصة بأنظمة Android بشكل أكبر من البرمجيات الخبيثة الخاصة بنظام IOS وهذا ما يزيد أهمية البحث عن الدليل الرقمي في الأجهزة التي تعمل بأنظمة Android .

3- **تطبيقات الهاتف الخلوي:** حيث يمكن الحصول على الدليل الرقمي من التطبيقات التي تعمل على جهاز الهاتف أو التي يتم تنصيبها عليه مثل تطبيقات المحادثات وتطبيقات مواقع التواصل الاجتماعي ومتصفحات الإنترنت والصور ومقاطع الفيديو.[26]

وفي حالة البحث عن دليل رقمي في الهاتف الخلوي يتم جمع معلومات عن نوع وحالة الجهاز، وتاريخ المكالمات والرسائل وجمع الصور ومقاطع الفيديو ومعلومات GPS

---

[24] "**Mobile Fact Sheet**". Pew Research Center Internet and Technology. Pew Research Center. February 5, 2018. Retrieved Nov 20, 2019. https://www.pewinternet.org/fact-sheet/mobile/

[25] فيصل حاكم الشمري " مستجدات التعليم الإلكتروني – تطبيقات الهواتف الذكية ومتاجر الويب) ورشة عمل- جامعة المجمعة، المركز الوطني للتعليم الإلكتروني والتعليم عن بعد، المملكة العربية السعودية، بدون تاريخ، ص 30.

[26] "Mobile Fact Sheet". Pew Research Center Internet and Technology. Ibid.

ومعلومات عن اتصالات الشبكة، ومعلومات عن كافة التطبيقات الموجودة على الهاتف وسجلات المحادثات وتاريخ تصفح الإنترنت.

ويتم خلق صورة طبق الأصل (الاستحواذ) لكامل محتوى الهاتف، ثم يوضع في حقيبة تمنع الإشارات اللاسلكية لضمان عزل اتصال الجهاز عن الشبكة أو عن أي اتصال مع الوسط الخارجي.[27]

ثالثاً: المعايير الواجب على الخبير اتباعها لاعتماد الدليل الرقمي أمام المحكمة

(1) **الاستحواذ (Acquiring)**: وفيها يتم خلق نسخة طبق الأصل Replica من المعلومات الموجودة بالقرص الصلب أو بمحل الدليل.

(2) **التوثيق (Authentication)**: تعد عملية التوثيق جزءاً هاماً من عمليات حفظ الأدلة الرقمية والتي تقوم بدورها في الحفاظ على الدليل في شكله الأصلي للتأكيد على مصداقية الدليل وعدم تعرضه للتحريف أو التعديل.[28] ويجب توثيق كل المعلومات والعمليات التي تمت في مكان الجريمة بما فيها الأجهزة المتصلة بالجهاز محل الجريمة كالاتصالات الحالية بالشبكة ونوع الحاسب ونوع نظام التشغيل، وكذلك توثيق كل أداة تم استخدامها في عملية فحص الجهاز الرقمي.

(3) **حماية الدليل المتحصل عليه:** حتى تأخذ المحكمة بالدليل الرقمي لابد من الحفاظ على سلامته كي يكون معتمداً كدليل إثبات، ولكي يتم ذلك يجب العمل على نسخة طبق الأصل من الدليل الرقمي وليس على الدليل الرقمي الأصلي بشكل مباشر –كما أوضحنا في

---

[27] جميل حسين طويلة، مرجع سابق، ص 101.

[28] محمد الأمين البشري "تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت" كلية التدريب، قسم البرامج التدريبية، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2008م، ص 29. انظر كذلك: محمد الأمين البشري "الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات" المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض،المجلد 17، العدد 33، سنة 2002م، ص 119.

مرحلة الاستحواز – ثم تتم عملية تحليل المعلومات التي تم تحريزها والتي تؤدي بدورها إلى كشف ملابسات الجريمة.[29]

كما يتم استخدام طرق وأجهزة مخصصة لمنع الكتابة على القرص الصلب قبل البدء بإنشاء صورة طبق الأصل مثل Ultra write أو Software write blocker. وفيما يتعلق بأجهزة الهواتف الخلوية فيتم عزل الجهاز عن الشبكة، كون من الممكن حذف البيانات عن بعد، حيث توجد خاصية حذف البيانات عن بعد في حال فقدان أو سرقة الهاتف الخلوي، كذلك من الممكن الاتصال بالجهاز عبر الشبكة اللاسلكية أو شبكة الهاتف نفسه والتعديل على البيانات الموجودة عليه. وإذا كان الدليل في الجهاز الخادم server والذي يحتوي على عدد من قواعد الويب، فمن الصعب قطع اتصال هذا الجهاز عن الشبكة أو حتى نقله، وعليه فإذا كان يوجد خادم احتياطي Backup فيتم وصله على الشبكة لحين إنشاء صورة طبق الأصل للخادم محل الدليل، وإذا لم توجد نسخة احتياطية يتم قطع اتصال الخادم عن الشكبة بشكل مؤقت لإنشاء صورة طبق الأصل ومن ثم إعادته للعمل.[30]

وتوجد بعض الحالات لا يتم فيها الوصول إلى الأجهزة الرقمية محل البحث عن الدليل، كما هو الحال في حالة اختراق أجهزة حكومية أو أجهزة منشأة عسكرية، ففي هذه الحالة يتم استخراج الدليل الرقمي عن بعد بإنشاء صورة طبق الأصل للجهاز محل الدليل عبر الشبكة.

(4) **إعداد تقرير المعمل الجنائي الرقمي:** يحتوي التقرير النهائي للمعمل الجنائي على كل المعلومات التي تتعلق بالقضية وكل الملفات التي تم اكتشافها وتحليلها، وكذلك الأدوات التي تم استخدامها وكافة المعلومات عن الجهاز محل الدليل. ويتم تقسيم التقرير إلى 1– ملخص القضية 2– طرق الفحص والتحليل 3– النتائج.

وقد اعتمدت المحاكم الأمريكية منذ عام 1993 اختبار داوبورت لقبول الدليل العلمي، والذي يختبر سلامة المنهجية المتبعة والطرق الفنية في استخلاص الدليل الرقمي للتدليل

---

[29] أزهري عبدالرحمن، نسرين بشير عثمان "جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فاعلية". المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC . جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات. الرياض، المملكة العربية السعودية، سنة 2015م، ص 15.

[30] جميل طويلة، مرجع سابق، ص 116.

على مدى مصداقية وفاعليته في الإثبات، حيث قررت المحكمة العليا الأمريكية ضرورة النظر في العوامل التالية أثناء تقييم الدليل:[31]

–هل تم اختبار الطريقة المتبعة في استخلاص الدليل في الظروف الميدانية الفعلية وليس فقط في المختبر؟

– ما هو معدل الخطأ المعروف أو المحتمل المرتبط بتطبيق هذه التقنية؟

–هل جرى نشر التقنية المتبعة وخضعت لمراجعة من قبل الآخرين؟

– هل توجد معايير للتحكم في تطبيق وتنفيذ هذه التقنية؟

– هل تم قبول هذه التقنية بشكل عام داخل المجتمع العلمي ذي الصلة؟

فعندما تقوم المحكمة بتقييم الدليل من حيث مصداقيته وأصالته فإنها تقوم أيضاً بتقييم الطريقة التي تم استخلاص الدليل بها من حيث كونها صحيحة ومعتمدة ومقبولة في المجال المعني؛ ذلك أنه على القاضي أن يقيم شهادة الخبراء وأساليب الحصول على الدليل التي قاموا بتطبيقها على الحقائق المطروحة حتى تساعد الخبرة الفنية على فهم الأدلة وتحديد حقيقتها.

خلاصة ما تقدم، أصبح الدليل الرقمي أحد أهم وسائل الإثبات في الوقت الراهن، ليس لإثبات الجرائم الإلكترونية فحسب بل وإثبات الجرائم التقليدية أيضاً، متى ما تم استنتاجه بناءً على أسس وقواعد علمية سليمة، كونه دليلاً غير ملموس. كما أنه يتمتع بالحداثة التي فرضها واقع التطور التقني، فضلاً عن خصوصية الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها، الأمر الذي يتطلب معه مشروعية وجود الدليل من حيث استخلاصه والحصول عليه. فالمشروعية تقتضي اتباع الإجراءات القانونية والتزامها بمبدأ الشرعية، حيث أن مشروعية الوجود تقتضي أن يكون الدليل قد تم قبوله ضمن أدلة الإثبات الجنائي، الأمر الذي ثارت معه العديد من الإشكاليات والتي سنتناولها على مدار دراستنا بشئ من التفصيل.

[31] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). supremecourt.gov. Retrieved Sep 7, 2018.

الفصل الأول

ذاتية البحث عن الدليل الرقمي في مرحلة جمع الاستدلالات

تمهيد:

تعرف الاستدلالات بأنها مجموعة من الإجراءات التمهيدية التي تسبق تحريك الدعوى الجنائية، بهدف جمع المعلومات في شأن جريمة ارتكبت كي يتم تحريك الدعوى الجنائية بناء عليها، وهذه الإجراءات غالباً يقوم بها مأموري الضبط القضائي.[32]

وقد نصت المادة 21 إجراءات مصري على أن "يقوم مأمور الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى". فمأمور الضبط القضائي هو أول من ينتقل إلى محل الجريمة، وتبدو أهمية الإجراءات التي يتخذها من قبيل المحافظة على الأدلة والوقوف على الدلائل التي تفيد في توجيه الاتهام أو نفيه، فدوره هو النواة التي تبدأ منها التحقيقات وجعل سلطة الاتهام قادرة على اتخاذ القرار بتحريك الدعوى الجنائية والمضي في التحقيق أو التصرف فيها بالأمر بالحفظ أو بألا وجه لإقامة الدعوى.

ولكن تثير مرحلة جمع الاستدلالات العديد من التساؤلات القانونية الهامة التي تتعلق بحدود سلطات مأمور الضبط القضائي في التعامل مع الدليل الرقمي (في المبحث الأول)، ثم نتطرق إلى تحديد مجال الاستدلالات من جانب مأمور الضبط القضائي لضبط الدليل الرقمي (في المبحث الثاني). ودراسة الحق في الخصوصية المعلوماتية وعلاقتها بجمع الاستدلالات (في مبحث ثالث).

المبحث الأول

مجال الاستدلالات من جانب مأمور الضبط القضائي

لضبط الدليل الرقمي من شبكة الإنترنت

- **مأمورو الضبط القضائي المتعاملون مع الدليل الرقمي**

[32] أشرف توفيق شمس الدين "شرح قانون الإجراءات الجنائية– (الجزء الأول– مرحلة ما قبل المحاكمة)" طبعة خاصة بالتعليم المفتوح . جامعه بنها، مصر، سنة 2012م، ص 134.

نظراً للسلطة الواسعة التي يتمتع بها مأموري الضبط القضائي في الدعوى الجنائية، وما يترتب على أعمالهم من آثار قانونية هامة قد تخول لهم اتخاذ إجراءات تمس الحرية الشخصية للشخص المشتبه به، فقد خصت غالبية الشريعات هذه السلطات الواسعة لمأموري الضبط القضائي وحدهم دون غيرهم من رجال السلطة العامة، وبناء على ذلك فإن انتفاء صفة مأمور الضبط القضائي أو كونه يخرج عن الأشخاص الذين يحددهم القانون نتيجة مؤداها بطلان بعض الإجراءات التي يتخذها مرءوس الضبط.[33]

ولم تحدد غالبية التشريعات طرقاً معينة ينتهجها مأمور الضبط في إجراء تحرياته[34]، بل له أن يتخذ من الوسائل أو الإجراءات ما يمكنه من مباشرة اختصاصه، على أن يثبت جميع الإجراءات التي يتخذها في محاضر موقع عليها وترسل هذه المحاضر إلى النيابة مع الأشياء المضبوطة. ولمأمور الضبط القضائي أثناء جمع الاستدلالات أن يستعين بأهل الخبرة وطلب رأيهم شفاهة أو كتابة، ويتم ندب خبير التقنيات أو تكنولوجيا المعلومات في جرائم تقنية المعلومات كونها تتسم بطابع فني، ولا يجوز له تحليف الخبير اليمين إلا للضرورة.[35]

---

[33] نصت المادة 23 من قانون الإجراءات الجنائية المصري في الفقرة (أ) على أن " يكون من مأموري الضبط القضائي في دوائر اختصاصهم:1- أعضاء النيابة العامة ومعاونوهم 2- ضباط الشرطة وأمناؤها والكونستبلات والمساعدون 3- رؤساء نقط الشرطة 4- العمد ومشايخ البلاد ومشايخ الخفراء 5- نظار ووكلاء محطات السكك الحديدية الحكومية. ولمديري أمن المحافظات ومفتشي مصلحة التفتيش العام بوزارة الداخلية أن يؤدوا الأعمال التي يقوم بها مأمور الضبط القضائي في دوائر اختصاصهم.

-كما نصت في الفقرة (ب) على أن" ويكون من مأموري الضبط القضائي في دميع أنحاء الجمهورية: (1) مدير وضباط إدارة المباحث العامة بوزارة الداخلية وفورعها بمديريات الأمن (2) مديرو الإدارات والأقسام ورؤساء المكاتب والمفتشون والضباط وأمناء الشرطة والكونستابلات والمساعدون وباحثات الشرطة العاملون بمصلحة الأمن العام وفي شعب البحث الجنائي بمديريات الأمن(3) ضباط مصحلة السجون (4) مدير الإدراة العامة لشرطة السكة الحديد والنقل والمواصلات وضباط هذه الإدارة (5) قائد وضباط أساس هجانة الشرطة (6) مفتشو وزارة السياحة.

[34] للمزيد انظر: مصطفى محمد موسى "قواعد وإجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية والتخطيط لها" بحث مقدم ضمن الدورة التدريبية "إجراءات التحري والمراقبة والبحث الجنائي"، الرياض. خلال الفترة من 25-5 /6-6-2012م.

[35] راجع المادة 29 إجراءات جنائية مصري.

ويجوز إضفاء صفة مأمور الضبط القضائي بقرار، حيث نصت المادة 5 من قانون مكافحة جرائم تقنية المعلومات المصري على أنه يجوز بقرار من وزير العدل بالاتفاق مع الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات، منح صفة الضبطية القضائية للعاملين بالجهاز القومي لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومى، بالنسبة إلى الجرائم التى تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم.[36]

وتكون هذه الطائفة من مأموري الضبط القضائي ذات الاختصاص النوعي المحدد بنوع معين من الجرائم – جرائم تقنية المعلومات– ويكون اختصاصها شاملاً إقليم الجمهورية كله أو مقصوراً على دائرة واحدة، كما هو الحال بالنسبة لمفتشي التموين ومفتشي الصحة ورجال الجمارك وغيرهم.[37]

كما خولت المادة 6 من قانون مكافحة جرائم تقنية المعلومات المصري مأموري الضبط القضائي سلطات تنفيذ أوامر النيابة العامة والقاضي في مجال التفتيش عن الدليل الرقمي وضبطه بناء على إذن بذلك. فقد أجازت المادة السابقة لجهة التحقيق المختصة – بحسب الأحوال– أن تصدر أمراً مسبباً لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على 30 يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلى : 1– ضبط المعلومات والبيانات..2– التفتيش ..."

ترتيباً على ذلك فلا يعني أن قيام جهات التحقيق بالبدء في التحقيقات سلب لسلطات مأمور الضبط في مرحلة جمع الاستدلالات، بل عليه القيام بما نص عليه القانون وإرسال ما يحرره من محاضر إلى جهة التحقيق لتكون بين يديها وعنصراً من عناصر الدعوى الجنائية.

وتقضي القواعد العامة في الاختصاص بأن وجود مأمور ضبط قضائي متخصص (ذي اختصاص نوعي محدد) لا يحول دون قيام مأمور ضبط ذي اختصاص نوعي عام

---

[36] راجع كذلك المادة 23 إجراءات جنائية مصري.

[37] أشرف توفيق شمس الدين، مرجع سابق، ص 122.

بإجراء يدخل في اختصاص مأمور ضبط ذي اختصاص نوعي محدد[38]. وبتطبيق ذلك على مأموري الضبط القضائي ذوي الاختصاص النوعي المحدد ممن نص عليهم في المادة (5) من قانون جرائم تقنية المعلومات لسنة 2018 يؤدي إلى القول بأن قيام مأمور ضبط من رجال المباحث بعمله لا يترتب عليه البطلان.

وجدير بالذكر أن المادة (5) سابقة الذكر تنص على أنه "يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز وغيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم". ويقصد بالجهاز وفقاً للمادة الأولى من القانون الجهاز القومي لتنظيم الاتصالات.

-مشروعية دخول وتفتيش أماكن استخدام شبكة الإنترنت أو الكمبيوتر

نفرق في هذه الحالة بين ما إذا كانت هذه الأماكن من المساكن أو الأماكن العامة أو من الأماكن الخاصة أو إذا ما كانت أماكن عامة بالتخصيص، وذلك على النحو التالي:

أ_ الأماكن الخاصة: لا يجوز لرجال السلطة الدخول والتفتيش إلا بناء على إذن قضائي أو إذا توافرت حالة الضرورة كتعقب مجرم هارب.

ب- الأماكن العامة بطبيعتها: وهي الأماكن التي يجوز لأي شخص ارتيادها دون إذن قضائي، كأندية الإنترنت أو السايبر. وفي حالة دخول مأموري الضبط القضائي هذه الأماكن يكون ذلك استعمالاً لسطلتهم الوظيفية في الضبط الإدراي لا القضائي، فلا يستهدف من دخولهم ضبط جريمة أو أشياء متحصلة عنها، بل غرضهم هو التأكد من تطبيق القوانين واللوائح؛ ومع ذلك إذا تم ضبط جريمة في هذه الأماكن فيكون الضبط صحيحاً وتتوافر حالة التلبس.

ج- الأماكن العامة بالتخصيص: هي أماكن ذات طبيعة عامة يباح الدخول فيها للجمهور خلال وقت معين كالنوادي والمقاهي والمكاتب، فإذا أغلقت أبوابها تحولت إلى أماكن خاصة غير جائز دخولها إلا بناء على إذن من سلطات التحقيق. فإذا خالف مأمور الضبط ذلك

[38] نقض 13 يونيه سنة 1977، مجموعة أحكام النقض س 28 ص 775 رقم 161 طعن رقم 245 لسنة 47 ق.

كان دخوله غير مشروع، ويستتبعه بطلان كل ما يقوم بضبطه من جرائم ولو كانت في حالة تلبس. بناء على ذلك يحق لمأمور الضبط دخول هذه الأماكن وقت إتاحتها للجمهور، للتأكد من تنفيذ القوانين واللوائح وعدم وقوع مخالفة لها، فإذا ضبط وقوع جريمة توافرت حالة التلبس.

ويشترط في ذلك أن تكون معاينة الجريمة قد تمت بشكل عرضي إثر الدخول المشروع لا أن يقوم مأمور الضبط بالتنقيب عنها. كما لا يجوز لمأمور الضبط البحث عن الأشياء غير الظاهرة. فإذا فتح مأمور الضبط جهاز الكمبيوتر لاستخدامه كشخص عادي فلا يجوز له البحث والتنقيب داخل جهاز الكمبيوتر بحثاً عن وجود صور مخلة بالآداب على سبيل المثال، بل إذا فتح الجهاز وظهرت أمامه دون التنقيب عنها يعد ضبطه هذا صحيحاً وتتوافر حالة التلبس.[39]

تطبيقا لذلك قضت المحكمة العليا للولايات المتحدة الأمريكية – في قضية Collins لعام 2016 بصحة ما تحصل عليه مأموري الضبط من الفيسبوك من صور لسيارة مسروقة كان المتهم قد قام بنشرها على صفحته. أما ما قام به بعد ذلك من تخطي سور المنزل والقيام برفع غطاء السيارة المتواجدة داخله واكتشاف أنها هي نفس السيارة. فإن ما قام به مأمور الضبط من الدخول على صفحة المتهم على الفيسبوك هو عمل مشروع أما ما قام به من تخطي سور المنزل فهو عمل غير مشروع ولا يصح معه ضبط السيارة المسروقة كدليل[40].

- **مدى مشروعية اعتراض الرسائل والمحادثات من قبل مأموري الضبط القضائي**

يعرف الاعتراض بأنه "الحيازة السمعية أو غيرها من محتويات أي أسلاك أو اتصالات إلكترونية أو شفهية من خلال استخدام أي جهاز إلكتروني أو ميكانيكي أو أي

---

[39] شيماء عبدالغني عطاالله "الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظامين اللاتيني والأنجلو أمريكي"، دار النهضة العربية، مصر، 2005م، ص199.

[40] Supreme Court of the United States: Collins v. Commonwealth, No. 16-1027, 584 U.S. January 9, 2018. www.hrccourtreporters.com.Retrieved March 30 2019.

جهاز آخر"[41]. ويعرف أيضاً بأنه الحصول على محتويات الاتصال، أو الاستماع إلى محادثة هاتفية لشخص آخر أو قراءة بريد إلكتروني أو رسالة نصية أو رسائل شخص آخر.[42] والاتصالات الإلكترونية هي التي لا تحتوي على الصوت البشري، ولكنها تحتوي على أشياء مثل الكلمات أو الصور كرسائل البريد الإلكتروني.[43]

وعرفت اتفاقية بودابست في المادة 3 اعتراض الاتصالات أو المراسلات غير القانوني بأنه ينطوي على التنصت على محتوى الاتصالات أو رصده أو مراقبته أو شراء محتوى البيانات سواء بطريقة مباشرة من خلال الولوج إلى نظام الكمبيوتر واستخدامه، أو بطريقة غير مباشرة عن طريق استخدام أجهزة اختلاس السمع أو التنصت الإلكترونية، ويمكن أن ينطوي الاعتراض أيضاً على التسجيل.

ولكي يمكن القول بوجود عملية اعتراض يجب أن يتم الاعتراض في نفس الوقت الذي يتم فيه الاتصال. لذا، فالاستماع إلى محادثة هاتفية مباشرة بمثابة اعتراض، إلا أن الوصول إلى الملفات المخزنة على جهاز كمبيوتر ليس كذلك(إلا إذا اعتبر هذا النشاط غير قانوني بشكل منفصل).

ونلاحظ وجود فارق بين الاعتراض والإفصاح، فالأخير يعني إخبار شخص آخر بمحتويات الاتصال، بالإضافة إلى إخباره بطابعه العام أو جوهره. ويكون الإفصاح مخالفاً للقانون في حال تم الاعتراض بشكل غير قانوني. ترتيباً على ذلك إذا قام شخص ما باعتراض اتصال هاتفي بشكل غير قانوني حيث يناقش فيه المشاركون تورطهم في جريمة، ويعطون هذه المعلومات لمراسل صحيفة مثلاً، فإن القائم بالتعقب يمكن أن يكون مسؤولاً

---

[41] **E-Commerce Law Week**, Issue 205, ©Copyright 2002, Steptoe & Johnson LLP. https://www.steptoe.com .Retrieved Nov 20, 2018.

[42] **Wiretap Act, (18 U.S. Code § 2511)** :"Interception" is the acquisition of the contents of a communication, or, in other words, listening to another person's telephone conversation or reading another person's email, text, or other messages.

[43] **Wiretap Act, (18 U.S. Code § 2511)**: An "electronic" communication is one that does not contain the human voice, but contains things like words or pictures. Email messages are the best example of such communications.

عن انتهاك القانون. فعلى الرغم من أنه كان يحاول الإعلان عن جريمة، لكن السلوك مع ذلك غير قانوني.[44]

ويلاحظ أن اعتراض الرسائل يشكل ضبطاً لمحتواها والاطلاع عليها. وهي بهذا الوصف تخالف الحق في الخصوصية ومن ثم لا تدخل في عموم جمع الاستدلالات ويلزم لها صدور إذن بذلك. ونرى قصور المشرع المصري في تحديد سلطة مأمور الضبط القضائي في هذا الخصوص.

-اعتراض حزم البيانات

أغلب الجرائم المعلوماتية تتم باستخدام الشبكة وعبر الإنترنت، وقد عرفت اتفاقية بودابست 2001 في مادتها الأولى الشبكة بأنها ترابط بين نظامي الكمبيوتر أو أكثر، ويمكن أن تكون الوصلات أرضية مثل الأسلاك أو الكابلات. أو لاسلكية مثل الراديو أو الأشعة تحت الحمراء أو القمر الصناعي أو كليهما، ويمكن أن تكون الشبكة محدودة جغرافياً في منطقة صغيرة (شبكات المنطقة المحلية) أو أن تمتد على مساحة شاسعة (شبكات المنطقة الواسعة). ويعتبر الإنترنت هو الشبكة العالمية والذي يتكون من العديد من الشبكات المترابطة التي تستخدم جميعها نفس البروتوكولات، وتوجد أنواع أخرى من الشبكات قد لا تكون متصلة بالإنترنت وتكون قادرة على تحويل بيانات الكمبيوتر بين أنظمة الحاسوب.[45]

ونظراً لترابط وسائل تكنولوجيا الاتصالات، فقد أدى ذلك إلى تلاشي إمكانية التمييز بين الاتصالات السلكية واللاسلكية والاتصالات عبر الحاسب، الأمر الذي يترتب عليه إمكانية اعتراض الاتصالات المرسلة بواسطة نظام الحاسب، والتي من الممكن أن تشتمل على نقل الاتصال من خلال شبكات الاتصالات قبل استلامها بواسطة نظام حاسب آخر. ويتم تحليل حزم البيانات بالتقاطها واعتراضها عبر الشبكة، ومن خلال هذه العملية يتم رؤية كل حزم البيانات التي يتم إرسالها أو استقبالها عبر الشبكة، وأشهر أدوات اعتراض والتقاط حزم البيانات هو Wire shark والمعروف باسم محلل البروتوكولات.

---

[44] Brian Farkas, **How the Wiretap Act Protects Personal Privacy?,** https://www.lawyers.com. Retrieved Nov 20, 2018.

[45] المادة الأولى، اتفاقية بودابست (اتفاقية الجريمة الإلكترونية 2001م).

ويلاحظ أن حزم المعلومات يجوز لمأمور الضبط القضائي اعتراضها مادامت لا تحتوي على معلومات تتعلق بحرمة الحياة الخاصة كما لو كانت تفيد اتصالات بجهاز شخص معين على الشبكة مع شخص آخر. وهذا يدخل في عموم جمع الا ستدلالات وبالتالي لا يلزم للقيام بها سبق الحصول على إذن.

-تنظيم القضاء الأمريكي لسلطات مأموري الضبط القضائي على شبكة الانترنت

عندما يتعلق الأمر بمراقبة شبكة الإنترنت من جانب مأموري الضبط القضائي للحصول على معلومات أو بيانات تفيد في كشف الحقيقة، فقد أجاز القضاء الأمريكي ذلك استناداً إلى أن تلك المعلومات قد سلمها صاحب الحساب بإرادته إلى مزود الخدمات مثل ياهو أو جوجل[46]. وتواترت أحكام القضاء الأمريكي في اعتبار أن الشخص ليس له توقع لحرمة الحياة الخاصة إذا تعلق الأمر بمعلومات أعطاها الشخص للغير، عندئذ لا يتوافر لديه توقع بتوافر حرمة الحياة الخاصة التي يضمنها الدستور الأمريكي[47]. وذلك على الرغم من أن هناك من الأحكام ما يشكك في صلاحية تلك القاعدة التي تسري في الأمور المعتاده إذا طبقناها في مجال التطور المعلوماتي الذي بسببه يضطر الأفراد إلى تسجيل بياناتهم عند مزودي الخدمات للحصول على الخدمة ويضطر إلى استخدام البريد الإلكتروني بديلاً للبريد العادي[48].

ترتيباً على ما تقدم قُضي بأن من حق مأموري الضبط القضائي أن يتابع تواصل مستخدم الإنترنت على الشبكة وأن يحصل على معلومات تخص اسمه وعنوانه والمواقع التي يدخل إليها وبيانات حسابه على الشبكة[49]. وكذلك فإن من حقه أن يتابع الايميلات التي يرسلها من حيث المرسل والمرسل إليه وبيانات عنهما، باعتبار أن صاحب تلك الايميلات لا يتوافر في حقه توقع حرمة الحياة الخاصة التي يضمنها الدستور[50]. وبناء عليه فإن هذه

---

[46] United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008).

[47] Ex. United States v. Miller, 425 U.S. 435, 443 (1976)

[48] United States v. Jones, 132 S. Ct. 945, 957 (2012)

[49] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)

[50] United States v. Forrester, op.cit.

الأفعال تدخل في نطاق أعمال الضبط الإداري وأعمال الضبط القضائي التي يجوز لمأمور الضبط القيام بها بدون تطلب إذن قضائي. غير أن ذلك يختلف عن محتوى البريد الإلكتروني، حيث أن الاطلاع عليه يعد اعتداء على حرمة الحياة الخاصة. حيث قضي بأن استعمال قلم التسجيل Register Pen الذي يسمح بمعرفة من يتواصل المتهم معهم عن طريق البريد الإلكتروني لا يخالف الحق في حرمة الحياة الخاصة ويدخل بالتالي في أعمال الضبط القضائي التي يقوم بها مأمورو الضبط دون تطلب شرط سبق صدور إذن بذلك[51].

وبخصوص استعمال تطبيق يسمى key logger system وهو تطبيق يتم إرساله إلى كمبيوتر شخص معين وبالتالي يتم ذراعته في جهازه بغير علمه، والذي يقوم بتحديد الحروف التي قام هذا الشخص باستعمالها في الكتابة وبالتالي يمكن تخمين ما قام بإرساله من رسائل، فإن المحكمة الفيدرالية الأمريكية قضت بجواز استعمال ذلك وعدم تعارضه مع التعديل الرابع للدستور الأمريكي[52]. وجدير بالذكر أن التعديل الرابع يكفل حماية للشخص والمسكن من التفتيش غير المعقول، حيث ينص على أنه "لا يجوز المساس بحق الناس في أن يكونوا آمنين في أشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم من أي تفتيش أو احتجاز غير معقول، ولا يجوز إصدار مذكرة بهذا الخصوص إلا في حال وجود سبب معقول، معزز باليمين أو التوكيد، وتبين بالتحديد المكان المراد تفتيشه والأشخاص أو الأشياء المراد احتجازها".

المبحث الثاني

دور مقدم الخدمة في مرحلة جمع الاستدلالات

عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018 مقدم أو مزود الخدمة بأنه "أى شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن ينوب عنه فى أي من تلك الخدمات أو تقنية المعلومات".

---

[51] Smith v. Maryland, 442 U. S. 735 (Decided June 20, 1979).

[52] United States v. Scarfo, 180 F. Supp. 2d 572, 581 (D.N.J. 2001)

واشترطت الفقرة ثانياً من المادة 2 من قانون مكافحة جرائم تقنية المعلومات المصري مع عدم الإخلال بأحكام قانون حماية المستهلك الصادر بالقانون رقم 67 لسنه 2006، بأنه يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته ولأى جهة حكومية مختصة، فى الشكل، وبالطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية (1) اسم مقدم الخدمة وعنوانه. (2) معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الالكترونى. (3) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لاشرافها. (4) أيه معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويحددها قرار من الوزير المختص.

وقد فرق القانون الفيدرالي الأمريكي للاتصالات المخزنة "SCA"[53] بين نوعين من مقدمي الخدمات، الأول هم مقدمي خدمة الاتصالات الإلكترونية ECS ، وتكمن مهمتهم في تقديم خدمة إلى مستخدمي الشبكة كتسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية.[54] أما النوع الثاني فهم مقدمي خدمة معالجة البيانات عن بُعد " Remote Computing Service "ويعرف مصطلح RCS بأنه تقديم خدمات معالجة البيانات بالوسائل السلكية أو الراديو أو الوسائل الكهرومغناطيسية أو الضوئية الإلكترونية أو الاتصالات الإلكترونية، وأي مرافق حاسوبية أو معدات إلكترونية ذات صلة بالتخزين الإلكتروني لمثل هذه الاتصالات.[55]

---

[53] **The U.S. federal Stored Communications Act**, 18 U.S.C. § 2701 et seq. https://en.wikibooks.org/wiki/US_Internet_Law/SCA#"Electronic_communication_service". Retrieved Dec 4, 2018.

[54] **The U.S. federal Stored Communications Act : 18 U.S.C. § 2510(15).** "any service which provides to users thereof the ability to send or receive wire or electronic communications."

[55] **The U.S. federal Stored Communications Act, (18 U.S.C. § 2510(14)**:"provision to the public of computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any

ويشير التاريخ التشريعي والسوابق القضائية إلى أن القضية الرئيسية في تحديد ما إذا كانت شركة ما توفر نظام ECS هو دور الشركة في توفير القدرة على إرسال أو تلقي الاتصالات الدقيقة المعنية، بغض النظر عن الأعمال الأساسية للشركة. وعليه يمكن لأي شركة أو كيان حكومي يوفر للآخرين وسيلة للتواصل إلكترونيًا أن يكون "مزودًا لخدمة الاتصالات الإلكترونية" فيما يتعلق بالاتصالات التي يوفرها، حتى لو كان تقديم خدمة الاتصالات هو مجرد عرضي للوظيفة الأساسية لمزود الخدمة. فشركة الطيران التي تزود وكلاء السفر بنظام الحجز المحوسب للسفر الذي يتم الوصول إليه من خلال محطات كمبيوتر منفصلة يمكن أن تكون مزود خدمة اتصالات إلكترونية.[56] وعلى العكس من ذلك فلا يتوافر نظام تقديم خدمة الاتصالات الإلكترونية ECS إذا لم توفر الخدمة القدرة على إرسال أو استقبال هذا الاتصال، فعلى سبيل المثال الشركة المصنعة لألعاب الفيديو التي قامت بالوصول إلى البريد الإلكتروني الخاص المخزن على خدمة لوحات النشرات الخاصة بشركة أخرى من أجل انتهاك حقوق النشر لم تكن موفر لخدمة الاتصالات الإلكترونية. أيضاً الشركات التي تستخدم أجهزة الفاكس وأجهزة الكمبيوتر ولكنها لم توفر القدرة على إرسال أو استقبال الاتصالات لم تكن موفر لخدمة الاتصالات الإلكترونية.[57]

يبدو أن الفارق بين مقدمي خدمة ECS ومقدمي خدمة RCS تكمن في أن الأول يقوم بحفظ ملفات العميل في طريقها إلى وجهة ثالثة كما في حالة إرسال شخص بريد إلكتروني إلى شخص آخر، فيمر البريد عبر مقدم خدمة الاتصالات الإلكترونية ESC

---

computer facilities or related electronic equipment for the electronic storage of such communications."

[56] United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993). Retrieved Dec 5, 2018. https://en.wikibooks.org/wiki/US_Internet_Law/SCA#"Electronic_communication_service".

[57] State Wide Photocopy v. Tokai Fin. Serves. Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995). See also: Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996). https://law.justia.com/cases/federal/district-courts. Retrieved Dec 5, 2018.

وتظل مخزنه لديه إلى أن يقوم المرسل إليه باستلام البريد الإلكتروني، أي أنه يقوم بحفظ البيانات إلى حين وصولها إلى طرف ثالث. أما مقدم الخدمة عن بعد RCS فيقوم بتخزين ومعالجة البيانات لديه هو كمقدم خدمات الإعلانات فهو مقدم خدمة عن بعد، كذلك في حالة وجود حاسب مركزي يقوم بتخزين البيانات لاسترجاعها في المستقبل فتتوافر خدمة RSC.

-التزامات وواجبات مقدم الخدمة

تضمنت المادة 2 من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018 التزامات وواجبات مقدم الخدمة بقولها : **أولاً** : مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم 10 لسنه 2003، يلتزم مقدمو الخدمة بما يلى :

(1) حفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات لمدة 180 يوماً متصلة وتتمثل البيانات الواجب حفظها وتخزينها فيما يلى :

أ- البيانات التى تمّكن من التعرف على مستخدم الخدمة.

ب- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرته.

ج – البيانات المتعلقة بحركة الاتصال.

د- البيانات المتعلقة بالأجهزة الطرفية للاتصال.

هـ – أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.[58]

(2) المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته أو أى بيانات أو معلومات متعلقه بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها.[59]

---

[58] يقصد به الجهاز القومي لتنظيم الاتصالات في مصر.

[59] وتعاقب المادة (31) من نفس القانون بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند

(3) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.

ثالثا : مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي، ووفقاً لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون.

رابعاً : يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين ويحظر على غير هؤلاء القيام بذلك.

وقد أصدر الكونغوس قانون حماية خصوصية الاتصالات الإلكترونية الأمريكي "ECPA" في محاولة لمعالجة الصدام بين التقدم التكنولوجي في هذا المجال والحق في الخصوصية. حيث نص هذا القانون على أن المقصود بالتخزين الإلكتروني "أي تخزين مؤقت أو وسيط لسلك أو اتصال إلكتروني عرضي للإرسال الإلكتروني منه" أو " أي تخزين لهذا الاتصال بواسطة خدمة اتصالات إلكترونية لأغراض الحماية الاحتياطية لمثل هذا الاتصال"[60]. ويستفاد من ذلك أن المقصود بالتخزين الإلكتروني أو حفظ نظام السجل المعلوماتي يشير فقط إلى التخزين المؤقت، الذي يتم إجراؤه أثناء الإرسال، من خلال مقدم خدمة الاتصالات الإلكترونية.

---

(2) من الفقرة أولا من المادة (2) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمى الخدمة.

-كما نصت المادة (33) من نفس القانون على عقوبة الغرامة التي لا تقل عن 5 ملايين جنية ولا تجاوز 10 ملايين، كل مقدم خدمة أخل بأى من التزاماته المنصوص عليها فى البند (1) من الفقرة أولاً من المادة (2) والفقرة الثانية من البند رابعاً من هذا القانون. وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة القضاء بإلغاء الترخيص.

[60](**Electronic storage 18 U.S.C. § 2510(17)** : "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," or in the alternative as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

وعلى الرغم من أن نفس القانون حظر من قيام أي شخص أو كيان يقدم خدمة اتصالات إلكترونية للجمهور بالكشف عمداً عن محتويات أي رسالة أثناء نقل هذه الخدمة إلى أي شخص أو كيان آخر غير المرسل إليه أو المستلم المقصود لمثل هذا الاتصال، إلا أنه سمح لمقدم الخدمة أن يكشف عن محتوى الاتصال في حالة توافر اعتبارات ملحة من المصلحة العامة تفوق الحق في الخصوصية، كما في حالة الطوارئ الملحة أو تصادف العلم بدليل على ارتكاب جريمة أو وجوب ذلك لحماية مقدم الخدمة نفسه أو وجود تصوير فاضح للأطفال.[61] وأوجب على مقدم خدمات الاتصالات السلكية واللاسلكية الإلكترونية أو خدمة المعالجة عن بعد، بناء على طلب من جهة حكومية، اتخاذ جميع الخطوات اللازمة للحفاظ على السجلات والأدلة الأخرى الموجودة في حوزته ريثما يتم إصدار أمر من المحكمة، ويتم الاحتفاظ بالسجلات لمدة 90 يومًا، والتي يتم تمديدها لمدة 90 يومًا إضافية بناءً على طلب مجدد من الجهة الحكومية.[62]

---

[61] Catherine Pelker; Anthony J. Palmer; Brittany Raia; Jamin Agosti, "**Computer Crimes"**, 52 Am. Crim. L. Rev. 793 (2015), p 822.

[62] **18 U.S. Code CHAPTER 121— STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS: (f) Requirement To Preserve Evidence.—**

(1) In general.—

A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.—

Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

ويثور تساؤل عما إذا كانت هناك تفرقة بين الاتصالات في أثناء تنقلها والاتصالات المخزنة.

يجيب عن ذلك القانون الأمريكي الفيدرالي حينما ميز بين الاتصالات المخزنة والتي خصص لحمايتها أحكام قانون "حماية خصوصية الاتصالات الإلكترونية" لسنة 1986 (ECPA) وبين الاتصالات في أثناء تداولها والتي خصص لها أحكام قانون الباب الثالث من التقنين الفيدرالي الأمريكي ((2014) 2510-2522 §§ .U.S.C 18) وقانون("PR/TT") Pen Register/Trap and Trace Act وكذلك قانون the Stored Communications Act **("SCA").** وفيما يتعلق بالرسائل الإلكترونية فقد اتجهت بعض أحكام للقضاء الأمريكي إلى عدم تطبيق قانون Wiretap Act عليها[63]. غير أنه يلاحظ بالنسبة لرسائل البريد الإلكتروني (الايميل) والتي يتم تخزينها في أثناء تداولها، فاتجهت أحكام للقضاء الأمريكي كما في قضية Councilman إلى التعامل معها على أنها اتصالات متداولة، مع استبعاد أي أثر للوضع المؤقت للبريد الإلكتروني الذي يتم تخزينه مؤقتاً في أثناء تداوله، فاعتبرته اتصالات متداولة تخضع لقانون Wiretap Act[64]. وعلى أية حال يمكن القول بأن البريد الإلكتروني الذي يصل إلى صندوق المرسل إليه يصبح مراسلات مخزنة[65]، أما في أثناء انتقاله وقبل وصوله فإنه يتصف بالمراسلات المتداولة.

---

[63] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 78 (9th Cir. 2002); United States v. Steiger, 318 E3d 1039, 1048-49 (11th Cir. 2003); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 14 (3d Cir. 2004). https://casetext.com/case/fraser-v-nationwide-mut-ins-co. Retrieved Apr 19, 2019.

[64] United States v. Councilman, 418 E3d 67 (1st Cir. 2005). supremecourt.gov. Retrieved Sep 15, 2018.

[65] Councilman, 418 E3d 67 (1st Cir. 2005)

وفي هذا الفرض تفرق أحكام القضاء الأمريكي بين محتوى الرسالة وبين معلومات الرسالة. ففي الأخيرة يقتصر الالتقاط على مرسل الرسالة من خلال IP والمرسل إليه والوقت (Metadata)، بينما يتعلق محتوى الرسالة بما تضمنته من معلومات[66].

لهذا كان الغرض من وضع قانون Pen Register and Trap and Trace ("PR/FL") الذي ينظم استخدام Pen Register وكذلك Pen trap . فهما وسيلتان تستخدمان للتعرف على الجهاز المرسل والجهاز المستقبل وخط سير الرسالة أو الاتصال. وقد جرّم القانون السابق استخدامهما في التعرف على تلك البيانات بدون إذن من القضاء أو توافر استثناء مما نص عليه القانون في المادة ((18U.S.C. § 3121(a)).[67]

أما قانون الأمن اليومي الفرنسي رقم 2001-1062 المؤرخ في 15 نوفمبر 2001م، فقد نص على أنه في حالة الضرورة ولكشف الجرائم الجنائية ولأغراض التحقيق وبهدف تقديم معلومات إلى السلطة القضائية، يتم احتفاظ مقدمي الخدمة بالمعلومات والبيانات الفنية لمدة عام واحد كحد أقصى.[68]مشترطاً أن تنحصر تلك البيانات في معلومات عن الأشخاص

---

[66] Klayman v. Obama, 957 E Supp.2d 1, 35 (D.D.C. 2013) supremecourt.gov. Retrieved Sep 15, 2018.

[67] (a)In General.—

Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

[68]**Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne - Code des postes et des communications électroniques>Article 29. (Article L32-3-1. Créé par Loi n°2001-1062 du 15 novembre 2001 - art. 29 JORF 16 novembre 2001)** : II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à

المقدم لهم الخدمة وكذلك أنواع الخدمات المقدمة من قبل مزود الخدمة، ولا يجوز بأي حال من الأحوال الاحتفاظ بمحتوى المراسلات المتبادلة ولا أي معلومات تتعلق بموضوع هذه المراسلات.[69]

ويلزم التمييز بين حفظ البيانات والاحتفاظ بالبيانات، فحفظ البيانات يعني إبقاء بيانات توجد بالفعل في شكل مخزن محمية من أي شئ من شأنه أن يتسبب في تغيير جودتها أو وضعها الراهن أو تدهورها، بينما الاحتفاظ بالبيانات يعني إبقاء بيانات في حوزة الشخص لاستخدامها في المستقبل. وينطوي الاحتفاظ بالبيانات على تراكم البيانات في الوقت الحاضر وإبقائها أو حيازتها لفترة زمنية مقبلة. ويعتبر الاحتفاظ بالبيانات بمثابة عملية تخزين لها، أما حفظ البيانات فيمثل النشاط الذي يبقي تلك البيانات المخزنة سليمة وآمنه.[70]

- المعلومات الواجب تقديمها من قبل مقدمي الخدمات

لم ينظم قانون جرائم تقنية المعلومات مدى سلطات مأموري الضبط القضائي في الحصول من مزودي الخدمات على بعض المعلومات التي تدخل في إطار جمع الاستدلالات وفي نفس الوقت تساعدهم في عمل التحريات اللازمة للكشف عن الجرائم ومرتكبيها. ولا يعني ذلك أنه لا يجوز مساعدة مأمور الضبط في عمل التحريات ولكن

---

disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. **(Dernière modification : 3 juillet 2014))** -https://www.legifrance.gouv.fr, Retrieved jan 21, 2019.

[69] **Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (Article 29)**: - IV. - Les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

[70] التقرير التفسيري لاتفاقية الجريمة الإلكترونية (بودابست 2001م) سلسلة المعاهدات الأوروبية رقم 185، الصادرة عن مجلس أوروبا.

الأمر متروك للقواعد العامة التي تقضي بأن مأمور الضبط من واجبه أن يقوم بعمل تلك التحريات والتي تتضمن:

1- الدخول إلى المواقع العامة على شبكة الإنترنت وهي التي يجوز لأي شخص أن يدخل عليها أو يشاهدها كما في حالة اليوتيوب والمواقع المفتوحة للجمهور وذلك استناداً إلى سلطة مأمور الضبط في دخول الأماكن العامة[71].

2- طلب أسماء المشتركين وأرقامهم والمكالمات والاتصالات مع آخرين، وكل ما يتعلق بمعلومات تتعلق بالحسابات وبأصحاب تلك الحسابات، دون إفشاء محتوى الرسالة أو الاتصال، كون الإفشاء يقتضي سبق الحصول على إذن من سلطة التحقيق بذلك.

فغير ذلك من البيانات المخزنة من قبل مقدم الخدمة، فإنها تقتضي إذناً من سلطة التحقيق. وتتمثل هذه البيانات في بيانات الكمبيوتر أو المعلومات التي قد تكون في حوزة أو تحت سيطرة مقدم الخدمة، ولا ينطبق ذلك إلا إذا احتفظ مقدم الخدمة بتلك البيانات أو المعلومات، حيث أن بعض مقدمي الخدمة لا يحتفظون بسجلات المتعاملين في خدماتهم.

ويؤكد التقرير التفسيري لاتفاقية الجريمة الإلكترونية (بودابست 2001) أن المعلومات التي يمكن الأمر بتقديمها هي المعلومات اللازمة لتمكين إجراء عمليات البحث والمصادرة أو النفاذ. ويجب أن تقتصر تلك المعلومات على ما هو معقول، فالإفصاح عن كلمة السر يكون أمراً معقولاً، بينما لا يكون ذلك معقولاً عندما يؤدي الكشف عن كلمة السر أو أي تدبير أمني آخر إلى تهديد غير معقول لخصوصية مستخدمين آخرين أو بيانات أخرى غير مرخص بالبحث فيها.[72]

ويظهر اختلاف القانون المصري عن نظيره الفرنسي عندما نص هذا الأخير على معلومات محددة يمكن لمقدم الخدمة الاحتفاظ بها وتقديمها للعدالة متى تطلب الأمر ذلك وحدد تلك المعلومات على سبيل المثال على عناوين بروتوكولات الإنترنت IP Address كذلك المواقع التي تم زيارتها، وعناوين الرسائل المرسلة والمستقبلة وعناوين المرسل إليهم. أما القانون المصري فعلى الرغم من أن مدة حفظ وتخزين البيانات لا تزيد عن ستة أشهر

---

[71] نقض 28 ديسمبر سنة 1965 مجموعة أحكام النقض س 16 ص 847 رقم 185؛ نقض 15 مايو سنة 1977 س 28 ص 591 رقم 125 طعن رقم 119 لسنة 47 ؛ 9 فبراير سنة 1995 س 46 ص 336 رقم 49 طعن رقم 3039 لسنة 63 قضائية.

[72] التقرير التفسيري لاتفاقية الجريمة الإلكترونية (بودابست 2001م)، مرجع سابق.

إلا أنه توسع في نوع البيانات والمعلومات التي سوف يتم الاحتفاظ بها وتقديمها كما هو موضح بنص الفقرة الأولى من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات. وخاصة الفقرة ب- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرته. وقد عرف القانون الأخير محتوى النظام المعلوماتي في مادته الأولى بأنه "أى بيانات تؤدى بذاتها، أو مجتمعه مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى". كما نص في الفقرة هـ – أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز، يبدو أن هناك توسع في أنواع البيانات التي يجب على مقدم الخدمة الاحتفاظ بها وتقديمها إلى الجهات القضائية في حال طلبها. الأمر الذي يجعلنا نتساءل هل يعد ذلك انتهاكاً للحق في الخصوصية المعلوماتية؟ وهو ما سوف نجيب عليه لاحقاً.

-مدى مشروعية الكشف عن الاتصالات

يقيد القضاء الأمريكي من مجال حرمة الحياة الخاصة فيما يتعلق بالمعلومات والبيانات التي يزودها صاحب الحساب على شبكة الإنترنت والتي يعطيها طواعية لمزود الخدمات[73]. حيث يحرم من يشارك بياناته مع جهة أخرى من توقع حرمة الحياة الخاصة فيما يسجله المتصفح من بيانات تخص المستخدم من عنوان الايميل والمواقع التي يدخل عليها وكذلك ما يدونه من بيانات على حساباته على الإنترنت. حيث قضت المحكمة العليا الأمريكية بعدم وجود حق للحياة الخاصة فيما يخص تلك البيانات[74]. وأكدت المحكمة مراراً على عدم توافر الحق في الحياة الخاصة بالنسبة لما يسجله صاحب الحساب من اسم وعنوان دفع الفواتير أو عناوين IP [75]. كما قضي بأنه لا حرمة للحياة الخاصة فيما يعطيه صاحب الحساب إلى المحرك yahoo[76].

---

[73] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)

[74] United States v. Forrester, id.

[75] United States v. Hambrick, No.99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000)

[76] United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008)

-مدى جواز مراقبة مقدمي الخدمة للاتصالات الإلكترونية للمشتركين

لم ينص قانون جرائم تقنية المعلومات في مصر لسنة 2018 على حالات يجوز فيها لمزود الخدمات أن يقوم بدون إذن بمراقبة أصحاب الحسابات. على خلاف ذلك أورد المشرع الأمريكي الفيدرالي أحكاماً في هذا الخصوص، حيث سمح قانون حماية خصوصية الاتصالات الإلكترونية الأمريكي "ECPA" بالتنصت ومراقبة الاتصالات الإلكترونية في الحالات التالية:[77]

- صدور إذن قضائي من المحكمة أو بموجب قانون مراقبة الاستخبارات الأجنبية لعام 1978، أو بناء على طلب من حكومة أجنبية يخضع لاتفاق تنفيذي حدده النائب العام وأقره الكونغرس.[78]

---

[77] **(18 U.S. Code § 2511) .(Interception and disclosure of wire, oral, or electronic communications prohibited):** (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

[78] **Electronic Communications Privacy Act of 1986 (ECPA) :"pen trap provisions that permit the tracing of telephone communications" (18 U.S. Code § 3121) :**(a) In General.— Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

- موافقة طرف في الاتصال على تسجيل الاتصال وفقاً لقانون Wiretap Act.[79]أي موافقة الطرف المنشئ أو المرسل إليه أو المتلقي المقصود من هذا الاتصال.
- موافقة طرف في الاتصال لمقدم الخدمة باستخدام قلم التسجيل Pen trap أو جهاز المصيدة أو التتبع Trap and Trace device.
- لمقدم الخدمات أن يكشف عن محتوى الاتصال في حالة توافر اعتبارات ملحة من المصلحة العامة تفوق الحق في الخصوصية ([80]).
- السماح لمقدم الخدمة بأن يتابع مقتحمي الكمبيوتر (الهاكر) (الباب الثالث من قانون حماية الحياة الخاصة والاتصالات الالكترونية).
- في حالة اكتشاف مزود الخدمة عن غير قصد وقوع جريمة، وتم إبلاغ وكالات إنفاذ القانون.

ويكون الأمر بتوفير المعلومات أو المساعدة الفنية من قبل مقدم الخدمة خلال فترة زمنية معينة، يجب خلالها ألا يكشف أي مزود لخدمات الاتصالات السلكية واللاسلكية الإلكترونية عن وجود أي اعتراض أو مراقبة أو الجهاز المستخدم لإنجاز الاعتراض أو المراقبة التي صدر بها الإذن من المحكمة، إلى أن يتم له السماح بذلك. [81]

المبحث الثالث

الحق في الخصوصية المعلوماتية وعلاقتها بجمع الاستدلالات

الحق في الخصوصية من الحقوق اللصيقة بالإنسان، إلا أنها تعد من المفاهيم النسبية التي تختلف وتتغير بحسب أنواع المجتمعات والثقافات. وفي عصر ثورة تكنولوجيا المعلومات التي اجتاحت العالم بأكمله، أصبحت تتميز بطابع خاص وبأهمية خاصة لاسيما

---

[79] وهو قانون التنصت الأمريكي رقم (18U.S. Code § 2511) والذي يعنى بحماية خصوصية الاتصالات اللاسلكية والشفهية، وتحديد الظروف والضوابط التي يجوز بموجبها اعتراض الاتصالات السلكية واللاسلكية، ووضع اجراءات الحصول على أوامر الإذن بالتنصت.

[80] Catherine Pelker; Anthony J. Palmer; Brittany Raia; Jamin Agosti, Computer Crimes,op.cit, p. 822

[81] (18 U.S. Code § 2511.) Interception and disclosure of wire, oral, or electronic communications prohibited.

في ظل التحول نحو العالم الرقمي، الأمر الذي يشكل خطراً لا يستهان به على حرمة الحياة الخاصة في مجال المعلوماتية. وهو ما يفرض على كثير من الدول سن التشريعات والقوانين الخاصة بتقنية المعلومات وجرائم الإنترنت وحرمة الاعتداء على الحياة المعلوماتية.

وقد اهتمت العديد من الاتفاقيات الدولية بحرمة الحياة الخاصة، ولعل من أهمها الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية (اتفاقية روما لعام 1950م) والتي نصت في المادة 8 على أنه" 1-لكل إنسان الحق في احترام حرمة حياته الخاصة، وحرمة منزله ومراسلاته 2- يمنع تدخل السلطة العامة في ممارسة الإنسان لحقه المذكور إلا في الأحوال التي يبينها القانون، وفي حالة حماية الأمن القومي للمجتمع الديمقراطي، أو لحماية سلامة الناس أو للمصلحة الاقتصادية أو لمنع حالات الفوضى أو ارتكاب الجرائم، أو لحفظ الصحة والأخلاق العامة، أو لحماية ورعاية حقوق وحريات الآخرين."

وفي عام 1981م وضع الاتحاد الأوروبي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية[82]. حيث تضمنت تلك الاتفاقية مبادئ حماية أساسية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة، وتمنع نقل أية معلومات خارج الحدود إلا للدولة التي تتوفر لها حماية موازية كاستثناء.

أما في عام 1997م فقد وضع الاتحاد الأوروبي دليلاً إرشادياً، أطلق عليه "دليل الاتصالات" وهو يُعنى بتوفير حماية خاصة تغطي الهاتف والتلفزيون الرقمي وشبكات الهواتف الخلوية وغيرها من نظم الاتصالات، ووضع قواعد تتعلق بتزويد الخدمات الإلكترونية ومسائل الاشتراكات والتعرف على المشتركين. ومع السرعة الهائلة في مجال تكنولوجيا المعلومات، أصدرت المفوضية الأوروبية في عام 2000م نموذجاً جديداً لحماية

---

[82] وقعت على هذه الاتفاقية 31 دولة وصادق منها 21 دولة، وأكملت باقي الدول تصديقها على الاتفاقية في 25 يناير عام 2012م بعد انضمام 8 دول أخرى إلى الاتفاقية، ليصبح عدد أعضاؤها 39 دولة موقعة ومصدقة على الاتفاقية.

- للمزيد راجع: شريف يوسف حلمي خاطر "حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الإطلاع على البيانات الشخصية في فرنسا" مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد إبريل 57 لسنة 2015م. كذلك انظر: إبراهيم داود "الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية: دراسة تحليلية مقارنة" مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الأسكندرية،المجلد الثاني، العدد الأول، سنة 2017م.

الخصوصية في قطاع الاتصالات الإلكترونية أوسع نطاقاً من دليل الاتصالات الصادر في عام 1997م، حيث تناول قواعد خاصة بالتقنيات الحديثة وأنواعها، وتناول تعريفات جديدة تتعلق بخدمات الاتصال والشبكات والمراسلات والمكالمات ومواقع الويب، بل ووضع قواعد لحماية مستخدمي الهواتف الخلوية، كل ذلك بهدف توسيع نطاق حماية الحياة الخاصة المعلوماتية وفرض سيطرة على كافة أنواع معالجة البيانات.

وفيما يتعلق بالتشريعات الداخلية فقد نصت المادة 2 من قانون مكافحة جرائم تقنية المعلومات المصري في فقرتها الثالثة والخاصة بتحديد التزامات وواجبات مقدم الخدمة على أنه "مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومى، ووفقاً لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون".

وقد نصت المادة 57 من الدستور المصري الصادر عام 2014م على حرمة الحياه الخاصة بقولها "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك".

ولم ينظم المشرع المصري في قانون جرائم تقنية المعلومات سلطات مأموري الضبط القضائي في هذا المجال تاركاً إياها للقواعد العامة، وهذا لا يكفي نظراً لذاتية الاتصالات الإلكترونية والمشكلات القانونية التي تثيرها من ناحية عمل التحريات. ومع ذلك فقد اهتم بحماية حرمة الحياة الخاصة من عدوان وسائل التواصل الاجتماعي خاصة في الفصل الثالث من القانون السابق.

على خلاف ذلك عُنيت العديد من التشريعات المقارنة بسلطات مأموري الضبط القضائي في مجال تقنية المعلومات والتي يراعى فيها حرمة الحياة الخاصة. كالمشرع الفرنسي الذي أصدر قانون حماية المعالجات الآلية للبيانات والحريات الصادر في يناير 1978، وقانون الأمن اليومي الصادر في نوفمبر 2001 والمعدل في 2003. أما كندا

فأصدرت قانون الخصوصية في يونيه 1982 وقانون حماية البيانات الشخصية والوثائق الإلكترونية لعام 2000. وفي بريطانيا صدر قانون حماية البيانات لعام 1998، وقانون حرية المعلومات لعام 2000، وكذلك العديد من الدول كالتشيك والدنمارك والبرازيل.[83]

وفي الولايات المتحدة الأمريكية نص التعديل الرابع للدستور الأمريكي على أنه «لا يجوز المساس بحق الناس في أن يكونوا آمنين في أشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم من أي تفتيش أو احتجاز غير معقول، ولا يجوز إصدار إذن بهذا الخصوص إلا في حال وجود سبب معقول، معزز باليمين أو التوكيد، بحيث يبين هذا الإذن بالتحديد المكان المراد تفتيشه والأشخاص أو الأشياء المراد احتجازها»[84]. وعلى الرغم من ذلك يمنح قانون الاتصالات المخزنة الأمريكي لعام 1986 "SCA" السلطات المختصة صلاحية إجبار مقدمي الخدمات على تقديم الأدلة الموجودة لديهم دون الحاجة إلى حصول على إذن قضائي بذلك، إضافة إلى السجلات المتعلقة بمستخدميهم وذلك في حالات محددة حصراً، وفي أحيان أخرى رفضت الحصول على سجلات المستخدمين وبياناتهم إلا بعد الحصول على إذن قضائي صادر من المحكمة المختصة، أما فيما يتعلق بالكشف عن محتوى الاتصال ذاته وعلاقته بالحق في الحياة الخاصة، فإن الأمر يتعلق في هذه الحالة بمدة الاحتفاظ بالمحتوى الإلكتروني، ففي جميع الأحوال أجاز قانون SCA لجميع أجهزة الدولة المختلفة الحصول على محتوى الاتصال المخزّن لمدة 180 يوماً أو أقل دون تضمين محتويات الاتصال إلا بعد الحصول على إذن قضائي بذلك أو بموافقة العميل أو مستخدم الخدمة على هذا الكشف. شريطة أن تقدم الجهة الحكومية وقائع محددة وقابلة للتوضيح

---

[83] إصدرات مركز هردو لدعم التعبير الرقمي "التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات" القاهرة، 2018م، ص 21.

[84] **The Fourth Amendment to the U.S. Constitution states that:** “The right of the people to be secure in their persons, houses, 35 papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.”

تبين وجود أسباب معقولة للاعتقاد بأن محتويات الاتصال الإلكترونية المخزنة أو غيرها من المعلومات المطلوبة ذات صلة وضرورية لإجراء تحقيق جنائي مستمر.[85]

أما إذا تجاوزت مدة الاحتفاظ بالمحتوى الإلكتروني 180 يوماً فعلى الأجهزة المختصة بموجب المادة 2703 من نفس القانون الحق في اتباع اختيار من ثلاثة حتى تستطيع الحصول عليه وهي: الحصول على إذن، أو إصدار أمر استدعاء إداري، أو الحصول على أمر من المحكمة المختصة بهذا الكشف.[86]

- إشكالية تحديد مكان المتصل بالهاتف الخلوي وحرمة الحياة الخاصة في القانون الأمريكي

تعرضت المحكمة العليا للولايات المتحدة الأمريكية لمسألة ما إذا كان تحديد مكان المتصل بالهاتف الخلوي واستخدام هذا المكان بوصفه قرينة على ارتكاب أحد الأشخاص لجريمة معينة، يعتبر مشكلاً لتفتيش يخالف الدستور الأمريكي وبالتالي الحق في

---

[85] **18 U.S. Code CHAPTER 121— STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS (D):**"A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation". https://www.law.cornell.edu. Retrieved Feb 7, 2019.

[86] **18 U.S. Code CHAPTER 121— STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS : (b) Contents of Wire or Electronic Communications in a Remote Computing Service.—** (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

Except that delayed notice may be given pursuant to section 2705 of this title.

الخصوصية أم لا. وفي ذلك قضت المحكمة العليا الأمريكية في قضية DAVIS لسنة 2015 بأن تحديد مكان المتصل وربطه بالجريمة عن طريق معرفة مدى اقترابه من مسرح الجريمة، يستلزم صدور إذن قضائي بالتفتيش لدى الجهاز الخادم مع توافر الدلائل الكافية probable cause لاشتراك المتهم في الجريمة. وقد تعلق الأمر في هذه القضيه بمتهم في جريمة سطو مسلح واستصدر وكيل النيابة من القاضي إذناً بإلزام صاحب الجهاز الخادم بتقديم بيانات تحدد مكان صدور مكالمات تليفونية من المتهم مع شركاء له في الجريمة كدليل على اشتراكه معهم. وقد صدر الأمر بالفعل وتم تحديد مكان وجود المتهم في ضوء الاتصالات الصادرة منه مع شركائه. ولم تتضمن المعلومات شيئاً عن محتوى الاتصال[87]. وقد كان ذلك تطبيقاً لقانون Stored Communications Act ("SCA")[88]. وكان رأي المحكمة أنه كان من الواجب على النيابة العامة أن تطلب من القاضي إذن تفتيش وليس إذناً بتقديم معلومات؛ ذلك أن الأول يقتضي توافر دلائل كافية probable cause بينما الثاني يكفي لصدوره reasonable grounds وهو ما يشكل قاعدة أضعف من الأول.

ويستفاد من حكم المحكمة أن تحديد مكان تواجد المتهم من خلال مكالماته مع الجهاز الخادم هو أمر يخالف حرمة الحياة الخاصة، كونه يشكل نوعاً من التفتيش المخالف للدستور. وقد ردت المحكمة على الزعم بأن التداخل مسموح به ذلك أنه يهدف إلى معرفة بيانات أودعها صاحب الهاتف لدى الغير وبالتالي يسري عليه ما يسري على ما قرره القضاء الأمريكي من عدم توافر حرمة الحياة الخاصة لبيانات الحسابات الخاصة بالعميل لدى البنك[89]. وبالمثل فإن القضاء الأمريكي لم ير في التعرف على أرقام التليفونات التي اتصل بها شخص متعلقاً بحرمة الحياة الخاصة مادام هذا الجهاز هو

---

[87] United States v. Quartavious Davis (No. 12-12928. D.C. Docket No. 1:10-cr-20896-JAL-2) .Decided May 5, 2015. Supremecourt.gov. Retrieved April 1, 2019.

[88] Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq. Section 2703 of the SCA.

[89] United States v. Miller, 307 U.S. 174 (Decided May 15, 1939) . supremecourt.gov. Retrieved May 1, 2019.

جهاز العمل وقد سلم إليه لأغراض القيام بعمله[90]. وهنا ميزت المحكمة بين السر البنكي، الذي فيه يسلم العميل بياناته إلى البنك والاتصال التليفوني الذي لا يتوافر هذا التسليم.

وعلى العموم فإن هذا التردد والغموض في تطبيق القواعد العامة التي أعدت لظروف تقنية وتواصل اجتماعي مختلف عما هو سائد الآن وهو ما يجب إزالته. ولا يتم ذلك إلاّ بتنظيم تلك السلطات في تفاصيلها بشكل يقطع الطريق نحو التضارب في الرأي.

الفصل الثاني

الطبيعة الخاصة لمرحلة التفتيش والضبط بحثاً عن الدليل الرقمي

سوف نعالج في هذا الفصل التفتيش في جرائم تقنية المعلومات (في مبحث أول) والضبط والتحفظ على الأدلة المتحصلة من الأجهزة الرقمية (في مبحث ثان). وذلك على النحو التالي:

المبحث الأول

التفتيش في جرائم تقنية المعلومات

-تفتيش الأنظمة المعلوماتية وحرمة الحياة الخاصة

للرسائل الإلكترونية والمحادثات التليفونية حرمة خاصة بصاحبها، فلا شك أن الإحساس بالأمن الشخصي في المحادثات والرسائل ضمان هام لممارسة الحق في الحياة الخاصة من خلال تلك الوسائل.[91] ومع ذلك أجازت أغلب التشريعات مراقبة واعتراض المحادثات والرسائل لضبط ما يفيد في كشف الحقيقة عن جريمة ارتكبت، وهو ما يعد قيداً على حرية الأشخاص.

---

[90] Smith v. Maryland, 442 U. S. 735 (Decided June 20, 1979). Supremecourt.gov. Retrieved May 1, 2019.

[91] إيهاب عبدالمطلب "موسوعة المخدرات معلقاً عليها بآراء الفقه والقضاء وأحكام محكمة النقض منذ تاريخ إنشائها حتى عام 2014" المجلد الرابع "الإثبات في جرائم المخدرات" الطبعة التاسعة، المركز القومي للإصدارات القانونية، القاهرة، سنة 2016م، ص 388.

ووفقاً لما تضمنته المادة 95 إجراءات مصري فلقاضى التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت فى مكان خاص متى كان لذلك فائدة فى ظهور الحقيقة فى جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. وفى جميع الأحوال يجب أن يكون الضبط أو الإطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لاتزيد على ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة. ولم يشترط القانون شكلاً معيناً أو عبارات خاصة للأمر الصادر من جهة التحقيق بتكليف مأموري الضبط القضائي بتنفيذ الإذن الصادر بمراقبة المحادثات السلكية واللاسلكية، فالشرط الأساسي أن يكون الإذن الصادر مسبباً.[92]

غير أن الاتجاه السائد في التشريعات المقارنة أن الرسائل الإلكترونية (الايميل) يختلف عن الرسائل البريدية وأن الاتصالات الإلكترونية تختلف عن الاتصالات السلكية أو اللاسلكية. ومن ثم فإنه لا يجوز قياس هذه على تلك في الأحكام وبالتالي فلا يسري حكم المادة (95) سابقة الذكر على الرسائل والاتصالات الإلكترونية نظراً للطبيعة الخاصة وذاتية تلك الرسائل والاتصالات.

وهو ما لفت عناية المشرع الأمريكي حينما سن الكونجرس في الولايات المتحدة الأمريكية قانوناً لتنظيم الاتصالات الالكترونية (CALEA)، والمعروف أيضاً باسم "قانون الاتصالات الهاتفية الرقمية". وهو قانون تنصت على المكالمات الهاتفية في الولايات المتحدة

---

[92] – وقد قضت محكمة النقض المصرية بأنه " لما كان البين من مطالعة المفردات أن الإذن الصادر بوضع جهاز التليفون الخاص بالطاعنة تحت المراقبة قد صدر من أحد القضاه بدرجة رئيس محكمة بناء على ندبه من رئيس المحكمة الابتدائية إعمالاً لنص المادة 61 من القانون رقم 46 لسنة 1972 في شأن السلطة القضائية التي تجيز لرئيس المحكمة ندب أحد قضاتها عند غياب زميل له أو قيام مانع لديه فإنه يكون صحيحاً في القانون، ولما كانت الطاعنة لا تجادل في الظروف التي حدت برئيس المحكمة لندب أحد قضاتها لإصدار إذن المراقبة التليفونية فإن الإذن يكون قد صدر صحيحاً ممن يملكه وما تثيره الطاعنة في غير محله، ومتى كان مأمور الضبط القضائي قد قام بتنفيذ إذن المراقبة التليفونية بناء على ندبه من النيابة العامة فإن الإجراءات تكون قد تمت وفقاً لصحيح القانون". (نقض مصري 1985/10/9 مجموعة المكتب الفني س 36، ص 831)

تم إقراره في 25 أكتوبر عام 1994م، ودخل حيز التنفيذ في يناير 1995م. وكان المقصود من CALEA تعزيز قدرة وكالات تطبيق القانون على إجراء اعتراض قانوني على الاتصال من خلال مطالبة شركات الاتصالات السلكية واللاسلكية وشركات تصنيع معدات الاتصالات السلكية واللاسلكية بتعديل وتصميم معداتها ومرافقها وخدماتها لضمان امتلاكها قدرات مدمجة للمراقبة المستهدفة، والسماح للوكالات الفيدرالية بالتنصت الانتقائي لأي حركة اتصالات هاتفية؛ ومنذ ذلك الحين تم تمديده ليشمل حركة الإنترنت عريضة النطاق و VoIP. وتقول بعض الوكالات الحكومية أنها تغطي المراقبة الجماعية للاتصالات بدلاً من مجرد استغلال خطوط محددة، ولا يتطلب اعتراض الاتصالات القائم على CALEA إصدار أمر قضائي بذلك.[93]

-تفتيش الأنظمة الإلكترونية مساس ضروري بالحياة الخاصة

إن البحث في مسرح الجريمة والأدلة التقليدية المتعلقة بالوثائق أو السجلات، ينطوي على جمع الأدلة التي تم تسجيلها أو تقييدها في الماضي في شكل ملموس، وفي هذه الحالة يقوم مأمور الضبط بالبحث في هذه البيانات التي قد تكون حبراً على ورق وفحصها، ومصادرة السجل الملموس أو إبعاده من الأدلة، إلا أن ذلك لا يحدث إلا إذا توافرت أسباب تدعو للاعتقاد بأن هذه البيانات موجودة في مكان معين ومن شأنها أن توفر أدلة على جريمة جنائية معينة.

أما في إطار البحث عن الأدلة في البيئة الرقمية قد تطبق نفس شروط وخصائص البحث التقليدية، إلا أنه يتم اتخاذ إجراءات جنائية من شأنها الحصول على البيانات الرقمية بنفس الدرجة من الفاعلية كالبحث في سجل مادي للبيانات ومصادرته؛ وذلك بسبب الطبيعة الخاصة للبيانات الرقمية خاصة وجودها في شكل غير ملموس.[94]ولا تختلف درجة الاعتقاد

---

[93] **Public Law 103-414 .Communications Assistance for Law Enforcement Act** .by the 103rd Congress of the United States. Pub.L. 103-414, 108 Stat. 4279, H.R. 4922, enacted October 25, 1994.

[94] المادة 19 من اتفاقية بودابست 2001م. التقرير التفسيري للإتفاقية الصادر عن سلسلة المعاهدات الأوروبية رقم 185، الصادرة عن مجلس أوروبا.

المطلوبة للحصول على إذن قانوني لإجراء البحث، سواء تعلق الأمر ببيانات في شكل ملموس أو في شكل إلكتروني.

وقد أورد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل عام 1984 عدداً من الأسس الواجب احترامها ومراعاتها في حال الضبط والتفتيش عن الدليل المرتبط بجرائم إلكترونية والتي تتمثل في الأتي:

1- وجوب تحديد السلطات التي تقوم بالتفتيش والضبط في بيئة تكنولوجيا المعلومات.

2- السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته مع استخدام الأدلة المتحصل عليها أمام المحاكم.

3- يجب مراعاة المسائل المرتبطة بفنية المعلومات وما يمثله ضياع الفرص الاقتصادية وانتهاك حرمة الحياة الخاصة وكذا تكلفة إعادة بناء قاعدة بيانات وهذا قبل كل تفتيش أو تحقيق.

4- إعادة النظر في قواعد الإثبات الإلكتروني ومصداقية الأدلة مع مراعاة القواعد التشريعية.

والتفتيش هو إجراء لاحق لارتكاب الجريمة، ويعني البحث في مستودع أسرار فرد معين عن أدلة تفيد التحقيق بشأن جريمة معينة –جناية أو جنحة– وقعت وتقوم دلائل جدية ضد هذا الشخص على ارتكابها، وقد يكون محل التفتيش شخص أو مكان له حرمته.[95]

–اتفاقية الجريمة الإلكترونية (بودابست) تم اعتمادها من لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/ تشرين الثاني 2001م) وفتح باب التوقيع في بودابست في (23 نوفمبر/ تشرين الثاني 2001م)، وترمي هذه الاتفاقية بشكل أساسي إلى:

1- مواءمة عناصر القانون الموضوعي الجنائي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية.

2- التنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائياً علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل إلكتروني.

3- إنشاء نظام سريع وفعال للتعاون الدولي.

[95] عبدالرءوف مهدي "شرح القواعد العامة للإجراءات الجنائية" دار النهضة العربية، مصر، 2007م، ص 489.

أما التفتيش في مجال تقنية المعلومات فيعني الولوج إلى نظم المعالجة الآلية للبيانات بحثاً وتنقيباً في البرامج المستخدمة وملفات البيانات المخزنة عما يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها.[96] وبما أن نظام الكمبيوتر يعني "أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة"، فينطبق البحث والتفتيش على الحاسب وعناصره ذات الصلة كآلة الطباعة وأجهزة التخزين ذات الصلة أو الشبكة المحلية، بل يجوز في بعض الأحيان الولوج إلى البيانات التي يتم تخزينها فعلياً على نظام أو جهاز آخر من خلال نظام الحاسب الذي يتم فيه التفتيش وفقاً لضوابط قانونية معينة.

كما أن معظم أحكام القضاء المقارن تبنت تفسيراً موسعاً لمدلول الأشياء محل التفتيش، حيث ينسحب إلى بيانات الحاسب حتى في ظل غياب نصوص خاصة تحكم إجراءات التفتيش في هذه الحالة. الأمر الذي يثير إشكالية أكثر أهمية، تتعلق بأن معظم جرائم الكمبيوتر قد تعتمد على نظام معلومات واحد أو قد تتجاوزه إلى أنظمة أخرى غير النظام المشتبه فيه،[97] وهو ما يستلزم معه امتداد التفتيش إلى أنظمة أخرى غير النظام محل الاشتباه وهو ما ينتج عنه إشكالية أخرى تتعلق بمدى احترام وعدم المساس بالحريات الشخصية وسرية الاتصالات للأشخاص الذين يمتد إليهم التفتيش.

- التفتيش في الجرائم المعلوماتية إجراء تحقيق وليس استدلال

يختلف التفتيش كإجراء استدلال عن التفتيش كإجراء تحقيق، فالأول لا يهدف إلى جمع الأدلة عن جريمة معينة، وإنما هو إجراء إداري قد يتم في أحوال الضرورة، وقد يكون الهدف منه التحري عن جريمة محتملة لا عن جريمة وقعت بالفعل. أما التفتيش كإجراء تحقيق يهدف إلى التنقيب عن الأدلة في جريمة وقعت بالفعل.

والأصل أن التفتيش كعمل من أعمال التحقيق تباشره سلطة التحقيق، بينما يخول استثناء لمأمور الضبط باعتباره عمل تحقيق يختص به استثناء بشرط الحصول على إذن من القاضي المختص أو النيابة وفق أحكام القانون. وفي هذه الحالة لا يجوز لغير مأموري

---

[96] أحمد سعد محمد الحسيني "الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية" رسالة دكتوراه، كلية الحقوق، جامعه عين شمس، سنة 2012م، ص 198.

[97] مصطفى إبراهيم العربي "دور الدليل الرقمي في الإثبات الجنائي" مجلة البحوث القانونية، كلية القانون- جامعة مصراته، العدد الأول، سنة 2016، ص90.

الضبط القضائي القيام بالتفتيش كإجراء تحقيق، على عكس التحريات كإجراء من إجراءات الاستدلال، إذ يجوز في بعض الأحوال أن يقوم شخص خوله القانون صفة الضبطية القضائية استثناء كأعضاء الجهاز القومي لتنظيم الاتصالات. ويسري ذلك على التفتيش عن الدليل الإلكتروني سواء أكان تفتيشاً مباشراً للجهاز أم تفتيشاً له عن بعد، وسواء أكان لجهاز معين أو لشبكة تربط عدة أجهزة.

وفي هذه الحالة يلتزم مأمور الضبط بما ورد في إذن التفتيش ولا يتعداه إلى تفتيش شخص أو مكان أخر، حيث قضت المحكمة بأنه "من المقرر أن الأمر الصادر من النيابة العامة لأحد مأموري الضبطية القضائية بإجراء تفتيش لغرض معين–فيديو وتليفزيون وأفلام منافية للأداب– لا يمكن أن ينصرف بحسب نصه والغرض منه إلى غير ما أذن بتفتيشه إلا إذا شاهد عرضاً أثناء إجراء التفتيش جريمة قائمة في إحدى حالات التلبس" .[98]

- **تنظيم تفتيش الأنظمة المعلوماتية في القانون المصري**

نظم قانون جرائم تقنية المعلومات تفتيش الأنظمة المعلوماتية واستلزم لها سبق صدور إذن بذلك من سلطة التحقيق.

في ذلك تنص المادة (6) من القانون السابق على أنه :

"لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي:

1- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لها مقتضى.

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

---

[98] حكم نقض مصري، الطعن رقم 1110 لسنة 68 ق، جلسة 19 مايو سنة 1998.

3- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو الجهاز التقني، وفى كل الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسبباً. ويكون استئناف الأوامر المقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة في المواعيد ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية".

- **الحماية من التفتيش غير المعقول في القانون الأمريكي**

يحمي التعديل الرابع من الدستور الأمريكي الأفراد من التفتيش غير المعقول. حيث قضت المحكمة العليا للولايات المتحدة الأمريكية بأن التفتيش يعتبر غير معقول إذا توافر توقع لحرمة الحياة الخاصة. ويتحقق هذا التوقع عند توافر شرطين: إذا توقع الشخص حرمة لحياته الخاصة بأن كان يحرص على عدم إطلاع الغير على ما يخصه. وكذلك إذا اعتبر المجتمع أن التفتيش يمس حرمة الحياة الخاصة وبالتالي فإنه يصبح غير معقول.

ويثار التساؤل عما إذا كان تفتيش الكمبيوتر يتماثل مع تفتيش الأشياء المادية وهو ما قصدته القوانين في البداية. حيث قضت المحكمة العليا الأمريكية بأن تفتيش الكمبيوتر يتماثل مع هذا النوع التقليدي من التفتيش[99]، فالشخص له حق في توقع الحياة الخاصة بالنسبة للكمبيوتر المتواجد في منزله[100]، وهو ما أقر به القضاء حينما قضي بأن الشخص له حق في توقع الحياة الخاصة في الكمبيوتر الخاص به والذي يحتفظ به في مسكنه[101]، وأن ما يمتلكه الشخص في مسكنه يغطيه الحق في الخصوصية، ومنه جهاز

---

[99] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, supremecourt.gov. Retrieved April 30, 2019.

740 (1979) (adopting Justice Harlan's privacy test). The Fourth Amendment also prohibits obtaining information by physically intruding on a constitutionally protected area. United States v. Jones, 132 S. Ct. 945, 950 n.3 (2012).

[100] United States v. Heckenkamp, 482 F3d 1142, 1146 (9th Cir. 2007)

الكمبيوتر[102].كما قُضي بأن هذا الحق يغطي الملفات التي وضع لها صاحبها كلمة سر(باسورد) لحمايتها على الرغم من أن زوجته قامت بتأجير هذا الجهاز لغيره[103].

- **تفتيش أجهزة كمبيوتر العمل والإدارات**

إذا تعلق الأمر بكمبيوتر ينتمي إلى موظف عام في جهة عمله، فهناك اعتبارين متعارضين؛ الاعتبار الأول أن الكمبيوتر ينتمي إلى الجهة العامة وهو مسلم إلى الموظف كي يستعمله في واجبات عمله فقط. والاعتبار الثاني أن الجهة الإدارية لم تعلن عن حقها في تفتيش الكمبيوتر، كما أن الموظف من حقه أن يضع رقماً سرياً على الكمبيوتر المسلم إليه. فالاعتبار الأول يسمح لجهة العمل بتفتيش كمبيوتر العمل بينما لا يسمح لها الاعتبار الثاني بهذا الإجراء. وفي ذلك اتجهت بعض أحكام القضاء الأمريكي إلى أن الأصل هو أن الموظف العام له حق في التوقع المعقول لحرمة الحياة الخاصة مادام الكمبيوتر مخصص له، إلاّ إذا وجدت مصلحة اجتماعية ملحة تبرر هذا التفتيش[104]. كما قضي بأن الموظف العام يتمتع بالحق في توقع الحياة الخاصة بالنسبة لما يرسله من هذا الجهاز من إيميلات[105]. أما إذا كانت التعليمات الداخلية بالعمل قد نصت على أن استعمال شبكة الإنترنت محل مراقبة من جهة العمل، فإن الموظف ليس له توقع في حرمة حياته الخاصة فيما يتعلق بذلك على ما قضت به المحكمة العليا للولايات المتحدة في قضية United States v. Simons[106].

ولا تختلف معطيات المشكلة في حالة العمل في القطاع الخاص حيث تعترف أحكام القضاء بأن المستخدم له حق في حرمة الحياة الخاصة، وعليه فلا يجوز لرب العمل أن

---

[101] United States v. Heckenkamp, 482 E3d 1142, 1146 (9th Cir. 2007)

[102] Guest v. Leis, 255 E3d 325, 333 (6th Cir. 2001).

[103] United States v. Buckner, 473 E3d 551, 554 n.2 (4th Cir. 2007)

[104] O'Connor v. Ortega, 480 U.S. 709, 719-20 (1987)

[105] United States v. Long, 64 M.J. 57 (C.A.A.F. 2006); United States v. Angeyine, 281 F.3d 1130, 1134-35 (10th Cir. 2002

[106] United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)

يقوم بمراقبة جهاز الكمبيوتر الخاص به أو أن يقوم في غيابه أو بدون موافقته بتفتيشه[107]. غير أنه في حالة وجود إخطار بأن الجهاز محل مراقبة، أو كانت المراقبة واضحة أو وقع المستخدم عقد عمله مع وجود هذا الشرط، فإن الموظف ليس له توقع في حرمة حياته الخاصة [108].

-طريقة التفتيش بحثاً عن الدليل الالكتروني

فيما يتعلق بطريقة تفتيش جهاز الكمبيوتر، أجازت أحكام القضاء الأمريكي أن يتم ضبط الجهاز تمهيداً لتفتيشه نظراً لصعوبة هذا التفتيش والوقت الطويل الذي قد يستغرقه[109]. كما أن القائم بالتفتيش لا يلتزم بفتح ملفات معينة والامتناع عن فتح ملفات أخرى لا يبدو منها أنها تتعلق بموضوع التفتيش؛ ذلك أن صاحب الجهاز قد يعمد إلى وضع اسم للملف يختلف عن محتواه[110].

كما أجاز هذا المفهوم الموسع لتفتيش جهاز الكمبيوتر ما قامت به سلطة التحقيق من تفتيش الهارد وير والسوفت وير وصولاً إلى التعرف على وجود ملفات معينة تحتوي ما يشكل جريمة مطلوب ضبط أدلة متعلقة بها[111]. وبناء عليه فإن أحكام القضاء الأمريكي تتجه إلى جواز تفتيش كل أجزاء الكمبيوتر وملحقاته عند صدور إذن بتفتيش الجهاز بحثاً عن أدلة جريمة معينة[112].

ومع ذلك يجب أن يكون إذن التفتيش محدداً بالبحث عن أدلة جريمة معينة وليس إذناً عاماً بتفتيش الكمبيوتر. في هذه الحالة الأخيرة يعتبر القضاء الأمريكي إذن التفتيش مخالفاً

---

[107] United States v. Long, 64 M.J. 57 (C.A.A.FI 2006)

[108] United States v. Angeyine, 281 E3d 1130, 1134 35 (10th Cir. 2002); United States v. Simons, 206 E3d 392, 398 (4th Cir. 2000)

[109] United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999)

[110] United States v. Gray, op.cit; United States v. Sissler, No.1:90-CR-12, 1991 WL 239000, at 4 (W.D. Mich. Aug. 30, 1991)

[111] United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998)

[112] United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998)

للقانون[113]. كما لا يعتبر إذناً معيباً بعدم التحديد – وفقاً لأحكام القضاء الأمريكي– أن يصدر بتفتيش كل جهاز خادم يتصل به المتهم لضبط ما يحوزه من ملفات تفيد نقل أو الدعاية أو التوزيع أو الحيازة لمواد إباحية خاصة بالأطفال.[114] وكذلك الإذن الذي أمر بضبط الملفات والصور دون الإشارة في الإذن إلى الجريمة المرتكبة والهدف من التفتيش[115].

ولا يشترط في تفتيش الكمبيوتر أن يتم انتقال القائم بالتفتيش إلى مكان وجود الجهاز؛ حيث أجازت أحكام القضاء أن يتم الدخول إلى الجهاز عن بعد بواسطة تطبيقات تسمح بذلك الدخول لمراقبة شاشة الكمبيوتر والمواقع التي يدخل عليها مستخدم الجهاز، ومن ثم ضبط الملفات المطلوب ضبطها كدليل عن الجريمة[116].

ونلاحظ أن مستخدمي الكمبيوتر ومواقع الإنترنت كثيراً ما يستخدمون أسماء مستعارة مضللة كعنوان للملفات التي ينشئونها داخل جهازهم، وهنا أجازت المحكمة العليا الأمريكية فتح الملفات على الرغم من أن ظاهرها عدم تعلقها بجرائم مالية وهي التي كانت الغرض من التفتيش. ومن ثم فإن اكتشاف احتواء مثل تلك الملفات على صورة مخلة للأطفال يكون منشئاً لحالة تلبس صحيح ويصح الدليل المستمد من تفتيشها[117]. وفي نفس المنطق قضي بأنه إذا كان التفتيش في الكمبيوتر عن جريمة تهديد وابتزاز، وعثر القائم بالتفتيش على ملفات تحوي صوراً مخلة للأطفال، فإن التفتيش يصح بناءً على حالة التلبس الجديدة[118]. وقضي بصحة التفتيش عن حيازة تلك الصور المخلة إذا كان الغرض من التفتيش هو ضبط دلائل عن تهريب المخدرات[119]. ومتى توافرات هذه الحالات فتلزم المحكمة القائم بالتفتيش

---

[113] Crowther v. State, 249 P.3d 1214, 1222 (Kan. Ct. App. 2011)

[114] United States v. Richards, 659 F.3d 527 (6th Cir. 2011)

[115] United States v. Clough, 246 F Supp. 2d 84 (2003)

[116] United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997)

[117] United States v. Stabile, 633 F.3d 219, 240–42 (3d Cir. 2011)

[118] United States v. Williams, 592 F.3d 511, 521–24 (4th Cir. 2010)

[119] United States v. Burgess, 576 F.3d 1078, 1096 (10th Cir. 2009)

في الكمبيوتر في حال فتحه جميع الملفات أن يقوم بحلف اليمين عند استجوابه، ومؤدى ذلك أنها أجازت التجول في الكمبيوتر وفتح جميع ملفاته[120].

ومع ذلك فإن هناك خلافاً بين أحكام القضاء الأمريكي بشأن مفهوم التفتيش بحثاً عن الجرائم الإلكترونية؛ هل يتخذ المفهوم الموسع؟ وهل يجوز ضبط ملفات لا تتعلق بالجريمة التي يتم التفتيش بحثاً عن دليل عنها؟ وهل يتوافر مفهوم التلبس عند تفتيش الكمبيوتر؟

فقد انقسم الرأي حول جواز قيام مأمور الضبط بفتح ملفات في الكمبيوتر ليس لها علاقة بالغرض الذي كان من أجله التفتيش؛ ذلك أن التفتيش يتقيد بالغرض منه، كما أن حالة التلبس تجيز التفتيش إذا كان من الظاهر أن الملف يشكل حيازته أو تخزينه في الكمبيوتر جريمة وفقاً للقواعد العامة[121]. إذن فالعبرة بظاهر الملف حتى ولو كان غير متعلق بالجريمة التي من أجلها يتم التفتيش. غير أن الأمر يثير إشكالية أكثر أهمية حول المظهر الخارجي؛ فمتى يتوافر بالنسبة للملف؟ هل من مجرد اسم الملف أو أنها تتوافر بعد فتح الملف؟ نعتقد أن اسم الملف يكفي، ذلك أن فتح الملف يتضمن تفتيشاً. غير أن القائم بالتفتيش يصعب أن يعلم بأن الملف الذي أمامه بعيد كل البعد عن غرض التفتيش فيتجنبه. وبالتالي فهو مضطر إلى فتحه. وإذا فتحه ووجد ما يشكل حيازته أو تخزينه في الكمبيوتر جريمة، فإن حالة التلبس تعد متوافرة وفقاً للقواعد العامة في التفتيش بناء على حالة التلبس plain view exception [122]. فالقائم بالتفتيش يقوم بتفتيش الكمبيوتر، إذن فهو يفتش محتويات الكمبيوتر وما يتضمنه من ملفات في أجزائه المختلفة. وبالتالي فإنه لا يتعدى الغرض المقصود من التفتيش. فمثلاً إذا كان يفتش عن صور مخلة للأطفال فإن ذلك يقتضي فتح جميع الملفات. وإذا كان يفتش عن برامج فيروسات أو أقول تتضمن تهديدات أو ابتزاز أو دعوة إلى الكراهية، وكان من الواضح أن الملف يتضمن فيلماً، فإن فتح هذا الفيلم لا يكون ضرورياً بالنظر إلى الغرض الذي من أجله كان التفتيش. أما إذا ظهرت صورة فاضحة لطفل من الأطفال قبل فتح الملف، فإن حالة التلبس تكون صحيحة

---

[120] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010)

[121] United States v. Hill, 459 F.3d 966, 974 (9th Cir. 2006)

[122] Horton v. California, 496 U.S. 128 (1990)

ويصح فتح هذا الملف على الرغم من أن الغرض من التفتيش كان لضبط أدلة تفيد في الكشف عن جريمة الدخول غير المشروع مثلاً.

وقد أثيرت مشكلة قانونية تتعلق بمدى توافر حالة التلبس في جرائم الكمبيوتر وبعد تردد أحكام للقضاء الأمريكي برفضها[123]، عادت لتقر توافرها وترتب آثارها في مجال الدليل الإلكتروني. وبررت المحاكم قراراتها بأنه مادام الملف كان واضحاً بأن كانت حيازته تشكل جريمة، فيجوز لمأمور الضبط أن يقوم بضبطه ويصح الاستناد إليه كدليل في الإدانة[124]. تطبيقاً لذلك قضي بأن مأمور الضبط الذي يفتش جهازاً للكمبيوتر لضبط أدلة جريمة من الجرائم المالية له أن يضبط ملفاً ظاهر الحال أنه يتضمن صوراً فاضحة للأطفال؛ ذلك أن حيازته تعد جريمة[125].

فلا شيء يحول دون توافر حالة التلبس إذا فوجئ مأمور الضبط في أثناء تفتيش صحيح بوجود ملف يحوي ما يشكل حيازته جريمة أو دليل على وقوع جريمة وهو ما استقرت إليه أغلب أحكام القضاء الأمريكي[126]. فإذا كان القائم بالتفتيش يبحث عن دليل في اتهام بجريمة مالية واضطر إلى فتح ملفات عليها أسماء مستعارة وفوجئ بوجود صور جنسية للأطفال فإن إجراءات الضبط تكون صحيحة[127]. حيث أن ضبط هذه الصور يعد صحيحاً وفقاً لفكرة التلبس إذا كان التفتيش بقصد ضبط دليل عن اتهام بتهديدات وتحرش عن طريق رسائل أرسلت بالايميل[128]. وبالمثل بالنسبة لمن يفتش الجهاز بحثاً عن أدلة تفيد في كشف الحقيقة عن جريمة اتجار بالمخدرات ثم وجد صوراً فاضحة للأطفال[129]. وفي بعض الأحيان تقرر

---

[123] United States v. Stabile, 633 F.3d 219, 240–42 (3d Cir. 2011)

[124] Horton, op.cit.

[125] United States v. Stabile, 633 F.3d 219, 240–42 (3d Cir. 2011)

[126] Horton v. California, 496 U.S. 128 (1990)

[127] United States v. Stabile, 633 F.3d 219, 240–42 (3d Cir. 2011)

[128] United States v. Williams, 592 F.3d 511, 521–24 (4th Cir. 2010)

[129] United States v. Burgess, 576 F.3d 1078, 1096 (10th Cir. 2009) : United States v. Stabile, 633 F.3d 219, 240–42 (3d Cir. 2011) : United States v. Williams, 592 F.3d 511, 521–24 (4th Cir. 2010)

المحاكم الأمريكية في العديد من الولايات القضائية عدم قبول الدليل الرقمي في حال تم الحصول عليه دون إذن من الشخص المعني، خاصة في الحالات التي يتم فيها الحصول على دليل في جريمة أثناء التحقيق في جريمة أخرى.[130]

- **مضمون إذن التفتيش:**

من شروط الإذن الصادر أن يكون مضمونه محدداً وفقاً للقواعد العامة في التفتيش. الأمر الذي أثار خلافاً بين الفقه يتعلق بمدى صلاحية جهاز الحاسب كمحل للتفتيش، فمنهم من أيد فكرة تفتيش الحاسوب ومكوناته مستنداً إلى أن إذن التفتيش يجب أن يتم تفسيره بمفهوم واسع يمتد ليشمل البيانات الإلكترونية بمختلف أنواعها المادية وغير المادية. بينما اتجه جانب آخر إلى القول بأنه لا ينطبق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير المحسوسة، بل يجب أن ينص الإذن صراحة على تفتيش المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب نفسها لعدم مخالفة مبدأ الشرعية.[131]

ويظهر موقف المشرع الفرنسي في المادة 94 من قانون الإجراءات الجنائية الفرنسي والمعدلة بالقانون رقم 47 لسنة 2010، بقوله" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على ماديات أو بيانات معلوماتية يكون كشفها مفيداً في إظهار الحقيقة".[132]

- على خلاف ذلك قضت المحكمة بعدم صحة تفتيش الكمبيوتر إذا كان يخص بيع مواد ممنوع بيعها controlled substance

- United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999)

[130] Stephen Manson,**"Expert in Cyber Security"**. http://www.stephenmason.eu/articles/electronic evidence.html.

[131] عبدالحليم ابن بادرة "إجراءات البحث والتحري عن الجريمة المعلوماتية: الخصوصية والإشكالات" مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر،العدد 23، سنة 2015م، ص 80.

[132] **Code de procédure pénale. Partie legislative; (Sous-section 1 : Des transports, des perquisitions et des saisies) Article 94**: "Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité". Modifié par LOI n°2010-768 du 9 juillet 2010.

ويثار التساؤل حول تحديد الإذن الصادر بتفتيش الكمبيوتر: هل يلزم أن يحدد مكاناً معيناً في هذا الجهاز؟ على هذا التساؤل أجابت المحكمة الفيدرالية للولايات المتحدة الأمريكية بأن الإذن الصادر بتفتيش الكمبيوتر بحثاً عن صور جنسية للأطفال يجيز البحث في كل الأماكن التي يمكن أن تستخدم في تخزين أو نقل أو توزيع أو الإعلان عن تلك الصور أو الأفلام الخاصة بممارسة أفعال جنسية على الأطفال[133]، وعللت المحكمة ذلك بأن تلك الصور يمكن تخزينها في أي مكان في الجهاز[134].

يبدو أن أحكام القضاء الأمريكي تتوسع في نطاق تفتيش الكمبيوتر لكي يشمل السوفت وير والهارد وير[135]. ومن ناحية السوفت وير لا يتحدد التفتيش بنوع معين من الملفات كملفات الأفلام أو الورد بنهايات معينة أو بأسماء معينة، حيث أن القائم بتخزين المعلومات التي تشكل دليلاً على جريمة قد يضعها في أي ملف ويعطيها اسماً مضللاً [136].

- **بيانات لا يجوز تفتيشها**

يقصد بهذه البيانات معلومات عن الحالة الصحية أو الاجتماعية للشخص أو بيانات تخص وظيفته أو انتماءاته السياسية والحزبية، وقد استقر المشرع الأمريكي في قانون حماية الحياة الخاصة الأمريكي (PPA) على حظر تفتيش هذا النوع من البيانات بل وعدم جواز تفتيشه بقوله: لا يجوز لرجال الضبط القضائي تفتيش أو الضبط للمواد في أحد الفروض الآتية:1-أن يتم إعداد تلك المواد أو إنتاجها أو تأليفها أو إنشاؤها بغرض العرض على الجمهور 2- أن تتضمن المواد الانطباعات العقلية أو الاستنتاجات أو النظريات الخاصة بمبتكرها 3- أن يعتقد على نحو معقول أن هدف الشخص من هذه المواد هو النشر

---

[133] United States v. Richards, 659 F3d 527 (6th Cir. 2011)

[134] United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010)

[135] United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998)

[136] United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) ; United States v. Sissler, No.1:90-CR-12, 1991 WL 239000, at *4 (W.D. Mich. Aug. 30, 1991)

للجمهور 4- أن تكون هذه المواد وثائقية تحتوي على معلومات **(The Privacy Protection Act of 1980)**[137].

واعتبرت المحاكم الأمريكية أن الطابع الشخصي لبعض الوثائق يبرر التقييد الصارم إن لم يكن الحظر الكامل من الاستيلاء عليها بواسطة السلطات الرسمية.[138]

- **صعوبات تفتيش النظام**

توجد العديد من العقبات التي تجعل تفتيش النظام صعباً وإن لم يكن مستحيلاً في بعض الأحيان، والتي من بينها:

- أن يلجأ صاحب النظام إلى تشفير الملفات.
- أن يلجأ إلى برنامج لحذف الملفات بسرعة لمجرد الضغط على مفتاح معين في قائمة المفاتيح.

---

[137] **The Privacy Protection Act of 1980**: Subject to certain exceptions , the PPA makes it unlawful for a government officer " to search for or seize " materials when ;

a-the materials are " work product materials " prepared , produced , authored , or created " in anticipation of communicating such materials to the pubic " , 42 U.S.C §2000aa-7 (b)(1) ;b-the materials include " mental impressions , conclusions , or theories " of its creator , 42 U.S.C §2000aa-7(b)(3) ; and

c- the materials are possessed for the purpose of communicating the material to the public by a person " reasonably believed to have a purpose to disseminate to the public " some form of " public communication ",42 U.S.C. §§ 2000aa-7(b)(3), 2000 aa(a); or

d-the materials are “documentary materials” that contain “information" 42 U.S.C. § 2000aa-7(a).

[138] **United States Supreme Court**. ZURCHER v. STANFORD DAILY(1978). No. 76-1484, Argued: January 17, 1978-Decided: May 31, 1978. https://caselaw.findlaw.com/us-supreme-court/436/547.html.

- يحتاج المفتش أحياناً إلى تعاون صاحب النظام، غير أن نصائح هذا الأخير قد تؤدي إلى عكس النتائج المبتغاه. لذا فمن الواجب إبعاده عن جهاز الكمبيوتر قبل تفتيشه.

ولمواجهة تلك الصعوبات يجب على القائم بالتفتيش أن يأخذ في اعتباره بعض الأمور على النحو التالي:

أ) عدم الاقتصار على ملفات معينة أو أجزاء معينة دون الأخرى في النظام. لذا يجب أن يكون التفتيش شاملاً، فقد يؤدي البحث في أجزاء دون الأخرى إلى ضياع الدليل الإلكتروني إن لم يتم تحريزه فوراً[139]. من ذلك الذاكرة المفصلة والساعات وملفات تخزين أو أرقام تليفونات أو أرقام سرية، وكذلك إذا وجد على مسرح الجريمة كتب تتعلق بالتشفير والأرقام السرية.

ب) سهولة الاتصال بالجهاز عن طريق الشبكة، وعليه يتعين على المحقق أن يفصل اتصال الجهاز بأي شبكة من شبكات الإنترنت حتى لا يتم تبادل معلومات مع شخص خارج المكان.

ج) من المناسب فصل الجهاز من التيار الكهربي بنزع الأسلاك المتصلة به وليس فقط بإطفائه من الجهاز نفسه. وإذا تعلق الأمر بالحاسب المحمول (اللاب توب) فإن فصل السلك الموصل لمصدر الكهرباء لا يكفي بل يلزم أيضاً نزع البطارية المثبتة به.

د) من المناسب تصوير الشاشة قبل إطفاء الجهاز، وعمل نسخة احتياطية للهارد و Drivers الأخرى.

- **إمكانية إجراء التفتيش دون الحصول على إذن قضائي**

أجاز قانون حماية الاتصالات الأمريكي ECPA استثناءً أن يتم التفتيش دون الحصول على إذن قضائي، وذلك متى توافرت حالة من الحالات التالية:[140]

---

[139] Alin Teodorus Dragan, Particularities regarding Computer Search and Field Research for Online Crimes, 2013 AGORA Int'l J. Jurid. Sci. 85 (2013), p. 87

[140] Georgia v. Randolph, 547 U.S. 103, 117 n.6 (2006) . Brigham City v. Stuart, 547 U.S. 398, 403-06 (2006). Illinois v. McArthur, 531 U.S. 326, 331-

1- إذا كان الدليل الرقمي معرض لخطر وشيك كالحرق أو التدمير.

2- وجود تهديد يضع الشرطة أو الجمهور في خطر.

3- إذا كانت الشرطة في مطاردة مع المشتبه به.

4- إذا كان من المرجح أن يفر المتهم قبل أن يتمكن مأمور الضبط من الحصول على إذن التفتيش.

وقد دلت قضية Georgia v. Randolph على إمكانية التفتيش دون الحصول على إذن عندما دخلت الشرطة بشكل مناسب منزل يقوم شاغليه بالتخلص والاعتداء على الأدلة ولم يستجيبوا لنداءات الشرطة الشفهية[141]. وفي قضية Illinois v. McArthur حيث استولت الشرطة على منزل لمدة ساعتين إلى أن يتم الحصول على إذن التفتيش[142]. وفي قضية Cupp v. Murphy تم القبض على المشتبه به في جريمة قتل مؤقتاً وكشط أظافره لمنع تدمير الأدلة التي برفقته.[143]

واعتبر التشريع الأمريكي أن من بين العوامل التي تبرر استثناء التفتيش دون إذن، أن يكون أول دليل على أن خطر تعرض الدليل للتدمير وشيك الحدوث هو الأكثر أهمية في سياق عمليات البحث في الكمبيوتر. وفي هذه الحالة يجب على مأمور الضبط القضائي مراعاة ما يلي: أ- توافر ضرورة ملحة للحصول على الدليل، ب- مقدار الوقت اللازم للحصول على إذن التفتيش، ج- ما إذا كانت الأدلة على وشك إزالتها أو تدميرها، د- إمكانية وجود خطر في الموقع محل الدليل، هـ- ما إذا كان المتهمون يعلمون بقدوم الشرطة إليها. كما في قضية Trowbridge حينما استولى مأموري الضبط بشكل مناسب على أجهزة الكمبيوتر دون إذن مسبق، مستنداً إلى وجود ظروف طارئة وتوافر ضرورة

---

33 (2001). Cupp v. Murphy, 412 U.S. 291, 294-96 (1973). supremecourt.gov. Retrieved May 4, 2019.

[141] Georgia v. Randolph, 547 U.S. 103 (2006)

[142] Illinois v. McArthur, 531 U.S. 326 (2001)

[143] Cupp v. Murphy, 412 U.S. 291 (1973)

ملحة تتمثل في قلقهم على سلامتها أثناء التحقيق، حيث كان من المحتمل أن يتم تدمير الأدلة الموجودة بالكمبيوتر.[144]

وقد اعتبرت المحاكم الأمريكية أيضاً أن من بين وسائل إتلاف الأدلة الرقمية المعتد بها كاستثناء لإجراء التفتيش دون إذن مسبق، وجود برامج تشفير قوية يمكن تشغيلها بمجرد الضغط على مفاتيح التشغيل، إضافة إلى عوامل أخرى كالرطوبة أو درجة الحرارة أو المجالات المغناطيسية كتمرير جسم مغناطيسي على القرص الصلب، أو في حالة تلف بطارية الجهاز أو وجود معلومات جديدة قد تتسبب في فقدان المعلومات القديمة. ففي قضية David قررت محكمة المقاطعة أن مأموري الضبط لم يكونوا في حاجة إلى الحصول على إذن بالتفتيش لأن أفعال المدعى عليه خلقت ظروفاً طارئة. فاستيلاء مأمور الضبط القضائي على جهاز الكمبيوتر فور رؤيته المدعى عليه يقوم بحذف الملفات من جهاز الكمبيوتر الخاص به يعد إجراءً صحيحاً. [145]

وفي قضية Romero-Garcia بررت المحكمة الحصول على المعلومات الموجودة بجهاز الاستدعاء الإلكتروني Pager دون الحصول على إذن قضائي مسبق لاعتقادهم بشكل معقول أنه كان من الضروري منع إتلاف الأدلة المخزنة في جهاز الاستدعاء، كما ولاحظت المحكمة أن الرسائل الواردة يمكن أن تحذف المعلومات المخزنة أو أن يؤدي تلف البطارية إلى محوها.

- **التفتيش الناتج عن قبض قانوني صحيح**

أجازت أغلب التشريعات التفتيش بالتبعية لوقوع قبض قانوني، ومن ثم يجوز لرجال الضبط القضائي القيام بتفتيش الشخص المقبوض عليه. فتنص المادة (46) من قانون الإجراءات الجنائية المصري على أنه "في الأحوال التي يجوز فيها القبض قانوناً على المتهم يجوز لمأمور الضبط القضائي أن يفتشه".

---

[144] United States v. Trowbridge, 2007 WL 4226385, at *4-5 (N.D. Tex. Nov. 29, 2007).

[145] United States v. David, 756 F. Supp. 1385 (D. Nev. 1991). See also United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001). United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997), aff'd on other grounds 168 F.3d 502 (9th Cir. 1999) .

أما التشريع الأمريكي فقد أجازت المحاكم لمأموري الضبط إجراء بحث كامل للشخص المعتقل وتفتيش معقول للمنطقة المحيطة به دون إذن قضائي. وذلك قياساً على قضيةRobinson حيث اكتشف ضابط شرطة أثناء القبض على المشتبه به في جريمة مرور، علبة سجائر مجعدة في جيب صدره الأيسر، ومع عدم معرفة ما تحتويه هذه العبوة، فتح الضابط العبوة واكتشف أربعة عشر كبسولة من الهيروين، ورأت المحكمة العليا الأمريكية أن تفتيش العلبة جائز على الرغم من أن الضابط لا يملك سبباً معقولاً لفتحها، إلا أن المحكمة أوضحت أن للضابط الحق في تفتيش كامل الشخص بالتبعية للقبض القانوني في ضوء الحاجة العامة إلى الحفاظ على الأدلة ومنع الضرر الذي قد يلحق بالضابط القائم بالقبض. [146]

ويجب ضرورة مراعاه النطاق الزمني المسموح به بالتفتيش الناتج عن القبض، بناء على ما إذا كانت العناصر التي تم البحث عنها عبارة عن عناصر ترتبط على الفور بشخص الموقوف، كملابسه أو محفظته أو الممتلكات الأخرى بالقرب من مكان القبض كالأمتعة.[147] واختلفت المحاكم الأمريكية في توضيح الوقت الكافي المسموح به بتفتيش العناصر المرتبطة بالشخص الموقوف، ففي قضية Edwards أيدت المحكمة تفتيش ملابس المدعى عليه بعد قضاء ليلة في السجن. على النقيض لم تؤيد المحكمة في قضية Chadwick ما قام به مأموري الضبط من تفتيش خزانه تبعد عن موقع القبض بعد تسعين دقيقة من إجراء القبض.[148]

كما اختلفت المحاكم الأمريكية حول ما إذا كان الهاتف الخلوي يشكل عنصراً مرتبطاً بشخص المعتقل يجوز تفتيشه عقب القبض وفقاً لمتطلبات زمنية صارمة، كما في قضيةChadwick أم يخضع لمتطلبات زمنية أكثر مرونة كما في قضية Edwards. وقد انتهت إحدى محاكم الاستئناف إلى أن الهاتف الخلوي يعد ملكية

---

[146] See United States v. Robinson, 414 U.S. 218, 235 (1973); Chimel v. California, 395 U.S. 752, 762-63 (1969).

[147] United States v. Chadwick, 433 U.S. 1, 15 (1977).

[148] United States v. Edwards, 415 U.S. 800, 808-09 (1974). United States v. Chadwick 433 U.S. at 14-16.

شخصية مرتبطة على الفور بشخص المعتقل وعليه يصح التفتيش الواقع على الهاتف الخلوي في مركز الشرطة بعد ساعتين ونصف من الاعتقال[149]. وعلى النقيض من ذلك اتجهت محاكم أخرى إلى تطبيق متطلبات زمنية صارمة، ورأت أن البحث في الهاتف الخلوي غير المتزامن مع الاعتقال يعد انتهاكاً للتعديل الرابع للدستور الأمريكي.[150]

- مدى إمكانية تفتيش الشبكات

قد يقوم مأمور الضبط القضائي بتفتيش جهاز حاسب للمتهم وعن طريق نفس الجهاز يتم الدخول إلى جهاز ينتمي إلى شخص آخر أو إلى عدة أجهزة أخرى باستخدام شبكة الإنترنت، فيثير التفتيش في هذه الحالة العديد من الإشكاليات التي تتعلق بهل يحق لمأمور الضبط في هذه الحالة الحصول على معلومات أو بيانات متعلقة بجهاز الشخص الأخر أو الأجهزة الأخرى إذا ما توافر لديه اعتقاد بوجود معلومات أو بيانات تفيد في كشف الحقيقة؟ وهل يحتاج في ذلك إلى الحصول على إذن قضائي جديد كون الإذن الأول الصادر بالتفتيش يجب أن يكون محدداً؟

اتجهت أغلب الاتفاقيات المعنية بمجال تقنية المعلومات إلى جواز امتداد التفتيش إلى نظام حاسب آخر إذا كان هناك أساس يدعو إلى الاعتقاد بأن المعلومات المخزنة بهذا النظام تفيد في التحقيقات وكشف الجريمة. حيث نصت اتفاقية بودابست في المادة 19 على أنه "من حق السلطة القائمة بتفتيش الكمبيوتر الموجود في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش".

---

[149] United States v. Wurie, 2009 WL 1176946, at *5 (D. Mass. 2009).

[150] United States v. Lasalle, 2007 WL 1390820, at *7 (D. Haw. May 9, 2007) (rejecting cell phone search more than two hours and fifteen minutes after arrest); United States v. Park, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007) (rejecting cell phone search approximately ninety minutes after arrest). See also: United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (search of cell phone performed at stationhouse after arrest could not be justified as incident to arrest).

كما نصت المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[151] في فقرتها الأولى على أن " تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى أ- تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها. ب- بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه. وأكملت فقرتها الثانية بأن "تلتزم كل دولة طرف بتبين الإجراءات الضرورة لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة الأولى إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والصول للتقنية الأخرى".

وفيما يتعلق بموقف التشريعات المختلفة، ففي عام 2016 سمح تعديل الفقرة ب للمادة 41 من قانون الإجراءات الأمريكي الفيدرالي بأن للقضاه الحق في إصدار أوامر تسمح لمكتب التحقيقات الفيدرالي ووكالات إنفاذ القانون الفيدرالية باستخدام أدوات الوصول عن بُعد لاختراق أجهزة الكمبيوتر خارج الولاية القضائية التي مُنح فيها الإذن، وبناء على ذلك يجيز القانون الأمريكي البحث في وسائل التخزين الإلكترونية وضبط أو تخزين أو نسخ المعلومات المخزنة إلكترونياً في أي جهاز آخر متصل غير الصادر بشأنه إذن التفتيش سواء أكانت تلك الوسائط داخل أو خارج تلك المقاطعة.[152] في

---

[151] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 2010/12/21م – حررت في القاهرة، مصر. جامعة الدول العربية، الأمانة العامة لجامعة الدول العربية (الأمانة العامة لمجلس وزراء الداخلية العرب). الموقع الرسمي لجامعة الدول العربية https://www.arableagueonline.org استرجاع بتاريخ 2019/4/16م.

[152] **Federal Rules of Criminal Procedure**. (Rule 41, titled Search and Seizure) 6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district. https://en.wikipedia.org/wiki/Rule_41

الوقت نفسه، اتجه أحد قضاه المحاكم الجزئية في الولايات المتحدة إلى القول بأن مكتب التحقيقات الفيدرالي لا يحتاج إلى أمر على الإطلاق للتسلل إلى جهاز كمبيوتر في الولايات المتحدة، قائلاً: بشكل عام، لا يتوقع المرء أي خصوصية معقولة في عنوان IP عند استخدام الإنترنت.[153] غير أن هذا التوسع يثير مخاوف خطيرة تتعلق بالخصوصية، حيث يمكن الوصول إلى مجموعة واسعة من البيانات الشخصية الحساسة وغير ذات الصلة أثناء التحقيق.

أما قانون الإجراءات الفرنسي، فقد أجازت الفقرة الأولى من المادة 57 منه لرجال الضبط القضائي أثناء عملية بحث يتم إجراؤها وفقاً للشروط التي نص عليها القانون، إمكانية الوصول إلى نظام كمبيوتر موجود في مكان إجراء البحث، والوصول إلى البيانات ذات الصلة بالتحقيق والمخزنة في هذا النظام أو في نظام كمبيوتر أخر، طالما أن هذه البيانات يمكن الوصول إليها من النظام الأصلي. وإذا ثبت أن هذه البيانات مخزنة في نظام كمبيوتر آخر خارج الإقليم الوطني، فيقوم مأمور الضبط بتجميعها مع مراعاة شروط الوصول المنصوص عليها في الإتفاقيات الدولية المعمول بها في هذا الشأن.[154]

---

153 "**How an obscure rule lets law enforcement search any computer?**" https://www.engadget.com/2016/12/01/rule-41-fbi-doj-hacking-power-expand-search-seizure/

154 **Code de procédure pénale. Livre Ier: De la conduite de la politique pénale, de l'exercice de l'action publique et de l'instruction., Chapitre Ier : Des crimes et des délits flagrants**: (Article 57-1) : Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre

كما يسمح القانون السويسري بتفتيش جهاز الكمبيوتر لضبط ما به من بيانات ومعلومات تفيد في كشف الحقيقة[155]، وذلك على النحو التالي:

- يكون تفتيش الكمبيوتر بناءً على إذن من النيابة ولكن يجوز للشرطة القيام بذلك في حالة وجود خطر في تأجيل التفتيش وفقاً للمادة (section 241(3) CCP)
- ينصح بأخذ نسخة احتياطية قبل تفتيش الجهاز.
- يجب الحذر من وجود برنامج لحذف البيانات يكون متواجداً في الكمبيوتر ويتم تفعيله عن بعد.

من حق صاحب الجهاز أن يتمسك بوجود بيانات يحميها السر المهني. عندئذ يقوم عضو النيابة أو الشرطة القائمين بالتفتيش بتحريز الجهاز ووضعه تحت الأختام ويرفع الأمر إلى المحكمة المختصة للحصول على إذن برفع الأختام . وعلى المحكمة أن تصدر قرارها في خلال شهر واحد، وقرارها في هذا الشأن نهائي غير قابل للطعن فيه (section 248 CCP).

ونظرً للطبيعة الخاصة للبيانات وقابليتها للمسح والتدخل في الكمبيوتر عن بعد، فإن بطء سير الإجراءات الإدارية لا يتمشى مع تلك الطبيعة. سواء تعلق الأمر بإجراءات داخلية مثل الحصول على الإذن القضائي بالتفتيش أو الانتقال إلى مكان توافر الجهاز أو إذا تعلق الأمر بإجراءات تعاون قضائي بين الدول والذي يتطلب تقديم طلب خاص بذلك أمام جهة أجنبية قضائية وانتظار البت فيه. فللمحكمة سلطة إصدار أمر بتسليم الكمبيوتر دون العبث به وفقاً للمادة (**CCP** sections 241-248) في شأن جرائم الكمبيوتر في كندا. وفي حالة عدم الامتثال لأمر المحقق يتعرض المخاطب بالأمر إلى جزاء جنائي أو تفرض عليه

---

système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. (Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003).

[155] Bertrand Perrin; Marc Remy; Romain Roubaty, Electronic Evidence in Swiss Criminal Procedure, 8 Digital Evidence & Elec. Signature L. Rev. 70 (2011)

غرامة تأديبية.(section 265(3) CCP). وفي هذه الحالة أيضاً يجوز اللجوء إلى إجراءات التفتيش والضبط.

ويجوز أيضاَ أن تلجأ سلطة التحقيق إلى إلزام طرف ثالث (الغير) بتقديم ما لديه من معلومات. حيث قد يلجأ شخص إلى استخدام تطبيقات للبيع أو الشراء في سرقة معلومات تخص شخص آخر. كما يجوز الإلزام بالحضور لأداء الشهادة وتسري عليه قواعد أداء الشهادة سواء أمام سلطة التحقيق أو أمام المحكمة.

غير أنه يتعين أن يأخذ المحقق في الاعتبار أمرين: الأمر الأول إذا كانت المعلومات التي يحوزها تنسحب عليها الالتزام بالسرية كأن تكون مشمولة بسر المهنة. والثاني إذا كان الشخص المطلوب شهادته متهماً أي توجد ضده قرائن على اتهامه أمام المحقق فلا يجوز إلزامه بالشهادة، لأن ذلك يخالف قاعدة أنه لا يجوز إجبار شخص على تقديم دليل ضد نفسه. كما أنه لا يجوز إجبار المتهم على حلف اليمين وفقاً لما هو مقرر في الإجراءات الجنائية. غير أن الالتزام بتقديم الجهاز يبقى قائماً حتى في مواجهة المتهم كون ذلك لا يتضمن التزام المتهم بتقديم بيانات ضده نظراً لاختلاف الشهادة عن هذا النوع من الالتزام.

ويجوز توجيه أمر إلى مزودي الخدمات بالاحتفاظ ببيانات معينة لحين تقديمها . من ذلك أن تبادل المراسلات والمشاركات والدخول إلى المواقع وكذلك البيانات التي تتعلق باشتراك مستخدمي الانترنت يرد عليها هذا الالتزام. وهو ما نص عليه القانون السويسري (3 – 15 of the Law on Postal Service and Telecommunication Providers (ISP)

ويميز واضعو القانون السويسري بين البيانات المتداولة in real time وبين البيانات المخزنة لدى مزودي الخدمات. في الحالة الأولى اعتبر المشرع أن شبكة الإنترنت ليس لها حرمة ويجوز لمأمور الضبط القضائي أن يدخل عليها باستخدام برامج عند اللزوم للاطلاع وضبط بيانات الأشخاص المتهمين بجرائم ضمن ما يعد من إجراءات الضبط القضائي. هذه البيانات تتعلق بشخص معين ومن يتعامل معهم والمواقع التي يدخل عليها ومن يراسلهم وكذلك محتوى المراسلات بينهم مادامت تلك المرسلات تتحرك على شبكة الانترنت in real time . غير أنه فيما يتعلق بمحتوى المراسلات فيميز القانون السويسري بين الجرائم فيسمح بالاطلاع على المحتوى في جرائم تتسم بمقدار من الخطورة (CCP 269 section) أما البيانات الأخرى فيكفي فيها الاتهام بجنحة (Section 273 CCP).

المبحث الثاني

الضبط والتحفظ على الأدلة المتحصلة من الأجهزة الرقمية

-ضرورة المحافظة على سلامة إجراءات ضبط الدليل الالكتروني

إن النتيجة الحتمية التي تنتهي إليها عملية التفتيش هي ضبط الأدلة التي تحصلت من خلالها، ويقصد بالضبط حجز وإبعاد الدعامة المادية التي سجلت عليها البيانات أو المعلومات أو إجراء نسخة من هذه البيانات أو المعلومات والاحتفاظ بها، وكذلك حجز البرامج اللازمة للنفاذ إلى البيانات التي تتم مصادرتها.[156] ولكي تلائم القوانين الإجرائية التقليدية البيئة الرقمية لابد أن يتم إدراج استخدام المصطلحات الحاسوبية الجديدة مع الإبقاء على اللغة التقليدية في الإجراءات الجنائية؛ فالبحث والمصادرة يقابلها بلغة التكنولوجيا النفاذ والاستنساخ.

والأصل عدم جواز ضبط الأشياء إلا التي تتعلق بالجريمة التي يجرى التحقيق من أجلها وصدر إذن التفتيش بخصوصها، ومع ذلك أجازت أغلب التشريعات ضبط الأشياء التي يتم الكشف عنها عرضاً أثناء القيام بتفتيش قانوني -على ما سبق وأوردنا- متى ما كانت الأشياء محل الضبط تعد حيازتها جريمة أي في حالة تلبس، أو كانت تفيد في كشف الحقيقية في جريمة أخرى.[157]

ويكون محل الضبط في البيئة الرقمية جهاز الحاسب ووحدات الإدخال كلوحة المفاتيح والقلم الضوئي، ووحدات الإخراج كالطابعه أو جهاز الماسح الضوئي، كذلك قد يقع الضبط على جهاز الهاتف الخلوي أوالكاميرات الرقميه أو أي جهاز رقمي تم استخدامه في ارتكاب الجريمة، ولا يمتد الضبط إلى ضبط المكونات المادية فحسب، بل يمتد إلى المعلومات والمعطيات والبيانات والبرامج المخزنة في النظام أو في النظم المرتبطة بالنظام محل الاشتباه، وكل المكونات ذات الطبيعة المعنوية لسهولة وسرعة تعرضها للتلف أو الضياع.

---

[156] المادة 19 من اتفاقية بودابست2001م.

[157] جاسم خربيط خلف "التفتيش في الجرائم المعلوماتية" مجلة الخليج العربي، مركز دراسات الخليج العربي، جامعة البصرة، المجلد 41 العدد 3،4، سنة 2013م، ص 250.

ويمكننا تطبيق قواعد ضبط الأدلة قياساً على المادة 95 من قانون الإجراءات المصري حيث أجازت ضبط المراسلات والخطابات والرسائل والمطبوعات بمعرفة قاضي التحقيق أو بمعرفة النيابة العامة لدى مكاتب البريد مشترطة أن يتم ذلك وفق ضمانات معينة على النحو التالي:

1- أن يكون لهذا الإجراء فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.
2- أن يكون الضبط قد تم بناء على أمر مسبب.
3- ألا تزيد المدة المسموح بالضبط خلالها على ثلاثين يوماً قابلة للتجديد لمدة أو لمدد مماثلة.

وإذا كانت النيابة العامة هي من قامت بالضبط، فيضاف إلى الضمانات السابقة ما يلي:

1- الحصول على إذن مسبب من القاضي الجزئي بعد إطلاعه على الأوراق، وللقاضي أن يجدد هذا الأمر لمدة أو لمدد مماثلة.
2- يجوز للنيابة العامة أن تطلع على الخطابات والرسائل والأوراق الأخرى المضبوطة على أن يتم هذا كلما أمكن ذلك بحضور المتهم أو الحائز لها أو المرسلة إليه مع تدوين ملاحظاتهم عليها، وللنيابة حسب ما ترى من الفحص أن تأمر بضم تلك المضبوطات إلى ملف الدعوى أو ردها إلى كل من كان حائزاً لها أو من كانت مرسلة إليه.

أما مأمور الضبط القضائي فلا يملك أي صلاحية في هذا الشأن، غير أنه يجوز لقاضي التحقيق ندبه لمباشرة هذا الإجراء وفقاً لما نصت عليه الفقرة الأولى من المادة 6 من قانون مكافحة جرائم تقنية المعلومات والتي نصت على أنه لجهة التحقيق المختصة – بحسب الأحوال– أن تصدر أمراً مسبباً، لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على 30 يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون "ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها فى أى 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 مقتضى".

- **الضبط دون الحصول على إذن تفتيش**

كما تناولنا سابقاً فقد أجازت المحاكم الأمريكية الحصول على الأدلة الرقمية دون إذن قضائي كاستثناء في حالة توافر ضرورة ملحة وأسباب تدعو للاعتقاد بأن الدليل سوف يمحى أو يتم تدميره. ومع ذلك أكدت المحكمة العليا الأمريكية في العديد من أحكامها أنه على الرغم من وجود ضرورة تبرر الاستيلاء على الدليل الرقمي، إلا أن ذلك لا يخول بالضرورة اتخاذ أي خطوات أخرى دون الحصول على إذن قضائي.

ففي حين توافر ظروف تبرر الاستيلاء على جهاز الاستدعاء الإلكتروني للحفاظ على الأدلة، إلا أن هذا الاستثناء لا يبرر التلاعب في جهاز الاستدعاء لاسترداد الرسائل. وتعيد المحكمة العليا الأمريكية تأكيدها على أنه في حالة غياب الضرورة الملحة للوصول إلى المعلومات، فيفضل الوصول إليها بناء على ضبط ناتج عن إذن قضائي بالتفتيش؛ ذلك أن الخبير الرقمي المختص يستطيع استخراج معلومات مفصلة وذات صلة من جهاز الكمبيوتر لا يمكن استخراجها من خلال بحث تم إجراؤه بشكل عاجل.[158]

خلاصة ما تقدم فضبط البيانات والتحفظ عليها له وظيفتين أساسيتين، الأولى: تتمثل في المساعدة في جمع الأدلة عن طريق جمع معدات الجهاز الرقمي كالحاسب أو الهاتف المحمول واستنساخ البيانات الأصلية، والحفاظ عليها من التلاعب أو التدمير. أما الوظيفة الثانية : فتنطوي على التحفظ على تلك الأدلة وجعل نسختها الأصلية غير قابلة للنفاذ أو الإزالة، بمعنى الحفاظ على سلامة البيانات.

---

[158] See: United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995); David, 756 F. Supp. at 1392 (exigency justified seizure but not search of computer); Morales-Ortiz, 376 F. Supp. 2d at 1142 n.2.

الفصل الثالث

ذاتية الأدلة الجنائية الرقمية في مرحلة المحاكمة

تمهيد:

بعد أن تناولنا ذاتية الضوابط الإجرائية في مرحلة ما قبل المحاكمة في الحصول على الدليل الرقمي، سوف نتناول بشئ من التفصيل الضوابط التي تحكم الأدلة المتحصلة عن الأجهزة الرقمية، والتي يجب أن يلتزم بها القاضي في تقديره للدليل لتفادي بطلان الإجراءات؛ ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما تصل قناعة القاضي إلى حد اليقين بثبوتية الدليل على المتهم.

لذا سوف نعالج إلزام مزودي الخدمات والغير بتقديم الدليل الإلكتروني في المبحث الأول) ونتناول حجية الدليل الرقمي في الإثبات الجنائي (المبحث الثاني)، إضافة إلى استبعاد الأدلة الجنائية الرقمية على سند من بطلانها (في مبحث ثالث).

المبحث الأول

إلزام مزودي الخدمات والغير

بتقديم الدليل الإلكتروني

لا تلجأ المحاكم عادة إلى إلزام الغير بتقديم مستندات أو معلومات تفيد في كشف الحقيقة في دعوى منظورة أمامها سواء أكانت تلك الدعوى مدنية أم جنائية. غير أنه مع انتشار جرائم التقنيه وصعوبة التعرف على فاعلها، فقد بدأت المحاكم في الإكثار من استعمال تلك الرخصة المقررة لها. فقد يكون تعاون جوجل أو هوت ميل أو يوتيوب أو غيرها من وسائل التواصل ضرورياً للتعرف على الفاعل في الجرائم الإلكترونية. وإذا كانت الدعاوى المدنية الأصل فيها أن الخصم هو الذي يقدم الدليل، فإن الأمر يختلف في الدعاوى الجنائية . وقد تزامن ذلك مع تطور دور القاضي الجنائي في النظم الأنجلو أمريكية حيث كان هذا الدور سلبياً فتقدم النيابة العامة أدلة الاتهام ويقدم المتهم أدلة النفي وينحصر دور المحكمة في تقييم كل من تلك الأدلة والحكم بالبراءة أو بالإدانة. أما الأن فقد أصبح للمحكمة دور فعّال في الكشف عن الحقيقة في الجرائم الإلكترونية التي تقتضي تعاوناً من

مزودي الخدمات. ومن هنا كثر استخدام طلب الإلزام بتقديم خدمات motion to compel.

- اختصاص سلطة التحقيق بإصدار أوامر بتقديم بيانات من مزودي الخدمات

نص القانون المصري لسنة 2018 في شأن جرائم تقنية المعلومات على اختصاص جهة التحقيق بإصدار إذن إلى مأمور الضبط بتوجيه أوامر إلى مزود الخدمات بتقديم بيانات أو معلومات تفيد في كشف الحقيقة. فتنص المادة (6) من القانون السابق على أن "لجهه التحقيق المختصة بحسب الأحوال أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي: 1-...2-... 3- أن تأمر مقدم الخدمة بتسليم ما لديه 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 النظام التقني".

ويلاحظ على أحكام القانون المصري في هذا الشأن ما يلي:

- أنه لم ينص على سلطة إعطاء ذلك الأمر إلى مأموري الضبط القضائي في إطار التحريات التي يقومون بها بدون إذن بذلك.
- كما أنه اشترط أن يكون الأمر بذلك مسبباً.
- أن هذا أمر مؤقت لمدة ثلاثين يوماً قابل للتجديد مدة واحدة.
- أنه لم يشترط تحديد المعلومات أو البيانات المطلوبة على وجه الدقة فيكفي أن يصدر الأمر بالكشف عن اتصالات المتهم مع أي شخص أو ما تداوله من رسائل إلكترونية أو ما يدخل عليه من مواقع.
- أنه يختلف عن الإذن بالتفتيش. وجدير بالذكر أن الإذن بالتفتيش يمكن أن يكون غير ذي فائدة، ذلك أن الأمور التقنية عادة ما تكون حكراً على مزود الخدمات ويمكن ألاّ يقوم بتنبيه خبراء الضبط القضائي عن التفاصيل التي يحتاجون إليها، بل يمكن أن يقوم بمحوها. ومن هنا كانت فائدة الأمر الصادر إلى مزود الخدمات بتقديم ما لديه من بيانات ومعلومات.

- القانون المصري يجيز إلزام الغير بتقديم مستندات

الأمر الصادر من المحكمة بإلزام الغير بتقديم مستند، هو أمر إفصاح ونوع من أوامر المحكمة الذي تكلف عادة طرف ثالث بتسليم المعلومات التي بحوزته والمتعلقة بالتحقيق. ويجب للحصول على أمر بالإفصاح من المحكمة، أن يقدم الكيان حكومي وقائع محددة ومفصّلة تثبت وجود أسباب معقولة للاعتقاد بأن المعلومات المطلوبة ذات صلة وموضوعية لإجراء تحقيق جنائي مستمر. ولا يُطلب من الكيانات الحكومية إظهار سبب محتمل للحصول على أمر بالإفصاح.

ويجيز القانون المصري للمحكمة أن تصدر أمراً للغير بتسليم ما يحوزه من مستندات تلزم للكشف عن الحقيقة. فتنص المادة 291 من قانون الإجراءات الجنائية المصري على أن "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أى دليل تراه لازماً لظهور الحقيقة". كما تنص المادة 427 من قانون الإجراءات الجنائية الفرنسي على أنه "ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات ويحكم القاضي بناء على اقتناعه الشخصي".[159]وهذا يعني أن للقاضي الجنائي الحرية الكاملة في تكوين عقيدته عند إصدار حكمه في الدعوى المنظورة أمامه. وله تقدير صحة الدليل المتحصل من الأجهزة الرقمية وما بها من قوة الدلالة، فلا يحكم في الدعوى إلا طبقاً لاقتناعه واعتقاده. وفي جميع الأحوال لا يستطيع القاضي أن يقبل دليلاً متحصلاً من إجراء غير مشروع ليس فقط لأنه يتعارض مع قيم العدالة، بل كونه أيضاً يمس بحق المتهم في الدفاع.[160] تطبيقاً لذلك قضت محكمة النقض المصرية أنه "من المقرر أنه من اللازم في أصول الاستدلال أن يكون الدليل الذي يعول عليه الحكم مؤدياً إلى ما رتبه عليه من نتائج في غير تعسف في الاستنتاج ولا

---

[159] **Code de procédure pénale. De l'administration de la prevue: (Article 427**)" Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction".

[160] محمد زكي أبو عامر " الإثبات في المواد الجزائية" دار الجامعة الجديد، مصر، سنة 2011م، ص122. راجع كذلك: فهد دخين العدواني "مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي، دراسة مقارنة" مركز تطوير التعليم الجامعي، جامعة عين شمس، مجلة دراسات في التعليم الجامعي، العدد 36، لسنة 2017م، ص 260 وما بعدها.

تنافر على حكم العقل والمنطق"، كما قضت "بوجوب بناء الأحكام على أسس صحيحة من أوراق الدعوى وعناصرها، وأن اعتماد الحكم في قضائه على رواية أو واقعة لا أصل لها في التحقيقات يعيب الحكم".[161]

ويقر القانون المصري سلطة المحكمة في أن تصدر أمراً للغير بتقديم مستند. فتنص المادة (20) من قانون الإثبات في المواد المدنية والتجارية بأنه "يجوز للخصم في الحالات الاتية أن يطلب إلزام خصمه بتقديم أي محرر منتج في الدعوى يكون تحت يده :

(أ) إذا كان القانون يجيز مطالبته بتقديمه أو تسليمه.

(ب) إذا كان مشتركاً بينه وبين خصمه، ويعتبر المحرر مشتركاً علي الأخص إذا كان المحرر لمصلحة الخصمين أو كان مثبتاً لالتزاماتهما وحقوقهما المتبادلة .

(ج)إذا استند إليه خصمه في أية مرحلة من مراحل الدعوى.

وواضح من الصياغة السابقة ما يلي:

- أن الأمر يتعلق بالمنازعات المدنية والتجارية.
- الأصل هو أن القاضي لا يلزم خصماً بتقديم هذا المحرر الذي يفيد خصماً آخر في الدعوى؛ فالإلزام ينحصر في حالات محددة.
- الصياغة جاءت محصورة في المحررات دون المعلومات وهو ما يجعل هذا الحكم قاصراً عن تطبيقه في مواد المعلومات الإلكترونية التي تشاطرها جهات التواصل الاجتماعي ومحركات الإنترنت. أما المادة (30.02) من قانون الإجراءات المدنية الكندي فقد نصت صراحة على الأصوات والأفلام وتسجيلات الفيديو والصور والرسوم والخرائط والجرافيك، والخطط والبيانات المتعلقة بفتح الحساب وإدارته والبيانات والمعلومات الإلكترونية[162].

---

[161] حكم نقض جلسة 1987/1/8، الطعن رقم 5963، لسنة 56 ق.

[162] (30.01 (1) In Rules 30.02 to 30.11): (a) "document" includes a sound recording, videotape, film, photograph, chart, graph, map, plan, and survey, book of account and data and information in electronic form.

- إن إصدار الأمر بتقديم مستند جوازي للمحكمة، على خلاف القانون الكندي الذي جعل الأمر وجوبياً بالنسبة للخصم وجوازياً بالنسبة للغير.
- يجوز للمحكمة أن تأمر بتقديم المحرر ولو من تلقاء نفسها أي بدون طلب من أحد الخصوم.
- أن هذا الحكم لا يسري على المحاكمات الجنائية، حيث لا يجوز إلزام شخص على تقديم دليل ضد نفسه.
- أن هذا الحكم لا يسري على المحررات التي يشملها الالتزام بالسرية.

والقاعدة هي تقديم أصل المحرر. ويفهم ذلك من نص المادة (24) من قانون الإثبات بقولها "إذا لم يقم الخصم بتقديم المحرر في الموعد الذي حددته المحكمة او امتنع عن حلف اليمين المذكورة اعتبرت صورة المحرر التي قدمها خصمه صحيحة مطابقة لأصلها، فإن لم يكن خصمه قد قدم صورة المحرر جاز الأخذ بقوله فيما يتعلق بشكله وموضوعه".

ويجوز للمحكمة أن تأمر بإدخال شخص معين خصماً في الدعوى وتطلب منه تقديم محرر معين. فتنص المادة (26) من قانون الإثبات على أنه "يجوز للمحكمة أثناء سير الدعوي ولو أمام محكمة الاستئناف أن تأذن بإدخال الغير لإلزامه بتقديم محرر تحت يده وذلك في الأحوال ومع مراعاة الأحكام والأوضاع المنصوص عليها في المواد السابقة".

-القانون الكندي يجيز للمحكمة إصدار أمر لمزود الخدمات بتقديم معلومات

أجاز القضاء الكندي إلزام مقدم الخدمات بتقديم ما لديه من معلومات تفيد في كشف الحقيقة[163]، شريطة أن يكون مقدم الخدمة له الحيازة والرقابة على تلك البيانات. وواضح أنه

[163] Leduc t'. Roman (2009), 308 D.L.R. (4th) 353, 73 C.P.C. (6th) 323, 2009 CanLII 6838 (Ont. S.C.); Wice v. Dominion of Canada General Insurance Co. (2009), 75 C.C.L.I. (4th) 265, [2009] O.J. No. 2946 (QL), 2009 CanLII 36310 (S.C.J.); Kourtesis v. Joris (2007), 160 A.C.WS. (3d) 414, 2007 CanLII 39367 (S.C.); Goodridge (Litigation Guardian of) v. King (2007), 161 A.C.W.S. (3d) 984, 2007 CanLII 51161 (S.C.J.); Murphy v. Perger, [2007] O.1. No. 5511 (QL), 67 C.P.C. (6th) 245 (S.C.J.).

يمارس تلك الرقابة على ما يقوم به صاحب الحساب من دخول على مواقع معينة، فبمقدوره أن يعرف تلك المواقع وعدد المرات التي دخل فيها صاحب الحساب وفقاً لقواعد استخدام الحساب. تطبيقاً لذلك قضت المحكمة الفيدرالية الكندية بإلزام مزود الخدمات الكندية eBay بأن يقدم إلى إدارة الضرائب أسماء بائعي بضاعة معينة ودخلهم الإجمالي لتقدير الضريبة عليهم منعاً للتهرب الضريبي من جانبهم[164]، وعلى الرغم من أن مزود الخدمات تمسك بأن المعلومات مخزنة على محرك في الولايات المتحدة، إلاّ أن المحكمة قدرت أنها مخزنة أيضاً في كندا وأنها في حيازة ورقابة مزود الخدمات الكندي.

ويلاحظ أن المادة 30.02 من قانون الإجراءات المدنية الكندي تنص على أن للمحكمة أن تأمر بإلزام الخصم في الدعوى بتقديم مستند معين أو معلومات معينة بناء على طلب الخصم[165]. وبالتالي فإن للخصم أن يطلب إصدار المحكمة لأمر في مواجهة جهات التواصل الاجتماعي أو غيرها من المحركات التي تتطلب من صاحب الحساب معلومات عن نفسه.

-القانون الأمريكي والقانون الكندي يجيزان للمحكمة إصدار أمر لمزود الخدمات بتقديم مستندات لديه

استقرت أحكام القضاء الأمريكي على أن الشخص لا يتوافر لديه توقع معقول لحرمة

---

[164] eBay Canada Limited v. Canada (National Revenue), 2007 FC 930 (CanLII). https://www.canlii.org/en/ca/fct/doc/2007/2007fc930/2007fc930.html. Retrieved, May 2, 2019.

[165] SCOPE OF DOCUMENTARY DISCOVERY Disclosure 30.02) “Every document relating to any matter in issue in an action that is or has been in the possession, control or power of a party to the action shall be disclosed as provided in Rules 30.03 to 30.10, whether or not privilege is claimed in respect of the document. Production for Inspection (2) Every document relating to any matter in issue in an action that is in the possession, control or power of a party to the action shall be produced for inspection if requested, as provided in Rules 30.03 to 30.10, unless privilege is claimed in respect of the document”.

الحياة الخاصة فيما يتعلق بما استودعه الغير من أسراره[166].

قبل قضية Carpenter كانت المحكمة العليا ترى باستمرار أن أي شخص ليس لديه توقعات مشروعة بالخصوصية فيما يتعلق بالمعلومات التي تم تسليمها طوعًا إلى أطراف ثالثة، وبالتالي لم يكن إذن التفتيش مطلوبًا للحصول على هذه المعلومات. تُعرف هذه النظرية القانونية باسم فكرة الطرف الثالث، التي أنشأتها قضايا المحكمة العليا الولايات المتحدة ففي قضية Miller لعام 1976 قررت المحكمة أن السجلات المصرفية لم تكن عرضة لتوقع الخصوصية، وفي قضيه Smith vs. Maryland في عام 1979 حددت حقوق الأفراد فيما يتعلق بالاتصالات الهاتفية.

غير أن القضاء الكندي اعترضت أحكامه على ما يتبعه بعض الخصوم من إدخال خصم معين لكي يأمره القاضي بتقديم بيانات أو معلومات تحت يده، باعتبار أن ذلك نوع من إساءة استعمال الحق في التقاضي[167]. وحيث أن الأمر متروك للسلطة التقديرية للمحكمة، فإنها في قضية Leduc v. Roman قضت بأنه لم يكن من المناسب إدخال Facebook لكي يمكن إلزامه بتقديم ما لديه من بيانات[168].

أما في قضية Warman v. Wilkins-Fournie فقد أصدرت أمراً إلى جهات الإنترنت بالكشف عن المعلومات التالية بخصوص مدعى عليهم قاموا بوضع رسائل على حساباتهم بأسماء وهمية؛

- عنوان البريد الإلكتروني للمدعى عليهم وكل ما يتعلق بهم من معلومات قاموا بتسجيلها وقت فتح حساباتهم.
- بروتوكول الإنترنت (IP) لأجهزة الكمبيوتر التي استخدموها لفتح الحسابات السابقة.
- بروتوكول الإنترنت (IP) لأجهزة الكمبيوتر التي استخدمها المدعى عليهم وقت

---

[166] United States v. Miller, 425 U.S. 435, 443 (1976)

[167] City of Saint John Employee Pension Plan v. Ferguson (2009), 177 A.C.W.S. (3d) 78, 2009 NBQB 121 at para. 17 (Q.B.); B. (A.) v. D. (C.).

[168] Leduc t'. Roman (2009), 308 D.L.R. (4th) 353, 73 C.P.C. (6th) 323, 2009 CanLII 6838 (Ont. S.C.)

وضع تلك الرسائل.

- أي معلومات أخرى تتعلق بالفواتير التي ربما دفع قيمتها المدعى عليهم والمواقع التي دخلوا عليها.

المبحث الثاني

حجية الدليل الرقمي في الإثبات الجنائي

تمهيد:

تتطلب التحديات التي تحيط بالأدلة الجنائية المتحصلة من الأجهزة الرقمية تأثيراً كبيراً يتعلق بمدى قبول الدليل عندما يتم جمعه وحفظه وتقديمه. وقد نصت المادة 11 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 "على أنه يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتى أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

وعليه سوف نعالج في هذا المبحث شروط صحة الدليل الرقمي كدليل صالح في الإثبات (في المطلب الأول) وسلطة القاضي في قبول الأدلة الرقمية (في المطلب الثاني).

المطلب الأول

شروط صحة الدليل الرقمي كدليل صالح في الإثبات (المصداقية والأصالة)

يجب لقبول الأدلة الرقمية أن تفوق قيمتها الإثباتية أي تأثير ضار، ولكن لأنه يمكن تكرارها أو تعديلها أو العبث بها بسهولة، فتثور مشكلة الكفاءة والصلاحية فيما يتعلق بطرق جمعها وتخرينها ومعالجتها. وتعتمد القيمة الثبوتية للدليل في المقام الأول على أصالته

والتثبت من أصالة الدليل يعني التحقق منه بهدف إقناع المحكمة بأن الدليل محل التحقق يتمتع بالمصداقية المطلوبة.[169]

وتطبق العديد من المحاكم الأمريكية قواعد الإثبات الفيدرالية على الأدلة الإلكترونية بطريقة مشابهة للغاية للطريقة التي يتم بها تطبيقها على الأدلة الورقية التقليدية، فنصت المادة 901 من قواعد الإثبات الفيدرالية على أنه " يتعين على الخصم أن يقدم دليلاً كافياً لإثبات صحة ما يدعيه". ومع ذلك فقد أقرت تلك المحاكم بالاختلافات من حيث الإجراءات والمعايير المعمول بها للأخذ بهذا الدليل.[170] ويؤكد ذلك ما نصت عليه المادة 1001 من قواعد الإثبات الفيدرالي والتي تقرر أنه" إذا تم تخزين البيانات في جهاز كمبيوتر أو جهاز مشابه فإن أي مطبوع أو مخرجات يمكن قراءته عن طريق البصر يعكس البيانات بدقة فهو دليل أصلي" [171]

وتنص المادة 1003 من قواعد الإثبات الفيدرالي على أنه " يمكن قبول نسخة مكررة من الدليل ما لم يكن هناك سؤال حقيقي يتعلق بدقة النسخة المكررة أو إذا لم يكن من العدل

---

[169] سامي حمدان الرواشدة " الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي" المجلة الدولية للقانون، دار جامعة حمد بن خليفة للنشر، قطر، سنة 2017م، ص 14.

[170] Stephen Manson, "**Expert in Cyber Security**". http://www.stephenmason.eu/articles/electronic-evidence.html.

[171] **Federal Rules of Evidence,** ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS: **Rule 1001. Definitions That Apply to This Article. (D)** An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout — or other output readable by sight — if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it. (Pub.L.93595,§1,Jan.2,1975,88Stat.1945;Apr.26,2011,eff.Dec.1,2011.) **https://www.law.cornell.edu/rules.**

لسبب ما قبول النسخة الأصلية بدلاً من النسخة المكررة".[172] وتعني تلك القاعدة قبول النسخ المكررة ما لم تكن هناك مشكلة حقيقية تتعلق بالأصالة ولا يوجد سبب آخر لطلب النسخة الأصلية.

ومنذ عام 1923م وحتى عام 1993م تم قبول الأدلة العلمية المتخصصة للكشف عن الجرائم ، واعتمدت المحاكم الأمريكية في عام 1973م المادة 702 من قواعد الإثبات الفيدرالية التي تنص على أنه " إذا كانت المعرفة العلمية أو التقنية أو غيرها من المعارف المتخصصة تساعد في فهم الأدلة أو تحديد حقيقة موضوعية يكون الشاهد مؤهلاً كخبير لمعرفته أو مهارته أو خبرته أو تدريبه أو تعليمه وله أن يشهد على ذلك في شكل رأي أو غير ذلك".

وتعترف المحاكم الأمريكية بمصداقية الدليل عادة عندما تحتوي الرسائل الإلكترونية على ميزات تعريف ذاتي. فعلى سبيل المثال يتم تمييز رسائل البريد الإلكتروني بعنوان البريد الإلكتروني للمرسل، ويتم تمييز الرسائل النصية برقم الهاتف الخلوي للمرسل، ويتم وضع علامة على رسائل موقع التواصل الاجتماعي facebook باسم وصورة الملف الشخصي للمستخدم. ومع ذلك ونظراً إلى أن هذه الرسائل يمكن أن يتم إنشاؤها بواسطة طرف ثالث تحت ستار المرسل المحدد، فقد اعتبرت المحاكم أن الاتصال الإلكتروني الذي ينشأ من بريد إلكتروني ما أو مواقع الشبكات الاجتماعية والذي قد يحمل اسم مؤلف مزعوم لا يكفي وحده للتدليل على المصداقية.[173]

ففي قضية Robert ELECK قام دفاع المدعى عليه بالتشكيك في مصداقية المدعية من خلال الإدعاء بأن المدعى عليه قد تلقى مجموعة من الرسائل من موقع

---

[172] **Federal Rules of Evidence,** ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS: **Rule 1003. Admissibility of Duplicates "**A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate."(Pub. L. 93–595,§1, Jan. 2,1975, 88 Stat. 1946; Apr.26, 2011, eff. Dec. 1, 2011.) **https://www.law.cornell.edu/rules**.

[173] Commonwealth v. Purdy ،459 Mass. 442 ،450 ،945 NE2d 372 (2011), https://www.leagle.com/decision/inctco20110809065.

التواصل الاجتماعي فيسبوك الخاص بالمدعية، إلا أن المحكمة رفضت إدعاء الدفاع وقضت بأن المتهم قد أخفق في إثبات أصالة الرسائل المرسلة إليه، وعليه لا يمكن قبول هذه الرسائل كدليل للطعن في أقوال المدعية، فعلى الرغم من أن المدعية أقرت بأن هذه الرسائل أرسلت من حسابها الشخصي على موقع فيسبوك، إلا أنها أنكرت أنها هي من قام بإرسالها، معللة أقوالها بأن حسابها الشخصي قد تم اختراقه من طرف غير معروف، وأن نظام الاتصال ذاته لم يكن آمناً.[174]

ومع ذلك أثارت قضية ELECK العديد من الإشكاليات والتي من بينها أن النيابة العامة لم تتساءل عما إذا كانت النسخة المطبوعة صحيحة ودقيقة. وبدلاً من ذلك كان الأفضل أن يتم التعامل مع أسماء المستخدمين كدليل ظاهر على الأصالة والتي يمكن النظر فيها جنباً إلى جنب مع الأدلة الأخرى. فمن غير المقبول التحقق من أصالة الدليل بشكل صارم، حيث يستطيع أي شخص أن يدعي أن حسابه قد تم اختراقه، وهو ما يترتب عليه استبعاد الدليل الذي يحتمل مصداقيته، وهو ما يستتبع استبعاد الدليل في أغلب جرائم التقنية ما لم يتم الحصول عليه من مزود الخدمة أو أن يعترف الشخص نفسه بارتكابه للفعل محل الدليل. كما أن هناك قضايا أخرى تتعلق بمقبولية المعلومات المخزنة إلكترونياً، والتي تثير العديد من الإشكاليات في ظل تطبيق قواعد الإثبات الحالية. على سبيل المثال، في حالة وجود موقع ويب يتم تحديثه بشكل متكرر، قد تنشأ مشكلات حول كيفية مصادقة محتوى موقع الويب كما ظهر في لحظة معينة في الماضي.[175]

وفي رأينا فعلى الرغم من أن اقتناع القاضي يبنى على الأدلة المطروحة أمامه وله أن يأخذ منها ما يطمئن إليه لحكمه، فإنه لا يلزم أن تكون الأدلة التي اعتمد عليها القاضي في حكمه قاطعة في كل جزئية من جزئيات الدعوى، إذ أن الأدلة في المواد الجنائية متساندة تكمل بعضها البعض، ومن خلالها جميعاً تتكون عقيدة القاضي فلا ينظر إلى دليل بعينه

---

[174] STATE of Connecticut v. Robert ELECK, 23 A.3d 818 (2011) .Argued May 31,2011.Decided August 9,2011.

https://www.leagle.com/decision/inctco20110809065

[175] See: Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 553 (D.Md.2007).

لمناقشته على حدة دون باقي الأدلة، بل يكفي أن تكون الأدلة في مجموعها مؤيدة إلى ما قصده الحكم منها.

ترتيباً على ما سبق يشترط لقبول الأدلة المتحصلة من الأجهزة الرقمية، أن تكون ذات كفاءة كدليل إذا كانت تمتلك الصلاحية العلمية المطلوبة وذات صلة. وقد أوضحت المادة 401 من قانون الإثبات الفيدرالي أن الأدلة تكون ذات صلة إذا كانت تميل إلى جعل الحقيقة أقرب أو أكثر احتمالاً في حال عدم وجود دليل، وتكون الحقيقة هي النتيجة المترتبة على الإجراء.[176] ويرى بعض الفقه أنه يتوجب على الطرف الذي يسعى إلى تقديم الدليل أن يقنع القاضي بأن المسألة المراد إثباتها من المحتمل أن تكون صحيحة على الأغلب.[177]

واعتبرت المحاكم الأمريكية عدة عوامل يجب أخذها في الاعتبار لقياس كفاءة الدليل الرقمي كدليل علمي صالح في الإثبات ومنها[178]:

1- عدم وجود أسباب معقولة للاعتقاد بأن الدليل يفتقر إلى الدقة بسبب الخطأ في استخلاصه.
2- أن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإن لم يكن كذلك يشترط عدم تأثير الجزء المعطل أو الذي لا يعمل بشكل جيد على استخراج الدليل أو التأثير على دقة محتواه.
3- في الحالة التي تم تسجيل أو تخزين الدليل الإلكتروني من جانب شخص غير طرف في الدعوى أثناء قيامه بأعماله المعتاده، يجب التأكد من كونه لم يكن يعمل لحساب أحد أطراف الدعوى.

---

[176] **Federal Rules of Evidence**. ARTICLE IV. RELEVANCE AND ITS LIMITS: **Rule 401**. **Test for Relevant Evidence**: Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and(b) the fact is of consequence in determining the action. **https://www.law.cornell.edu/rules**.

[177] Paul F. Rothstein, "Evidence in a nutshell"- Evidence (Law) -- United States. St. Paul, MN : West, Thompson Reuters., (2012)., p 9.

[178] نزار أولاد مومن "الإثبات في الميدان الجنائي من خلال الدليل المعلوماتي" مجلة الفقه والقانون، الناشر صلاح الدين دكداك، المغرب، العدد 71، سنة 2018م، ص 49.

4- إذا قدم الخصم في الدعوى دليلاً وكان هذا الدليل مستخرجاً من جهازه يصبح معتمداً؛ ذلك أنه بتقديمه هذا الدليل بنفسه يشهد على صحته.

المطلب الثاني

سلطة القاضي في قبول الأدلة الرقمية

-سلامة الحصول على الدليل الالكتروني شرط لقبول المحكمة له

يلزم أن يكون الدليل الإلكتروني صحيحاً حتى تقبله المحكمة في الإثبات وخاصة عند صدور حكم بالإدانة. هذه القاعدة تستمد قوتها من المبادئ العامة التي تقضي بأن دليل الإدانة على خلاف دليل البراءة يجب أن يكون صحيحاً[179]. وهو لا يكون كذلك إذا كان الحصول عليه قد تم بالمخالفة لقواعد الاختصاص كونها من النظام العام كما لو كان الأمر بتقديم البيان قد صدر من مأمور الضبط وليس من سلطة التحقيق المختصة. كما يكون باطلاً إذا تم التحصل عليه بطريق التفتيش وكان هذا التفتيش باطلاً.

غير أن بعض التشريعات تعطي القاضي الجنائي سلطة تقديرية في تحديد قيمة الدليل ولو كان دليلا باطلاً. من ذلك أن محكمة النقض الفرنسية بتاريخ 15 يناير 1993 قضت بإلغاء حكم محكمة استئناف كان قد رفض قبول دعوى مدنية أمام القضاء الجنائي، مؤسسة حكمها على أن المدعي بالحق المدني كان قد حصل على الدليل المؤيد لدعواه من خلال انتهاك الحق في سرية المراسلات دون أن يناقش ما إذا كانت الوثيقة المتحصلة بطريق غير مشروع من شأنها أن تساعد في إثبات الجريمة، واعتبرت محكمة النقض أن الحكم المطعون فيه قد خالف المادة 427 إجراءات فرنسي والتي تكرس مبدأ حرية الإثبات في المواد الجنائية.[180]

وفيما يتعلق بالأدلة الرقمية كونها من وسائل الإثبات الحديثة والتي تتطور يوماً بعد اليوم، فتثار الإشكالية عندما يجد القاضي نفسه في صراع بين مصالح متعارضة، مصلحة المجتمع في الردع ومصلحة الفرد في الحفاظ على حقوقه وحرياته. ومع ذلك فله السلطة

([179]) نقض 15 مايو سنة 2000 مجموعة أحكام النقض س 51 ص 477 رقم89.

[180] مشار إليه: أحمد عوض بلال "قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة" الطبعة الثالثه، دار النهضة العربية، القاهرة،سنة 2013، ص 117.

المطلقة في قبول أو رفض الدليل الرقمي بناء على اقتناعه الذاتي، معتمداً في ذلك على طريق المنطق والعقل والذي يراعى فيه خصوصية الأدلة الرقمية باعتبارها من المسائل العلمية الدقيقة وارتباطها بوسائل فنية ورقمية حديثة. وله في ذلك الاستعانة بأهل الخبرة، لتقدير المسائل الفنية التي تحتاج إلى معرفة فنية لا تتوافر لدى القاضي.

بناء على ما تقدم فالأحكام يجب أن تبنى على الأدلة التي يقتنع منها القاضي بإدانة المتهم أو براءته، وذلك بناءً على عقيدة يحصلها هو مما يجريه من التحقيق مستقلاً بنفسه لا يشاركه فيها غيره. وتدليلاً على ذلك قضت محكمة النقض المصرية أن "الأصل أن المحكمة تعول في تكوين عقيدتها على التحريات باعتبارها معززة لما ساقته من أدلة، طالما أنها كانت مطروحة على بساط البحث، إلا أنها لا تصلح وحدها لأن تكون دليلاً أساسياً على ثبوت التهمة، ولما كان الثابت أن محرر المحضر لم يبين للمحكمة مصدر تحرياته لمعرفة ما إذا كان من شأنها أن تؤدي إلى صحة ما انتهى إليه من أن الطاعن يؤجر وينسخ ويبيع الأفلام المضبوطة للغير لإثارة شهوات الجمهور وغرائزه، فإن التحريات بهذه المثابة لا تعدو أن تكون مجرد رأي لصاحبها يخضع لاحتمالات الصحة والبطلان والصدق والكذب إلى أن يعرف مصدره ويتحدد كنهه ويتحقق القاضي منه بنفسه، حتى يستطيع أن يبسط رقابته على الدليل، ويقدر قيمته من حيث صحته أو فساده وإنتاجه في الدعوى من عدمه، وإذا كانت المحكمة قد جعلت أساس اقتناعها رأي محرر المحضر، فإن حكمها يكون قد بني على عقيدة حصلها الشاهد من تحريه لا على عقيدة استقلت المحكمة بتحصيلها بنفسها، وكان الحكم المطعون فيه خلا من قيام الدليل على توافر ركن القصد الجنائي لدى الطاعن فإنه يكون معيباً بالقصور المستوجب للنقض".[181]

تأكيدا لذلك صدر قانون جرائم تقنية المعلومات المصري لسنة 2018 ليقرر في المادة (11) منه القاعدة التالية "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من

---

[181] حكم نقض جلسة 20 مارس لسنة 2000، الطعن رقم 17759 لسنة 64 ق.

راجع كذلك: الناجم كوبان "سلطة القاضي الجنائي في تقدير الأدلة الرقمية الناتجة عن الجرائم المعلوماتية في إطار نظرية الإثبات الجنائي"،مجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، العدد 4، سنة 2017م، ص 281.

أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

- **ما يضعف من قيمة الدليل الإلكتروني أمام المحكمة**

يتصف الدليل الرقمي بالضعف من حيث طريقة الحفاظ عليه؛ حيث يسهل التخلص منه عن طريق الحذف أو التخريب. لذا يسمح القانون الكندي[182]– متأثرا بالقانون العرفي – للقاضي بأن يصدر أمراً بناءً على طلب أحد الخصوم بالتحفظ على جهاز الكمبيوتر الخاص بالخصم والذي يحتوي على دليل يحتاج إليه في دعواه[183]. وللقاضي أن يصدر أمراً بذلك يسمى Anton Piller order وهو أمر التحفظ على الجهاز المحتوي على بيانات معينة. فإذا قام الخصم بحذفه توافرت في مواجهته قرينة قانونية قابلة لإثبات العكس بأن تلك البيانات لم تكن في مصلحته بل كانت في مصلحة الخصم طالب الأمر. وعندئذ يخسر الخصم الذي قام بحذف البيانات دعواه. ويمكن أن يضاف إلى هذا الجزاء التعويض عن هذا الخطأ. وهو ما قضت به محكمة Ontario بكندا عندما طلبت من المدعى عليه تسليم جهاز الكمبيوتر الخاص بشركته فقام بذلك بعد مضي ثلاثة أشهر واكتشف الخبير أنه قام باستخدام برامج معينة لمسح بيانات في الكمبيوتر لا يمكن استعادتها[184]. بل ويمكن أن يكون إتلاف الدليل الإلكتروني من جانب المدعي نفسه، كما حدث في كندا في قضية Brandon Heating & Plumbing[185].

-ضرورة المواجهة بالدليل الالكتروني

يتعين مناقشة المخرجات الرقمية والكشف عنها أمام الخصوم، سواء أكانت مطبوعة أم بيانات معروضة على شاشة الحاسوب أو الهواتف الخلوية أو أياً كان شكلها، وذلك في

---

[182] Rule 1.04 of the Rules of Civil Procedure.

[183] Berkley D. Sells; Ian Collins, Strategies to Obtain Electronic Evidence, 36 ADVOC Q. 295 (2010).

[184] iTrade Finance Inc. v. Webworx Inc. (2005), 18 C.P.C (6th) 117, [2005] O.J. No. 3492 (QL), 255 D.L.R. (4th) 748 (S.C.J.) (iTrade 2).

[185] Brandon Heating & Plumbing (1972) Ltd. v. Max Systems Inc (2006), 202 Man. R. (2d) 278, 42 C.P.C. (6th) 267, [2006] M.J. No. 149 (QL) (Q.B.).

حضور جميع الخصوم، حيث تطرح الأدلة لمناقشتها ومواجهة الشهود بها، فالقاضي لا يبني قناعته إلا بناء على عناصر الإثبات التي طرحت أثناء جلسات المحاكمة وخضعت لحرية مناقشة جميع أطراف الدعوى.[186]

ويتيح القانون الكندي للمدعي الراغب في الاطلاع على المستندات الإلكترونية التي يحوزها المدعي عليه حيث تسمح القاعدة 30.06 من قواعد الإجراءات المدنية الكندي للقاضي أن يستجيب لطلب المدعي الاطلاع على المستند الإلكتروني الذي يتواجد في حوزة المدعى عليه أو كان تحت سيطرته، طالما اقتنعت المحكمة بضرورة ذلك للفصل في النزاع. فقد أصبح تعبير المستند يشمل المستندات الالكترونية بالإضافة إلى المستندات الورقية.

وفي قضية Stirling بمقاطعة فلوريدا بالولايات المتحدة الأمريكية صادرت الجهات الأمنية المختصة جهاز كمبيوتر شخصي لمتهم بجريمة إتجار بالمخدرات بناء على إذن قضائي، كما قامت تلك الأجهزة بفحص القرص الصلب في جهاز الكمبيوتر، وتم الحصول على 214 صفحة تتعلق بمحادثات تمت عبر موقع Skype من جهاز الكمبيوتر المملوك للمتهم، وهذه الصفحات لا تظهر بسهولة بمجرد فتح الملفات التي تظهر على القرص الصلب. ولم يتم تزويد محامي الدفاع بهذه المعلومات إلا في نهاية المحاكمة، وذلك في صباح اليوم المخصص لمناقشة الخبير الذي طلبه محامي الدفاع. وقد كان لسجلات الكمبيوتر تأثير حاسم على المتهم حيث أنها دحضت إفادته التي قدمها أثناء استجوابه، الأمر الذي ترتب عليه إدانته بالجريمة المنسوبة إليه. قدم المتهم طلباً بإعادة المحاكمة، فقضت المحكمة بإعادة المحاكمة، وجاء في حيثيات قرار المحكمة أنه إذا كان المتهم بحاجة إلى خبير مختص في الكمبيوتر للحصول على برنامج لاسترجاع المعلومات المخزنة وغير الظاهرة، فإنه يتعين على الأجهزة المختصة التي تعلم بوجود تلك المعلومات إخبار المتهم بحقيقة الأمر، كما أن المعلومات تم تقديمها في شكل غير صالح للاستخدام، بل

[186] خالد مصطفى الجسمي، مرجع سابق، ص 31. انظر كذلك: لعوارم وهيبة "مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي" مجلة الفقه والقانون، العدد 20، الناشر صلاح الدين دكداك، المغرب، سنة 2014م، ص 110.

على العكس من ذلك، فقد تم تقديمها بصورة تنطوي على إخفاء للمعلومات المتوفرة. وما تعرفه الأجهزة المختصة كان ضمن الأدلة التي اعتزمت تقديمها في المحاكمة.[187]

- **حجية البريد الإلكتروني في الإثبات (E-mail)**

عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م البريد الإلكترونى بأنه، "وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعى أو إعتبارى، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما فى حكمها".

وتتفق هذه النتيجة مع ما قضت به المحاكم الأمريكية بأن الإيميل الفردي والذي ليس وليداً للتدخل الجماعي في شركة أو جهة معينة ليست له حجية ولا يمكن الاعتماد عليه كدليل في الإدانة، على الرغم من أن الدفاتر التجارية لها حجية في الإثبات[188].

على العكس من ذلك فإن الإيميل إذا صدر من جهة عامة وكان هذا النوع من الإيميلات يصدر بشكل روتيني ومتكرر فإنه يصلح أن يكون حجة في الإثبات على ما قضت به المحاكم الأمريكية[189].

-مدى صحة الدليل الالكتروني في مواجهة الحق في التعبير

أثيرت مسألة حرية التعبير في خصوص ما يتم نشره على شبكة الإنترنت خاصة في القانون الأمريكي. في ذلك قبلت المحاكم الأمريكية المحادثة الإلكترونية التي تم التقاطها والتي اعترف فيها المتهم لأحد الشهود، باعتبار أن أقواله في تلك المحادثة تمثل جزءً من اعترافه ويكتمل بما شهد به الشاهد[190]. فهنا أقوال الشاهد تؤكد ما جاء بأقوال المتهم الإلكترونية وتعززها.

---

[187] United States v. Stirling, Case No 11-20792-CR-ALTONAGA, United States District Court, S.D. Florida, Miami Division, April 10, 2012.

[188] United States v. Shah, No. 5:13 CV 328 FL, 2015 WL 3605077 (E.D.N.C. June 5, 2015)

[189] United States v. Gonzales-Perales, 313 F. App'x 677, 681 (5th Cir. 2008)

[190] United States v. Gonzales-Perales, 313 F. App'x 677, 681 (5th Cir. 2008).

كما أظهر القضاء الأمريكي ثقته لما قام به المتهم من إرسال رسائل الغير التي وصلته (forward) باعتبار أنه يوافق عليها واعتبرها اعتراف ضمني منه adoptive admission وذلك بالنظر إالى سياق ومحتوى هذه الرسائل[191].

وقد قضت المحاكم الأمريكية في عديد من أحكامها بأن التعديل الأول للدستور الأمريكي الذي يكرس حرية التعبير لا يحول دون وقوع جرائم بطريق الانترنت في حالة التهديد والابتزاز[192]والتحريض على العنف[193] وفي حالة القذف والسبب وفي حالة ارتكاب جرائم إذاعة صور فاضحة للأطفال . وقد أفاد بعض مقدمي خدمات البريد الإلكتروني أن

---

[191] United States v. Burt, 495 F.3d 733, 738 39 (7th Cir. 2007)

[192] See: Watts v. United States, 394 U.S. 705, 707–08 (1969) (holding that defendant's statement that "if they ever make me carry a rifle the first man I want in my sights is L.B.J." was political hyperbole, not a true threat, and was therefore protected under the First Amendment). Compare Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 E3d 1058, 1085–86 (9th Cir. 2002) (en banc) (finding website labeling abortion providers "GUILTY" and featuring their pictures, names, and addresses was a true threat of force and therefore unprotected), with United States v. Hardy, 640 F. Supp. 2d 75, 80–81 (D. Me. 2009) (holding that threats that are "meant to communicate a serious expression of . .. Intent to [perform] an act of unlawful violence ... cannot reasonably be construed as 'political hyperbole' and are therefore not protected speech).

[193] United States v. Morales, 272 F.3d 284, 288 (5th Cir. 2001) (rejecting defendant's claim that his threat to kill people at his school could not constitute a "true threat" because it was made over the Internet to a third party). 18 U.S.C. § 875, which outlaws transmitting threats to kidnap or injure a person, has been used to successfully prosecute individuals who send threatening communications via the Internet. *But see* United States v. Baker, 890 F. Supp. 1375, 1390 (E.D. Mich. 1995) (granting defendant's motion to quash indictment against him for statements he made over the Internet because they were not true threats).

مقدار 75 إلى 90 بالمائة من جميع رسائل البريد الإلكتروني هي رسائل تطفلية.[194]

غير أنه بالنسبة لإنشاء حساب بإسم وهمي، قضت المحكمة العليا لولاية فرجينا في الولايات المتحدة الأمريكية في سنة 2008 بعدم دستورية قانون صادر من الولاية بتجريم إنشاء واستعمال ايميل باسم مجهول وإرسال رسائل منه باعتبار أن ذلك يشكل إرسال رسائل مزعجة spam. ومع أن كثرة هذه الرسائل تستخدم لشغل ايميلات الآخرين مما يعجزهم عن استعمالها، إلاّ أن المحكمة قد استندت في رأيها إلى أن التجريم من الاتساع بحيث لا يفرق بين الرسائل التي تنطوي على رأي والرسائل التجارية، وبالتالي فإنها تتعارض مع الحق في التعبير ولو بإسم مصطنع وليس بإسم صاحب الحساب[195].

وتتجه أحكام القضاء الأمريكي إلى أن من حق الشخص أن يخفي اسمه الحقيقي عندما ينشيء حساباً أو بريد إلكتروني يراسل به الآخرين باعتبار أن ذلك يتصل بحقه في التعبير[196]، وذلك عندما تتعلق الرسائل برأي سياسي أو أدبي أو اجتماعي أو ديني. وبناء على ذلك قُضي بعدم دستورية قوانين تسمح بالكشف عن الشخصية الحقيقية بالمخالفة للحق في التعبير[197]. تأكيداً لذلك أيضاً قضت المحكمة العليا لولاية فرجينيا بإلغاء قانون نص على تجريم إنشاء حساب أو إيميل باسم مزيف. وقد حددت المحكمة في حكمها أن سبب التجريم جاء عاماً دون أن يميز بين سبب إنشاء الحساب أو الإيميل، وبالتالي فقد شكل بذلك افتئاتاً على الحق في التعبير الذي يسمح بذلك التعبير ولو كان باسم مجهول

---

[194] مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية " البند 8 من جدول الأعمال (التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) سلفادور، البرازيل 12-19 إبريل 2010، ص 2.

[195] Jaynes v. Commonwealth, 666 S.E.2d 303, 313 (Va. 2008); see also McIntyre v. Ohio, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of the publication, is an aspect of freedom of speech protected by the First Amendment.").

[196] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995); Matthew Mazzotta, Note, Balancing

Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers, 51 B.C. L. REv. 833, 833.(2010).

[197] McIntyre, 514 U.S. at 342.

أو مغاير للحقيقة[198]. وقد ارتأت المحكمة أن المشرع في هذا القانون كان من الواجب عليه أن يحدد ما إذا كان الغرض من إنشاء الحساب أو الإيميل هو لأغراض تجارية أو غير تجارية. هذه الأخيرة إذا كانت مشمولة بالحق في التعبير، فإنها لا يصح أن تكون محلاً للتجريم.

أما إذا تعلق الأمر برسائل تجارية مزعجة الغرض منها تعطيل البريد الإلكتروني بسبب كثرة الأعداد التي يرسلها المرسل عن عمد بقصد تعطيل إيميلات الأشخاص أو الشركات، فليس من حقه أن يخفي شخصيته الحقيقية ويمكن الكشف عنها ومثوله أمام القضاء.

المبحث الثالث

استبعاد الأدلة الجنائية الرقمية

على سند من بطلانها

تمهيد:

من القواعد المستقر عليها أن القاضي حر في تكوين عقيدته ومدى قبوله للدليل، شريطة أن يكون الدليل قد تم الحصول عليه بطريق مشروع، وأن يكون قد طرح على المحكمة وتمت مواجهة الخصوم به. وانطلاقاً من ذلك يجب لقبول الدليل الرقمي كدليل صالح في الإثبات أن يكون وليد إجراءات جنائية مشروعة. فالحقيقة والدليل هما الغاية التي تبتغيها مجريات العدالة، إلا أن وسائل الوصول إليها يجب أن تتم بوسائل مشروعة دون انتهاك أو مساس بحقوق الإنسان وحرياته، فمن المسلم به أن الغاية لا تبرر الوسيلة، لاسيما وأن العدالة هدفها الأول الحفاظ على مصالح المجتمع وتحقيق التوازن بينها وبين حريات وحقوق الأفراد فيه.

وتتجلى إشكالية بحث قواعد الاستبعاد في عدم وضوح الرؤى في تعداد الأسباب التي تؤدي إلى تطبيق تلك القواعد، علاوة على عدم تحديد نطاق قواعد استبعاد الأدلة الجنائية الناتجة عن إجراءات غير مشروعة، وتباين دور القضاء في تطبيقها. بل ويثور تساؤل أكثر

[198] Jaynes v. Commonwealth, 666 S.E.2d 303, 313 (Va. 2008); *see also McIntyre,* 514 U.S. at 342.

أهمية، فهل يؤتي تطبيق قاعدة استبعاد الدليل المتحصل بطرق غير مشروعة ثماره بإهدار أي إجراءات مخالفة من حيث الأثار القانونية المترتبة عليه واستبعاد النتائج المحتملة من وراء تلك الإجراءات؟ وهو ما سنتاوله من خلال المطالب الآتية:

المطلب الأول: استبعاد الأدلة المتحصل عليها بطرق غير مشروعة

المطلب الثاني: أسباب استبعاد الأدلة غير المشروعة

المطلب الأول

استبعاد الأدلة الرقمية المتحصل عليها

بطرق غير مشروعة

قاعدة الاستبعاد هي قاعدة إجرائية تحكم قبول الدليل أمام المحاكم الجنائية بهدف عمل موازنة بين حق المجتمع في مكافحة الجريمة ووجوب حماية حقوق الأفراد وحرياتهم وصيانتها من أي انتهاك.[199] ويستند ذلك إلى قاعدة أن أحكام الإدانة لا يجب أن تقوم على دليل باطل.

ومن ذلك أن الدليل يستبعد في حالة مخالفة التعديل الرابع للدستور الأمريكي قاعدة الاستبعاد Exclusionary Rule ويسري ذلك مع العلم بأن قاعدة الاستبعاد ليست قاعدة مستمدة مما ورد بالتعديل الرابع من متطلبات، وهو ما يعطي السلطة التشريعية إمكانية مخالفتها بنصوص تشريعية أخرى. كما أن قاعدة الاستبعاد ليست مستمدة من سلطة المحكمة في الإشراف على العمل القضائي ولكن من متطلبات الدستور.[200]

فالمشروعية تنبع من أمرين: الأول صحة إجراءات الحصول على الدليل كونه تم وفق إجراءات قانونية مشروعة، أما الثاني فيتعلق بمشروعية طرق الحصول عليه، لاسيما وأن

---

[199] مشاري خليفة العيفان "قاعدة استبعاد الدليل المتحصل من القبض والتفتيش غير المشروعين في القانون الأمريكي" مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، المجلد 35 ، العدد الرابع، ديسمبر سنة 2011، ص 123.

[200] نفس المرجع السابق، ص 132-133.

اقتناع القاضي لا يبنى إلا على أدلة صحيحة تمت وفق القانون. وهنا تنشأ قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة، والتي يظهر أساسها في الربط بين نظرية البطلان ونظرية الإثبات الجنائي، والتي تدلل على أن كل ما يستمد بالمخالفة لنظرية البطلان لا يمكن قبوله ضمن قواعد الإثبات أمام القاضي الجنائي. وهو ما انتهت إليه محكمة النقض المصرية حيث قضت " بأنه وإن كان من المسلم به أنه لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون، إلا أن تقرير هذا المبدأ بالنسبة لدليل البراءة غير سديد؛ لأنه لما كان من المبادئ الأساسية في الإجراءات الجنائية أن كل متهم يتمتع بقرينة البراءة إلى أن يحكم بإدانته بحكم نهائي، وأنه إلى أن يصدر هذا الحكم له الحرية الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى وما يحيط نفسه من عوامل الخوف والحرص والحذر وغيرها من العوارض الطبيعية لضعف النفوس البشرية، فقد قام على هدي هذه المبادئ حق المتهم في الدفاع عن نفسه وأصبح حقاً مقدساً يعلو على حقوق الهيئة الاجتماعية التي لا يفيدها تبرئة مذنب بقدر ما يؤذيها ويؤذي العدالة معاً إدانة بريء ولا يقبل تقييد حرية المتهم في الدفاع عن نفسه باشتراط مماثل لما هو مطلوب في دليل الإدانة".[201]

ترتيباً على ذلك وعلى هدي ما قضت به محكمة النقض المصرية، لا يجوز الاستناد في الإدانة إلى أدلة غير مشروعة جاءت ثمرة لانتهاك حرمة الحياه الخاصة. أما في البراءة فالأمر يختلف حيث أن الأصل في المتهم البراءة، فعلى سبيل المثال يجوز للمحكمة الاستناد إلى رسائل بريد إلكتروني أو محادثات تليفونية ولو تضمنت معلومات عن الحياة الخاصة للمرسل أو المرسل إليه أو الغير، فعلى الرغم من أن التمسك بهذه المحادثات فعل غير مشروع ويعد انتهاكاً لحرمة الحياه الخاصة، إلا أن الدليل المستمد من هذا الفعل ليس استصحاباً على أصل عام هو البراءة، وبناء على ما قضت به محكمة النقض يمكن الاستناد إليه.

على أية حال فقاعدة الاستبعاد أمر ضروري لا غنى عنه لضمان سلامة إجراءات المحاكمة. ولا يتعين استبعاد كل دليل مستمد من إجراء باطل، فيجب أن تتوافر الصفة لا المصلحة فيمن يطالب بتطبيق قاعدة الاستبعاد، فليس كل متهم في الدعوى وإن كانت له

[201] نقض 25 يناير 1965، مجموعة أحكام النقض المصرية، س 16، رقم 21، ص 587.

مصلحة في تطبيق قاعدة الاستبعاد له صفة في المطالبة بتطبيق قاعدة الاستبعاد؛ ويعزى السبب في ذلك أن هذه القاعدة ترتبط وجوداً وعدماً بالإجراء الباطل الذي يقتصر فيه الأمر على إثارة عدم مشروعيته لمن خضع له. وهذا يتفق ما نصت عليه المادة 322 من قانون الإجراءات الجنائية المصري والتي تضمنت بأنه يجب للتمسك ببطلان التفتيش ألا يكون المتمسك به هو المتسبب في حصوله.

المطلب الثاني
أسباب بطلان الأدلة الرقمية

مشروعية الأدلة الجنائية تعني الحصول عليها وفقاً للضوابط التي حددها القانون، ودون الخروج عن روح نصوصه، وذلك في إطار الإجراءات التي تقوم بها السلطات المختصة لإثبات وقوع جريمة ما ونسبتها لمرتكبها. بناء على ذلك فكل إجراء لم يجزه المشرع يعد غير مشروع ولا يرتب أي أثر قانوني.[202]

وسوف نتناول عدداً من الدفوع التي أثارت العديد من القضايا والإشكاليات فيما يتعلق بالدليل الرقمي المتحصل عليه بطريق غير مشروع، على النحو التالي:

1- التحريض على ارتكاب الجريمة

يعد من بين الدفوع التي قد يدفع بها المتهم أمام المحكمة أن التهمة الموجهه إليه تمت بناء على إجراءات تنطوي على تحريض قد تم للإيقاع به وهو ما يخالف القانون. حيث قد يصدر التحريض عن أشخاص عاديين وقد يكون صادراً عن سلطات الدولة (التحريض الرسمي)، ففي الحالة الأولى يقوم أشخاص عاديين دون صفة بمعاونة سلطات إنفاذ القانون في البحث والتقصي بهدف الإيقاع بالجاني وكشف جرائمه، إلا أن هذا الأمر يأخذ أهمية وتحدِ قانوني حينما تستند المحكمة إلى أدلة تم الحصول عليها من هؤلاء الأشخاص العاديين. فلم تتوافر لهم صفة رسمية من البداية للكشف عن المجرم أو الجريمة، كما لم يكن لديهم الخبرة والمعرفة الكافية بالإلتزامات القانونية المحددة مسبقاً للحصول على الأدلة محل الجريمة. فعلى

[202] محمد فالح حسن "مشروعية الوسائل العلمية في الإثبات الجنائي" الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 1987م.

سبيل المثال يقوم الشخص بانتحال شخصيات غير حقيقية كانتحاله صفة طفل في الجرائم الجنسية أو قيامه بتزييف مواقع أو حسابات لتبدو وكأن أصحابها نساء للإيقاع بالجناه أو الكشف عن هويتهم. ومع نجاح انخراط أشخاص عاديين في مجال التحقيقات الجنائية كمخبرين سريين إلا أن هذا الأمر ينطوي على العديد من المخاطر إذا ما تم تطبيق القانون بهذه الوسيلة، بل وقد تستخدم تلك الوسيلة في الإساءة إلى سمعة بعض الأفراد والجهات من خلال استخدام رسائل مضللة ووهمية. فضلاً عن تحريضهم للمتهمين بارتكاب الجريمة كي يستطيعون الكشف عنهم وإدانتهم.

ومع ذلك قد تجد المحاكم صعوبة في بطلان الأدلة المتحصلة عن تحريض وقع من أشخاص عاديين بقصد الإيقاع بالجاني خاصة إذا تعلقت تلك الأدلة بجرائم خطيرة كالنصب الإلكتروني أو استخدام الأطفال والنساء في إنتاج مواد جنسية عبر المواقع الإلكترونية. فالدفع الذي يمكن للمتهم التمسك به في هذه الحالة هو أن التحقيقات القائمة بناء على هذا الدليل من شأنها الإخلال بمحاكمة جنائية عادلة.

وفيما يتعلق بالنوع الثاني وهو التحريض الرسمي، فيتم عن طريق سلطات الدولة نفسها، كأن يدعي رجل الشرطة نفسه صفة طفل على المواقع الإلكترونية الخاصة باستغلال الأطفال للإيقاع بالمشبته بهم في ارتكابهم جرائم جنسية. وهذه الأعمال تبقى مشروعة متى كانت تستهدف الكشف عن الجريمة أو مرتكبيها ومتى كانت إرادة الجاني حرة غير معدومة.[203] وقد عرف مجلس اللوردات الإنجليزي الضباط السريين بأنهم ضباط إنفاذ القانون المدربون تدريباً خاصاً والذين يعملون في وضع التخفي تحت توجيهات في تحقيق مصرح به، بهدف كشف مؤامرة حالية أو اعتقال مجرمين مشتبه بهم، فهم يضعون أنفسهم في وضع يسمح لهم بأن يصبحوا ضحية للجريمة بغرض القبض على الجاني.[204] وأكد مجلس اللوردات على

---

[203] أشرف توفيق شمس الدين، مرجع سابق، ص 145.

[204] **HOUSE OF LORDS. (OPINIONS OF THE LORDS OF APPEAL FOR JUDGMENT IN THE CAUSE)** Regina, V Looseley. "It deals with the employment of "undercover officers", "test purchasers" and "decoys". Undercover officers are defined as specially trained law enforcement officers working incognito "under direction in an authorised investigation" to infiltrate an existing

أنه لا يجوز لسلطات إنفاذ القانون بالدولة إساءة استخدام إجراءاتها ومن ثم قمع مواطني الدولة باستخدام وسيلة المصيدة، وأوضح أنه من غير المقبول أن تغري وتحرض الدولة مواطنيها على ارتكاب أفعال يحظرها القانون ثم تسعى إلى مقاضاتهم، فهذا يعد إساءة استخدام لسلطة الدولة.[205] ومع ذلك اشترط مجلس اللوردات لقبول قيام سلطات إنفاذ القانون بهذا السلوك "المصيدة" أن يأخذ بعين الاعتبار عدة عوامل لتحديد ما إذا كان ما قام به رجال الشرطة يعد تحريضاً رسمياً على ارتكاب الجريمة من عدمه، والتي يعد من بينها نوع الجريمة وصعوبة كشفها وسريتها وتقدير الأفعال التي قام بها رجال الشرطة.

وقد فسرت المحكمة العليا في استراليا في قضية Ridgeway v The Queen أن معيار قبول استخدام رجال الشرطة لوسيلة المصيدة للإيقاع بالجاني يرتبط بشكل عام بما إذا كان سلوك الشرطة متوقعاً أم لا، فيمكن للدولة أن تبرر استخدام التقنيات الحديثة للحث على ارتكاب جريمة أو تشارك في اصطناع حيل عادية أو استخدام نوع من الخداع للكشف عن الجريمة، شريطة ألا تتجاوز الدولة الحدود المألوفة، وإلا تحول حدوث الجريمة إلى جريمة وقعت بوسائل مصطنعة. فطبيعة الجريمة وصعوبة كشفها والطريقة التي يتم بها إجراء النشاط الإجرامي من الأمور الواجب مراعاتها عند تقدير مدى مقبولية ما قام به رجال الشرطة من

---

conspiracy, arrest suspected criminals or counter a threat to national security. Test purchasers are appropriately trained law enforcement officers who seek "by means of authorised activity, to establish the nature and/or availability of a commodity or service, the possession, supply or use of which involves an offence". Test purchasers are used mainly in the drug trade. Decoys are officers who place themselves passively in a position to become a victim of crime for the purpose of arresting the offender". (ATTORNEY GENERAL'S REFERENCE NUMBER 3 OF 2000 ON 25 OCTOBER 2001) . https://publications.parliament.uk.

- مجلس اللوردات هو المجلس الأعلى في برلمان المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية.

[205] Ibid.

تصيد للجاني.[206] فعلى سبيل المثال قيام رجل الشرطة بشراء أشرطة تحوي منتجات جنسية من متجر أو نوادي الإنترنت بوصفه رجل مدني، بهدف ضبط الجاني أو مكان بيع منتجات مخلة بالآداب يعد عملاً مقبولاً.

ويجب لقبول وسيلة المصيدة أن تكون الشرطة قد تصرفت بحسن نية وليس كجزءً من ثأر ضد فرد أو جماعة. كذلك توافر أسباب معقولة للشك، ليس فقط في الشخص بل قد تتركز الشكوك في مكان معين كمنزل عام مثلاً وقد يكون الاختبار العشوائي لعدد من الأشخاص هو الطريقة العملية الوحيدة لمراقبة نشاط تداول معين، شريطة أن يتوافر لدى الشرطة أسباب كافية للاشتباه في ارتكاب جريمة يعاقب عليها القانون.[207]

ترتيباً على ذلك فإن مسألة تقدير وسيلة التحريض للإيقاع بالجاني متروكة لقاضي الموضوع فله أن يقبل بها لاستبعاد الأدلة، شريطة أن يراعي في ذلك معايير تطبيق سلطات إنفاذ القانون لهذه الوسيلة وهل كان لديها توقع معقول وشك في سلوك المشتبه به. ونفس الحال ينطبق في حال كان التحريض صادراً عن أشخاص عاديين، فيتم التأكد من كون ما قام به الشخص العادي من الإيقاع بالجاني لم يكن تحريضاً صريحاً للقيام بالفعل المجرم. ونحن نؤيد اتباع وسيلة الإيقاع بالجناه عن طريق التحريض لإثبات ارتكابهم لأفعال يحظرها القانون خاصة في جرائم تقنية المعلومات والتي يصعب كشفها عادة كونها عابرة للحدود وترتكب في عالم افتراضي من الصعب الكشف عنها باستخدام وسائل أخرى، فما يقوم به رجل الشرطة في هذه الحالة مجرد إعطاء فرصة للمتهم بالشروع في ارتكاب جريمة مماثلة بهدف الحصول على دليل لإدانته.

ويتمشى ذلك مع ما هو مستقر في القضاء المصري من أن مأمور الضبط له أن يصطنع من الوسائل ما يسلس لمقصوده في ضبط الجريمة مادامت إرادة المتهم باقية حره، وذلك بما لا يتصادم مع أخلاق الجماعة. فتفرق أحكام القضاء المصري بين الكشف عن

---

[206] **HIGH COURT OF AUSTRALIA**. Ridgeway v The Queen. [1995] HCA 66; 184 CLR 19; 129 ALR 41; 78 A Crim R 331. https://jade.io/article/188

[207] Regina, V Looseley . Ibdi.

الجريمة كمن يتقدم لتاجر مخدرات للشراء منه والتحريض على وقوع الجريمة كمن يحرض مدمناً على التعاطي لكي يقوم بضبطه[208].

2- إجراء التفتيش عن الدليل الالكتروني دون إذن قضائي

تناولنا أن التعديل الرابع للدستور الأمريكي قد تضمن عدم جواز انتهاك حقوق الأشخاص في أن يكونوا آمنين في أشخاصهم ومنازلهم وأوراقهم ضد عمليات التفتيش والمصاردة غير المعقولة.[209] وبناء على ذلك أصدرت المحاكم الأمريكية أحكاماً عديدة باستبعاد الأدلة المتحصلة بطرق غير مشروعة، وقررت أن قاعدة الاستبعاد في تلك الحالات تعتبر ضرورة منطقية ودستورية باعتبارها جزءً لا يتجزأ من الحق نفسه. بل وهو طريق لا سبيل للتخلي عنه للتأكيد على سلامة العمل القضائي.

ففي قضية Weeks v. United States قضت محكمة مدينة كانساس بولاية ميسوري بالإجماع، أن الاستيلاء بدون إذن قضائي على مواد من مسكن خاص بطريق غير مشروع يشكل انتهاكاً للتعديل الرابع للدستور، فكان قد تم القبض على المدعى عليه weeks والذي أدين باستخدام بريد شركة اكسبريس التي يعمل بها في نقل تذاكر اليانصيب، وقام ضباط الشرطة بالتحرك إلى منزل weeks لتفتيشه، وأخبرهم أحد الجيران أين يمكنهم العثور على مفتاح المنزل، وعلى إثر ذلك دخل ضباط الشرطة إلى منزل المدعى عليه دون إذن قضائي واستولوا على الأوراق والمقالات الموجودة بالمنزل، ثم عاد ضباط الشرطة في وقت لاحق من نفس اليوم ولا يزالون دون أمر بالقبض، وصادروا الرسائل والمظاريف التي وجدوها في أحد أدراج المكتب، واستخدمت تلك الأوراق كدليل إدانة ضد المدعى عليه في نقل تذاكر اليانصيب عبر البريد. إلا أن المحكمة قضت باستبعاد الأوراق المتحصل عليها بطريق غير مشروع ومخالف للدستور؛ كون البحث والتفتيش تم بطريق غير قانوني. وبررت المحكمة موقفها بأن فرض قاعدة استبعاد الأدلة المتحصل عليها بطريق غير مشروع أمر ضروري لحماية النصوص الدستورية، فإن لم يحدث ذلك فسيتم الاستخفاف بالعمل القضائي، وإذا قبل

---

[208] نقض 15 أبريل سنة 1968 مجموعة أحكام النقض س 19 ص 438 رقم 83؛ نقض 25 أكتوبر سنة 1976 س 27 ص 774 رقم 176.

[209] **The Fourth Amendment states**: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated".

القضاه بتلك الأدلة غير المشروعة، فسوف يكونوا شركاء في تجاهل متعمد لأحكام الدستور الواجب عليهم احترامه.[210]

وعلى الرغم من أنه قد يبدو للوهلة الأولى أن قضية weeks تنبئ عن توجه المحكمة نحو التوسع في نطاق تطبيق قاعدة الاستبعاد إلا أن قرارات المحكمة اللاحقة أثبتت عكس ذلك، ففي عام 1987 تناولت المحكمة العليا حقوق التعديل الرابع لموظفي الحكومة الخاضعين للتحقيق الإداري في قضية O'Connor v. Ortega، وهي قضية تتعلق بالبحث في سجلات مكتب الطبيب المشرف والذي يعمل في مستشفى كاليفورنيا العام. حيث قضت المحكمة بأنه في حين أن الموظفين العموميين يتمتعون بحماية التعديل الرابع، فإن البحث كان معقولًا ودستوريًا، وأن عمليات البحث بدون إذن عن ممتلكات الموظفين العموميين أو أماكن العمل حيثما ينطبق ذلك، مسموح بها بالمثل طالما كانت ذات صلة بالعمل من البداية.[211]

وفي قضية Ontario لعام 2010 انتهت المحكمة العليا الأمريكية إلى صحة الأدلة المتحصل عليها وعدم مخالفة الحق في خصوصية الاتصالات الإلكترونية في مكان العمل الحكومي. حيث حصلت إدارة شرطة أونتاريو OPD على عشرين جهاز استدعاء رقمي (بيجر–pager) لتوزيعها على ضباط وحدة SWAT حتى يتمكنوا من تنسيق عملهم بشكل أفضل، وتم إبرام عقد بين الإدراة وشركة Arch Wireless المعروفة الأن باسم USA Mobility وتضمن العقد شرط استخدام ثابت قدره 25000 ألف حرف في الشهر وإلا سوف يتم فرض رسوم زائدة على الإدراة. ووافق الموظفون بإدراة شرطة أونتاريو على أن تحتفظ الإدارة بحقها في مراقبة وتسجيل جميع أنشطة الشبكة بما في ذلك استخدام البريد الإلكتروني والإنترنت مع أو بدون إشعار مسبق، ولم تذكر سياسة الإدارة الرسائل النصية على وجه التحديد، وقد تم إخبار الموظفين شفهياً بذلك، مع عدم إمكانية إجراء اتصالات شخصية خلال ساعات العمل، وذكرت أنه لن يتم التسامح مع استخدام لغة غير لائقة أو مهينة أو فاحشة أو

---

[210] Fremont Weeks v. United State 232 U.S. 383 (1914), Argued and submitted December 2 and 3, 1913.– Decided February 24, 1914.

[211] O'Connor v. Ortega, 480 U.S. 709 (1987). https://en.wikipedia.org/wiki/O%27Connor_v._Ortega

تشهيرية في نظام البريد الإلكتروني. وقد قامت إدارة شرطة أنتاريو بمراجعة أجهزة بيجر عن طريق مزود الخدمة Arch ووجدت العديد من الرسائل أغلبها كانت شخصية وبعضها كان جنسيًا صريحًا لضابط شرطة يدعى Quon وآخرون، وبناء عليه صدر ضدهم جزاء تأديبي جراء فعلهم. وكان المدعى عليه قد دفع بأن تفتيش جهاز بيجر قد تم انتهاكاً ليس فقط لحقوقهم الدستورية ولكن لقوانين خصوصية الاتصالات الأمريكية، ودفعوا بأن رئيسهم في العمل قد وعد بأن رسائل الاستدعاء نفسها لن تتم مراجعتها إذا قام الضباط بسداد تكاليف الإدراة التي تتكبدها في حال تجاوزوا الحد المسموح به لعدد من الأحرف الشهري. ومع ذلك قضت المحكمة العليا الأمريكية بالإجماع بصحة الأدلة المستمدة من المراجعة التي تتعلق بالعمل وبالتالي لم تنتهك حماية التعديل الرابع ضد التفتيش والمصادرة غير المعقولين.[212]

وعلق قاضي يدعى واردلاو على قرار المحكمة بقوله أن استخدام رسائل البريد الإلكتروني والرسائل النصية وغيرها من الوسائل الإلكترونية الحديثة، أظهر حدودًا جديدة في فقه التعديل الرابع الذي لم يتم استكشافه بعد، منتقداً ما قامت به إدارة OPD من مراجعة الرسائل التي اعتقدت جميع الأطراف بشكل معقول أنها خالية من مراجعة الطرف الثالث وكان بإمكان OPD الحصول على المعلومات بعدد من الطرق الأقل تدخلاً دون مشاهدة محتوى الرسائل ، مثل تحذير Quon في وقت مبكر أو الطلب منه تنقيح الرسائل الشخصية دون مراجعة نصوص هذه الرسائل.[213]

وبتاريخ 22 يونيو 2018 أثارت قضية Carpenter ضجة كبيرة وأحدثت نوعاً من الخلاف بين القضاه والفقهاء، حينما استبعدت المحكمة العليا الأمريكية الأدلة المستمدة من خلال الوصول إلى سجلات تتبع مواقع تواجد الهاتف الخلوي historical cell-site records دون الحصول على إذن تفتيش، وقررت المحكمة أن فكرة الطرف الثالث المطبقة على الاتصالات الهاتفية في قضية -Smith v. Maryland والتي تفيد عدم توقع الخصوصية عن المعلومات التي يسلمها الشخص إلى طرف ثالث- لا يمكن تطبيقها على تكنولوجيا الهواتف الخلوية، واستندت المحكمة إلى أنه كان يجب أن تحصل الحكومة على إذن تفتيش من أجل الوصول إلى سجلات تتبع موقع الهاتف الخلوي عن طريق GPS، وأكملت

[212] Ontario v. Quon, 560 U.S. 746 (2010).

[213] Ibdi

قولها بأنه إذا كانت التكنولوجيا قد وفرت لأجهزة إنفاذ القانون أداة جديدة وقوية للقيام بمسؤولياتها الهامة، ففي الوقت نفسه فإن السلطات تتجاوز وتخاطر باستخدام هذه الأداة بالمخالفة لما أورده الدستور.[214]

على وجه الخصوص، كان قرار قضية Smith هامًا من قبل المحكمة وقاد المحاكم الفيدرالية منذ ذلك الحين بشأن المسائل المتعلقة بالخصوصية والهواتف. فرأت المحكمة في Smith أنه لا يجوز للحكومة التنصت على مكالمة هاتفية، ومع ذلك يمكن الحصول على أرقام الهاتف التي طلبها الشخص على هاتفه دون أمر قضائي. وقررت المحكمة أيضًا أن التعديل الرابع لا يحمي الجمهور من السماح للحكومة بالحصول على المعلومات اللازمة للحصول على الاتصالات من النقطة أ إلى النقطة ب. على سبيل المثال، دون أمر يمكن أن تحصل عليه الحكومة من خطاب أو حزمة من المرسل، المتلقي، عناوين التسليم والتسليم، وحجم الحزمة، ومع ذلك كان يتعين على الحكومة الحصول على إذن قبل فتح الحزمة أو

---

[214] **Supreme Court of the United State** :Timothy Ivory Carpenter v. United States of America. No. 16-402, 585 U.S. (2018) Argued November 29, 2017. Decided June 22, 2018. supremecourt.gov. Retrieved March 30 2019.

- يستطيع مقدمي الخدمات اللاسلكية من الأطراف الثالثة (مثل AT&T و Sprint و T-Mobile و Verizon) العثور على موقع الهواتف المحمولة من خلال بيانات نظام تحديد المواقع العالمي (GPS)، أو معلومات (CSLI) وهي معلومات الهاتف الخليوي التي تم التقاطها بواسطة الأبراج الخلوية القريبة؛ وهذه المعلومات قادرة على تجميع أو تحديد موقع الهواتف المحمولة. فيلتقط مقدمي الخدمات الخارجيون هذه البيانات ويخزنونها لأغراض تجارية، مثل استكشاف الأخطاء وإصلاحها، وزيادة كفاءة الشبكة إلى الحد الأقصى، وتحديد ما إذا كان سيتم فرض رسوم تجوال العملاء على مكالمات معينة. ويمكن أن توفر البيانات أيضًا الحركات التاريخية لمواقع تواجد الهاتف محمول. وبالتالي فإن أي شخص لديه حق الوصول إلى هذه البيانات لديه القدرة على معرفة مكان وجود الهاتف وما الهواتف المحمولة الأخرى الموجودة في نفس المنطقة في وقت معين. على افتراض أن أصحاب الهواتف المحمولة يسافرون مع هواتفهم المحمولة ، يمكن لهذه البيانات أن توفر نظريًا كل مكان سافر إليه شخص تقريبًا وكل شخص قابله. راجع في ذلك:

- Oliver, Nancy K. "**Location, Balancing Crime Fighting Needs and Privacy Rights**." U. Balt. L. Rev. 42 (2012), P 485, 490-491.

الحصول على محتوياتها.[215] و كانت العديد من المحاكم في ذلك الحين مترددة في إصدار أوامر للكشف تسمح للحكومة بالحصول على البيانات التي تحتفظ بها أطراف ثالثة.

وحينما أصدر الكونغرس قانون الاتصالات المخزنة، حسم الأمر فيما يتعلق بخصوصية اتصالات الإنترنت المخزنة في الولايات المتحدة. حيث يحمي هذا القانون المعلومات الشخصية التي يخزنها بعض مقدمي الخدمات، مثل الاتصالات الإلكترونية ومقدمي خدمات الكمبيوتر عن بُعد. ويحظر عليهم الإفصاح عن قصد عن محتويات اتصالات العملاء الإلكترونية أو سجلات المشتركين، إلا أنه يتعين على مقدم الخدمة الكشف عن المعلومات إلى وكيل أو وكالة حكومية أمريكية إذا حصلوا على إذن أولاً. وينص القسم 2703 (18 USC § 2703) على القواعد التي يجب على الحكومة اتباعها من أجل إجبار مقدم خدمة كطرف ثالث على الكشف عن محتوى "العميل أو المشترك" والمعلومات غير المتعلقة بالمحتوى. وسمح القسم (د) من هذا القانون للقاضي بإصدار أمر من المحكمة بالإفصاح كلما أظهرت الحكومة الفيدرالية أن المعلومات المطلوبة كانت ذات صلة بالتحقيق الجنائي.

وفي قضيةCarpenter أوضحت المحكمة نوع التفويض القانوني المطلوب من قِبل كيان حكومي من أجل إجبار مزودي الخدمة اللاسلكية على تسليم السجلات التاريخية التي تحتوي على تحديد مواقع الهواتف المحمولة. حينما فرقت بين إذن التفتيش وأمر الكشف أو الإفصاح، حيث جادل محامو المدعى عليه بأن التفويض يجب أن يكون أمر تفتيش. وجادل محامو الولايات المتحدة بأن التفويض يجب أن يكون أمر محكمة للكشف. فمتطلبات الحصول على "أمر الكشف" أقل صرامة من متطلبات الحصول على أمر قضائي [216].

وبموجب التعديل الرابع لدستور الولايات المتحدة، يتمتع الأشخاص بالحماية من عمليات التفتيش غير المعقولة لـ "الأشخاص والمنازل والأوراق" ما لم تحصل الجهة الحكومية

---

[215] **Supreme Court of the United States**: Smith v. Maryland, 442 U.S. 735 (1979), https://www.supremecourt.gov/ . Retrieved April 2, 2019.

[216] Orin Kerr. "**Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case**". washingtonpost.com. The Washington Post. (June 5, 2017), Retrieved March 30 2019.

على أمر تفتيش. وللحصول على أمر تفتيش، لا بد من وجود سبب محتمل. فيوجد سبب محتمل للبحث عندما تتوافر الحقائق والظروف التي تشكل الأساس الذي يجعل الشخص المعقول يعتقد أن الجريمة قد ارتكبت والأشياء المطلوب البحث عنها ذات صلة بالجريمة.

وقد عارض عدد من القضاه الحكم الصادر في قضية Carpenter حيث ذكر القاضيKennedy "أن هذه القضية تنطوي على تكنولوجيا جديدة، لكن خروج المحكمة بشكل صارخ عن سوابق ومبادئ التعديل الرابع ذات الصلة لا لزوم له وغير صحيح ومخالف للدستور، فالقاعدة الجديدة– قاعدة استبعاد الأدلة المتحصل عليها بطريق غير مشروع– التي تضعها المحكمة تضع التحقيقات الجنائية اللازمة والمعقولة والمقبولة والمشروعة والمصرح بها من قبل الكونغرس في خطر شديد في القضايا الخطيرة، وغالبًا ما يسعى تطبيق القانون إلى منع تهديد جرائم العنف. بل وتفرض هذه القاعدة قيوداً لا مبرر لها على إجراءت سلطات مأمور الضبط القانونية والضرورية التي تمارسها ليس فقط من قبل الحكومة الاتحادية، ولكن أيضا من قبل سلطات الضبط القضائي في كل ولاية ومحلية في جميع أنحاء البلاد. فكان الالتزام بالسوابق الطويلة الأمد والإطار التحليلي لهذه المحكمة هو الطريقة الصحيحة والحكيمة لحل هذه القضية".[217]

ويضيف الفريق المعارض ومنه القاضي Alito والذي على الرغم من أنه يشارك المحكمة قلقها بشأن تأثير وسائل التكنولوجيا الحديثة على الخصوصية الشخصية، لكنه يخشى أن قرار اليوم سيضر أكثر بكثير من نفعه. واعتبر أن المنطق الذي اعتمدت عليه المحكمة يكسر دعامتين أساسيتين من التعديل الرابع للدستور، وهو بذلك يضمن عاصفة من الدعاوى القضائية بينما يهدد العديد من ممارسات التحقيق المشروعة والقيمة التي اعتمد عليها إنفاذ القانون بحق.[218]

أما القاضي Grouch فقد وقف موقفاً وسطاً فعلى الرغم من أنه وافق قرار الأغلبية لكنه لم يوافق على تعليل الأغلبية، فوافق غوروش على أن مأموري الضبط القضائي يجب أن يحصلوا على إذن للحصول على بيانات الهاتف الخلوي، ومع ذلك لم يوافق على أن التعديل الرابع يوفر الحق في التوقع المعقول للخصوصية. فسجلات مواقع الهواتف الخلوية هي ملك

[217] Timothy Ivory Carpenter v. United States of America .ibdi.

[218] Timothy Ivory Carpenter v. United States of America .ibdi.

لأصحابها، وبموجب التعديل الرابع لا يمكن لوكالات إنفاذ القانون أن تبحث عن ممتلكات الأشخاص دون الحصول على إذن قضائي. ويرى غوروش أن التعديل الرابع يمنح الحق في التمسك بضماناته عندم يتم تفتيش أو مصادرة أحد الأشياء المحمية الخاصة بالشخص بشكل غير معقول. بل ويطالب بضرورة إلغاء المحكمة مبدأ "التوقع المعقول للخصوصية" إضافة إلى إلغاء "فكرة الطرف الثالث" لأنها لا تتسق مع المعنى الأصلي للتعديل الرابع للدستور.[219]

ونحن نتفق مع ما انتهى إليه القاضي غوروش فمن الضروري إعادة النظر في الفرضية القائلة بأن الفرد ليس لديه أي توقع معقول للخصوصية في المعلومات التي يتم الكشف عنها طوعًا لأطراف ثالثة. هذا النهج غير مناسب للعصر الرقمي، فثمة حالات يكشف فيها الناس عن قدر كبير من المعلومات عن أنفسهم لأطراف ثالثة أثناء قيامهم بعمليات تخص حياتهم العادية واليومية.

3- إجبار المتهم على الإفصاح عن كلمة السر

تثير هذه المسألة إشكالية قانونية هامة تتعلق بحقوق لصيقة بالشخص في إجراء محاكمة عادلة وهي حقه في ألا يجرم نفسه، وحقه في التزام الصمت. وكانت اتفاقية بودابست قد أكدت على أن المعلومات الواجب تقديمها إلى مأموري الضبط القضائي يجب أن تكون معقولة، واعتبرت أن الإفصاح عن كلمة السر قد يكون معقولاً في بعض الأحيان، وقد يؤدي إلى تهديد غير معقول لخصوصية مستخدمين آخرين أو بيانات أخرى غير مرخص بالبحث فيها في أحيان أخرى.

وتباينت الآراء بشأن هذه المسألة، فثمة رأي يرفض إجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي، مستنداً إلى أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته؛ إذ من حقه التزام الصمت دون أن يُفسَّر ذلك الصمت ضد مصلحته. وفي المقابل اتجه رأي آخر إلى القول بأنه يجوز إجبار الشخص على الإدلاء بمعلومات ضد نفسه، متى كانت هذه المعلومات في حوزته قياساً على

---

[219] Article by: Vania Mia Chaker "**The U.S. Supreme Court's Most Recent Fourth Amendment Ruling**", UNIVERSITY OF FLORIDA JOURNAL OF TECHNOLOGY LAW AND POLICY, Vol. 23 (2018), Issue 1. Retrieved March 20 2019. Featured.http://www.journaloftechlaw.org.

إجبار الشخص على تسليم مفتاح الخزنه الذي بحوزته. إلا أن الرأي الأخير وجه إليه عدد من الانتقادات، من بينها عدم قبول قيام المعلومة التي تكون بحوزة المتهم على مفتاح الخزنة حيث أن المعلومة شئ معنوي بينما المفتاح شئ مادي محسوس قابل للتسليم، كما أن المتهم يستطيع التذرع بنسيان تلك البيانات أو تباينها في ذاكرته.[220]

ومع ذلك فإن المحكمة الأوروبية لحقوق الإنسان أكدت مراراً أن الحق في محاكمة عادلة من الحقوق الاساسية، فضلاً عن أنه يجب إجراء موازنة بين الحق في محاكمة عادلة والحاجة إلى منع الجرائم الخطيرة في المجتمع. وأكدت في قضية Stott v. Brown على أنه لا يمكن المساس بالعدالة في المحاكمة الجنائية. ومع ذلك فإن حقوق الشخص أثناء محاكمتة سواء صريحة أو ضمنية والتي جاءت بالمادة 6 من الاتفاقية الأوروبية لحقوق الإنسان ليست مطلقة، فالتقييد المحدود لهذه الحقوق يعد مقبولاً حيث تعترف المحكمة بضرورة الحاجة إلى إيجاد توازن عادل بين تحقيق المصلحة العامة للمجتمع والحقوق الشخصية للفرد حيث أن البحث عن التوازن متأصل في الاتفاقية بأكملها.[221]

وفي رأينا أن كلمة السر الخاصة بالبريد الإلكتروني أو بمواقع التواصل الاجتماعي لها وجود مستقل عن إرادة المتهم، بل ويجوز إجبار المتهم على الإفصاح عنها في الجرائم الماسة بسلامة المجتمع وأمنه، وإلا سوف يتم اللجوء إلى مقدمي الخدمة، حيث أنهم قادرون على تزويد جهات التحقيق بكلمات السر بل وبالمحتوى أيضاً.

---

[220] موسى مسعود ارحومة " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، سنة 2009م، ص 9.

[221] Stott v. Brown [5 Dec 2000] 1 AC 681, 704. https://www.alrc.gov.au. Retrieved April 6 2019.

الخاتمة

نخلص مما سبق عرضه إلى أن وسائل تقنية المعلومات والاتصالات الرقمية لم يعد ثمة مجال للاستغناء عن استخدامها في حياة الأفراد، سواء على المستوى الشخصي أو المستوى العملي، بل وعلى النطاق العالمي ككل. وهو ما جعل البيئة الرقمية مصدراً خصباً للأدلة التي يمكن استخدامها أمام المحكمة، ولعل التطورات المتزايدة في مجال تقنية المعلومات ألقى بظلاله على القواعد القانونية لاسيما قواعد الإثبات الجنائي، خاصة فيما تثيره تلك الأدلة من إشكاليات تلقي عبئاً على القضاء في ممارسة أقصى درجات الحذر عند تقدير الأدلة الرقمية وتقييم مدى إمكانية قبولها من استبعادها. وبعد تناولنا لذاتية ومدى مواءمة التدابير الإجرائية ومشروعيتها في البيئة التكنولوجية، والتحديات التى تواجهها تلك الإجراءات للحفاظ على الدليل الرقمي كدليل إثبات في الجرائم الجنائية، خلص البحث إلى عدد من النتائج والتوصيات على النحو التالي:

أولاً: النتائج

1- تتعدد وتتنوع الأدلة الرقمية، والتي تكون مخزنة عادة في الأجهزة الرقمية المختلفة أو منقولة عبر شبكات الاتصال، وتشكل ثروة للعدالة الجنائية ومجالاً خصباً في المحاكمات متى أحسن استخلاصها والحفاظ عليها وفق أساليب فنية وإجراءات قانونية سليمة.
2- الأدلة الجنائية الرقمية لا تستخدم في اكتشاف وإثبات جرائم تقنية المعلومات فحسب، بل تمتد لتكشف آثار الجرائم التقليدية التي تلعب التقنية دوراً بارزاً فيها. وعلى النقيض فجرائم تقنية المعلومات أيضاً لا تعتمد في إثباتها على الأدلة الرقمية فقط بل من الممكن إثباتها بأدلة الإثبات التقليدية كالشهادة أو الإعتراف.
3- لوحظ أن الأدلة الجنائية سابقاً كانت تقتصر على أدلة مادية ملموسة أو مرئية أو مسموعة للرجل العادي أن يتعامل معها، إلا أنه مع ظهور جرائم التقنية أدى إلى وجود طبيعة معلوماتية غير ملموسة ومسرح افتراضي غير مرئي، ولا يستطيع التعامل معها إلا ذوي الخبرة الفنية في استخدام التقنيات المعلوماتية.
4- للأدلة الجنائية الرقمية حجية في الإثبات، ولعل إمكانية إثبات مصداقيتها بناء على أسس علمية ثابتة، جعلها تنال الثقة في الاستناد إليها كدليل علمي، وتؤهلها لتكون إضافة جديدة لتقنيات الأدلة الجنائية. بل إن قيامها على نظريات حسابية مؤكدة، جعل منها

وسيلة يقينية لا يتطرق إليها الشك. وعن طريق نفس الأسس العلمية يمكن تأكيد ما إذا كانت تلك الأدلة قد تعرضت لتعديل أو تحريف ومن ثم إمكانية استبعادها.

5- لم تحدد غالبية التشريعات طرق معينة ينتهجها مأمور الضبط في إجراء تحرياته، بل له أن يتخذ من الوسائل والإجراءات ما يمكنه من مباشرة اختصاصه شريطة ألا تخالف تلك الإجراءات مبدأ المشروعية.

6- الأصل عدم جواز اعتراض الرسائل والمحادثات احتراماً للحق في خصوصية الاتصالات، ومع ذلك أجازت أغلب التشريعات ومن بينها القانون المصري استثناء مراقبة واعتراض المحادثات والرسائل لضبط ما يفيد في كشف الحقيقة، وهو ما يعد في نظرنا قيداً على حرية الأشخاص لاسيما الأشخاص الذين هم على صلة بالجاني وليس لهم علاقة بالجريمة.

7- يوفر أمر تقديم البيانات من قبل مقدمي الخدمات تدبيراً مرناً، يُمكن مأموري الضبط القضائي من الحصول على البيانات الرقمية، حيث يلتزم مقدم الخدمات السلكية واللاسلكية أو خدمة الحوسبة عن بعد، باتخاذ جميع الإجراءات الواجبة عليه في حفظ السجلات والأدلة الموجودة في حوزته وتقديمها إلى العدالة متى وجدت اعتبارات ملحة من المصلحة العامة تفوق الحق في الخصوصية.

8- الحق في الخصوصية المعلوماتية من الحقوق اللصيقة بالشخص، وتعد من المفاهيم النسبية باختلاف المجتمعات. ومع ذلك لم يصدر المشرع المصري تقنيناً خاصاً بحماية الحق في الخصوصية المعلوماتية على عكس العديد من التشريعات المقارنة كالتشريع الفرنسي والأمريكي والبريطاني وغيره.

9- البحث والتنقيب عن الأدلة في البيئة الرقمية ينطبق عليه نفس شروط وخصائص البحث التقليدية، إلا أنه يتم اتخاذ إجراءات جنائية تتميز بطابع خاص من شأنها تطبيق قواعد فنية من شأنها الحصول على البيانات الرقمية بنفس الدرجة من الفاعلية؛ وذلك بسبب الطبيعة غير الملموسة للبيانات الرقمية. بل ولا تختلف درجة الاعتقاد المطلوبة للحصول على إذن قانوني لإجراءات البحث سواء تعلق الأمر ببيانات في شكل ملموس أو في شكل إلكتروني.

10- أثار التفسير الموسع لمدلول الأشياء محل التفتيش – في ظل غياب نصوص خاصة تحكم هذه المسألة – العديد من الإشكاليات، كان من أهمها أن جرائم الكمبيوتر تعتمد

على نظام معلومات واحد أو قد تتجاوزه إلى أنظمة أخرى غير النظام المشتبه به، وهو ما يستلزم امتداد التفتيش إلى أنظمة أخرى غير النظام محل التفتيش، الأمر الذي قد يؤدي إلى الاعتداء على الحريات الشخصية وسرية الاتصالات التي يمتد إليها التفتيش. ومع ذلك حسمت الاتفاقيات الدولية المعنية بمجال تقنية المعلومات وأغلب التشريعات المقارنة هذه المسألة، بجواز امتداد التفتيش إذا كان هناك أساس يدعو إلى الاعتقاد بأن المعلومات المخزنة بهذا النظام تفيد التحقيقات في كشف الحقيقة. مع ملاحظة أنه لا شئ يحول دون توافر حالة التلبس أثناء تفتيش قانوني صحيح.

11- يواجه تفتيش النظام المعلوماتي العديد من الصعوبات التي تتعلق بتشفير الملفات أو الاتصال بالجهاز الرقمي عن طريق الشبكة أو حذف جميع الملفات والبيانات بضغطة زر واحدة، وهو ما يتطلب معرفة تقنية وكاملة عن كيفية البحث والنفاذ إلى النظام المعلوماتي.

12- يحمي الدستور الأمريكي الأفراد من التفتيش غير المعقول، ويعد التفتيش غير معقول إذا توافر توقع لحرمة الحياة الخاصة، ويتوافر هذا التوقع إذا توقع الشخص حرمة لحياته الخاصة بأن كان يحرص على عدم اطلاع الغير على ما يخصه، أو إذا اعتبر المجتمع أن التفتيش يمس حرمة الحياة الخاصة وبالتالي فإنه يصبح غير معقول.

13- يجوز إجراء التفتيش دون الحصول على إذن قضائي متى وجدت أسباب تشير إلى تعرض الدليل لخطر وشيك كالحرق أو التدمير أو وجود تهديد يضع الشرطة أو الجمهور في خطر، وكذلك مراعاة العوامل الأخرى التي ترتبط بالرطوبة أو درجة الحرارة أو المجالات المغناطيسية المحيطة بالدليل.

14- يتم ضبط البيانات والأدلة المتحصل عليها نتيجة عملية البحث والنفاذ، حيث تتمثل وظيفة الضبط في المساعدة في جمع الأدلة واستنساخ البيانات الأصلية والمحافظة على سلامتها من التلاعب أو التخريب.

15- تعتمد القيمة الثبوتية للدليل أمام المحكمة في المقام الأول على أصالة الدليل وصلاحيته، ويكون كذلك إذا كان يمتلك الصلاحية العلمية المطلوبة وذات صلة بالفعل المجرم. وللقاضي الحرية الكاملة في تكوين عقيدته واقتناعه الشخصي بالدليل المقدم إليه معتمداً في ذلك على طرق المنطق والعقل، والذي يراعى فيه خصوصية الأدلة الرقمية باعتبارها من المسائل العلمية الدقيقة وارتباطها بوسائل فنية ورقمية حديثة.

16- يجب مناقشة جميع المخرجات الرقمية أمام الخصوم. والأصل ألا تلجأ المحكمة إلى إلزام الغير بتقديم معلومات تفيد في كشف الحقيقة في دعوى منظورة أمامها سواء مدنية أو جنائية، إلا أنه مع انتشار جرائم تقنية المعلومات وصعوبة التوصل إلى مرتكبيها، بدأت المحاكم من الإكثار من هذه الرخصة، كتعاون مقدمي الخدمات وأصحاب مواقع جوجل أو هوت ميل أو فيس بوك.

17- تطبق قاعدة استبعاد الأدلة المتحصل عليها بطرق غير مشروعة في حال انتهاك القانون أو عدم مشروعية الإجراءات التي تم على إثرها الحصول على الدليل، حيث أن المشروعية تتبع من أمرين، صحة إجراءات الحصول على الدليل كونه تم وفق إجراءات قانونية مشروعة، أما الثاني فيتعلق بمشروعية طرق الحصول عليه.

18- عدم وضوح الرؤى في تعداد الأسباب التي تؤدي إلى تطبيق قاعدة استبعاد الأدلة غير المشروعة، فضلاً عن تباين دور القضاء في تطبيق تلك القاعدة ومازالت تستخدم في نطاق ضيق، على الرغم من أنها أمر ضروري لا غنى عنه لضمان سلامة إجراءات المحاكمة. مع ضرورة ملاحظة أن قاعدة الاستبعاد لا تحول- في جميع الأحوال- من استخدام الدليل غير المشروع في المحاكمة.

19- في جميع الأحوال لا يقبل القاضي دليلاً متحصلاً من إجراء غير مشروع، ليس فقط لأنه يتعارض مع قيم العدالة، بل كونه أيضاً يمس بحق المتهم في الدفاع.

ثانياً: التوصيات

إدراكاً لأهمية دور الجهات المعنية وتطوير وسائل تقنيات الأدلة الجنائية من أجل ترسيخ مبادئ العدالة الجنائية، والتعامل الفعّال مع الجريمة ولاسيما جرائم تقنيه المعلومات. لما تمثله تلك الجرائم من خطورة على المجتمع وزعزعة الأمن والاستقرار. وحرصاً على تعزيز دور تلك الجهات في مجال مكافحة الجريمة والوقاية منها، نوصي بما يلي:

1- يتطلب التعامل مع الأدلة الجنائية الرقمية معرفة تامة بأصولها العلمية ونظرياتها الحسابية، وهو ما يلقي على عاتق الجهات المعنية – وبصفة خاصة الجهاز القومي لتنظيم الاتصالات- مسئولية التوعية بثقافة الأدلة الرقمية بين مختلف فئات المجتمع ومؤسساته، لاسيما رجال القانون من محققين وفنيين لرفع مستواهم المعرفي والتقني

وتوفير الإمكانات المادية اللازمة من معامل ومختبرات. وهذا لن يتأتى إلا بدعم وتعاون كافة الجهات المعنية وأجهزة الدولة.

2- الحاجة إلى وجود قواعد قانونية وتشريعات إجرائية خاصه تتناسب والصبغة الخاصة للأدلة الرقمية، بحيث تنظم إجراءات جمع وتأمين الأدلة الرقمية بالقدر الذي يتوافر معه الحفاظ على مشروعيتها ومشروعية طرق الحصول عليها، وبما يخلق نوع من التوازن بين مصالح تطبيق وتنفيذ القانون من جهة واحترام الحقوق الدستورية من جهة أخرى.

3- ضرورة مواكبة التشريعات للتطورات المتسارعة في مجال تقنية المعلومات والبرامج، للحد من انتشار جرائم تقنية المعلومات، ومتابعة كل ما هو جديد ومستحدث في هذا المجال، إضافة إلى وضع تدابير وقائية جادة وخطط للمكافحة، مع ضرورة إيلاء الاهتمام لسد ثغرات التشريعات القائمة، مع تعزيز اتساق تلك التشريعات وتوافقها لتحقيق الغايات المرجوة منها.

4- من الضروري أن يحدد القانون المصري سلطات مأموري الضبط القضائي عند مراقبة شبكة الإنترنت في إطار سلطته في جمع الاستدلالات والتي لا يحتاج للقيام بها إذناً من سلطة التحقيق.

5- ضرورة تحقيق التعاون المشترك بين الأجهزة الأمنية وشركات تقنية المعلومات، في إطار قانوني، ودون التعدي على حقوق الأفراد. وهو ما يتطلب تضافر جهود فريق مكون من رجال الشرطة والعلوم الجنائية وسلطات التحقيق، ومتخصصوا البرمجة ونظم المعلومات، فليس بمقدور جهة واحدة منهم أن تكون ملمة بجميع المهارات اللازمة لكشف خبايا تلك الجرائم والحصول على الأدلة المرتبطة بها.

6- العمل على إرساء قواعد التعاون الإقليمي والدولي في مجال التكنولوجيا، والجرائم التي تنتج عن استخداماتها، والسعي نحو إيجاد إطار قانوني للتعاون بين الجهات المختصة، لاسيما في تبادل المعلومات.

7- نوصي عند الحصول على أدلة رقمية، توثيق جميع إجراءات ضبط تلك الأدلة، وتأمينها وحفظها، وعند الحاجة للاطلاع عليها، يجب أن يكون الشخص المطلع مؤهلاً وذو خبرة في ذلك.

8- عقد دورات وورش عمل لتدريب القضاه علي فهم القواعد الفنية للأدلة الرقمية، حتي يستطيع القاضي مناقشه الأدلة المطروحه أمامه، وتقدير مدى ملاءمتها في بناء قناعته وتأسيس حكمه.

9- نشر برامج التوعية في المجتمعات حول مخاطر جرائم التقنية، وتعريفهم بكيفية الحفاظ على معلوماتهم الخاصة، وعدم الإفصاح عنها كحساباتهم البنكية وكلمات السر الخاصة بالأجهزة الرقمية أو البريد الإلكتروني.

10- نوصي المشرع المصري بتحديد نصوص خاصة بالدليل الرقمي يتحدد فيها ما يعد إجراء صحيحاً وما يعد إجراء باطلاً.

قائمة المراجع

أولاً: المراجع العربية

(1)معاجم اللغة

- ابن منظور، أبو الفضل جمال الدين محمد بن مكرم "لسان العرب". بيروت. دار إحياء التراث العربي. 1983م.

(2)كتب الفقه

- ابن قيم الجوزية، محمد بن أبي بكر بن أيوب بن سعد شمس الدين"إعلام الموقعين عن رب العالمين"، الطبعة الأولى، تحقيق محمد عبدالسلام إبراهيم، بيروت، دار الكتب العلمية. الجزء الأول، سنة 1411هـ- 1991م.

(3)الكتب القانونية

(أ) الكتب العامة

- أشرف توفيق شمس الدين "شرح قانون الإجراءات الجنائية- الجزء الأول- مرحلة ما قبل المحاكمة)" طبعة خاصة بالتعليم المفتوح . جامعه بنها، مصر، سنة 2012م.
- إيهاب عبدالمطلب "موسوعة المخدرات معلقاً عليها بآراء الفقه والقضاء وأحكام محكمة النقض منذ تاريخ إنشائها حتى عام 2014" المجلد الرابع "الإثبات في جرائم المخدرات" الطبعة التاسعة، المركز القومي للإصدارات القانونية، القاهرة، سنة 2016م.

- عبدالرءوف مهدي "شرح القواعد العامة للإجراءات الجنائية" دار النهضة العربية، مصر، 2007م.
- محمد زكي أبو عامر " الإثبات في المواد الجزائية" دار الجامعة الجديد، مصر، سنة 2011م.

(ب) الكتب المتخصصة

- أحمد عوض بلال "قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة" الطبعة الثالثه، دار النهضة العربية، القاهرة، سنة 2013م.
- أزهري عبدالرحمن، نسرين بشير عثمان "جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق أكثر فاعلية". المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC . جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات. الرياض، المملكة العربية السعودية، سنة 2015م.
- إبراهيم داود "الحماية القانونية للبيانات الشخصية من منظور الحق في الخصوصية:دراسة تحليلية مقارنة" مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الأسكندرية،المجلد الثاني، العدد الأول، سنة 2017م.
- الناجم كوبان "سلطة القاضي الجنائي في تقدير الأدلة الرقمية الناتجة عن الجرائم المعلوماتية في إطار نظرية الإثبات الجنائي"،مجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، العدد 4، سنة 2017م.
- أمير فرج يوسف "الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، دراسة مقارنة للتشريعات العربية والأجنبية" مكتبة الوفاء القانونية، مصر، سنة 2016م.
- جاسم خربيط خلف "التفتيش في الجرائم المعلوماتية" مجلة الخليج العربي، مركز دراسات الخليج العربي، جامعة البصرة، المجلد 41 العدد 3،4، سنة 2013م.
- خالد مصطفى الجسمي "الإثبات الجنائي بالأدلة الرقمية" دار السلام للطباعة والنشر، مجلة القانون المغربي، العدد 34، سنة 2017م.
- دليل ورشة عمل "الدليل الرقمي وحجيته في الإثبات الجنائي" جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، الرياض، في الفترة من 9-10 أكتوبر 2018م.

- عبدالحليم ابن بادرة "إجراءات البحث والتحري عن الجريمة المعلوماتية: الخصوصية والإشكالات" مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر ،العدد 23، سنة 2015م.
- علي محمود علي حمودة "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي" المؤتمر العلمي الأول "الجوانب القانونية والأمنية للعمليات الإلكترونية" أكاديمية شرطة دبي، في الفترة من 26-28 إبريل 2003م.
- عمر محمد يونس "الجرائم الناشئة عن استخدام الإنترنت" القاهرة، دار النهضة العربية، 2004م.
- سامي حمدان الرواشدة " الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأمريكي" المجلة الدولية للقانون، دار جامعة حمد بن خليفة للنشر، قطر، سنة 2017م.
- شريف يوسف حلمي خاطر "حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الإطلاع على البيانات الشخصية في فرنسا" مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد إبريل 57 لسنة 2015م.
- شيماء عبدالغني عطاالله "الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظامين اللاتيني والأنجلو أمريكي"، دار النهضة العربية، مصر، 2005م.
- فهد دخين العدواني "مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي، دراسة مقارنة" مركز تطوير التعليم الجامعي، جامعة عين شمس، مجلة دراسات في التعليم الجامعي، العدد 36، لسنة 2017م.
- فيصل حاكم الشمري "مستجدات التعليم الإلكتروني – تطبيقات الهواتف الذكية ومتاجر الويب) ورشة عمل- جامعة المجمعة، المركز الوطني للتعليم الإلكتروني والتعليم عن بعد، المملكة العربية السعودية، بدون تاريخ.
- طاهر الشيخ، "نظم تشغيل المعلومات" معهد إدارة الحاسب، مصر، سنة 1991م.
- لعوارم وهيبة "مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي" مجلة الفقه والقانون، العدد 20، الناشر صلاح الدين دكداك، المغرب، سنة 2014م.

- محمد الأمين البشري "الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات" المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض،المجلد 17، العدد 33، سنة 2002م.

:"التحقيق في الجرائم المستحدثة" جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2004م.

:"تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت" كلية التدريب، قسم البرامج التدريبية، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2008م.

- محمد حسن السراء "الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية" مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد الحادي والعشرون، إبريل العدد 81، سنة 2012م.
- محمد فالح حسن "مشروعية الوسائل العلمية في الإثبات الجنائي" الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 1987م.
- مشاري خليفة العيفان "قاعدة استبعاد الدليل المتحصل من القبض والتفتيش غير المشروعين في القانون الأمريكي" مجلة الحقوق، جامعة الكويت، مجلس النشر العلمي، المجلد 35 ، العدد الرابع، ديسمبر سنة 2011م.
- ممدوح عبدالحميد :"استخدام أدوات التحليل التناظري الرقمي في بحث وتحقيق جرائم الحاسب الآلي"مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد 11، العدد 4، سنة 2003م.

:"أدلة الصور الرقمية في الجرائم عبر الكمبيوتر" مركز شرطة دبي، سنة 2005م.

:"البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت" دار الكتب القانونية، مصر ،سنة 2006م.

- مصطفى إبراهيم العربي "دور الدليل الرقمي في الإثبات الجنائي" مجلة البحوث القانونية، كلية القانون– جامعة مصراته، العدد الأول، سنة 2016م.

- مصطفى محمد موسى "قواعد وإجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية والتخطيط لها" بحث مقدم ضمن الدورة التدريبية "إجراءات التحري والمراقبة والبحث الجنائي"، الرياض. خلال الفترة من 25-5 /6-6-2012م.
- موسى مسعود ارحومة " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، سنة 2009م.
- نزار أولاد مومن "الإثبات في الميدان الجنائي من خلال الدليل المعلوماتي" مجلة الفقه والقانون، الناشر صلاح الدين دكداك، المغرب، العدد 71، سنة 2018م.

(4)الرسائل الجامعية

- أحمد سعد محمد الحسيني "الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية" رسالة دكتوراه، كلية الحقوق، جامعه عين شمس، سنة 2012م.

(5)التقارير والاتفاقيات الدولية والإصدرات

- اتفاقية الجريمة الإلكترونية (بودابست) تم اعتمادها من لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/ تشرين الثاني 2001م) وفتح باب التوقيع في بودابست في (23 نوفمبر/ تشرين الثاني 2001م.
- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية " البند 8 من جدول الأعمال (التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية) سلفادور، البرازيل 12-19 إبريل 2010م.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 2010/12/21م – حررت في القاهرة، مصر. جامعة الدول العربية، الأمانة العامة لجامعة الدول العربية (الأمانة العامة لمجلس وزراء الداخلية العرب.
- التقرير التفسيري لاتفاقية الجريمة الإلكترونية (بودابست 2001م) س.لسلة المعاهدات الأوروبية رقم 185، الصادرة عن مجلس أوروبا.
- إصدرات مركز هردو لدعم التعبير الرقمي "التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات" القاهرة، 2018م.

(6)أحكام النقض المصرية:

- نقض 25 يناير 1965، مجموعة أحكام النقض المصرية، رقم21،س 16.
- نقض 15 أبريل سنة 1968 مجموعة أحكام النقض س 19 رقم 1؛ نقض 25 أكتوبر سنة 1976 س 27 رقم 1.
- نقض 13 يونيه سنة 1977، مجموعة أحكام النقض س 28 رقم 161 طعن رقم 245 لسنة 47 ق.
- نقض 9 أكتوبر 1985 مجموعة المكتب الفني س 36.
- نقض 8 يناير 1987، الطعن رقم 5963، لسنة 56 ق.
- نقض 19 مايو سنة 1998، الطعن رقم 1110 لسنة 68 ق.
- نقض 20 مارس لسنة 2000، الطعن رقم 17759 لسنة 64 ق.

(7)المواقع الإلكترونية:

- جميل حسين طويلة "التحليل الجنائي الرقمي" دليل عملي لطرق التحليل الجنائي الرقمي في الجرائم المعلوماتية"، كتاب منشور عبر موقع. https://arabcyberwarrior

- سامر الغدا "مفهوم قواعد البيانات"، دراسة منشورة عبر موقع http://qu.edu.iq

- https://www.supremecourt.gov

https://www.law.cornell.edu

https://www.leagle.com

https://www.alrc.gov.au

www.hrccourtreporters.com

https://publications.parliament.uk

https://www.arableagueonline.org

http://qu.edu.iq

ثانياً: المراجع الأجنبية

***Books and Articles:**

- Berkley D. Sells; Ian Collins, Strategies to Obtain Electronic Evidence, 36 ADVOC Q. 295 (2010).

- Alex Cameron, “Fundamentals of Electronic Evidence and Discovery” LexisNexis Canda, April 2010

- Eoghan Casey, “Digital Evidence and Computer Crime”, 3rd Edition, London, Academic Press, 2011,

- Vania Mia Chaker, Article: "The U.S. Supreme Court's Most Recent Fourth Amendment Ruling", UNIVERSITY OF FLORIDA JOURNAL OF TECHNOLOGY LAW AND POLICY, Vol. 23 (2018). http://www.journaloftechlaw.org.

- Brian Farkas, Article: “How the Wiretap Act Protects Personal Privacy?” https://www.lawyers.com.

- Caroline Fehr; Christine LiCalzi; Thomas Oates, Computer Crimes, 53 Am. Crim. L. Rev. 977 (2016).

- Alexander Galicki; Drew Havens; Alden Pelker: “Computer Crimes, 51 Am. Crim”. L. Rev. 875 (2014).

- Orin Kerr. "Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case". washingtonpost.com. The Washington Post. (June 5, 2017).

- Stephen Manson, “Expert in Cyber Security”. PDF, .http://www.stephenmason.eu/articles/electronicevidence.html

- Oliver, Nancy K. "Location, Balancing Crime Fighting Needs and Privacy Rights." U. Balt. L. Rev. 42 (2012).

- Catherine Pelker; Anthony J. Palmer; Brittany Raia; Jamin Agosti, "Computer Crimes", 52 Am. Crim. L. Rev. 793 (2015).

- Pew Research Center Internet and Technology. Pew Research Center, February 5, 2018, "Mobile Fact Sheet": https://www.pewinternet.org/fact-sheet/mobile/

- Paul F. Rothstein, "Evidence in a nutshell"- Evidence (Law) United States. St. Paul, MN: West, Thompson Reuters., (2012).

- Steptoe & Johnson LLP. E-Commerce Law Week, Issue 205, ©Copyright 2002, https://www.steptoe.com.

- Alin Teodorus Dragan, Particularities regarding Computer Search and Field Research for Online Crimes, 2013 AGORA Int'l J. Jurid. Sci. 85 (2013).

***Decisions of Courts:**

- Fremont Weeks v. United State 232 U.S. 383 (1914).

- United States v. Miller, 307 U.S. 174 (Decided May 15, 1939).

- Katz v. United States, 389 U.S. 347, 360 (1967).

- Watts v. United States, 394 U.S. 705, 707-08 (1969).

- See Chimel v. California, 395 U.S. 752, 762-63 (1969).

- Cupp v. Murphy, 412 U.S. 291 (1973).

- United States v. Robinson, 414 U.S. 218, 235 (1973).

- United States v. Edwards, 415 U.S. 800, 808-09 (1974).

- United States v. Miller, 425 U.S. 435, 443 (1976).

- United States v. Chadwick, 433 U.S. 1, 15 (1977).

- Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

- Smith v. Maryland, 442 U. S. 735 (Decided June 20, 1979).

- United States v. Leon, 468 U.S. 897 (1984).

- O'Connor v. Ortega, 480 U.S. 709, 719-20 (1987).

- Horton v. California, 496 U.S. 128 (1990).

- United States v. Sissler, No.1:90-CR-12, 1991 WL 239000, at 4 (W.D. Mich. Aug. 30, 1991).

- United States v. David, 756 F. Supp. 1385 (D. Nev. 1991).

- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)

- United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993).

- United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995).

- McIntyre v. Ohio, 514 U.S. 334, 342 (1995).

- State Wide Photocopy v. Tokai Fin. Serves. Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995).

- United States v. Baker, 890 F. Supp. 1375, 1390 (E.D. Mich. 1995).

- Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996).

- United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997).

- United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997).

- United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998).

- United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

- United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

- Saint John (City) Employee Pension Plan v. Ferguson, NBQB 121 S/C/53/07 (2009).

- United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

- Stott v. Brown,1 AC 681, 704 (5 Dec 2000).

- United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000).

- Illinois v. McArthur, 531 U.S. 326 (2001).

- United States v. Morales, 272 F.3d 284, 288 (5th Cir. 2001).

- Guest v. Leis, 255 E3d 325, 333 (6th Cir. 2001).

- United States v. Scarfo, 180 F. Supp. 2d 572, 581 (D.N.J. 2001)

- United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).

- Compare Planned Parenthood of Columbia/Willamette, Inc. v. Am. Coal of Life Activists, 290 E3d 1058, 1085-86 (9th Cir. 2002).

- Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 78 (9th Cir. 2002).

- United States v. Angeyine, 281 F.3d 1130, 1134-35 (10th Cir. 2002).

- United States v. Clough, 246 F Supp. 2d 84 (2003).

-United States v. Steiger, 318 E3d 1039, 1048-49 (11th Cir. 2003).

- Fraser v. Nationwide Mut, Inc., 352 F.3d 107, 113 14 (3d Cir. 2004).

- United States v. Councilman, 418 E3d 67 (1st Cir. 2005).

- iTrade Finance Inc. v. Webworx Inc, O.J. No. 3492 (QL), 255 D.L.R.(2005)

- United States v. Long, 64 M.J. 57 (C.A.A.F. 2006).

- Georgia v. Randolph, 547 U.S. 103 (2006).

- Brigham City v. Stuart, 547 U.S. 398, 403-06 (2006).

- United States v. Hill, 459 F.3d 966, 974 (9th Cir. 2006).

- Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 553 (D.Md.2007).

- United States v. Buckner, 473 E3d 551, 554 n.2 (4th Cir. 2007).

- United States v. Burt, 495 F.3d 733, 738 39 (7th Cir. 2007).

- United States v. Heckenkamp, 482 F3d 1142, 1146 (9th Cir. 2007).

- United States v. Lasalle, 2007 WL 1390820, at 7 (D. Haw. May 9, 2007).

- United States v. Park, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007).

- United States v. Trowbridge, 2007 WL 4226385, at 4-5 (N.D.Tex. Nov. 29, 2007).

- eBay Canada Limited v. The Minister of national Revenue 378 N.R. 233 FCA (April 17, 2008).

- Jaynes v. Commonwealth, 666 S.E.2d 303, 313 (2008).

- United States v. Gonzales-Perales, 313 F. App'x 677, 681 (5th Cir. 2008).

- United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

- United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008).

- United States v. Wall, 2008 WL 5381412, at 3-4 (S.D. Fla. Dec. 22, 2008).

- United States v. Burgess, 576 F.3d 1078, 1096 (10th Cir. 2009).

- United States v. Hardy, 640 F. Supp. 2d 75, 80-81 (D. Me. 2009).

- United States v. Wurie, 2009 WL 1176946, at 5 (D. Mass. 2009).

- United States v. Williams, 592 F.3d 511, 521-24 (4th Cir. 2010).

- United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010).

- United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010).

- State of Connecticut v. Robert Eleck, 23 A.3d 818 (2011).

- United States v. Stabile, 633 F.3d 219, 240-42 (3d Cir. 2011).

- United States v. Richards, 659 F.3d 527 (6th Cir. 2011).

- Crowther v. State, 249 P.3d 1214, 1222 (Kan. Ct. App. 2011).

- United States v. Jones, 132 S. Ct. 945, 950 n.3 (2012).

- United States v. Stirling, Case No 11-20792-CR-ALTONAGA, United States District Court, S.D. Florida, Miami Division, April 10, (2012).

- Klayman v. Obama, 957 E Supp.2d 1, 35 (D.D.C. 2013).

- Riley v. California, 573 U.S. (2014).

- United States v. Quartavious Davis (No. 12-12928. D.C. Docket No. 1:10-cr-20896-JAL-2), (Decided May 5, 2015).

- United States v. Shah, No. 5:13 CV 328 FL, 2015 WL 3605077 (E.D.N.C. June 5, 2015).

- Utah v. Strieff, 579 U.S., 136 S. Ct. 2056 (2016).

- Collins v. Commonwealth, No. 16-1027, 584 U.S(January 9,2018).

- Timothy Ivory Carpenter v. United States of America, No. 16-402, 585 U.S. (2018).