الدليل الرقمي في المادة الجنائية

Digital evidence in criminal matters

Tahour Abdelkrim طاهور عبد الكريم

دكتور في القانون الخاص

أستاذ زائر بجامعة مُحَمَّد الخامس

الملخص :

مما لا شك فيه أن التحول الذي شهدته بنية الجريمة، وما صاحب ذلك من صعوبات في مواكبة إجراءات التحقيق الكلاسيكية لهذا التحول، فرض على المشرع التفكير في اليات جديدة متطورة كفيلة باحتواء هذا التحول بضبط الجريمة سواء في بعدها المادي واللامادي، وبالعطاء التحقيق الجنائي مصداقية وشفافية. تبعا لذلك بدأ التفكير في الدليل الرقمي وعلاقته بالمادة الجنائية، باعتباره عنصرا حاسما ليس فقط في الجرائم الالكترونية، ولكن كل أشكال الانحراف التي تنبني على الأدوات الرقمية. فالدليل الرقمي هو عبارة عن مجموعة من الحقائق المادية وغير المادية مرتبطة ببيانات غير ملموسة والتي تتوافق مع إجراءات البحث الجنائية.

يرتبط الدليل الرقمي بجانبين، إما بجانب الجاني مثل التحقيق تحث اسم مستعار، او تحديد موقع الجاني، او بجانب مسرح الجريمة مثل: بيانات الكمبيوتر أو برامج التجسس الى غير ذلك من الإجراءات. وعموما سواء ارتبط الدليل الرقمي بهذا الجانب او بذاك، فإنه لازال يطرح نقاشا في الساحة القانونية حول إجراءات الوصول إلى الدليل الرقمي، وبين حماية حقوق وحريات الأفراد خاصة في ظل غياب إطار قانوني مؤطر لكفية الحصول على الدليل الرقمي.

الكلمات المفاتيح :الدليل الرقمي، البيانات اللامادية، إجراءات التحقيق الجنائي.

Synopsis:

Undoubtedly, the transformation witnessed in the structure of crime, and the accompanying difficulties in keeping pace with traditional investigative procedures, have forced legislators to consider new, advanced mechanisms capable of containing this transformation by controlling crime, both in its tangible and intangible dimensions, and by providing credibility and transparency to criminal investigations. Consequently, consideration has begun to be given to digital

evidence and its relationship to criminal material, as it is a crucial element not only in cybercrimes, but also in all forms of deviation based on digital tools. Digital evidence is a collection of tangible and intangible facts linked to intangible data that are compatible with criminal investigation procedures. Digital evidence is linked to two aspects: either the perpetrator, such as investigation under a pseudonym or identifying the perpetrator's location, or the crime scene, such as computer data, spyware, and other procedures. In general, whether digital evidence is linked to one aspect or another, it continues to generate debate in the legal arena regarding the procedures for accessing digital evidence and the protection of individual rights and freedoms, especially in the absence of a legal framework governing the process of obtaining digital evidence.

Key words: Digital evidence, intangible data, criminal investigation procedures.

مقدمة:

أصبحت الأدلة الرقمية نتيجة للانفجار الهائل في التكنولوجيات الرقمية، ذات أهمية حاسمة في معظم التحقيقات الجنائية، فغالبا ما تكون البيانات الوصفية وسجلات الإرسال ومحتوى البريد الإلكتروني ضرورية لجمع أدلة متسقة حول المشتبه به. كما هو معلوم أصبحت الوثائق الرقمية ضرورية سواء في الحياة الشخصية أو المهنية: تبادل رسائل البريد الإلكتروني، وتتبع تصفح الإنترنت، وبرامج المحاسبة، والمذكرات الإلكترونية، والهاتف المحمول، وتحديد المواقع الجغرافية عبر الأقمار الصناعية. وبالتالي أضحت هاته الأدلة الرقمية المتنوعة في صميم التحقيقات الجنائية، خاصة تلك التي تتطلب في كثير من الأحيان البحث ليس فقط داخل البلاد ولكن أيضا خارجه، وهو ما تطلب خلق قنوات لتعاون بين السلطات الحكومية ومقدمي خدمات الانترنيت والحوسبة من أجل الوصول إلى الأدلة الجنائية الرقمية. مع ضرورة التوفيق بين حماية الحريات الأساسية مثل احترام الخصوصية ومتطلبات الأمن والنظام العام.

ونتوخى من خلال هذه المقاله البحث في الإطار القانوني للدليل الرقمي في البحث الجنائي.

تبعا لذلك يجدر بنا أولا تحديد المقصود بالدليل الرقمي وبيان خصائصه المميزة له عن الدليل العادي (المحور الأول) على أن نستعرض لسبل استنباط الدليل الرقمي في (المحور الثاني).

المحور الأول: ماهية الدليل العملي في المادة الجنائية

يعرف الدليل حسب دومات[1] بأنه "ما يقنع العقل بالحقيقة.»] ... [وعلى مستوى القضائي نطلق على الأدلة اسم الأساليب التي ينظمها القانون لاكتشاف وإثبات حقيقة واقعة متنازع عليها. وإذا كان هذا التعريف لا يزال صالحا، فإن الدليل والرقمي يبدوان مسبقا كمفهومين متباعدين إلى حد ما، حيث يبدو الرقمي عابرا وقابلا للتعديل بسهولة وبالتالي بعيدا عن أي يقين.

إن إثبات الجرائم في بيئة رقمية يفرض إلى حد كبير تحديات جديدة على كل من الأجهزة التحقيقية والنظام القضائي. هكذا يصبح الدليل الرقمي كمفهوم على الرغم من عدم تحديده بشكل كامل كهوية رقمية، يبقى عنصرا حاسما في كثير من الأحيان في مكافحة، ليس فقط الجرائم الإلكترونية، ولكن كل شكل من أشكال الانحراف الذي يستخدم اليوم أدوات رقمية التي يسهل الوصول إليها.

فالأدلة الرقمية هي الحقائق ذات الصلة التي يتم من خلالها إثبات إدانة الشخص أو براءته، فهي تشمل جميع الأدلة

[1] DOMAT Jean., Les lois civiles dans leur ordre naturel (1689), Paris, p. 204.

الموجودة في شكل رقمي أو إلكتروني، في هذا الإطار حددت المفوضية الأوربية[1] مكونات الأدلة الالكترونية في أنواعً مختلفة من البيانات ذات تنسيق إلكتروني مفيدة في التحقيقات والملاحقات الجنائية، بما في ذلك "بيانات المحتوى"، مثل رسائل البريد الإلكتروني والرسائل القصيرة أو الرسائل النصية والصور ومقاطع الفيديو، والتي غالبا ما يتم تخزينها على خوادم مقدمي الخدمات عبر الإنترنت، بالإضافة إلى فئات أخرى من البيانات، مثل بيانات المشتركين أو معلومات حركة المرور حول حساب عبر الإنترنت. غالبا ما تكون هذه الأنواع من البيانات ضرورية في التحقيقات الجنائية لتحديد هوية فرد أو الحصول على معلومات حول أنشطته الإجرامية.

وهكذا، فان الأدلة الرقمية في السياق الجنائي مجانية وتتوافق مع أي معلومات يمكن استخدامها في الإجراءات القانونية لإثبات أو الطعن في الحقائق المزعومة. ويتكون الدليل الرقمي من جميع العناصر المادية أو غير المادية مثل الأقراص الصلبة وهواتف وملفات المستخدم والسجلات التي تم جمعها وتحليلها وفقا للتشريعات السارية والملائمة مع حالتها التقنية في تلك اللحظة. فعلى عكس المجالات التقليدية مثل المجال المدني حيث تنشأ الأدلة مباشرة من الحقائق التي يمكن ملاحظتها، فإن المجال الرقمي يتميز عموما بكون الأدلة فيه مخفية في عالم غير مادي يتطلب نهجا منهجيا محددا ومعقدا في بعض الأحيان للوصول إليها.

وقد تثار بشكل حاد مسألة القواعد التي يجب احترامها للاحتفاظ بهذه المعلومات بشكل قانوني، خاصة بالنسبة للأدلة الرقمية التي هي هشة بطبيعتها غير مادية متقلبة ومتطورة مما يشكل في بعض الأحيان عقبة أمام قبولها كدليل. كما أن الطبيعة العابرة للبيانات تزيد من صعوبة جمع الأدلة وحفظها. بالإضافة إلى أنه يمكن نقل الأدلة الرقمية وحذفها وحتى تدميرها بشكل قانوني، مما قد يجعل الوصول إليها صعبًا.

في هذا الإطار استبعدت محكمة باريس العليا في قضية تتعلق بلاعبي الرجبي البريطانيين[2] لقطة شاشة من الأدلة المقدمة والمعترض عليه من طرف الخصم الناتجة عن نسخ شاشة الحاسوب. حيث اعتبرت المحكمة بأن عنوان موقع الويب الوارد أسفل الصفحة غير مكتمل، كما أن نسخ الشاشة لا يتضمن تاريخ التقاطها. وعليه يبقى سبب استبعاد هذا الدليل في الإمكانية الفنية لتعديل الصفحة دون اتصال بالإنترنت، أو حتى طباعة نسخة من الصفحة المتنازع عليها والتي كانت موجودة في ذاكرة التخزين المؤقت للكمبيوتر.

[1] Communication de UE. Fiche d'information, Questions et réponses : mandat pour la coopération entre l'UE et les États-Unis en matière de preuves électronique. http://europa.eu/rapid/press-rel.

[2] TGI Paris, 17e ch., 10 avr. 2013, James H. c/ Lionel D. : www.legalis.net.

وقد تتعرض مصداقية المعلومات التي يتم إنشاؤها وتخزينها على جهاز الكمبيوتر للتحدي بسبب وجود ثغرات أمنية في البرامج وأنظمة التشغيل والتي قد تهدد سلامة المعلومات الرقمية. مما يجعل العثور على الأدلة الرقمية أكثر تعقيدا وبشكل متزايد، لأنها غالبا ما توجد في "الحوسبة السحابية" أو "السحابة[1]"، وهو مصطلح يشير إلى استخدام خوادم الكمبيوتر البعيدة المتواجدة في مراكز البيانات المتصلة بالأنترنيت من اجل تخزينها وادارتها ومعالجتها بدلا من القرص الصلب لجهاز كمبيوتر الشخص.

نشير إلى أن مفهوم الأدلة الرقمية يغطي أنواعا مختلفة من البيانات غير الملموسة التي قد تكون موضع اهتمام المحققين في سياق تحقيقاتهم. فهي تشمل كل من:

أ- بيانات المحتوى (Les données de contenu)

لم يتم تعريف بيانات المحتوى في اتفاقية بودابست بشأن الجرائم الإلكترونية[2]، ولكن وفقًا للتقرير التوضيحي لها فإنها تعني "محتوى المعلومات في الاتصال، أي معنى الاتصال أو الرسالة أو المعلومات التي ينقلها الاتصال.

ب- بيانات المرور - (Les données de trafic

يمكن اعتبار البيانات المسجلة أو المضمنة أو المنقولة بواسطة جسم متصل بمثابة "بيانات كمبيوترية" التي يُسمح لضباط الشرطة القضائية بالوصول إليها أثناء التفتيش) قانون المسطرة الجنائية، المادتان 59و(60، سواء من مكان البحث أو من مصلحتهم إلى "سحابة"[3] أو تطبيقات عن بعد مستخدمة من أنظمة الكمبيوتر التي تم ضبطها أثناء البحث.

---

[1] Le Cloud Computing " ou " informatique en nuage, la pratique consistant à utiliser des serveurs informatiques à distance héberger dans des centres des donnes connecté à l'internet pour stocker et traiter des donnes plutôt qu'un serveur local ou un ordinateur personnel, dictionnaire of the internet oxford université press.

[2] Convention sur la cybercriminal le 23 Novembre 2001 et le Protocoled additional à ladies convention, https://www.sgg.gov.ma/Portals/0/lois/Convention-cyberciminalite_

صادق المغرب على اتفاقية بدبابيس بتاريخ 18 يونيو 2018 وعلى البرتوكول الاضافي الثاني الملحق بالاتفاقية وحول محاربة الجرائم الالكترونية بتاريخ ماي 12 2022.

[3] السحابة هي مجموعة من الخوادم المتصلة بالشبكة بما في ذلك أنظمة التشغيل والبرامج وتخزينها .

"cloud" Informatique en nuage modèle d'organisation informatique permettant l'accès à des= =ressources numériques dont le stockage est externalisé sur plusieurs serveurs.

https://www.larousse.fr/dictionnaires/francais/fadette/186905

ج – بيانات الاتصال (Les données de connexon)

إن بيانات مستخدمي خدمات الاتصالات الإلكترونية، والتي تسمى "البيانات الوصفية"، تسمح باستخلاص استنتاجات دقيقة للغاية بشأن الحياة الخاصة للأشخاص الذين تم تخزين بياناتهم، مثل عادات حياتهم اليومية، وأماكن الإقامة الدائمة أو المؤقتة، والحركات اليومية أو غيرها، والأنشطة التي يقومون بها، والعلاقات الاجتماعية لهؤلاء الأشخاص والأماكن الاجتماعية التي يرتادونها. فالبيانات الوصفية تمكن أجهزة التحقيق باستخلاص قدر كبير من المعلومات الضرورية والتي تشكل أرضا خصبة لأجهزة التحقيق والقضاة.

فمثلا، تشير كلمة فاديت[1] إلى سجل المكالمات الهاتفية التي يرسلها مشغلو الهواتف المحمولة والتي تسمح بتحديد هوية المحاورين. نشير الى أنه ينبغي التمييز بين "فاديت" والتنصت على الهاتف من جانب أن فاديت لا يظهر أي شيء عن محتوى المحادثات والتي تظل غير متاحة. وهو ما أشار إليه السيد فرانسوا مولينز، النائب العام لدى محكمة النقض.[2]

و قد تشكل الأشياء المتصلة المستعملة من قبل المجرمين أو الضحايا مصدرا للمعلومات الرقمية المفيدة في التحقيقات الجنائية[3]، كما هو الحال بالنسبة للهواتف الذكية والأجهزة اللوحية، وبيانات تحديد الموقع، على والأجهزة القابلة للارتداء مثل الأساور الإلكترونية، أو الساعات والنظارات المتصلة، وحتى المركبات المتصلة الطائرات بدون طيار، فقد يشكل تحليل بيانات سجلات الأحداث التي تم إصدارها للكائن المتصل أو المسجلة بواسطته، مسرحا للمحققين. فمثلا فتح أبواب السيارة والذي قد يشير إلى وجود راكب، أو ربط الهواتف الذكية بمركبة أو مكبر صوت محمول والذي قد يشير إلى وجود شخص في مكان معين، أو الأجهزة المنزلية التي تعطي مؤشرات على وجود الأفراد في المنزل مع بيان الأوقات أو المدة أو حتى العدد.

إذا كان الدليل الرقمي يتميز بتعدده وتنوعه بما يسمح بالكشف عن الجرائم والجناة وبالتالي الوصول إلى الحقيقة، فإنه بالمقابل ينبغي أن يكون مؤطرا بنظام قانوني متين يوازي بين الوصول الى الدليل الرقمي وبين حماية حقوق الافراد وحرياتهم.

المحور الثاني: طرق الوصول إلى الأدلة الرقمية

أفضى تطور التكنولوجيا الرقمية في معظم التحقيقات الجنائية، بالمشرع إلى تكييف الإجراءات التقليدية مثل المصادرة

[1] فاديت بيان تفصيلي للمراسلات المرسلة من الهيأة Fadettes

https://www.dictionnaire-juridique.com/

[2] F. Molins, La protection des citoyens européens dans un monde ultra-connecté : Revue Fondation Robert Schuman, Question d'Europe, n° 510, 8 avr. 2019.

[3] Gaël Burroni La preuve pénale par les données issues des objets connectés ; https://www.dalloz-actualite.fr/node/preuve-penale-par-donnees-issus-des-objets-connectes.

والالتقاط مع متطلبات وخصوصيات الأدلة الرقمية، مع خلق إجراءات جديدة للتحقيق مثل الاسم المستعارة أو التقاط البيانات أو تحديد الموقع الجغرافي او التنصت عن طريق الاتصالات الإلكترونية، والوصول عن بعد إلى المراسلات المخزنة.

وعليه سنستعرض بداية للإجراءات الكلاسيكية للوصول إلى الأدلة الرقمية، على أن نتناول بعدها الاجراءات العصرية للوصول إليها.

قام المشرع بتكييف قانون الإجراءات الكلاسيكي تدريجيا لتحسين البحث عن الأدلة الرقمية لتشمل عمليات التفتيش والحجز، والخبرة الجنائية وطلبات الحصول على البيانات، واعتراض المراسلات،

1- عمليات التفتيش والحجز

تسمح المادة 104 من قانون المسطرة الجنائية[1] لضابط الشرطة القضائية بالاطلاع على البيانات قبل أن يتم حجزها. وهكذا يتم حجز المعطيات المعلوماتية إما عن طريق وضع تحت يد العدالة للحامل المادي لهاته المعطيات مثل الحاسوب، اللوحات الالكترونية، الهاتف المحمول، القرص الصلب للحاسوب، مفتاح صلب، أو عن طريق أخذ نسخة منهم بحضور الأشخاص المعنيين بها.

وهكذا يمكن لضابط الشرطة القضائية أثناء التفتيش الوصول من خلال نظام معلوماتي مثبت في المكان الذي يجري فيه التفتيش إلى البيانات ذات الصلة بالتحقيق الجاري والمخزنة في النظام المذكور أو في نظام معلوماتي آخر، شريطة أن تكون هذه البيانات متاحة من النظام الأولي أو متاحة للنظام الأولي.

2- الخبرة الجنائية في المجال الرقمي

يجوز أثناء التحقيق القضائي كلما عرضت مسألة تقنية أن يقوم خبراء قانونيون يتم تعيينهم بأمر من قاضي التحقيق أو هيآت الحكم أن تأمر بإجراء خبرة[2]، بعمليات تتضمن استغلال الوسائط الحاسوبية. حيث تتمثل مهمة الخبير الجنائي في إجراء التحقيقات في العناصر الرقمية: أجهزة الكمبيوتر، والأجهزة اللوحية، والهواتف الذكية، وشبكات الإنترنت، وما إلى ذلك، بناء على أمر صادر عن قاضي التحقيق. ويجب أن يشار في هذا الأمر إلى سياق القضية وفترة البحث حتى يكون الإجراء فعالا. وتكون الخبرة الجنائية في المجال الرقمي مطلوبة إذا كانت البيانات الرقمية تبدو حاسمة لجوهر القضية من أجل تأمين الإجراء بشكل

[1] تنص الفقرة الأولى من الماد ة 104: إذا تبين أثناء التحقيق ما يستوجب البحث عن وثائق، فيجب التقيد بالمقتضيات المنصوص عليها في الفقرة الثالثة من المادة 59 ويكون لقاضي التحقيق وحده أو لضابط الشرطة القضائية المنتدب من طرفه حق الاطلاع على الوثائق قبل حجزها ما لم يتعلق الموضوع بالمس بأمن الدولة الداخلي أو الخارجي.

[2] تنص المادة 194 من قانون المسطرة الجنائية على ما يلي: يمكن لكل هيئة من هيئات التحقيق أو الحكم كلما عرضت مسألة تقنية، أن تأمر بإجراء خبرة إما تلقائيا وإما بطلب من النيابة أو من الأطراف.

مرض، كاستشارة المواقع التي تروج للإرهاب، أو تزوير الوثائق على أجهزة الكمبيوتر، أو تبادل الرسائل مع الضحية أو الشركاء، أو استعادة البيانات المحذوفة.

ويمكن أن تتم عملية الخبرة أثناء البحث، مع الخبير المرافق لضباط الشرطة القضائية أو الدرك، أو في وقت لاحق، على المعدات التي تم ضبطها أثناء البحث. مثل البيانات الموجودة أو سابقة على القرص الصلب لجهاز الكمبيوتر أو في ذاكرة الهاتف المحمول، أو تحليل آثار الاتصالات عبر الشبكة الرقمية للشركة أو الإنترنت، أو البحث عن أوجه التشابه بين برنامجين. ويمكن أن تتخذ تدخلاتهم أشكالا عديدة. قد تكون على شكل مجرد ملاحظات بسيطة، وكفاءتها الفنية تهدف فقط إلى توصيف الحقائق. وقد تكون أيضًا على شكل تحليل عناصر القضية. وتهدف الخبرة إلى تمكين القاض ي من "فهم" الحقائق وتوصيفها بشكل أفضل.

3- طلبات الحصول على بيانات الاتصال

تهدف الطلبات الموجهة إلى مشغلي الاتصالات لغرض الحصول على بيانات الاتصال إلى استرداد المعلومات التصريحية: الهوية والعنوان ورقم الهاتف ووسائل الدفع بالإضافة إلى البيانات التي تمكن من تحديد موقع نظام المعالجة الآلي مثل الكمبيوتر. وهكذا يجوز للنيابة العامة أو بترخيص منها لضابط الشرطة القضائية، أن يطلب بأي وسيلة باستدعاء أي شخص لسماعه، إذا تبين له أنه يمكنه أن يمده بمعلومات حول الأفعال أو الأشياء أو الوثائق المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة[1] كما يمكنه أن يطلب من كل مؤسسة أو منظمة خاصة أو عامة أو أي إدارة عامة قد تحتفظ بمعلومات ذات صلة بالتحقيق، بما في ذلك المعلومات المستمدة من نظام معلوماتي أو معالجة البيانات الشخصية، أن تزوده بهذه المعلومات، ولا سيما في شكلها الرقمي عند الاقتضاء دون أن يكون من الممكن معارضته بالتزام السرية المهنية. يسمح هذا المقتضى للنيابة العامة أو ضابط الشرطة القضائية بطلب البيانات المخزنة من أي شخص أو مؤسسة أو هيئة خاصة أو عامة أو أي إدارة عامة دون إخطار مسبق لحاملي هذه البيانات.

ينبغي التذكير بأن طلب الحصول على المعلومات الرقمية وغير الرقمية، يجب أن يتم بناء على طلب محدد ومكتوب ومعلل، يستهدف أشخاصا معينين على وجه التحديد، يتم تحديدهم بشكل مباشر أو غير مباشر.

نشير الى أن طلبات الحصول على بيانات الاتصال أقرها البرتوكول الإضافي الثاني لاتفاقية بدبابيس بالمتعلقة بالجريمة الكترونية بشأن تعزيز التعاون والكشف عن الأدلة، والتي وقع عليها المغرب بتاريخ 12 ماي2022، حيث نصت المادة 8 من البرتوكول على: "يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من التدابير الضرورية لتمكين سلطاته المختصة من إصدار أمر يتم تقديمه كجزء من الطلب الموجه لطرف آخر بغرض إجبار مقدم خدمات في إقليم الطرف المتلقي على تقديم:

[1] تنص المادة 60 من قانون المسطرة الجنائية على ما يلي: يمكن لضابط الشرطة القضائية أن يستدعي أي شخص لسماعه، إذا تبين له بوسع هذا الشخص أن يمده بمعلومات حول الأفعال أو الأشياء أو الوثائق المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة.

أ. معلومات المشترك؛

ب. بيانات حركة الاتصال المحددة والمخزنة والموجودة في حيازة مقدم الخدمات أو تحت تحكمه، عندما تكون هذه المعلومات والمعطيات ضرورية للتحقيقات أو الإجراءات الجنائية المحددة التي يقوم بها الطرف.

4 – اعتراضات المراسلات

تنطبق الأحكام المتعلقة باعتراض المراسلات المرسلة عن طريق الاتصالات على الأنترنت خاصة على الرسائل الإلكترونية، بحيث يشمل هذا الإجراء التكنولوجيا الرقمية عندما تتعلق التحقيقات بالمراسلات الخاصة بين الأشخاص المتصلين. ويتعرف تقنية اعتراض المراسلات على أنها تقنية تقوم على أساس التدخل عن طريق اشتقاق على خط المشترك لإجراء التسجيل المغناطيسي للمحادثة. فهي ذات أهمية أكيدة لفعالية الملاحقة الجنائية لأنها تجعل من الممكن تتبع هوية وعنوان المستخدم المرتبط بجهاز الكمبيوتر مرتكب الجريمة.

ب. الإجراءات الجديدة في التحقيق الجنائي

ابتكرت التشريعات إجراءات جديدة للتكيف مع الجرائم الرقمية المتزايدة محاطة بضمانات[1]، شملت كل من: التحقيق تحت اسم مستعار، والتقاط بيانات الكمبيوتر، وتحديد الموقع الجغرافي.

1– التحقيق تحت اسم مستعار

يشكل التحقيق المستعار أحد التقنيات التي تتكيف بشكل مثالي مع التكنولوجيا الرقمية، والتي تحولت تدريجيا إلى إجراء قانوني عام.[2] لقد تم إعمال التحقيق تحث اسم مسعار من أجل الوقوف على الجرائم الخطيرة وجمع الأدلة المرتبطة بها والبحث عن مرتكبيها وتحديد هويتهم. ويطلق على هذه الوسيلة أحيانا اسم "التسلل الرقمي"؛ أو مصطلح "الدوريات السيبرانية"، أو حتى "التسلل السيبراني".

ويتضمن التحقيق المستعار التفاعل مع المشتبه بهم عبر الإنترنت من خلال التبادلات الإلكترونية بهدف جمع أدلة على ارتكابه للجريمة، دون أي تحريض على ارتكابها. وترتكز هذه التقنية على الأنترنت باستخدام أسماء مستعارة بهدف تتبع الأشخاص الذين يرتكبون الجرائم والوصول إلى شبكاتهم. ويمكن لضباط الشرطة القضائية استعمال هاته التقنية من أجل جمع الأدلة الرقمية لإثبات جرائم معينة، مثل جرائم بيدوفيل، أو الجرائم المرتبطة بإنتاج أو عرض أو توزيع أو الحصول على مواد إباحية عن الأطفال

[1] F. Vadillo, Techniques d'enquêtes numériques judiciaires, enjeux numériques n° 3, sept. 2018, annales des mines : www.annales.org/enjeux-numeriques/2018/en-2018-03/EN-2018-09-12.pdf.

[2] M. Quéméner, Infiltrations numériques : JCl. Communication, fasc. 1110.

عبر نظام الكمبيوتر أو بواسطة دعامة لتخزين بيانات الكمبيوتر (المادة 9 من اتفاقية بدبابيس). حيث يحافظ العملاء على إخفاء هويتهم من خلال استخدام هوية مفترضة للمشاركة في المناقشات والتواصل مع مرتكبي هذه الجرائم، وخاصة على شبكات التواصل الاجتماعي وفي المنتديات المختلفة، على سبيل المثال عن طريق إنشاء ملفات تعريف وهمية.

لقد استعملت هاته التقنية في جرائم تعريض القاصرين للخطر، وكذلك الاتجار بالبشر وعندما ترتكب هذه الجرائم بوسائل الاتصال الإلكترونية.

ينبغي التذكير الى أن محكمة النقض الفرنسية[1] أكدت أنه لا توجد حاجة لإحالة مسألة ذات أولوية دستورية إلى المجلس الدستوري تتعلق بالانتهاك المحتمل لمبدأ المساواة أمام القانون والعدالة، والحق في احترام الحياة الخاصة وحقوق الدفاع بموجب المادة 1-87- من قانون المسطرة الجنائية الفرنسية، ورأت محكمة النقض على وجه الخصوص أن هذا النص الذي يجيز للمحقق المختص جمع الأدلة والبحث عن مرتكبي بعض الجرائم المحددة، دون أن يكون قادرا على التحريض على ارتكابها، من خلال المشاركة معهم في تبادل الرسائل الإلكترونية تحت اسم مستعار، لا ينطوي على أي انتهاك لحقوق الدفاع ولا أي تدخل في الحياة الخاصة للشخص الذي يظل حرا في الرد على الرسائل المذكورة من خلال تقييم محتوى رده بحرية.

2- الكشف عن بيانات الكمبيوتر

أشارت إلى هاته التقنية المادة 9 من اتفاقية بدبابيس تحت عنوان الكشف السريع عن بيانات الكمبيوتر، المخزنة في حالة الطوارئ، وهكذا نصت المادة على ما يلي: " يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من الإجراءات التي قد تكون ضرورية، في حالة الطوارئ، حتى تتمكن نقطة الاتصال المتاحة على مدار الساعة وسبعة أيام في الأسبوع، المنصوص عليها في المادة 35 من الاتفاقية، التابعة للدولة طرف أخرى تلقي طلب من هذه الأخيرة من أجل التمتع بمساعد فورية في الحصول من مقدم الخدمات الموجود فوق تراب تلك الدولة الطرف على الكشف السريع عن بيانات الكمبيوتر المخزنة في حوزته أو تحت حكمه دون طلب المساعدة القضائية.

3- برامج التجسس القانونية

يرتبط برامج التجسس بالسيطرة جزئيا على محطة الكمبيوتر المستهدفة من أجل استخراج بيانات معينة خلسة. وذلك عن طريق إجراء حقن البرنامج للتجسس عن بعد، أو عن طريق الاتصال الفعلي بالجهاز.

وتتميز هذه الوسيلة بميزة خاصة تتمثل في التحايل على تشفير الاتصالات. فهو يسمح نظريا بالبحث عن بعد في القرص الصلب للجهاز المستهدف للحصول على معلومات مفيدة لكشف الحقيقة. دون موافقة الأشخاص المعنيين، والوصول في أي

[1] Cass. crim., 7 fév. 2018, n° 17-90.026: Juris Data n° 2018-001408.

مكان إلى بيانات حاسوبية، وتسجيلها، وتخزينها، ونقلها، في نظام حاسوبي.

4- تحديد الموقع الجغرافي

تسمح هذه التقنية بتحديد موقع شيء ما في وقت المعين، وذلك بفضل انبعاثات جهاز يوضع على الشيء، كشريحة هاتف أو كمبيوتر محمول. فتحديد الموقع الجغرافي على الرغم من طبيعته التدخلية، يبدو كأنه بمثابة تقنية تستخدم لإثبات الوقائع القانونية.[1]

نشير إلى أن المجلس الدستوري الفرنسي اعتبر بأن تحديد الموقع الجغرافي، وهو إجراء من إجراءات الشرطة القضائية، لا ينطوي على فعل إكراه الشخص المستهدف، ولا اعتداء على سلامته الجسدية، أو الاستيلاء أو اعتراض المراسلات أو تسجيل الصور أو الصوت.[2]

5- صائد أمسى (IMSI)International Mobile Subscriber Identity catchers

فهو نظام يقوم على نوع من الهوائيات المتنقلة المحمولة والتي تحل محل هوائيات المشغلين ضمن دائرة نصف قطرها بضع كيلومترات، مما يتيح التقاط البيانات المرسلة أو المستقبلة من الأجهزة المتصلة به. ويسمح بجمع بيانات الاتصال الفنية التي تمكن من تحديد الأجهزة الرئيسية أو رقم اشتراك المستخدم.

خاتمة

يبدو أن الطفرة الرقمية المتجددة والمتسارعة ما فتئت أن أفرزت لنا حالات وقائع قانونية استعصت على الإطار القانوني التقليدي ضبطها وتنظيمها، فكان لابد من مواكبة تشريعية كفيلة للاستجابة لهاته المتغيرات في محاولة لضبط التجاوزات والخروقات التي يفزها التطور الرقمي بالاعتماد على الأدلة العلمية الرقمية المعاصرة، والتي يمكن استثمارها في مجال البحث والتحقيق عن الجرائم الرقمية مع الأخذ بعين الاعتبار الضمانات الحقوقية للمشتبه بهم.

[1] M. Quéméner, Géolocalisation dans le cadre pénal JCl. Communication, fasc. 982.

[2] Cons. const., 21 mars 2019, n° 2019-778 DC: Juris Data n° 2019-004275.