تطبيق القواعد الجزائية الإجرائية على الجريمة الإلكترونية: تحديات وآفاق

د. محمد حبحب*

الملخص:

يتمحور موضوع البحث حول كيفية تطبيق القواعد الإجرائية الجزائية أثناء التحقيق في الجرائم التي ترتكب في البيئة الرقمية، دون أن تحيد عن الهدف الذي ابتغاه المشرع اللبناني من وراء النص على هذه القواعد. فالتحقيق عادة ما يلامس حقوق الأفراد المتعلقة بحرياتهم الشخصية وحياتهم الخاصة، هذه الحقوق التي يمكن أن تصبح معرضة للانتهاك في حال تطبيق القواعد التقليدية الموجودة حالياً والتي لا تتلاءم بالمطلق مع الطبيعة غير المادية للجريمة الإلكترونية.

وعليه لمعالجة هذه الإشكالية تم تقسيم هذا البحث إلى مبحثين اثنين تناولنا في الأول الثغرات التي تعتري النصوص الحالية وضعفها في تعقب الفاعلين الذين يستفيدون من المميزات الهائلة التي تمنحها تقنية المعلومات، كما والحالات التي يمكن للضابطة العدلية أن نقوم فيها بانتهاك الحياة الخاصة للأفراد وحرياتهم الشخصية، إضافة إلى كيفية وجوب احترام المبادئ والنصوص (مبدأ الإقليمية والنصوص المتعلقة بالتعاون الدولي) الواجب تطبيقها في حالات اشتمال الجريمة على عنصر أجنبي. وتناولنا في المبحث الثاني الحدود التي يقف عندها القاضي للأخذ بالأدلة الرقمية المستخلصة من الإجراءات المتخذة من قبل الضابطة العدلية، بالإضافة لمدى احترامه لمبدأ المشروعية أثناء تقييمه لتلك الأدلة، لنخلص في نهاية البحث إلى وجود ثغرات تعتري القواعد القانونية الحالية التي يمكن بسببها أن يفقد الدليل قيمته في الإثبات، لذلك يتحتم تدخل المشرع اللبناني لسن نصوص قانونية تجيز بشكل صريح إجراء التفتيش في البيئة المعلوماتية، وتبيان حدود سلطات التحقيق وصلاحيات الضابطة العدلية من أجل الحفاظ على حريات الأفراد. كما أوصى البحث بضرورة النص على كيفية التعاون بين سلطات التحقيق والمؤسسات الخاصة المعنية بتخزين المعلومات والبيانات الخاصة التي تساعد تلك السلطات في الكشف عن الحقيقة.

---

* أستاذ القانون الجنائي المشارك، كلية الحقوق، الجامعة اللبنانية وجامعة الجزيرة في دبي.

المقدمة:

تشكل تكنولوجيا المعلومات في الوقت الراهن العصب الرئيسي الذي تقوم عليه معاملات الأفراد في مختلف ميادين الحياة المالية، الاجتماعية والثقافية، والركيزة الأساسية للتحول إلى الحكومات الذكية وبناء الدولة الحديثة، المتطورة والقوية. وهذا التطور الذي غزا العالم بأكمله ولد وجهاً مظلماً أرخى بظلاله على الجانبين الاقتصادي والأمني على السواء، فمن ناحية أولى، قدرت الخسائر التي تكبدها العالم جراء الجريمة الإلكترونية في عام 2016 بنحو 650 بليون دولار، والمبلغ مرجح للارتفاع إلى أكثر من تريليون دولار بحلول عام 2020 [1]. ومن ناحية أخرى، شكلت شبكة الإنترنت والخدمات المتفرعة عنها مساحة واسعة لحرية التعبير وتداول المعلومات، لكن في الوقت نفسه رأت فيها العصابات المنظمة والجماعات الإرهابية بيئة خصبة ووسيلة ناجعة لاستهداف أمن الأفراد ومصالح الدول الأمنية والقومية من خلال نشر الأفكار المتطرفة وغسيل الأموال وتمويل الإرهاب.

إن العقاب على الجرائم المذكورة أعلاه لا يشكل دائماً إشكالية قانونية كبيرة، كون معظم الدول تبنت في تشريعاتها نصوصاً قانونية تستهدف تلك الأفعال وتحدد العقاب الملائم لها[2]. لكن الإشكالية الحقيقية تكمن في صعوبة إثبات عناصر هذه الجرائم

(1) تقرير مقدم إلى الدورة الرابعة لمعرض ومؤتمر الخليج لأمن المعلومات «جيسيك»، «إنترنت الأشياء 2017» ، دبي، 21 ايار/مايو 2017. بالمقابل تفيد التقارير الحديثة الصادرة سنة 2017 بأن منطقة الخليج العربي ليست بمنأى عن خطر الجرائم الإلكترونية، حيث تكبد الاقتصاد الخليجي خسائر بقيمة 850 مليون دولار، جراء قرصنة البرمجيات التي باتت تشكل تهديداً حقيقيا للهيئات الحكومية ومجتمع الأعمال. تقرير منشور في «العربية سكاي نيوز»، 29/6/2014 على الموقع التالي: https://www.skynewsarabia.com/technology/677798-800-

(2) لكن في لبنان لم يتدخل المشرع بعد لتجريم الأفعال غير المشروعة التي ترتكب على شبكة الإنترنت، حيث يتم العقاب على الجرائم الإرهابية بالمواد 314 وما يليها من قانون العقوبات الصادر سنة 1943 وكذلك يعاقب على جرائم تبييض الأموال بموجب القانون رقم 547/ 2003 بشأن مكافحة تبييض الأموال وتعديلاته وبموجب بعض التعاميم الصادرة عن مصرف لبنان، لمزيد حول هذا الموضوع راجع: د. جنان الخوري، تبييض الأموال جريمة جزائية مصرفية وتبعية، مجلة الجيش، بيروت، 2013، العدد 85، وأيضاً، هناك القانون رقم 44 الصادر بتاريخ 24/11/2015 الخاص بمكافحة تمويل الإرهاب وتبييض الأموال. لكن المشرع الكويتي قد أصدر القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، والذي يتضمن موادا تعاقب على الأعمال الإرهابية وغسل الأموال والاتجار بالبشر (المواد 8 و 9 و10) إذا تمت بالطرق الإلكترونية، كما نص المشرع الكويتي على القانون رقم 106 لسنة 2013 في شأن مكافحة غسيل الأموال وتمويل الإرهاب.

وملاحقة مرتكبيها لتقديمهم إلى العدالة، ومدى اقتناع القاضي الجزائي بالأدلة الرقمية المستخلصة التي تبرزها سلطة الاتهام ومرد ذلك يعود: إما إلى الطبيعة غير المادية لشبكة الإنترنت أو إلى طبيعتها الدولية. فالطبيعة غير المادية للشبكة والتطبيقات التي تمنحها للمستخدمين ولدت صعوبة في تطبيق القواعد الإجرائية الحالية غير الملائمة مع الطبيعة الجديدة للجرائم الإلكترونية[3]، بل على العكس، يشكل تطبيقها في بعض الأحيان خرقاً لحقوق الأفراد الأساسية كالحق في الخصوصية والحرية الشخصية. هذا من ناحية، أما من ناحية أخرى، فقد سهلت الطبيعة الدولية لهذه الشبكة انتشار الجريمة الإلكترونية بين الدول بطريقة أكثر سهولة، بحيث خلق، إلى جانب إشكالية اختيار القانون الواجب التطبيق، إشكالية أخرى تتعلق بمدى احترام الدولة صاحبة الاختصاص لمبدأ الإقليمية عند إجراء التحقيقات وجمع الأدلة الناتجة عن جريمة تتخطى الحدود الجغرافية.

تكمن أهمية هذا البحث في تحديد الثغرات القانونية التي تعيق تطبيق قواعد الإجراءات الجنائية في لبنان وإلقاء الضوء على القوانين المقارنة، لا سيما الغربية منها والاطلاع على أحكام القضاء فيها، بغية الاستفادة منها وتطبيقها في نظامنا القانوني الحالي. وسوف نستخدم في هذا البحث المنهج العلمي التحليلي للخروج ببعض النتائج والتوصيات التي يمكن أن تؤسس لقواعد قانونية قادرة على استقصاء هذا النوع من الجرائم، مع الاهتداء بالتجربتين الفرنسية والأميركية في هذا السياق، لما لهما من باع طويل على جميع الأصعدة التشريعية والأمنية والقضائية.

وعليه، لتحليل إشكالية الدراسة والوقوف على الحلول المناسبة، ارتأينا تقسيمها إلى مبحثين، نتناول بدايةً القيود التي يواجهها رجال الضابطة العدلية أثناء قيامهم بالإجراءات الهادفة لجمع الأدلة (المبحث الأول)، ومن ثم نقف على مدى اقتناع القاضي بها أثناء المحاكمة (المبحث الثاني)، كل ذلك في ظل قواعد الإجراءات المنصوص عليها في قانون أصول المحاكمات الجزائية رقم 328 الصادر في 2/8/2001.

(3) د. عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين»، أكاديمية نايف العربية للعلوم الأمنية، 1999، ص 10 وما يليها. د. رامي علي وشاح، الصعوبات المادية التي تعترض الإثبات بالمحررات الإلكترونية، الأكاديمية للدراسات الاجتماعية والإنسانية، 2010، عدد 3، ص 44 وما يليها.

المبحث الأول

قيود استخلاص أدلة الإثبات الجنائي في البيئة الرقمية

استفاد المجرمون من الطبيعة غير المادية لشبكة الإنترنت، فقد استطاع هؤلاء، بفضل التقنيات التي تمنحها الشبكة، لإخفاء مسارهم بسهولة وإلغاء أي دليل يشير إلى الأفعال التي قاموا بها (المطلب الأول)، وبالتالي فإن إتباع القواعد القانونية المتعلقة بالضبط والتفتيش المنصوص عليها في قانون أصول المحاكمات الجزائية اللبناني يؤدي في بعض الأحيان إلى مخالفات قانونية تطال حقوق الأفراد الأساسية التي نص عليها الدستور اللبناني، خصوصاً إذا سلمنا أن القانون المذكور قد وضع أصلًا لإجراء التوازن بين حقوق هؤلاء الأفراد وتحقيق العدالة ومصلحة المجتمع[4] (المطلب الثاني). كما أن الطبيعة الدولية للشبكة وضعت على جدار البحث مدى احترام السلطات المناطة بالتحقيق لمبدأ الإقليمية الذي يحتم عليها عدم امتداد اختصاصها خارج حدود الدولة (المطلب الثالث). وسنقوم بشرح تلك الإشكاليات في ثلاثة مطالب متتالية.

المطلب الأول

صعوبة تتبع الفاعل

لكي يكون هناك عقاب على جريمة، يجب إثبات عناصرها وتحديد فاعلها، وهذا العمل يتم عبر جمع الأدلة التي يستطيع من خلالها القاضي ربط خيوط الجريمة بعضها ببعض من أجل استخلاص الحقيقة، لكن تحقيق هذا الهدف في البيئة الرقمية يصبح صعب المنال، إذا ما أخذنا بعين الاعتبار التقنيات المنبثقة عنها والتي يتوسل إليها الجناة من أجل تحقيق أهدافهم الإجرامية، دون ترك أي أثر أو دليل يمكن الاستدلال من خلاله على أماكنهم[5]. لذلك سمحت البيئة الرقمية للجناة باستخدام برامج معلوماتية لها خاصية إخفاء أو تدمير للبيانات المتعلقة بمسارهم، أو استخدام تقنية الغفلية[6] (Anonymat) أو وسائل

(4) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية للنشر، القاهرة، 1995، ص 5.

(5) C. Boulanger et F. Frafer، "Cybercriminalité: un aperçu du monde des criminels virtuels" Classe International.، 4 janv. 2014، p. 12 et s.

(6) M. Raymond، Les auteurs de crimes sexuels sur internet، Revues Psychiatrie et violence، Volume 14، n. 1، 20152016–، parag. 4.

حماية مثل أنظمة الترميز والتشفير التي تمنع اكتشاف أماكن تواجدهم[7]. فعلى سبيل المثال، يقوم مرتكبو جرائم دعارة الأطفال باستخدام أنظمة مشفرة من أجل بث الصور والأفلام والتواصل مع ضحاياهم دون معرفة مكان تواجدهم[8]، أضف إلى ذلك العوائق المتمثلة بنقص الاحتفاظ بالبيانات من قبل مقدمي خدمة الإنترنت التي تقف في طريق تحديد هوية المشتبه في تورطهم في قضايا نشر المواد الإباحية التي تتعلق بالأطفال وتعيين مواقعهم[9]، وينطبق هذا الأمر على الإرهابيين أيضاً، حيث أصبحت تطبيقات شبكة الإنترنت وأنظمة التخفي المعلوماتية وسيلة فعالة بالنسبة إليهم[10]، لأن التواصل فيما بينهم أصبح أكثر سهولة وأقل خطراً[11].

كما يستطيع غاسلو الأموال وممولو الإرهاب استخدام وسائل حديثة كالبطاقات الذكية (SMARD CARD) لتحويل ولصرف النقود دون وسيط [12] مع تشفير عملية التحويل بفضل استحداث تقنية جديدة تعرف بتقنية «موندكس» (Mondex) [13]، وتلعب النقود

(7) د. موسى أرحومة، الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28–29/ 10/ 2009، ص3 وما يليها.

(8) د. أسامة العبيدي، جريمة الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة ، حزيران/ يونيو2013، العدد53، ص 73.

(9) مؤسسة كونز العائلية للقانون الدولي والسياسة، تقرير حول المواد الإباحية المتعلقة بالأطفال: التشريع النموذجي والاستعراض العالمي للتشريعات، الطبعة السابعة، 2012، ص 6.

(10) Rapport de Délégation ministrielle aux industries de sécurité et à la lutte contre les cybermenaces – État de la menace، janv 2017، p.11

(11) تعتبر شبكة الإنترنت الوسيلة الأسرع والأنجع لبث الأفكار الإرهابية والتحريض على العنف والترويج للأفكار الدينية المتشددة، وذلك لاستقطاب الطاقة البشرية وتجنيدها وإدماجها في المشاركة في العمليات الإرهابية، حيث لا يمكن لأحد أن ينكر دور مواقع التواصل الاجتماعي في هذا المجال، انظر بهذا الخصوص، د. ليتيم فتيحة، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، العدد الثاني، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، 2010، ص. 237

(12) نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، لبنان، 2007، ص83 وما بعدها.

(13) «موندكس» هي بطاقة ذكية تحمل وتوزع النقد الإلكتروني وهي منتج لمؤسسة ماستر كارد العالمية، تتمتع بمرونة عالية لاستخدامها في عمليات الشراء عالمياً وفي عمليات التحويل من رصيد بطاقة إلى أخرى من خلال آلات الصرف الآلي (ATM) أو من خلال استخدام أجهزة (Laptop) عبر الإنترنت. وتتيح للعميل القيام بعمليات السحب أو الإضافة من حساب الشخص دون الرجوع =

الإلكترونية[14] دوراً مهماً في إتمام مثل هذه العمليات الخاصة عبر إجراء تحويلات جداً معقدة، خصوصاً أن التعامل بتلك النقود يتم دون الحاجة إلى ظهور الهوية الحقيقية للمتعاملين، مما يجعل مهمة السلطات المختصة بمراقبة الجريمة صعبة بسبب استحالة مراقبة السجلات والعمليات المالية التي تجري بواسطة هذه الطريقة[15]، أضف إلى أن وجود تقنيات مثل (Steganography) ساعدت بالتواصل بين الجناة بشكل سري عبر إخفاء الرسائل والملفات الهامة داخل ملفات أخرى مشروعة مثل الصورة أو الفيديو أو الملفات الصوتية دون الظهور على مسرح الجريمة إطلاقاً[16]، ويمكن استخدام مواقع التواصل الاجتماعي كوسيلة لتحقيق أهداف إجرامية مثل الانتحال والغش وسرقة الهوية وإقامة وإدارة الشبكات الإجرامية، عبر إجراء الحسابات المزيفة على هذه المواقع[17].

وقد منحت شبكة الإنترنت لمرتكبي الجرائم مميزات غير عادية في التخفي بشكل يسير جدا وذلك بفضل استخدام تقنيات ووسائل عديدة، فمن الوسائل التي يستخدمها المجرمون في هذا المجال ال»phishing» أو «التصيد» بالعربية، حيث يقوم المجرم بإخفاء هويته الحقيقية أو بإنشاء نسخة مطابقة لموقع مؤسسة مالية بهدف خداع المستخدم للحصول على بياناته الشخصية مثل كلمة المرور والأرقام السرية الخاصة بوسائل الدفع[18]. وهناك طرق أخرى للتخفي مثل (IP Spoofing)، حيث يقوم المجرمون بتزويد عنوان بروتوكول الإنترنت (IP) المرفق مع حزمة البيانات المرسلة، فيظهر للنظام المعتمد في تبادل المعطيات على بروتوكولات النقل بأنه عنوان صحيح مرسل من داخل الشبكة،

= إلى الحساب الجاري لدى البنك. ٠ راجع بهذا الخصوص: د. أحمد المحرزي ود. حمادة فوزي، برنامج مهارات التسويق والبيع: التسويق عبر الإنترنت، ص 208، متوافر على الرابط التالي: http://www.olc.edu.bu.eg/olc/images/internet.pdf

(14) نادر عبد العزيز شافي، المرجع السابق، ص 83.

(15) د. محمد حبحب، وسائل الدفع الإلكتروني في مواجهة الجريمة، بحث مقدم إلى المؤتمر الدولي الرابع حول التجارة الإلكترونية، صلالة– عمان، 26 و27 / 7 / 2016، ص 8 وما يليها.

(16) تختلف هذه الطريقة عن التشفير بأنها تلجأ لإخفاء المعلومات داخل ملفات أخرى عوضاً عن تشفيرها. فهي طريقة أو تقنية لحجب و إخفاء البيانات داخل وسيط رقمي، حتى يتم إخفاء أن هناك اتصالاً أو تبادل معلومات يتم في الخفاء، ولا يكون على علم بهذا الاتصال إلا الأشخاص المعنيون.

(17) سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأميركي، المجلة الدولية للقانون، 2017، عدد 3، ص 11 وما يليها.

(18) د. محمد حبحب، المرجع السابق، ص9.

عند إذن يسمح هذا النظام بمرور تلك البيانات بعدما تراءت له أنها مشروعة[19]. كما يمكن الحصول على هويات وبيانات المستخدمين لانتحالها فيما بعد والتخفي وراءها، وذلك عن طريق إرسال الرسائل المزعجة (Spam) أو الاستدراج بطريقة (Pharming) أو عن طريق إرسال بعض أنواع من الفيروسات إلى حواسيب المستخدمين كفيروس (Trojan horse) (حصان طروادة)[20].

أمام هذه التقنيات الهائلة، أصبح من الصعب مواجهة الجريمة الإلكترونية بأشكالها المتعددة، دون وجود وسائل تقنية حديثة بيد المحققين تستطيع خرق هذه المنظومة ذات التقنية العالية. وهذا فعلاً ما تقوم به الدول. فعلى الصعيد المحلي مثلاً، هناك في لبنان مكتب خاص بمكافحة جرائم المعلوماتية والملكية الفكرية[21] والذي يملك قدرات تقنية تؤهله لمواجهة هذا النوع من الجرائم. لكن يبقى السؤال يتمحور حول مدى قانونية الإجراءات التي يقوم بها المحققون التابعون لهذا المكتب بصفتهم ضابطة عدلية يأتمرون بأوامر النيابة العامة وقضاة التحقيق وفق النصوص الموجودة حالياً في قانون الإجراءات الجزائية اللبناني؟.

المطلب الثاني

وجوب احترام الحقوق الأساسية للأفراد

يشكل قانون الإجراءات الجزائية الإطار القانوني الذي يحدد اختصاصات كل من القضاة والنيابة العامة ومأموري الضبط القضائي، حيث تتمحور مهمتهم بالكشف عن عناصر الجريمة حال وقوعها، ولهم في سبيل ذلك التوسل إلى مختلف الطرق التي حددها القانون بهدف جمع الأدلة والقرائن المفيدة في إظهار الحقيقة، إلى جانب البحث في جميع الأماكن التي يمكن العثور فيها على أشياء يكون اكتشافها مفيداً للتحقيق[22].

فقد نصت المادة 47 من قانون أصول المحاكمات الجزائية اللبناني أنه: «يتولى الضباط العدليون، بوصفهم مساعدي النيابة العامة، المهام التي تكلفهم النيابة العامة فيها

(19) د. محمد حبحب، المرجع السابق، ص.9

(20) راجع بالتفصيل حول هذه الوسائل، محمود عبد الرحمن محمود، ورقة فنية حول تهديدات البنية التحتية الحرجة للمعلومات، جامعة عين شمس، الإسكندرية، ص 3 وما يليها.

(21) أُنشئ هذا المكتب بموجب مذكرة خدمة رقم 609/204 ش2 تاريخ 8/3/2006.

(22) د. محمود نجيب حسني، المرجع السابق، ص451 وما يليها.

استقصاء الجرائم غير المشهودة وجمع المعلومات عنها والقيام بالتحريات الرامية إلى كشف فاعليها والمسهمين في ارتكابها وجمع الأدلة عليهم، بما يستلزم ذلك من ضبط المواد الجرمية وإجراء كشوفات حسية على أماكن وقوع الجرائم ودراسات علمية وتقنية على ما خلفته من آثار ومعالم...»، وفي ذات السياق حدد المشرع الكويتي في المادة 39 من القانون رقم 17 لسنة 1960 الخاص بالإجراءات والمحاكمات الجزائية أعمال مأموري الضبط القضائي، وذلك: «بإجراء التحريات اللازمة للكشف عن الجرائم ومعرفة مرتكبيها وجمع كل ما يتعلق بها من معلومات لازمة. ثانيا – تنفيذ أوامر سلطات التحقيق والمحاكمة في كل ما يتعلق بالتحقيقات والمحاكمات. ثالثا – تولي من ثبت له من رجال الشرطة صفة المحقق للتحقيق في الأحوال التي ينص فيها القانون على ذلك».

إلا أن تطبيق الإجراءات المذكورة في البيئة الرقمية يظهر عدم فاعليتها في الوصول إلى النتائج المرجوة، بل يمكن أن يؤدي إلى نتائج غير مرضية في بعض الأحيان[23]، لا سيما إذا أخذنا بعين الاعتبار أن المشرع ارتأى من خلال هذه القواعد إيجاد توازن جدي بين المصلحة العامة المتمثلة بالبحث عن الحقيقة وتحقيق الردع العام وبين المصلحة الفردية المتمثلة في الحفاظ على الحياة الخاصة للأفراد وحرياتهم الشخصية. هذا التوازن يجد له سنداً إضافة إلى الدستور اللبناني[24]، القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية[25] والقانون رقم 140 الصادر في 27/10/1999 الرامي إلى صون الحق في سرية المخابرات. لكن المتغيرات الجارية بفعل الثورة التكنولوجية وعدم وضع نصوص قانونية مباشرة تستهدف العالم الرقمي يقودنا كباحثين إلى التساؤل عن مدى صلاحية النصوص التقليدية الموجودة حالياً لمواجهة الجريمة الإلكترونية دون التعرض

(23) Serge Migaryon، Trois ans de constats et de saisies informatiques: un états de lieu، Colloque، CNEJITA، 242012/5/، p 9.

(24) المادة 13 والمادة 14 من الدستور اللبناني، وكذلك نصت المادة 31 من الدستور الكويتي أنه: «لا يجوز القبض على انسان أو حبسه أو تفتيشه أو تحديد اقامته أو تقييد حريته...» والمادة 39 التي نصت على أن: « حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة الرسائل، أو إفشاء سريتها إلا في الأحوال المبينة في القانون وبالإجراءات المنصوص عليها فيه». كما أن حماية الحياة الخاصة تجد سندها في الاتفاقيات والمعاهدات والإعلانات الدولية، كالعهد الدولي للحقوق المدنية والسياسية الصادر عام 1966 (المادة 17)، والاعلان الأميركي لحقوق الإنسان (المادة 5)، والاتفاقية الأوروبية لحقوق الإنسان (المادة 8)، والإعلان العالمي لحقوق الإنسان (المادة 12)، والميثاق العربي لحقوق الإنسان (المادة 21).

(25) المادتان 48 و107 والمادة 400 وما يليها.

إلى حقوق الأفراد المتعلقة بالحياة الخاصة (الفرع الأول) والحرية الشخصية (الفرع الثاني).

الفرع الأول

احترام الحق في الخصوصية

إن أول ما تستهدفه سلطة التحقيق في بحثها عن الأدلة هو أجهزة الحواسيب الخاصة بالجاني أو المجني عليه، أو حتى الحواسيب والأنظمة المعلوماتية الخاصة بمقدم الخدمة، هذا طبعاً دون أن نستثني الهواتف الذكية، فأي جريمة معلوماتية لا بد أن ترتكب من خلال هذه الأدوات التي تعتبر مصدراً غنياً لأدلة الجريمة[26]، لكن في ذات الوقت يمكن أن تحتوي أحياناً على معلومات هائلة تتعلق بنشاطات الأفراد ورغباتهم وأسرارهم الشخصية والمهنية، هذه المعلومات جميعها تدخل ضمن إطار البيانات المتعلقة بالحياة الخاصة للفرد[27].

ويعني احترام الحياة الخاصة عدم المساس بكل ما يعتبره الفرد خاصاً به ولا يريد من أحد الاطلاع عليه أو الغوص بتفاصيله إلا برضاه، ويشمل هذا الحق حرمة المنزل وسرية المراسلات والاتصالات بأنواعها المختلفة[28]، وقد نصت المادة 8 من الدستور اللبناني على أن: «الحرية الشخصية مصونة وفي حمى القانون». ونصت المادة 9 من قانون تنظيم الأصول الإدارية والمالية في المديرية العامة للبريد والبرق الصادر بالمرسوم الاشتراعي رقم 126/59 تاريخ 12/6/1959 على أن: «سر المراسلات البريدية مصون لا يجوز إفشاؤه».

كذلك واحتراما لهذا الحق، قررت محكمة التمييز الفرنسية أن: "فعل المحققين المتمثل

(26) د. هلالي عبد اللاه أحمد، تفتيش نظم الحسب الآلي وضمانات المتهم المعلوماتي، دار النهضة، القاهرة، 2008، ص81، د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007، ص 207، د. أسامة العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، العدد 58، الرياض، ص 109.

(27) للمزيد حول هذا الموضوع راجع : د. هانيا فقيه، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لواقع الحماية وتحديات العصر، بيروت، 2018، ص 3، منشور في القاعدة البيبليوغرافية، مركز المعلوماتية القانونية، الجامعة اللبنانية.

(28) د. محمد يوسف علوان، ومحمد خليل الموسى، القانون الدولي لحقوق الإنسان: الجزء الثاني، الحقوق المحمية، ط 1، دار الثقافة للنشر والتوزيع، عمان، ، 2007، ص 289.

بتصوير أرقام لوحات السيارات الموجودة داخل ملكية خاصة من أجل استخدامها لتحديد هوية شخص مشتبه فيه هو مخالف لنصوص قواعد الإجراءات الجنائية ويعتبر انتهاكا على الحياة الخاصة"[29]، واعتبرت أيضاً أن: «قيام المحققين باعتراض الاتصالات في مرحلة التحقيق الأولي يشكل اعتداءً على حريات وخصوصيات الأفراد»[30].

لقد فرض المشرع اللبناني التزاما على أشخاص الضابطة العدلية أو مأموري الضبط القضائي باحترام حقوق الأفراد أثناء قيامهم بإجراءات التفتيش والضبط وإلا كانت تلك الإجراءات باطلة[31]، فالمبدأ العام يقضي أن أي مساس بالحياة الخاصة للأفراد أو حرياتهم الشخصية لا يعد مشروعاً إذا جاء مخالفاً للقانون[32]، لكن استناد الضابطة العدلية إلى المواد الموجودة حالياً لجمع الأدلة الناتجة عن الجرائم الإلكترونية يعرض إجراءاتها في بعض الأحيان للبطلان بسبب عدم مواءمة هذه المواد مع الطبيعة غير المادية التي تتمتع بها هذه الجرائم (ثانياً)، وكذلك الأمر، أن القانون رقم 140 / 1999 الرامي إلى صون الحق في سرية المخابرات أجاز اعتراض الاتصالات ومراقبتها بأمر من القضاء، لكنه يقتضي بحث حدود هذا الحق الممنوح لرجال الضابطة العدلية إذا ما تم الاستناد إلى القانون المذكور عند اللجوء إلى المراقبة الإلكترونية (أولاً).

أولاً– حق الخصوصية في مواجهة القواعد المتعلقة بمراقبة الاتصالات:

تعتبر المراقبة عن طريق اعتراض الاتصالات أو التنصت سيفا ذو حدين، فهي من جهة وسيلة ناجعة يلجأ إليها المحققون لضبط أدلة الجريمة وكشف الأعمال التحضيرية التي تسبق الأفعال الإجرامية، ومن جهة أخرى تعتبر وسيلة خطرة نظراً لقدرتها على الدخول في تفاصيل حياة الفرد الخاصة وكشف ما تحتويها من أسرار[33]. لقد نصت

(29) Cass. Crim 21، mars، 2007 n، 89.444–06. Bull. crim، 2007، n89.

(30) Cass. Crim، 27 fev. 1996، Bull. crim. 1996، n. 93

(31) تنص المادة 105 من قانون أصول المحاكمات الجزائية على أن: « كل تفتيش يجري خلافاً للأصول المبينة آنفاً يكون باطلاً. تبطل تبعاً له إجراءات التحقيق المسندة إليه».

(32) Cyberlex et CECYF، Rapport sur " la procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique"، 242018 / 1 /، p. 10

(33) د. نادر عبد العزيز شافي، بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني، مجلة الجيش، 2007، عدد 263، ص وما يليها، د. شيماء عطالله، تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، بحث مقدم الى المؤتمر العلمي الثاني لكلية القانون الكويتية العالمية، منشور بمجلة كلية القانون الكويتية العالمية، العدد (10)، السنة الثالثة، يونيو 2015، الكويت، ص 501 وما يليها.

المادة الأولى من القانون رقم 99/140 أن: " الحق في سرية التخابر الجاري داخلياً وخارجياً من وسائل الاتصال السلكية أو اللاسلكية (الأجهزة الهاتفية الثابتة، والأجهزة المنقولة بجميع أنواعها بما فيها الخليوي، والفاكس، والبريد الإلكتروني..) مصون وفي حمى القانون، ولا يخضع لأي نوع من أنواع التنصت أو المراقبة أو الاعتراض أو الإفشاء إلا في الحالات التي ينص عليها هذا القانون وبواسطة الوسائل التي يحددها ويحدد أصولها"[34]. كما أشارت المادة 174 من قانون المخدرات والمؤثرات العقلية والسلائف رقم 1998/673 إلى كيفية مراقبة الاتصالات الهاتفية والتنصت عليها في إطار ضبط جرائم المخدرات. وكذلك أجازت المادة 2 من قانون الدفاع الوطني اللبناني الصادر بالمرسوم الاشتراعي رقم 83/102 تاريخ 1983/9/16 على التنصت على مخابرات المواطنين واتصالاتهم عند اعلان حالة التأهب أو التعبئة[35].

ونص المشرع الكويتي في المادة 46 من قانون رقم 37 لسنة 2014 بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات على أنه: "يحظر تداول أجهزة التنصت بأنواعها كما يحظر بيعها أو عرضها للبيع ولا يجوز لغير الجهات الرسمية المختصة والتي يصدر بتحديدها مرسوم حيازة أجهزة التنصت بأنواعها، كما لا يجوز لأي من هذه الجهات استعماله بدون الحصول على إذن مسبق من النيابة العامة وذلك في الحالات ووفقا للإجراءات والأحكام المنصوص عليها في قانون الإجراءات والمحاكمات الجزائية الكويتي".

لقد سهلت تكنولوجيا المعلومات عمليات الرصد والتنصت، وأصبحت السلطة المكلفة بالمراقبة تمتلك معدات حديثة تستطيع رصد الأفراد "رصداً ينطوي على تعسف

(34) فنصت على أنه: «للضابطة العدلية، بموافقة النيابة العامة، أن تضع تحت المراقبة أو التنصت خطوط الهاتف التي يستعملها أشخاص تتوافر دلائل جدية تفيد اشتراكهم في إحدى جرائم المخدرات. لكنه لا يمكن اعتبار المكالمات التي حصل عليها بهذه الطريقة كإقرار، بل يستفاد منها في رصد تحركات الجناة وحسب والاستفادة من ذلك لكشف الجريمة».

(35) لقد نصت على أنه: «إذا تعرض الوطن أو جزء من أراضيه أو قطاع من قطاعاته العامة أو مجموعة من السكان للخطر، يمكن إعلان حالة التأهب الكلي أو الجزئي، أو حالة التعبئة العامة أو الجزئية، وتعلن التدابير بمراسيم تتخذ في مجلس الوزراء بناءً على توصية المجلس الأعلى للدفاع، ويمكن أن تتضمن أحكاماً خاصة تهدف إلى: تنظيم مراقبة النقل والانتقال والمواصلات والاتصالات. ويمكن الاستنتاج من هذا النص حق الدولة في الحالات المشار اليها في التنصت على مخابرات المواطنين واتصالاتهم عند اعلان حالة التأهب أو التعبئة، على أن يكون ذلك بموجب مراسيم في حالات استثنائية محصورة وضيقة جداً».

واقتحام الخصوصية، حتى أنه قد يتعذر على الفرد أن يعرف حتى أنه مراقب"[36]، فهناك أنظمة خاصة لمراقبة الإنترنت كتكنولوجيا "باكيت شيبر" التي تتيح مراقبة ورصد تفاعلات المستخدمين على مواقع التواصل الاجتماعي مثل فيسبوك، تويتر، غوغل ميل، وسكايب[37]، وتستطيع كشف هويات وأسماء المستخدمين وحتى كلمات السر. كما أن هناك برامج تدعى (Packet Sniffer) تستخدم في التنصت على الحزم الواردة والصادرة إلى ومن حساب معين وحفظ نسخة منها. كما أن هناك أيضاً شبكة تجسس عالمية أكثر خطورة تسمى (Echelon) مهمتها التجسس على الاتصالات الرقمية السلكية واللاسلكية والاتصالات عبر الأقمار الصناعية، وخطورة هذا البرنامج تكمن بتسجيله كل الاتصالات دون وجود عنصر بشري في عملية المراقبة، حيث يعمل بدون توقف في رصد كل شيء[38].

إذا كانت الأجهزة الأمنية في لبنان تستخدم تلك الوسائل اليوم تحت غطاء القوانين الموجودة حاليا، إلا أن هذه القوانين لا تشمل كافة المعايير التي تتناسب مع البيئة الحديثة لمراقبة الاتصالات، لا سيما مبدأ التناسب والشفافية والرقابة الشعبية[39]، فالقدرات المستخدمة في عمليات المراقبة تتجاوز الإطار الذي رسمها لها القانون، فعلى سبيل المثال نجد أن الإجراءات المنصوص عليها في القانون الحالي محكومة من حيث النطاق الزماني والمكاني، بمعنى آخر فإن أي رقابة تستند إلى القانون رقم 140 / 99 بحاجة إلى إذن من قاضي التحقيق الذي يسمح للضابطة العدلية بالقيام به في حدود زمنية معينة[40]، بحيث

(36) راجع التقرير المعد من قبل الجمعية العامة للأمم المتحدة حول «تعزيز وحماية الحق في حرية الرأي والتعبير»، مجلس حقوق الإنسان، الدورة الثالثة والعشرون، 2015، ص 5.

(37) راجع بهذا الخصوص: تقريراً حول «حق الخصوصية في لبنان»، معد من قبل منظمة تبادل الإعلام الاجتماعي الخصوصية الدولية، جمعية الاتصالات التقدمية، 2015، بند 15.

(38) للمزيد حول هذا الموضوع راجع: د. وليد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، الإسكندرية، 2012، ص 184 وما يليها.

(39) إن المبادئ الدولية لتطبيق حقوق الإنسان فيما يخص مراقبة الاتصالات هي: القانونية، مشروعية الغرض، الضرورة، الملاءمة، التناسب، السلطة القضائية، الكفء، المحاكمة العادلة، إخطار المستخدم، الشفافية، الرقابة الشعبية، سلامة الاتصالات ونظمها، ضمانات التعاون الدولي، ضمانات ضد النفاذ غير القانوني، راجع بهذا الخصوص التقرير الخاص بالمبادئ الدولية لحقوق الإنسان المنشور على الموقع التالي: https://necessaryandproportionate.org/principles

(40) نصت المادة 3 منه على أنه: «يحدد القاضي بالاعتراض وسيلة الاتصال التي يتناولها الاجراء والجرم موضوع الملاحقة أو التحقيق، والمدة التي تتم خلالها عملية الاعتراض على ألا تتجاوز هذه المدة الشهرين، وعلى أن لا تكون قابلة للتمديد إلا وفق الأصول والشروط عينها».

لا تبقى المدة الزمنية للمراقبة والاعتراض منوطة برغبة الضابطة العدلية. كما ويجب أن يحدد من حيث النطاق المكاني ومن حيث الأشخاص، وألا تجرى بطريقة جزافية تطال الأشخاص الذين ليس لهم أية علاقة بالجرائم التي تجري بسببها المراقبة. لكن الواقع العملي يخالف تلك الأحكام، فإجازة الحكومة لوزارة الداخلية بالحصول على داتا الاتصالات يبقى محل نظر، لا سيما أنه ليس هناك أية شفافية حول كيفية استخدامها واستغلالها، وقد كان للهيئة القضائية المستقلة قراراً قضى بـ «عدم الموافقة على قرارات الاعتراض (...) لعدم قانونيتها»، حيث رأت الهيئة أن وثائق طلب كامل داتا المعلومات «بما تضمنته من طلبات عامة وشاملة لا تخدم عملية متابعة الشبكات الأمنية والإرهابية المشبوهة التي تبرر مثل هذه الطلبات، وإنما بعكس ذلك فإنها تشكل مساساً بالحريات الفردية التي كفلها الدستور وصانها القانون رقم 140/99، ذلك أنها تجعل أشخاصا لا علاقة لهم بالشبكات الإرهابية عرضة لخرق سرية اتصالاتهم لو بحدها الأدنى»[41].

تنص المادة 51 من القانون رقم 58 لسنة 2015 المعدل لبعض أحكام القانون رقم 37 لسنة 2014 على أن: «تعتبر المكالمات الهاتفية والاتصالات الخاصة من الأمور السرية التي لا يجوز انتهاك حرمتها ولا يجوز إخضاعها للمراقبة بأي وسيلة كانت إلا بعد الحصول على إذن من السلطة القضائية المختصة ويجوز للنيابة العامة متى استدعت مصلحة التحقيق في جريمة ما إصدار أمر تعقب مصدر الموجات، (...) ويجب أن يتضمن الأمر تحديداً واضحاً للموجة المراد تعقب مصدرها ولا يستمر ذلك الأمر لمدة تزيد على ما تقتضيه ضرورة التحقيق». يتبين من المادة المذكورة أن المشرع الكويتي كفل الحق في سرية التخابر باعتباره متعلقا بحق الخصوصية، ولم يسمح بإجراء أي نوع من أنواع الاعتراض إلا بعد وقوع جريمة، بمعنى آخر لا تجيز المادة المذكورة أعلاه إطلاقاً التنصت على الاتصالات إذا لم يكن هناك جريمة قد وقعت بالفعل، وهذا ليس إلا صورة من صور الضوابط المتعلقة بكيفية احترام التوازن بين حريات الأفراد وحقوق المجتمع. لكن من ناحية أخرى يؤخذ على المادة المذكورة عدم تحديد نقطتين مهمتين: أولهما: إباحة تعقب مصدر الموجات لفترة زمنية غير محددة على عكس ما فعله المشرع اللبناني في المادة 3 من القانون رقم 140/99، التي حددت مدة اعتراض الاتصالات بشهرين قابلة للتمديد، وتبقى عبارة قابلة للتمديد محل نظر، حيث يقتضي برأينا التزام المحقق بالتقيد بمهلة

(41) القرار الصادر عن الهيئة القضائية المستقلة لمراقبة الاتصالات تاريخ 21 آذار/مارس 2012 منشور على الموقع التالي: www.mpt.gov.lb/.../2012/04-2012-reply%20-05-on%20total%20tel

الشهرين فقط وجعل التمديد بيد سلطة قضائية أعلى بعد بحثها الجدوى من التمديد. فتعبير «ما يقتضيه التحقيق» يبقى «فضفاضاً»، حيث كان يقتضي تحديد فترة زمنية معينة تكون كافية لتحقيق المهمة المبتغاة وعدم ترك الأشخاص محل التعقب رهينة بيد سلطة التحقيق التي تملك وحدها القرار بإنهائه أو إبقائه الأمر الذي يفقد معه القصد الذي ابتغاه المشرع الكويتي من هذه المادة وهو صون سرية التخابر والحفاظ على الحياة الخاصة للأفراد.

أما النقطة الثانية فتتمحور حول عدم تحديد المادة المذكورة لنوع الجريمة، أي أنه يحق لسلطة التحقيق بتعقب الاتصالات مهما كان نوع الجريمة ومدة العقاب عليها. وليت المشرع الكويتي يحذو حذو نظيره اللبناني في هذا السياق الذي لا يجيز اعتراض الاتصالات بمناسبة التحقيق بالجرائم التي تقل مدة العقاب عليها عن سنة[42].

وتثير المراقبة الإلكترونية إشكاليات قانونية تتعدى حدود الخصوصية في بعض الأحيان، فقد ينتج عن استخدام بعض برامج المراقبة تغيير أو تحريف في محتوى «داتا» (بيانات) الاتصالات بصورة مقصودة أو غير مقصودة، مما يؤثر ذلك سلباً على صحة هذا الدليل أمام القضاء إذا استطاع الشخص المعني إثبات ذلك.

وخلاصة القول، إن لجوء سلطات التحقيق إلى مراقبة الاتصالات على النحو الآنف الذكر من أجل جمع الأدلة المتعلقة بالجريمة أو تتبع الفاعلين تصطدم بمبدأ قانوني عالمي وهو الحق في الخصوصية، وانتهاك هذا الحق يمكن أن يؤدي إلى تجريد هذه الأدلة من مشروعيتها، وبالتالي إهمالها من قبل القضاء.

ثانياً- حق الخصوصية في مواجهة إجراءات الضبط والتفتيش:

حدد قانون أصول المحاكمات الجزائية أحكام الضبط والتفتيش في المادتين 33 و47 والمواد الممتدة من 98 حتى 105، وتحصر هذه المواد إجراء البحث عن الدليل ضمن نطاق أمر التفتيش الذي يستهدف جمع وتحريز المعلومات والأدلة التي تساعد على كشف الحقيقة فقط، دون أن يتعدى الأمر تفتيش وضبط مواداً وأشياء أخرى غير متعلقة بالجرم بشكل مباشر[43]. تثور أثناء تفتيش الحواسيب أو الأنظمة المعلوماتية مسألة مهنية سلطات التحقيق في عدم انتهاك مبدأ التناسبية (Principe de proportionnalité)

(42) المادة 2 من القانون رقم 140 / 99.

(43) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، المرجع السابق، ص538 وما يليها.

الذي يقضي بضرورة الفصل بين المعلومات أو الأشياء المتعلقة بالجريمة وتلك التي تتعلق حصراً بخصوصية الجاني أو المجني عليه، إن كان أثناء مرحلة التفتيش عن الدليل أو أثناء مرحلة جمع وحفظ المعلومات المضبوطة وإرسالها لتفريغها ووضعها في سياق ممنهج في محضر التحقيق، فوفقاً للمبدأ المذكور لا يجوز الاطلاع على المعلومات التي تعتبر خاصة أو شخصية وغير متعلقة بالجريمة موضوع التحقيق احتراما للحق في الخصوصية وحرية الأفراد بالحفاظ على بياناتهم الشخصية(44).

لقد أكد المشرع اللبناني على احترام مبدأ التناسبية في المادة 98 من قانون أصول المحاكمات الجزائية، فقد نصت على أنه: «إذا ضبطت أثناء التفتيش وثائق سرية فترقم ولا يطلع عليها سوى قاضي التحقيق وصاحبها....». ونص أيضاً على أنه: «لا يحق لقاضي التحقيق إفشاء مضمون أي برقية أو رسالة مضبوطة دون موافقة صاحب العلاقة»، وحظر في المادة 100 من ذات القانون من مغبة خرق سرية المهنة أثناء التفتيش في معرض ملاحقة المحامي. كذلك الأمر، تنص المادة 33 من ذات القانون على أن: «للنائب العام أن يدخل إلى منزل المشتبه فيه للتفتيش عن المواد التي يقدر أنها تساعد على إنارة التحقيق. له أن يضبط ما يجده منها وينظم محضراً بما ضبطه واصفاً إياه بدقة وتفصيل وأن يقرر حفظ المواد المضبوطة بحسب طبيعتها... وإذا وجد النائب العام أثناء التفتيش أشياء ممنوعة فيضبطها وإن لم تكن من المواد الناتجة عن الجريمة أو المستعملة فيها أو المتعلقة بها وينظم محضراً بها على حدة".

ويستقر اجتهاد المحاكم الفرنسية على احترام هذا المبدأ، فقد قررت محكمة التمييز أن: «المعلومات التي يجب على المحققين الحصول عليها هي فقط تلك التي تساعد في كشف الحقيقة، ولا يتعداها ما يتعلق بتواريخ وأماكن الإجازات الخاصة بالمتهم وعائلته التي لم يكن من داع لكشفها واستغلالها.....»(45). وفي ذات الاتجاه، أعلنت المحكمة براءة شخص بسب عيب في الإجراءات بعدما تبين لها أن الشرطة علمت بالجريمة التي ارتكبها من خلال فيلم موجود على هاتف محمول جرى تفتيشه بمناسبة وقوع جريمة مغايرة، وبررت المحكمة قراراها بأنه لم يكن يحق للشرطة تفتيش الهاتف الذي لم يكن أداة للجريمة الأولى ولا يؤدي تفتيشه للحصول على أدلة متعلقة بها– دون موافقة صاحب

(44) Pierre Kayser، La protection de la vie privée par le droit، Protection du secret de la vie privée، 3e éd.، Paris، Economica، 1995، n° 135، p. 235.

(45) Cass. Crim.، n. 0813 ،85.456– nov. 2008.

الشأن احتراما لحق الخصوصية[46].

وبالتالي، فإنه في ظل القانون الحالي، لا يمكن لهذا المبدأ أن يصمد بوجه الطبيعة الخاصة للمعلومات الموجودة داخل الحاسوب أو النظام المعلوماتي موضوع التفتيش. فالضابطة العدلية تقوم بنفسها أو بواسطة خبراء في بعض الأحيان بتفتيش الأنظمة وفقاً للإذن الممنوح لها بدخول الحاسوب أو النظام المعلوماتي، لكن ما هي الضمانة القانونية التي تكفل عدم قيامها بالتفتيش في المعلومات الشخصية، لا سيما أنها تستخدم برامج معلوماتية قادرة على الوصول إلى أية بيانات أو معلومات موجودة وفك رموز الشيفرة المتعلقة بها إذا كانت محمية، من دون معرفة صاحبها أو دون إذن من الشخص الذي له الحق في نقل هذه البيانات[47].

من ناحية أخرى، يثير التفتيش الإداري الذي يسمح به القانون أثناء إعلان حالة الطوارئ إشكالية كبيرة على هذا الصعيد، حيث يمكن لغير الضابطة العدلية أو الشرطة القضائية أن تجري تفتيشاً، عند وجود خطر على النظام العام حتى قبل وقوع جريمة. وقد نظم المشرع اللبناني في المرسوم الاشتراعي رقم 52 الصادر بتاريخ 5 آب 1967، الأحكام العرفية وحالة الطوارئ، عند تعرض الدولة للكوارث وحالة الحرب الخارجية أو الثورة المسلحة أو أعمال واضطرابات تهدد النظام والأمن العام، إذ يترتب على ذلك: «انتقال صلاحيات الشرطة إلى السلطات العسكرية التي ستمنح صلاحية فورية للمحافظة على الأمن، وتصبح صلاحياتها متجاوزة لقواعد الشرعية القانونية العادية، مثل تفتيش المنازل والمساكن ليلا ونهاراً....»[48]، حيث إنه أثناء حالة الطوارئ، «تتحرر السلطة الإدارية من موجب مراعاة أحكام القوانين والأنظمة، بما في ذلك الحريات العامة المكفولة دستورياً وقانونياً، كالحد من الحرية الشخصية أو الملكية الفردية أو حرية التجارة ، شرط أن تكون تدابيرها محصورة بالظرف الذي أملاها وضمن مواجهته»[49].

وكانت قد أثيرت مسألة تفتيش المعلومات الإلكترونية في فرنسا من قبل السلطة الإدارية

(46) Cass. Crim.، n. 1530 ،86693– mars 2016.

(47) Alain Bensoussan، L'accés des autorités aux données personnelles، Partie I، JTIT International، juillet 2013، n. 4، p. 2 et s.

(48) المرسوم الاشتراعي اللبناني رقم 52 الصادر بتاريخ 5 آب / أغسطس 1967.

(49) د. يوسف سعد الله الخوري، القانون الإداري العام – الجزء الثاني – القضاء الاداري – مسؤولية السلطة العامة، ط2، بيروت، 1998، ص143.

أثناء حالة الطوارئ، فقد صدر حديثاً القانون رقم 2016/987 الصادر في 2016/7/21 المعدل للقانون رقم 55/385 الصادر بتاريخ 1955/4/3 المتعلق بتنظيم حالة الطوارئ، والذي سمح للسلطة الإدارية بتفتيش أي بيانات أو معلومات إلكترونية تتعلق بالخطر الذي يهدد الصالح العام، واستغلالها بعد طلب الإذن من القاضي الإداري.

وتطبيقاً للقانون المذكور، قام قائمقام (Prefet) قطاع مدينة (Allier) الفرنسية بإعطاء إذن إداري استنادا إلى قانون الطوارئ المذكور أعلاه، بحجة التهديدات الإرهابية التي تعرضت لها فرنسا مؤخراً، حيث كان هذا الإذن معللا بالحفاظ على الأمن والنظام العام. وأثناء التفتيش، تم نسخ المعلومات الموجودة داخل الهاتف المحمول للشخص المعني والتحفظ عليها لدى المسؤول عن إجراء التفتيش، دون استغلالها بانتظار الإذن بذلك من القضاء. لكن قاضي العجلة في المحكمة الإدارية المختصة رفض إعطاء الإذن بحجة عدم وقوع جريمة تتطلب الاطلاع على تلك المعلومات واستغلالها[50]. طعن وزير الداخلية بالقرار المذكور أمام مجلس الدولة الذي بدوره فسخ قرار المنع وسمح باستغلال المعلومات استنادا إلى القانون رقم 2016/7/21، واعتبر أن: «إجراءات التفتيش والحجز واستغلال المعلومات الناتجة عنها لا يعد تعديا على الحياة الخاصة، طالما أن تلك الإجراءات متوافقة مع المادة 11 من القانون الصادر سنة 1955»[51].

من ناحية أخرى، أعطى القانون في كل من الولايات المتحدة الأميركية وفرنسا الحق لسلطات التحقيق إجبار شركات مواقع التواصل الاجتماعي وموردي الخدمة على تقديم معلومات مخزنة لديهم دون حاجة للحصول على أمر قضائي. فقد نصت المادة 60–2 من قانون الإجراءات الجزائية الفرنسي على إلزام المؤسسات الخاصة بوضع جميع المعلومات التي تساعد في كشف الحقيقة بتصرف سلطات التحقيق، وكذلك منح قانون Communication Act The Stored الصادر سنة 1986 الأميركي سلطات التحقيق القدرة على إجبار مزودي الخدمة على تسليم المراسلات والتغريدات التي يقوم بها الأفراد، إضافة إلى السجلات المتعلقة بالزبائن مثل الاسم والعنوان وذلك في حالات محددة[52]. لكن القانون ذاته يوفر حماية للحياة الخاصة للأفراد، من خلال تحديد مدة

(50) Juge des référés du tribunal administrative، ordonnance n: 1601380 du 8 août 2016.

(51) CE، ordonnance du 12 août 2016، ministère de lOintérieur c/ M. B...،n: 402348.

(52) سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأميركي، المرجع السابق، ص 14 وما يليها.

الاحتفاظ بالمحتوى إلكترونياً وهي 180 يوماً أو أقل بعد الحصول على إذن بذلك. وإذا اضطرت تلك الأجهزة إلى الاحتفاظ بتلك السجلات أكثر من هذه المدة، تكون مجبرة إما الحصول على إذن إداري، أو الحصول على أمر من المحكمة المختصة بموجب المادة 2703 (d) من القانون المذكور أعلاه.

الفرع الثاني

احترام الحرية الشخصية للأفراد

تنص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه: «لا يعرّض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه أو سمعته. ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات». كما أنه يتبين من مفهوم المادة 14 من الدستور اللبناني أن حماية الفرد من التدخل في حياته الخاصة ومراسلاته واتصالاته مصانة.

وفي الكويت، أكد المشرع على احترام هذا الحق المصان في الدستور[53]، ويتبين ذلك من خلال مقارنة بسيطة بين القانون رقم 37 لسنة 2014 والقانون رقم 85 المعدل لبعض أحكامه والصادر عام 2015، لا سيما البند م من المادة 3 [54]، حيث ورد في التعديل إضافة عبارة "وذلك إعمالاً للحق الدستوري في كفالة الحرية الشخصية"، حيث جاء هذا التعديل ليؤكد حرص المشرع على حماية الفرد من أي انتهاك لحرياته وخصوصياته حتى ولو كان ذلك بمناسبة قيام السلطة العامة بإجراءات ينص عليها القانون.

يجدر القول إنه في غير حالات الجريمة المشهودة، لا يمنح إذن التفتيش إلا بعد التأكد من وقوع جريمة[55]، وهذا يعني أنه يجب أن يكون قد أجرى مسبقاً استقصاءات كافية للتأكد من ارتكاب شخص لجريمة معينة تجنباً لوقوع خطأ يؤدي إلى المساس بحرية الشخص المعني. فإذا كان باستطاعة النيابة العامة وبمساعدة الضابطة العدلية طبعاً إجراء الاستدلالات اللازمة في حالات الجرائم التقليدية، فكيف يمكن أن تقوم بذلك بمناسبة وقوع جريمة على شبكة الإنترنت، وكيف يمكن أن تحصل على الأدلة الكافية دون

(53) تنص المادة 30 من الدستور الكويتي على أن»الحرية الشخصية مكفولة».

(54) تنص المادة 3 (البند م) من القانون اللبناني رقم 37 لسنة 2014 المعدل بالقانون رقم 58 لسنة 2015 على أن: « تعقب مصدر أي موجة راديوية للتحقق من ترخيص ذلك المصدر دون المساس بسرية الرسائل....، وذلك إعمالاً للحق الدستوري في كفال الحرية الشخصية».

(55) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، المرجع السابق، ص451 وما يليها.

الدخول إلى حاسوب المشتبه فيه، والاستناد إلى أي دليل لإثبات التهمة عليه، وقد أثيرت هذه المسألة في لبنان مؤخراً، وما لبثت أن تحولت إلى قضية رأي عام عرفت ب «قضية زياد عيتاني»، حيث تتلخص وقائع الدعوى بقيام جهاز أمن الدولة باتهام ممثل مسرحي يدعى زياد عيتاني بجرم التعامل مع إسرائيل، استنادا إلى صورة (screenshot)[56] تظهر تواصل هذا الأخير مع ضابطة إسرائيلية، فتم توقيفه بجرم التعامل والادعاء عليه والتحقيق معه ما يقارب الثلاثة أشهر، ليتبين أخيراً أن الشخص المذكور بريء ولا علاقة له بالموضوع، وما كان إلا ضحية لعملية انتقام قامت بها إحدى الضابطات اللبنانيات بمساعدة قرصان معلوماتي الذي استطاع إجراء محادثة وهمية بين زياد والضابطة الإسرائيلية[57].

كما أن عادة ما تكون الأنظمة المعلوماتية أو الحواسيب مزودة بنظام حماية أو كلمة سر تحول دون دخول أي شخص غير مصرح له، ولذلك يثور تساؤل حول مدى إمكانية المحققين إكراه هذا الأخير على الإفصاح عن كلمة السر أو إجباره على فك الشيفرة ؟

يقودنا هذا السؤال إلى البحث في مسألتين هامتين: المسألة الأولى متعلقة بمبدأ عدم إجبار المتهم على تقديم دليل ضد نفسه، هذا المبدأ المكرس في الفقرة 3 من المادة 14من العهد الدولي المتعلق بحقوق الإنسان المدنية والسياسية الصادر بتاريخ 16/12/1966 والتي تنص على أنه: «لا يجوز إكراه الشخص على الشهادة ضد نفسه أو الاعتراف بذنب»، إذ أن إفصاح الشخص المتهم أو المشتبه فيه عن كلمة السر أو إعطاء المحققين مفتاح فك الشيفرة كأنما هو عمل يقوم فيه بالاعتراف على نفسه عبر تقديم الأدلة التي تثبت إدانته، في حين أن هذه المهمة مناطة حصراً في سلطتي الادعاء والاتهام دون غيرهما[58].

أما المسألة الثانية، فتتعلق بمدى احترام مبدأ حق المتهم في الصمت[59] الذي يستند إلى قرينة البراءة، المصدر الأساسي لجميع الضمانات المقررة للمتهم أو للمشتبه فيه. فهو

(56) علماً أن القضاء الغربي يجمع على عدم قبول هذا الدليل كوسيلة إثبات.

(57) قضية زياد عيتاني تثير شكوكاً بنزاهة الأمن، تقرير منشور على العربية نيوز، بتاريخ 5/1/2018 منشور على الموقع التالي: https://www.skynewsarabia.com/

(58) P. Quarré، Le droit au silence، J.T.، 1974، p. 526. R. Garnon et A. Garnon، note sous l'arrêt J.C.P.، 1993، II، n° 22.073، p.244

(59) ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012، ص 132. هلالي عبداللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط 2، دار النهضة العربية للنشر، القاهرة، 2008، ص 160.

بمثابة الدستور الأساسي لضمان حريته الشخصية وتدعيم موقفه أمام جهة الإدعاء، فأصل البراءة يعني أن القاضي و سلطات الدولة كافة يجب عليها أن تعامل المتهم، و تنظر إليه على أساس أنه لم يرتكب الجريمة محل الاتهام ما لم يثبت عليه ذلك بحكم قضائي غير قابل للطعن بالطرق العادية[60].

كما أن المشرع اللبناني كرس مبدأ حق المتهم في السكوت في مختلف مراحل الدعوى الجزائية لا سيما في مرحلة التحقيق الأولي، حيث نصت المادة 41 من قانون أصول المحاكمات الجزائية على أنه: "..له أن يستجوب المشتبه فيه شرط أن يدلي بأقواله بإرادة واعية حرة ودون استعمال أي وجه من وجوه الإكراه ضده. إذا التزم الصمت فلا يجوز إكراهه على الكلام"[61]. وكذلك أكد المشرع الفرنسي على هذا الحق في المادة 1-63 من قانون الإجراءات الجزائية الفرنسي. لكن المحكمة الأوروبية لحقوق الإنسان كان لها رأي مغاير حيال هذه الحجج، حيث أعلنت أن: "الحقوق الأساسية المنصوص عليها في المادة السادسة من الاتفاقية الأوروبية لحقوق الإنسان، صراحةً أو ضمناً، ليست حقوقاً مطلقة، وإن التقييد المحدود لهذه الحقوق يعد مقبولاً إذا كانت السلطات العامة قد استهدفت من وراء ذلك تحقيق مصلحة عامة ملائمة وواضحة طالما أن هذه القيود المفروضة ليست أكثر مما يتطلبه الموقف، وحق الإنسان في عدم تجريم نفسه ليست من الحقوق التي وردت بصورة صريحة في الاتفاقية، كما أنه ليس من الحقوق المطلقة، وبالتالي يمكن تقييده لإقامة التوازن بين الحق في المحاكمة العادلة وحماية المجتمع من خطر الإجرام"[62].

لقد حسم المشرع الفرنسي مسألة إمكانية الدخول إلى المعلومات الموجودة داخل النظام

(60) ضياء محمود، حق الصمت في الدعوى الجزائية، مجلة جامعة البعث، 2017، المجلد 39، عدد 136، دمشق، ص116 وما يليها.

(61) كذلك تنص المادة 47 أنه : « إذا امتنعوا أو التزموا الصمت فيشار إلى ذلك في المحضر ولا يحق لهم إكراههم على الكلام أو استجوابهم تحت طائلة بطلان إفاداتهم. وتنص المادة 77 أنه: «على قاضي التحقيق أن يراعي مبدأ حرية إرادة المدعى عليه أثناء استجوابه وأن يتأكد من أنه يدلي بإفادته بعيداً عن كل تأثير خارجي عليه سواء أكان معنوياً أم مادياً وإذا رفض المدعى عليه الإجابة والتزم الصمت فلا يحق لقاضي التحقيق أن يكرهه على الكلام». وأيضاً تنص المادة 180 على أنه: « إذا رفض المدعى عليه الإجابة والتزم الصمت فلا يحق للقاضي أو المدعي أن يكرهه على الكلام. لا يجوز للقاضي أن يتخذ من صمته قرينة لإدانته». كما تنص المادة 253 على أنه: « إذا رفض المتهم الإجابة والتزم الصمت فلا يجوز إكراهه على الكلام».

(62) CEDH، 1er décembre 2009، Ahmet Engin Satir c. Turquie.

من دون موافقة صاحب العلاقة، دون أن يكون ذلك الإجراء انتهاكا للحياة الخاصة أو الحرية الشخصية للمشتبه فيه أو للمتهم. فقد نص القانون رقم 267–2011 الصادر بتاريخ 14/3/2011 والمعروف بقانون LOPPSI II ، لا سيما المواد 34 و 36 و39 على السماح لرجال التحقيق بعد الحصول على إذن قضائي وضع أجهزة تقنية أو أي برامج معلوماتية متخصصة تكون مهمتها الوصول إلى المعلومات حتى دون إذن صاحبها، وكذلك الدخول إليها من أي مكان وتسجيلها والتحفظ عليها، لكن جميع هذه الإجراءات تبقى تحت مراقبة القضاء، مع الأخذ بعين الاعتبار أن هذه الإجراءات تتخذ فقط في حال الجرائم المنظمة والجرائم الإرهابية والجرائم المتعلقة بالانتهاكات الجنسية ضد الأطفال وجرائم غسيل أو تبييض الأموال. إضافة إلى أن القانون في كل من الولايات المتحدة الأميركية وفرنسا – كما ذكرنا سابقاً– أعطى الحق لسلطات التحقيق على إجبار شركات مواقع التواصل الاجتماعي وموردي الخدمة على تقديم معلومات مخزنة لديهم دون حاجة للحصول على أمر قضائي.

وكذلك الأمر، نصت المادة 32 من القانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية في الكويت على أنه: «لا يجوز في – غير الأحوال المصرح بها قانوناً – للجهات الحكومية أو الهيئات أو المؤسسات العامة أو الشركات أو الجهات غير الحكومية أو العاملين بها الاطلاع دون وجه حق أو إفشاء أو نشر أية بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة المعالجة الإلكترونية.....». وبالتالي، فإنه وفقاً لمفهوم المخالفة، يمكن لسلطات التحقيق الطلب من هذه الجهات تزويدها بالمعلومات المتعلقة بالمشتبه به.

والخلاصة، أنه وفقاً لهذه القوانين يمكن لسلطات التحقيق الطلب من هذه المؤسسات تزويدهم بكلمة السر ومحتوى المعلومات، دون الوقوف على موافقة الشخص المعني بالموضوع([63]). لذلك فإنه يقتضي على المشرع اللبناني التدخل لحسم هذا الجدل ووضع قواعد صريحة يحدد من خلالها صلاحيات سلطات التحقيق في هذا المجال لكي لا تبقى حريات الأفراد وخصوصياتهم معرضة للانتهاك.

(63) سامي حمدان الرواشدة، مرجع سابق، ص 42.

المطلب الثالث

وجوب احترام مبدأ الإقليمية

انعكس الطابع الدولي لشبكة الإنترنت على الجريمة الإلكترونية، وتخطت أبعادها إطار القوانين المحلية، حيث أصبحت سلطات التحقيق في أي دولة عاجزة عن استخلاص الأدلة وتتبع الجناة بمفردها، بل هي بحاجة حكماً لتدخل ومساعدة من قبل سلطات التحقيق في الدول الأخرى. لذلك ثار التساؤل حول حدود تطبيق قواعد الإجراءات الجزائية في ظل عالمية الجريمة الإلكترونية وتخطيها للحدود اللبنانية حول طبيعة أو شكل التعاون الذي يمكن أن يجري بين سلطتي التحقيق اللبنانية والأجنبية، علماً أن مسألة التنازع الإيجابي بين الدول حول ادعاء كل منها الاختصاص لمحاكمها وقانونها للنظر بالجريمة التي تقع عبر الإنترنت ما زالت تشكل إشكالية قانونية في الفقه والقضاء[64].

تضع التشريعات الجنائية في العالم نصوصاً صريحة تحدد من خلالها الاختصاص لمحاكمها. فقد نص المشرع اللبناني في المادة 15 من قانون العقوبات على مبدأ إقليمية هذا القانون بالقول إنه: «– تطبق الشريعة اللبنانية على جميع الجرائم المقترفة في الأرض اللبنانية. تعد الجريمة مقترفة1 –– إذا تم على هذه الأرض أحد العناصر التي تؤلف الجريمة، أو فعل من أفعال جريمة غير متجزئة أو فعل اشتراك أصلي أو فرعي– 2 – إذا حصلت النتيجة في هذه الأرض أو كان متوقعا حصولها فيها». ويقصد بهذا المبدأ تطبيق قانون العقوبات اللبناني على كل جريمة ترتكب في إقليم الدولة دون النظر إلى جنسية الجاني أو المجني عليه[65]، أي سواء كان الجاني أو المجني عليه مواطنا أم أجنبيا. ويطبق هذا المبدأ سواء وقعت الجريمة كلها، أو جزء منها على إقليم الدولة[66].

تتعلق مسألة تطبيق القانون الجزائي بسيادة الدولة على إقليمها والتي يقتضي من جهة أولى، ألا يسري غير قانونها الوطني على أية جريمة تقع ضمن نطاق هذا الإقليم (الوجه الإيجابي)، وألا يمتدّ من جهة أخرى تطبيق ذلك القانون إلى خارج حدود إقليمها

(64) André Huet، Le droit pénal international et Internet، les petites affiches، 10 Nov. 1999، p.39 n°224.

(65) تمييز لبناني، قرار رقم 25 تاريخ 1997/2/25، منشور في القاعدة البيبليوغرافية، مركز المعلوماتية القانونية، الجامعة اللبنانية.

(66) M–D. Torbey، L'internationalisation du droit pénal، le Liban dans le monde arabe، L.G.D.J.، Paris، 2007، n°42.

(الوجه السلبي). ولأنه وفقاً لمبدأ وحدة الاختصاصين التشريعي والقضائي، ينسحب مبدأ الإقليمية على تحديد النطاق المكاني للضابطة العدلية وقضاة التحقيق والحكم التي تعمل وفقاً للقواعد القانونية المنصوص عليها في قانون أصول المحاكمات الجزائية، فهم يستمدون سلطتهم من هذه القواعد ويتقيدون بها خلال اتخاذ الإجراءات المناسبة لتتبع الجناة وجمع الأدلة التي تساعد على كشف الحقيقة ولا يحق لهم تطبيق أي قانون جزائي أجنبي على إقليمهم[67].

يثير احترام مبدأ الإقليمية إشكاليات عديدة على الصعيد القانوني خلال البحث عن الأدلة التي تساعد على كشف الجرائم المرتكبة في العالم الافتراضي[68]. فقد يتبين لرجال التحقيق أن النظام المعلوماتي الخاضع للتفتيش بموجب الإذن الصادر وفقاً للإجراءات التي ينص عليها القانون اللبناني موصولاً بأجهزة أو أنظمة أخرى تحتوي على معلومات تفيد التحقيق وموجودة داخل أو خارج إقليم الدولة اللبنانية. عادة ما يحدد في إذن التفتيش المكان المراد تفتيشه، بحيث لا يحق لرجال الضابطة العدلية الخروج عن النطاق المكاني المحدد. لكن ماذا عن الإذن الممنوح لتفتيش نظام معلوماتي تبين أن له امتداداً مع أنظمة معلوماتية أخرى في أكثر من مكان على الأراضي اللبنانية، بل ويمكن أن يصل هذا الامتداد إلى خارج الحدود. ففي هذه الحالة، لا يحق للمحققين متابعة التحقيق لعدم وجود إذن قانوني بذلك، حيث لا يستطيعون الدخول إلى النظام دون إذن وإذا أرادوا الاستحصال عليه وفق الآلية التي رسمها القانون سيتطلب الأمر بعض الوقت، يمكن أثناءها أن يضيع الدليل أو يعمد مرتكبي الجريمة إلى إخفائه[69].

ففي الحالة الاولى، إذا كان النظام المعلوماتي موضوع التفتيش موصولاً بأنظمة أخرى، فلا بد لرجال التحقيق الحصول على إذن جديد للدخول إليها، هذا طبعاً بعد التأكد من أنها تحتوي على أدلة تفيد التحقيق. وعليه، فلا تستطيع الدخول من تلقاء نفسها في غياب النص الصريح الذي يجيز لها ذلك، حيث إنه لا يمكن التوسع في تفسير النصوص القانونية، لا سيما تلك المتعلقة بالحرية الشخصية. وقد التفت المشرع الفرنسي إلى هذه

(67) B.Bouloc، Procédure Pénale، 20ème édition، Dalloz، 2006، n°537.

(68) C.Marsella ، L'effectivité du processus répressif dans le traitement de la cybercriminalité، enquête sur le système judiciaire français، thèse universitaire، Lille 3، 2005، n°235 ets.

(69) M.Habhab، le droit pénal libanais a l'épreuve de la cybercriminalité، sader، 2012، p.176 et s.

الحالة، فسمح بشكل صريح في المادة 1-57 من قانون الإجراءات الجزائية، المعدلة بموجب القانون رقم 239/2003 لسنة 18/3/2003 الخاص بحفظ الأمن الداخلي[70]، لرجال الشرطة والتحقيق توسيع دائرة التفتيش دون الرجوع إلى النيابة العامة شرط أن يكون ذلك النظام أو تلك الأجهزة المرتبطة بالنظام موضوع الجريمة موجودة داخل حدود الدولة الفرنسية. ويكون القانون الفرنسي قد وسع بذلك من نطاق عمل المحققين في هذا السياق الذين أصبح بإمكانهم الدخول إلى أي نظام معلوماتي للتفتيش فيه عن بيانات أو معلومات تساعد في كشف خيوط الجريمة، دون أن يعتبر ذلك تعد على الحياة الخاصة للفرد، طالما أن المشرع الفرنسي قد ارتأى تغليب المصلحة العامة على المصلحة الفردية. وكذلك فعل المشرع الفدرالي الأميركي في الفقرة الأولى من المادة 41 من قانون الإجراءات الجنائية الفدرالي والتي نصت على ذات الأحكام التي تباناها التشريع الفرنسي. أما الحالة الثانية، وهي إذا كان الجهاز أو النظام موضوع التحقيق موصولاً بأنظمة أخرى خارج إقليم الدولة اللبنانية، فإنه بطبيعة الحال لا يحق لرجال التحقيق الدخول إليها دون إذن الدولة المعنية، حيث يقتضي إجراء إنابة قضائية للسلطات المختصة بهذه الدولة لمتابعة التفتيش، وفي كلتا الحالتين، يمكن لهذه الإجراءات أن تعيق الوصول إلى الحقيقة، نظراً لسرعة اختفاء الدليل في العالم الإلكتروني من جهة وبطء إجراءات الإنابات القضائية من جهة أخرى[71].

رفض الفقه والقضاء الغربي الإجازة لسلطات التحقيق بتفتيش نظم الحاسب الآلي الموجودة خارج إقليم الدولة التابعة لها حتى ولو كانت تلك الأنظمة مرتبطة بنظام داخل تلك الدولة، ما لم توجد اتفاقية دولية في هذه الشأن، ذلك أن السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى وخرقاً للقوانين الثنائية والوطنية المتعلقة بالتعاون القضائي[72].

من جهتها، فقد أشارت الاتفاقية الأوروبية المتعلقة بمواجهة الجرائم الإلكترونية والموقعة في بودابست سنة 2001 تلك المسألة. فقد نصت بالمادة 29 على وجوب التعاون

(70) والمعدلة أيضاً بموجب القانون رقم 731/2016 الصادر في 3/6/2016 الخاص بتعزيز مكافحة الجريمة المنظمة وجرائم الإرهاب وتمويلها.

(71) M. Habhab، le droit pénal libanais à l'épreuve de la cybercriminalité، sader، 2012، p.331 et s.

(72) راجع بهذا الخصوص د. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية للنشر، القاهرة، 2009، ص 656 وما يليها.

بين الدول في هذا السياق، بعدما أكدت في المادة 19 على ضرورة قيام الدول الموقعة على الاتفاقية على ضرورة تشريع التفتيش في البيئة المعلوماتية لإزالة كل العوائق أمام التعاون الدولي في هذا المجال. وقد قامت العديد من الدول بتبني هذه الاتفاقية وتعديل تشريعاتها لتتلاءم مع الجرائم المرتكبة في العالم الافتراضي، فقد نصت المادة 1-57 من قانون الإجراءات الفرنسي المعدلة على أنه يمكن لرجال التحقيق الدخول إلى المعلومات المخزنة خارج إقليم الدولة الفرنسية شرط أن يكون الدخول إلى هذه المعلومات مسموحاً في فرنسا.

وقد تبنى القضاء الأميركي هذا الاتجاه، حيث قررت محكمة الاستئناف الفيدرالية في مانهاتن في حكم حديث لها صادر بتاريخ 2016/7/14 أن إذن التفتيش الصادر في الولايات المتحدة الأميركية لا يسمح للسلطات الاميركية المختصة الحصول على المعلومات المخزنة لدى شركة مايكروسوفت في إيرلندا، لأن إعمال هذا الإذن خارج الأراضي الأميركية ليس له أثر قانوني بالنسبة للقضاء الأميركي(73). جاء هذا القرار بعدما كانت سلطات التحقيق الأميركية قد طلبت من شركة مايكرسوفت تزويدها بالمعلومات المخزنة لدى فرعها الكائن في إيرلندا، حيث يمكن لهذه الأخيرة أن تقوم بذلك بطريقة تقنية سهلة جداً بدلاً من اللجوء إلى إجراء إنابات قضائية دولية، وذلك لكسب الوقت. فالمحكمة أعلنت أن المشرع الأميركي هو وحده من يجيز التمدد في مسألة الاختصاص بموجب نصوص صريحة تنص على ذلك كما يفعل في بعض الجرائم المتعلقة بالإرهاب(74).

(73) Microsoft Corp. v. United States، 5. 829 F.3d 197 (2d Cir.92016 /12/).

(74)Winston Maxwell، édition Multimédia، 19 sep. 2016، أنظر تعليقاً على هذا القرار: n.152

المبحث الثاني

حدود قبول القاضي لأدلة الإثبات الجنائي في البيئة الرقمية

استتبع التطور المستمر للجريمة المعلوماتية والوسائل المستخدمة من قبل الفاعلين تغيير الأسلوب المعتمد من قبل رجال التحقيق للبحث عن الأدلة، لأنه يجب أن تكون هذه الوسائل متلائمة وفعالة مع التقنيات التي يتوصل إليها المجرمون، لا سيما أنه يقتضي على رجال التحقيق سرعة استخلاص الأدلة قبل اختفائها. تعتبر التحريات التي يقوم بها رجال الضابطة العدلية لجمع الأدلة من قبيل الأعمال القانونية التي نص عليها المشرع في قانون الإجراءات الجزائية. ويشترط للبدء بها وجود قرائن وأمارات قوية على وقوع جريمة. فالهدف من التحريات هو الوصول إلى الحقيقة بفاعلية وكفاية. كما يجب أن تتوافر في كل عنصر من عناصر الإثبات الشروط والمبادئ التي توازن بين تحقيق المصلحة العامة والحفاظ على حقوق الأفراد. فإذا كان قانون أصول المحاكمات الجزائية اللبناني قد أكد في المادة 179 على حرية استخلاص الدليل[75]، إلا أنه لم ينظم بعد القواعد الخاصة بكيفية استخلاصه في البيئة الرقمية. لذلك يقتضي البحث في هذا الجزء من الدراسة في مدى إمكانية استيفاء الأدلة الرقمية ضمن إطار الحفاظ على مبدأ المشروعية لكي لا تفقد قوتها الثبوتية أمام القضاء. وعليه، فإذا كانت القاعدة العامة تقتضي أن يكون استيفاء الأدلة محاطاً بمبدأ المشروعية (المطلب الأول)، إلا أن هذه القاعدة ليست مطلقة في ظل البحث الدائم على الحقيقة وملاحقة المجرمين المرتكبين لجرائم يصعب تحديد عناصرها بسهولة ومنها الجرائم الإلكترونية (المطلب الثاني).

المطلب الأول

نطاق تطبيق مبدأ مشروعية الدليل

يرى بعض الفقه أن القاعدة العامة تقتضي أن يكون استيفاء الأدلة محاطاً بمبدأ المشروعية[76]، باعتبار أن عدم احترام هذا المبدأ يفقد الدليل قيمته القانونية ولا يمكن التعويل عليه في الإثبات[77]. كما وأنه ضماناً لحق الدفاع، يجب أن تناقش الأدلة بشكل

(75) تنص المادة 179 من قانون أصول المحاكمات الجزائية اللبناني أنه: «يمكن إثبات الجرائم المدعى بها بطرق الإثبات كافة ما لم يرد نص مخالف. لا يمكن للقاضي أن يبني حكمه إلا على الأدلة التي توافرت لديه شرط أن تكون قد وضعت قيد المناقشة العلنية أثناء المحاكمة. يقدر القاضي الأدلة بهدف ترسيخ قناعته الشخصية».

(76) J. Bouisson، Procédure pénale، Litec، édition 2، 2002، p.471.

(77) د. محمد ذكي أبو عامر، الإثبات في المواد الجزائية، دار الجامعة الجديدة، الإسكندرية، 2011،

علني أمام القضاء وفي حضور الخصوم، بحيث إن المحكمة لا يمكن أن تبني قرارها إلا على الحجج والأدلة التي أتيح للخصوم مناقشتها علنياً. والجدير بالقول، إن هذه القواعد تستهدف الأدلة بمجملها، بما فيها تلك التي تتمتع بطابع رقمي، لأن هذه القواعد هي عبارة عن مبادئ مسلم بها ولا يمكن الانحراف عنها. فاستخدام الوسائل العلمية الحديثة في الحصول على الدليل الإلكتروني وفقاً للقواعد العامة جائز طالما أنها تستخدم في إطار الشرعية الإجرائية[78].

يبقى قبول الدليل الإلكتروني مرتبطاً بتضافر باقي وسائل الإثبات الأخرى التي تساعد القاضي الجنائي على تكوين قناعته. فالهدف الأساسي من الدليل الجنائي بشكل عام هو الكشف عن الحقيقة بغية تحقيق العدالة، لكن هذه الغاية تعترضها في بعض الأحيان مسألة الشرعية في الوصول إلى حقيقة الإثبات، وذلك من خلال تقيد رجال التحقيق بكافة الضمانات القانونية الإجرائية والموضوعية التي تقتضيها عملية الحصول على الدليل. فوفقاً لبعض الفقه فإن شرعية محاكمة المتهم تتعلق بشرعية الحصول على الدليل الذي يوصل إلى الحقيقة[79].

تستند فكرة شرعية الحصول على الدليل الجنائي إلى عدة مصادر قانونية، دولية ومحلية. ومن أهم المصادر الدولية الاتفاقيات الدولية والإعلان العالمي لحقوق الإنسان اللذين نصا على وجوب تأمين محاكمة عادلة للمتهم[80]. أما على الصعيد الداخلي، فقد نص قانون أصول المحاكمات الجزائية في المادة 151 على وجوب اعتماد «المحكمة في اقتناعها على الأدلة المستمدة من التحقيق الذي أجرته في القضية أو من التحقيقات السابقة على المحاكمة، ولها الحرية المطلقة في ترجيح دليل على دليل وتكوين اقتناعها حسبما يوحيه إليه ضميرها. لا يجوز للقاضي أن يعتمد في حكمه على معلوماته الشخصية». فأهم أهداف هذا القانون وضع الأسس والضوابط لاستخلاصه الأدلة وتأمين محاكمة عادلة للمتهم وحفظ حقوقه التي نص عليها الدستور.

ص122. د. عبد الحكيم فودة، أدلة الإثبات والنفي في الدعوى الجنائية في ضوء الفقه والقضاء، منشاة المعارف، الإسكندرية، 2007، ص194.

(78) د. هلالي عبداللاه أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، الطبعة الأولى، دار النهضة العربية للنشر، القاهرة، 1997، ص 121.

(79) M. Mekki، Vérité et preuve، univ. Paris 13، I.R.D.A.، 2013، p.4

(80) المادة 10 من الإعلان العالمي لحقوق الإنسان والمادة 1/14 من العهد الدولي للحقوق المدنية والسياسية الصادر عام 1966.

كما وأن أحكام القضاء تؤكد على احترام مبدأ المشروعية كأساس للوصول إلى الحقيقة، دون الأخذ به على إطلاقه، باعتبار أنه يمكن أن يشكل تطبيقه في بعض الأحيان عائقاً أمام تحقيق العدالة[81]. وقد كان للقضاء الفرنسي مبرراته للخروج عن مبدأ المشروعية، فإثبات بعض الجرائم الهامة التي تهدد حياة الشعب كان يعوزها الدليل. ولذلك كان رجال الشرطة يجدون أنفسهم مدفوعين إلى استعمال وسائل غير سليمة تمكنهم من ضبط الجريمة وفاعليها. فكان على القضاء في هذه الحالات أن يوازن بين اعتبارات متناقضة: حماية أمن الجماعة التي تستدعي غض النظر عن تجاوزات رجال الشرطة عند ملاحقة المخلين بالأمن والقبول بأية وسيلة إذا كان من شأنها تحقيق هذه الغاية، وحماية حقوق الأفراد المشروعة وعدم المساس بها إلا ضمن المعايير التي يحددها القانون. وقد أخذ القضاء الفرنسي في تلطيف حدة هذا التناقض، بطريقة لا تهدر إحداهما الأخرى بالكامل وتوصل إلى حلول مختلفة بعد إعمال تقديره في كل قضية على حدة. فتسامح بعض الشيء في حالات خاصة كان الخروج عن مبدأ الشرعية تحتمه ضرورة ناتجة عن أهمية الجريمة أو طبيعة الحقوق المعتدى عليها كأمن الدولة أو كيانها المالي، مشترطاً أن يبقى هذا الخروج ضمن الحد المألوف والجائز التسامح به وأن لا يتحول إلى أساليب مرتجلة وغير سليمة[82]. لكن إذا كان هذا الاتجاه والذي نؤيده هو الراجح حالياً، فإنه هناك اتجاها آخراً يسانده بعض أحكام القضاء ينادي بضرورة احترام مبدأ المشروعية[83]. كما سبق وأشرنا، يسعى رجال الشرطة دائماً للسيطرة على الجريمة، لا سيما الجرائم التي توصف بالخطيرة، كالإرهاب وتبييض الأموال والانتهاكات الجنسية الجسيمة ضد الأطفال. لذلك تحاول الاستفادة من الخدمات التقنية

(81) د. عبد الحكيم الحكماوي، الإثبات في الجريمة الإلكترونية، سلسلة ندوات، محكمة الاستئناف، الرباط – المغرب تحت عنوان تأثير الجريمة الإلكترونية على الائتمان المالي، العدد السابع، 2014، ص 156.

(82) راجع بهذا الخصوص محكمة التمييز اللبنانية التي أسهبت في إظهار مبررات القضاء الفرنسي حول التخلي عن مبدأ مشروعية الدليل في بعض الجرائم، قرار رقم 119 لسنة 1993، تاريخ 7/7/1993، القاعدة البيبليوغرافية، مركز المعلوماتية القانونية – الجامعة اللبنانية.

(83) د. محمد ذكي أبو عامر، الإثبات في المواد الجزائية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 122. د. عبد الحكيم فودة، المرجع السابق، ص 170، إدريس النواذلي، موقف القضاء من الجريمة الإلكترونية، منشورات كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، 2010، ص 103. د. عبد الحفيظ بلقاضي، التجريم والعقاب في أقوى نزعاتهما تسلطاً: القانون الجنائي للعدو، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2006، العدد 26، ص 396.
Myriam Quéméner ،Yves Charpenel ،Cybercriminalité – Droit pénal appliqué، 2010Economica ،p،171.Cass .Crim 4 .juin ،2008 Bull .Crim ،2008 ،n141.

التي تمنحها شبكة الإنترنت للمستخدمين ومن وجود مواقع التواصل الاجتماعي[84]. فمثلما تشكل هذه الخدمات وسيلة ناجعة للمجرمين لإتمام جرائمهم، فإنها تعتبر أيضاً ورقة رابحة لرجال التحقيق الذين أصبحوا يملكون القدرة على اختراق ودخول أي موقع بشكل سهل وفوري، دون تطلب مهارة كبيرة، و الاطلاع على ملايين المعلومات وتجميعها وتتبعها.

وقد أجاز القضاء الأميركي هذه الطريقة، فقد رفضت المحكمة الدفع المقدم من قبل المتهم حول بطلان الدليل الذي تم الحصول عليه من حسابه الشخصي على فيسبوك على سند من القول أن أجهزة الشرطة قد انتهكت حقوقه المتعلقة بالخصوصية المنصوص عليها في الدستور الأميركي. فالمحكمة اعتبرت أنه: «إذا كانت إعدادات الضبط المتعلقة بالخصوصية على «فيسبوك» تسمح برؤية المراسلات من قبل الأصدقاء فتستطيع أجهزة الدولة الولوج إلى هذه المعلومات من خلال تعاون أحد الأشخاص المسجل كصديق على حساب المتهم دون أن يشكل ذلك انتهاكا لحق الخصوصية»[85].

من ناحية أخرى، إذا كانت المحاكم تبدي تساهلاً في تطبيق مبدأ المشروعية، إلا أنه ليس معناه أنها تسمح بانتهاكه، فقد استبعدت المحاكم الأميركية والإنجليزية جميع الأدلة المتحصلة بممارسات النسخ واللصق[86]، كما استبعدت أي دليل متحصل من لقطة الشاشة (screenshot) على جهاز الحاسوب[87]، لكن بالمقابل جرى قضاء هذه المحاكم على القبول بالرسالة الإلكترونية متى كانت تشير إلى شخص مرسلها وعنوانه الإلكتروني وتعكس بصورة واضحة وصادقة ما ظهر على شاشة جهاز الحاسوب ولا يوجد ما يثبت عكس ما ورد فيها[88].

المطلب الثاني

اقتناع القاضي بالدليل الرقمي

يتحصل الدليل المتعلق بالجريمة الإلكترونية في بعض الأحيان عن طريق يعتبر في

(84) سامي حمدان الرواشدة، مرجع سابق، ص 14 وما يليها.

(85)United States V .Meregildo ،N 11.Cr) 576 WHP 2012 ،(WL3264501 ،at2.)S.D.N.Y .Aug(10.2012.

(86) See also People v. Lenihan، 911 N.Y.S. 2d 588، 592 Sup. Ct. 2010.

(87) EWCA (Crim) 1439، (2006) Crim. L. R. 56، Court of Appel (Crim. Div) ، 2005

(88) EWCA (Crim) 3067، Court of appeal (Crim. Div.)، 2003

القانون غير مشروع، فيثور التساؤل عن مدى أهميته وقانونية إدراجه بين الأدلة الأخرى التي تعرض على القضاء الذي يبقى له الكلمة الفصل بالأخذ به أو رفضه.

الفرع الأول

الحصول على الدليل عن طريق تحديد الموقع الجغرافي

لقد سبق وذكرنا أن تطور الجريمة الإلكترونية حتم على رجال التحقيق اللجوء إلى أساليب عديدة لتتبع المجرمين واستخلاص الأدلة عن الأفعال الجرمية التي ارتكبوها. ومن أهم هذه الطرق هي المراقبة الإلكترونية. تعتبر المراقبة من أبرز أساليب التحريات في الجرائم الإلكترونية، فهي الوسيلة الأنجع للحصول على المعلومات بشكل سري وصحيح، حيث تعتبر ذات فاعلية عالية للكشف عن الجرائم المنظمة والإرهابية والأنشطة التجسسية وجرائم المخدرات. لقد أنتجت التقنيات الحديثة وسائل فعالة للمراقبة يستطيع المحققون من خلالها تحديد الموقع الجغرافي للشخص ومعرفة جميع تحركاته، إن كان عن طريق عنوان برتوكول الإنترنت (IP) الخاص به أو عبر اتصال الشبكة اللاسلكية أو حتى عبر شريحة نظام تحديد المواقع العالمي (GPS). ويتميز هذا النوع من المراقبة بسهولة اعتراض المعلومات عن بعد، حيث يتيح للمحققين الحصول عليها دون جهد كبير، ودون إثارة انتباه المشتبه فيه [89].

لم يضع المشرع اللبناني حتى الآن تشريعاً خاصاً بهذا النوع من الرقابة، لذلك يثور التساؤل عن مدى شرعيته بلجوء رجال الضابطة العدلية إليه، عند استحالة استخدام أي طريقة أخرى من الطرق المعروفة في القانون. لقد طرحت مسألة مشروعية استخدام رجال التحقيق للطرق التقنية المؤدية لتحديد الموقع الجغرافي أمام القضاء الفرنسي الذي تأرجحت أحكامه بهذا الخصوص بين مؤيد ومعارض لها. بدايةً، لا بد من التمييز بين نوعين من هذه المراقبة: المراقبة بشكل مباشر وآني، ومراقبة عن طريق التسجيل، هذه الأخيرة يمكن إسنادها للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية وفقاً لما ذهب إليه الفقه والقضاء في فرنسا، بينما اعتبرت النوع الأول من هذه المراقبة

(89) Myriam Quéméner، la Géolocalisation à l'épreuve de la procédure pénale، Lamy Droit de l'immateriel، 2013، n.99، H.Matsopoulou، la surveillance par géolocalisation à l'épreuve de la convention européenne des droits de l'homme، Dalloz، 2011، p.724.

تدخلاً صارخاً في الحياة الخاصة للأفراد وأقرت بعدم شرعيته على الإطلاق[90].

ويمكن للقضاء اللبناني أن يذهب في ذات الاتجاه الذي ذهب إليه نظيره الفرنسي، فملاحقة الشخص وتتبع مساره عن طريق مراجعة سجلات الاتصال لمعرفة الأمكنة التي لجأ إليها أو معرفة مكان وجوده أثناء وقوع الجريمة هي أفعال تدخل حتماً ضمن الأفعال العادية التي يقوم بها المحققون أثناء جمع أدلة الجريمة. وبالتالي فإن هذا النوع من المراقبة ليس بحاجة إلى قانون خاص ينظمه. لكن الإشكالية تثور عند تحديد الموقع الجغرافي للشخص بالوقت الحقيقي أو المباشر، أي متابعة مساره وتحركاته لحظة بلحظة بذات الوقت الذي يتحرك به[91].

لقد تأرجحت أحكام محكمة التمييز الفرنسية بين مؤيد ومعارض لهذا النوع من الرقابة. فقد أقرت المحكمة الإجراءات التي قامت بها الضابطة العدلية الفرنسية بإذن من قاضي التحقيق، استنادا إلى المادة 81 من قانون الإجراءات الجزائية بمراقبة مسار السيارة بشكل آني، معتبرة أن اللجوء إلى هذه الرقابة كان يتناسب مع نوع الجرم[92]. وقد كانت المحكمة الأوروبية لحقوق الإنسان قد اعتبرت أن المراقبة عن طريق (GPS) لشخص مشتبه به بتهمة الإرهاب لا يعد اعتداءً على حقه في الحفاظ على حياته الخاصة المنصوص عليه في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، طالما أنه هناك هدف مشروع وهو تحقيق المصلحة العامة والأمن للمجتمع[93]. إلا أن محكمة التمييز الفرنسية قد غيرت من اتجاهها فيما بعد في حكمين متتاليين وأعلنت عدم قانونية هذا النوع من الرقابة، معتبرةً أنه يشكل انتهاكاً للحياة الخاصة للأفراد[94]، أمام هذا التعارض في الاجتهاد، تدخل المشرع الفرنسي لحسم هذه المسألة، وبالفعل تم اقرار القانون رقم 372/2014 الصادر بتاريخ 28/3/2014 الذي حمل ضمن مواده أحكاماً تتعلق بالمراقبة عن طريق

(90) Cass. Crim. 2 nov. 2016، n°1682.376–، Cyberlex et CECYF، Rapport sur "la procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique"، 242018/1/، p.28، Myriam Quéméner، la Géolocalisation à l'épreuve de la procédure pénale، précité، p.3.

(91) Cyberlex et CECYF، Rapport sur "la procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique"، 242018/1/، p.27.

(92) Cass. Crim. 22 Nov 2011، n.1184.308–.

(93) CEDH، 2 Sep.2010، n.3562305/، Uzun c/Allemagne.

(94) Cass. Crim.، 22 Oct. 2013، n. 1381.945– et n.1381.949–.

تحديد الموقع الجغرافي في الوقت الآني أو الحقيقي، حيث تم بموجب هذه المواد تعديل المادتين 230–32 و230–44 من قانون الإجراءات الجزائية الفرنسي. وسمح فقط لقاضي التحقيق وقاضي الحريات والاحتجاز بإعطاء الإذن لهذا النوع من المراقبة، وقد أقر المشرع الفرنسي حديثاً القانون رقم 2017/1510 الصادر بتاريخ 2017/10/30 والذي سمح للمدعي العام بإعطاء الإذن أيضاً لهذا النوع من المراقبات.

وبناءً على ما تقدم وفي ظل سكون المشرع اللبناني بعدم التدخل لتحديد موقفه من هذه المسألة، يبقى السؤال قائماً حول مشروعية تلك الأفعال، وإن كنا نميل إلى ضرورة إجازة القضاء للمراقبة عن طريق تحديد الموقع الجغرافي بشكل آني ومباشر، وذلك نظراً للظروف والتحديات التي تواجه رجال التحقيق والأمن اللبناني، إن كان من جهة الخلايا الإرهابية الموجودة على الأرض اللبنانية، أو من حيث وجود جواسيس وعملاء يشكلون خطراً على المجتمع اللبناني، بحيث أصبح كل مواطن بهذا المجتمع يسمح بالتهاون باحترام حقوقه الخاصة بمقابل تفادي حصول هجمات إرهابية أو ما شابه تؤرق أمنه وأمانه.

الفرع الثاني

الحصول على الدليل عن طريق التحريض

سوف نتناول في هذا الفرع حالات الحصول على الأدلة عن طريق التحريض الممارس من قبل السلطة العامة (أولاً) والتحريض الممارس من قبل الأفراد (ثانياً)، وذلك على النحو التالي:

أولاً– التحريض الممارس من قبل أفراد السلطة العامة :

لا شك أن أمن المعلومات أصبح يشكل الحيز الأهم من الهواجس التي تؤرق السلطات في كل دولة، نظراً لخطورتها من جهة، ولصعوبة اكتشافها من جهة أخرى. لذلك فإنها تلجأ في بعض الأحيان إلى أساليب غير مألوفة لجمع الأدلة وكشف الجرائم، قد تصل إلى حد حث المجرم وتقديم له التسهيلات لدفعه لارتكاب الجريمة. وهناك بعض الطرق التي تستخدم من قبل رجال التحقيق للإيقاع بالجناة، كالاستعانة بعملاء سريين أو مخبرين للانغماس بينهم للحصول منهم على اعترافات أو تسجيل المحادثات التي تجرى بينه وبينهم، أو إنشاء مواقع وهمية لجذب الأشخاص الذين تحوم حولهم الشبهات بارتكابهم

جرائم معينة[95]، وعليه، فما هي الحدود المسموحة للسلطات باللجوء إلى هذه الوسائل للإيقاع بالمجرمين، وما هي المعايير والضوابط الواجبة التطبيق؟.

لقد رفضت محكمة التمييز الفرنسية بدايةً الخروج عن نطاق مبدأ المشروعية واعتبرت أن أي دليل يستخلص من أفعال غير مشروعة هو بحكم المنعدم ولا يمكن الأخذ به، وقد قررت أنه: «يتبين من الوقائع أن التحريات قد تمت نتيجة خدعة..... ولم تراع مبدأ المشروعية لأنها وقعت نتيجة تحريض»، وعليه فقد ألغت جميع الأدلة الناتجة عن تلك الإجراءات بالرغم من تحقق إدانة المتهم بالجرائم التي أسندت إليه[96]. لكن في قرار آخر لها صادر بتاريخ 2014/4/30[97] فرقت المحكمة بين نوعين من التحريض: التحريض الذي يستهدف دفع المتهم إلى ارتكاب جريمة، والتحريض الذي يستهدف من ورائه الحصول على معلومات أو أدلة إثبات دون أن يكون الهدف إيقاع الأشخاص ودفعهم لارتكاب الجرم. وتتلخص الدعوى التي صدر على أساسها القرار المذكور بقيام السلطات العامة الأميركية بإنشاء موقع إلكتروني لا يستطيع الدخول إليه إلا أشخاص يملكون خبرة كبيرة في خفايا وأمور البطاقات المصرفية، بحيث يستطيع المستخدمون من خلاله المحادثة وتداول المعلومات حول عدة مواضيع تتعلق بكيفية إجراء عمليات غش واحتيال على الإنترنت عبر استخدام هذه البطاقات، تم بالفعل تحديد عدة أشخاص، بينهم شخصان يحملان الجنسية الفرنسية، فجري تفتيش للحواسيب التي يملكانها وتم بالفعل اكتشاف عدة أعمال غير مشروعة قام بها هذان الشخصان على الإنترنت بواسطة البطاقات المصرفية. دفع هذان الأخيران أمام القضاء بعدم صحة الأدلة كون السلطات الأميركية مارست نوعا من التحريض عن طريق تخويل هؤلاء الاشخاص الدخول إلى الموقع للمحادثة، إلا أن جواب محكمة التمييز جاء بأن السلطات لم تقم سوى بفتح المجال للقاء أشخاص مع بعضهم البعض دون انتظار قيامهم بارتكاب أي جريمة، وإن ما قاموا به لا يعدو أن يكون إلا عملاً يدخل ضمن المهام الموكلة إليهم وهو حفظ الأمن وجمع المعلومات والأدلة الناتجة عن الجرائم المرتكبة.

أما القضاء الأميركي، فلم يتبن معياراً واضحاً حول هذه المسألة، بل ترك الأمر لتقدير القاضي في كل دعوى، فيطلع إذا كانت ما قامت به الشرطة يُشكل تحريضًا على ارتكاب

(95) سامي حمدان الرواشدة، المرجع السابق، ص 8 وما يليها

(96) Cass. Crim. 4 juin 2008، Bull. Crim، 2008، n.141.

(97) Cass. crim.، 20 sept. 2016، n° 1680.820–، Bull. crim.، n.244.

الجريمة والأسباب التي دفعتها للقيام بذلك، وطبيعة ونطاق هذه المشاركة[98]، ومن ناحية أخرى، يمكن للقضاء أن يبرر للسلطات المختصة اللجوء إلى وسائل التحريض للحمل على ارتكاب الجريمة، ولكن في حالة ما إذا كانت تتوافق مع الإغراءات والحيل العادية لمواجهة الأنشطة الإجرامية كالخداع والإلحاح أو عن طريق استخدام حساب وهمي، شرط ألا ترتبط تلك الإجراءات بالقيام بأي أمر من شأنه أن يؤدي لارتكاب الجريمة من قِبل شخص ما يتجنب عادة ارتكاب هذا النوع من الجرائم[99].

وتعتبر قضية "R v. Jones" [100] دليلًا على ذلك، وتتلخص وقائع هذه القضية في أن المتهم أعلن عن رغبته بإقامة علاقات جنسية مع فتيات قاصرات مقابل المال، طالباً التواصل من خلال رقم هاتفه الذي كتبه في إحدى عربات القطار . تظاهر أحد رجال الشرطة بأنه فتاة وقام بالاتصال به، مجرياً معه حواراً لاستدراجه وإلقاء القبض عليه، وأسندت له جريمة محاولة إغواء أو تحريض فتاة على القيام بأفعال جنسية طبقاً للمادة 8 من قانون الجرائم الجنسية الصادر سنة 2008. قضت المحكمة بصحة الإجراءات التي قام بها الشرطي، مؤكدة أن هذا النوع من الجرائم يرتكب بصورة سرية عبر استخدام وسائل الاتصال الحديثة مثل الإنترنت والهواتف المحمولة. وبالتالي فإنه هناك صعوبة بكشفها، مما يعتبر ذلك ظروفاً مادية تبرر الحاجة الملحة للشرطة للقيام بتحريات سرية أو خفية للكشف عن هذه الأنشطة الإجرامية ويُعد سلوك الشرطة في هذه الحالة مجرد إعطاء فرصة للمتَّهم للشروع في ارتكاب جريمة مماثلة، والحصول على دليل ضروري للحكم بالإدانة[101].

لم يذهب القضاء اللبناني بعيداً عن هذا السياق، حيث ذهب بالاتجاه الذي سلكه القضاء الفرنسي، حيث اعتبرت محكمة التمييز اللبنانية أن: «الأفعال التي صدرت عن المتهم بحرية وبعد تفكير وهي كافية للتدليل على قيام النية الجرمية بصورة أكيدة لديه. وبما أن المحكمة في ضوء كل ما تقدم وبالرغم من أن المتهم دفع فعلاً إلى الجريمة ترى بحالها

(98) Andrew Ashworth، Re–drawing the boundaries of entrapment، 2002 Crim. L. Rev. 16.

(99) R v Jones [2007] EWCA (Crim) 1118؛ [2008] QB 460 at 472.

(100) R v Jones [2007] EWCA (Crim) 1118؛ [2008] Q.B 460.

(101) The Court of Appeal held that "Far from instigating the offence، the police officer's conduct provided only the opportunity for the appellant to attempt to commit a similar offence and provide the evidence necessary for a conviction." Id. at 23.

عن حق في تقدير الوقائع والأدلة أن هذا الدفع إلى الجريمة لم يؤثر على إرادته بشكل قاطع بحيث أفقدها حرية التقدير والتقرير وليس من شأنه بالتالي أن يؤدي إلى انتفاء مسؤولية المتهم عن حيازة ونقل كمية المخدرات بقصد بيعه»[102].

ثانياً – التحريض الممارس من قبل الأفراد العاديين :

ليس هناك ما يمنع الأفراد العاديين بالتعاون مع سلطات التحقيق في الكشف عن الحقائق وتقديم الأدلة التي في حوزتهم، دون أن يخل ذلك الأمر بمبدأ المشروعية. فقد نصت المادة 427 من قانون الإجراءات الفرنسية صراحة على هذا المبدأ. وقد استقر على ذلك اجتهاد محكمة التمييز الفرنسية [103]، حيث أعلنت أنه: «لا توجد أحكام قانونية لا تسمح للقاضي الجزائي أن يستبعد استعمال أدلة متحصل عليها من شخص قدمه لجهاز التحقيق لمجرد أنه تم الحصول عليها بطريقة غير مشروعة أو غير قانونية»[104]، بل ذهبت محكمة التمييز إلى أكثر من ذلك، حيث استندت في حكمها إلى أدلة متحصلة من مستندات مسروقة من قبل الطرف الذي قام بتقديمها للمحكمة[105]. وبناءً على ما تقدم، فإن القضاء الفرنسي لم يتردد بالأخذ بأدلة الإثبات الجنائي التي قدمها المدعون بالحق المدني بعدما قام هؤلاء بأعمال تحريضية دفعت المتهمين بقيام بأفعال تنم عن تمييز عنصري معاقب عليها جزائياً في فرنسا [106]. وفي ذات السياق قررت محكمة التمييز الفرنسية أن التفتيش الذي أجري من قبل رجال التحقيق في الملفات الإلكترونية المسروقة من الموظف الذي يعمل في مصرف HSBC يعتبر صحيحاً وأجري وفقاً للأصول، وأن هذه الملفات لا يمكن استبعادها من وسائل الإثبات[107].

من ناحية أخرى، فلو كان القانون اللبناني لم ينص صراحة على هذا المبدأ إنما ليس

(102) تمييز جزائي لبناني، رقم 119 لسنة 1993، تاريخ 7/7/1993، القاعدة البيبليوغرافية، مركز المعلوماتية القانونية – الجامعة اللبنانية.

(103) Cass. crim.، 31 janv. 2007 : Bull. crim. 2007، n° 27. – Cass. crim.، 27 janv. 2010، n° 0983.395– : JurisData n° 2010051634–

(104) Cass. Crim.، 27 Janvier 2010، pourvoi n. 0983.395–، Bulletin criminel 2010، n. 16

(105) Cass. crim. 15 juin 1993، bull. crim.، n. 210.

(106) Cass. Crim. 11 juin 2002، 0185.560–، Non publié au bulletin.

(107) Cass. Crim. 27 Nov. 2013، n. de pourvoi 1385042–، consultable sur le site suivant: https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000028255498.

هناك برأينا مانع من تطبيقه، طالما أن هذه الأدلة سوف تساعد رجال الضابطة العدلية على كشف الحقيقة. إن تطبيق هذا المبدأ يجد سنده في قانون أصول المحاكمات المدنية باعتباره القانون العام الذي يمكن الاستناد إليه عند غياب النص الصريح في قانون أصول المحاكمات الجزائية. فالمادة 131 من القانون المذكور تنص على أن: «الإثبات هو إقامة الدليل أمام القضاء على واقعة أو عمل قانوني يسند إلى أي منهما طلب أو دفع أو دفاع. ويتعين على كل شخص أو يؤازر القضاء في سبيل جلاء الحقيقة». وحيث يستفاد من هذا المبدأ أن مهمة جلاء الحقيقة تقع على عاتق القاضي أولاً، وانطلاقاً من ذلك يحق له إثارة أية مسألة تكون منتجة لجلاء الحقيقة، ويدخل من ضمن ذلك إثارة القاضي أي دليل يكون منتجاً في القضية ويساعد على تحقيق العدالة.

فخدمات الإنترنت ومواقع التواصل الاجتماعي سهل على الأفراد إمكانية الانخراط أكثر في التحقيق وتجميع الأدلة التي تساعد في كشف الحقائق والوصول إلى المجرمين. وبالرغم من جزمنا بأهمية الدور الذي يلعبه الأفراد في كشف الدليل، إلا أنه لا يمكن استبعاد إمكانية نشوء ظاهرة سلبية تتمثل بقيام بعضهم باختلاق أدلة كاذبة ومراسلات مضللة وكيدية يكون الهدف منها الإيقاع بأشخاص أبرياء، لا سيما أن هذا الفرد بعكس رجال الضابطة العدلية غير مقيد بإجراءات معينة أو التزامات ملقاة على عاتقه، كما حصل مؤخراً في لبنان في قضية «المخرج المسرحي زياد عيتاني». وبالتالي، فإنه يجب على القضاء استبعاد الدليل المتحصل من قبل الأفراد العاديين، خصوصاً إذا تعلق بجرائم خطيرة، كالإرهاب أو تبييض الأموال أو الأفعال المتعلقة بالممارسات الإباحية.

الخاتمة :

أثبت التطبيق العملي تأثر قواعد الإجراءات الجزائية بالتقدم التكنولوجي والتقني، بحيث كلما تطورت هذه التكنولوجيا ازدادت معها صعوبة الكشف عن الجرائم التي ترتكب في البيئة الرقمية. وإذا كان القاضي الجزائي يتمتع بسلطة تقديرية كبيرة وفقاً لما ينص عليه مبدأ حرية الإثبات في المواد الجزائية، إلا أنه هناك حدود معينة يتعين أن تقف عندها هذه الحرية. فمثلما تقتضي مصلحة المجتمع مكافحة الجرائم وتحقيق الردع العام، تكمن أيضاً في ضرورة الحفاظ على حقوق الأفراد وحرياتهم. لذلك أصبح لزاماً على الدولة اللبنانية إعادة النظر بكيفية تحقيق التوازن بين هذين الحقين في معرض البحث عن الأدلة الناتجة عن الجريمة الإلكترونية.

وعليه، فقد استنتجنا من خلال هذا البحث أموراً عديدة نوردها أموراً كما يلي:

1 – هناك ثغرات عديدة تعتري القواعد القانونية الحالية التي تستند إليها الضابطة العدلية لاستخلاص أدلة الإثبات المتعلقة بالجريمة الإلكترونية، حيث تصطدم في الكثير من الأحيان بمبادئ دستورية كالحرية الشخصية وحق الخصوصية، ويمكن في حال مخالفة هذه المبادئ أن يفقد الدليل المستخلص قيمته في الإثبات ويحمل القاضي على إطراحه وعدم الاستناد إليه، مما قد يؤدي إلى ضياع فرصة كشف الجريمة أو عدم تحقق الإدانة رغم معرفة الجاني.

2 – الخروج عن مبدأ المشروعية اتجاه مقبول في القانون الجزائي بهدف تحقيق العدالة، حيث يمكن الأخذ بالدليل المتحصل عن طريق استخدام وسيلة غير مشروعة. لكن تبقى الخشية ماثلة من تعسف الضابطة العدلية إذا ما ترك لها مطلق الفاعلية باستخدام تلك الوسائل دون تحديد ضوابط واضحة.

لذلك فإننا نوصي بما يلي:

1 – سن نصوص قانونية تجيز بشكل صريح إجراء التفتيش في البيئة المعلوماتية، وبيان حدود سلطات التحقيق وصلاحيات الضابطة العدلية من أجل الحفاظ على حريات الأفراد، والنص على كيفية التعاون بين سلطات التحقيق والمؤسسات الخاصة المعنية بتخزين المعلومات والبيانات الخاصة التي تساعد تلك السلطات في الكشف عن الحقيقة.

2 – تعديل القواعد الخاصة بالتفتيش، لا سيما تفتيش الأنظمة المعلوماتية وبيان حالة ما

إذا كانت هذه الأنظمة مرتبطة بأنظمة أخرى موجودة خارج حدود الدولة ويمكن أن تساعد في كشف الحقيقة، بحيث يقتضي النص على التوسع في تنفيذ إذن التفتيش والسماح بالتالي للسلطة المخولة بالتفتيش بالنفاذ بهذه الأنظمة حتى ولو كانت خارج الحدود اللبنانية.

3 – الإسراع باتخاذ الإجراءات اللازمة للتوقيع على اتفاقية بودابست الصادرة سنة 2001 الخاصة بمواجهة الجرائم الإلكترونية، لأن هذه الاتفاقية تحتوي على مختلف النصوص الموضوعية والإجرائية، حيث يمكن إسقاطها في قانوننا لأنها تسد الكثير من الثغرات القانونية التي تكلمنا عنها في بحثنا الراهن.

المراجع:

• المراجع العربية:

- إدريس النواذلي، موقف القضاء من الجريمة الإلكترونية، منشورات كلية العلوم القانونية والإقتصادية والإجتماعية، مراكش، 2010.
- د.أحمد المحرزي ود.حمادة فوزي، برنامج مهارات التسويق والبيع: التسويق عبر الإنترنت، متوافر على الرابط التالي: http://www.olc.bu.edu.eg/olc/images/internet.pdf
- د. أسامة العبيدي..
  - التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، العدد 58، الرياض، 2015.
  - جريمة الإستغلال الجنسي للأطفال عبر شبكة الإنترنت، مجلة الشريعة والقانون، حزيران/ يونيو 2013، العدد53، جامعة الإمارات العربية المتحدة.
- د. جنان الخوري، تبييض الأموال جريمة جزائية مصرفية وتبعية، مجلة الجيش، العدد 85، بيروت 2013.
- د. رامي علي وشاح، الصعوبات المادية التي تعترض الإثبات بالمحررات الإلكترونية، الأكاديمية للدراسات الإجتماعية والإنسانية، 2010.
- سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الإجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الإنجليزي والأميركي، المجلة الدولية للقانون، عدد 3، قطر، 2017.
- د. شيماء عطالله، تراجع الحق في الخصوصية في مواجهة الإتصالات الإلكترونية، بحث مقدم الى المؤتمر العلمي الثاني لكلية القانون الكويتية العالمية، منشور بمجلة كلية القانون الكويتية العالمية، العدد 10، السنة الثالثة، يونيو 2015.
- ضياء محمود، حق الصمت في الدعوى الجزائية، مجلة جامعة البعث، 2017، المجلد 39، عدد 136، دمشق.
- د. عبد الحفيظ بلقاضي، التجريم والعقاب في أقوى نزعاتهما تسلطاً: القانون الجنائي

للعدو، مجلة الشريعة والقانون، 2006، العدد 26، جامعة الإمارات العربية المتحدة.

– د. عبد الحكيم الحكماوي، الإثبات في الجريمة الإلكترونية، سلسلة ندوات، محكمة الإستئناف، الرباط – المغرب تحت عنوان تأثير الجريمة الإلكترونية على الإئتمان المالي، العدد السابع، 2014.

– د. عبد الحكيم فودة، أدلة الإثبات والنفي في الدعوى الجنائية في ضوء الفقه والقضاء، منشأة المعارف، الإسكندرية، 2007.

– د. عبد الفتاح بيومي حجازي،

- الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دار النهضة العربية للنشر، القاهرة، 2009.
- مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007.

– د. ليتيم فتيحة، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، العدد الثاني،2010، كلية الحقوق والعلوم السياسية، جامعة بسكرة.

– د. محمد حبحب، وسائل الدفع الالكتروني في مواجهة الجريمة، بحث مقدم إلى المؤتمر الدولي الرابع حول التجارة الإلكترونية، صلالة– عمان، 26 و27 / 2016/ 7.

– د. محمد ذكي أبو عامر، الإثبات في المواد الجزائية، دار الجامعة الجديدة، الإسكندرية، 2011.

– د. محمد يوسف علوان، ومحمد خليل الموسى، القانون الدولي لحقوق الإنسان، الجزء الثاني، الحقوق المحمية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007.

– د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية للنشر، القاهرة، 1995.

– محمود عبد الرحمن محمود، ورقة فنية حول تهديدات البنية التحتية الحرجة للمعلومات، جامعة عين شمس، الإسكندرية، 2010.

– د. موسى أرحومة، الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية. بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 10/ 29–28/ 2009.

– د. نادر عبد العزيز شافي، بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني، مجلة الجيش، عدد 263، بيروت، 2007.

– نادر عبد العزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، بيروت،2007.

– د. ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

– د. هانيا فقيه، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لواقع الحماية وتحديات العصر، 2018، منشور في القاعدة البيبليوغرافية، مركز المعلوماتية القانونية، الجامعة اللبنانية.

– د. هلالي عبداللاه أحمد،

- تفتيش نظم الحسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية للنشر، القاهرة، 2008.
- حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية للنشر، القاهرة، 1997.

– د. وليد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، الإسكندرية، 2012.

– د.عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت، «دراسة مسحية عن ضباط الشرطة في دولة البحرين»، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999.

– د. يوسف سعد الله الخوري، القانون الإداري العام –الجزء الثاني –القضاء الاداري مسؤولية السلطة العامة، بيروت، 1998.

• المراجع باللغة الفرنسية

- A.Huet, Le droit pénal international et Internet, les petites affiches, 10 Nov. 1999.
- Alain Bensoussan, L'accés des autorités aux données personnelles, Partie I, JTIT International, juillet 2013, n.4.
- B.Bouloc, Procédure Pénale, 20ème édition, Dalloz, 2006.

- C.Boulanger et F.Frafer, "Cybercriminalité: un aperçu du monde des criminels virtuels" Classe International., 4 janv. 2014.
- H.Matsopoulou, la surveillance par géolocalisation à l'épreuve de la convention européenne des droits de l'homme, Dalloz, 2011.
- J.Bouisson, Procédure pénale, Litec, édition 2, 2002.
- M. Mekki, Vérité et preuve, univ. Paris 13, I.R.D.A., 2013.
- M. Raymond, Les auteurs de crimes sexuels sur internet, Revues Psychiatrie et violence, Volume 14, n. 1, 2015-2016.
- M. Habhab, le droit pénal libanais a l'épreuve de la cybercriminalité, sader, 2012.
- M-D. Torbey, L'internationalisation du droit pénal, le Liban dans le monde arabe, L.G.D.J., Paris, 2007.
- Myriam Quéméner,
    - la Géolocalisation à l'épreuve de la procédure pénale, Lamy Droit de l'immateriel, 2013, n.99.
    - Yves Charpenel, Cybercriminalité - Droit pénal appliqué, Economica,2010.
- P.Quarré, « Le droit au silence »،J.T., 1974, p. 526. R.Garnon et A. Garnon, note sous l'arrêtJ.C.P., 1993, II, n° 22.073.
- Pierre Kaysser, La protection de la vie privée par le droit. Protection du secret de la vie privée, 3e éd., Paris, Economica, 1995.
- Serge Migaryon, Trois ans de constats et de saisies informatiques: un états de lieu, Colloque, CNEJITA, 24/5/2012.
- Winston Maxwell, édition Multimédia, 19 sep. 2016, n.15

• التقارير باللغة العربية

– مؤسسة كونز العائلية للقانون الدولي والسياسة، تقرير حول المواد الإباحية المتعلقة بالأطفال: التشريع النموذجي والإستعراض العالمي للتشريعات، الطبعة السابعة،

.2012

– تقرير مقدم إلى الدورة الرابعة لمعرض ومؤتمر الخليج لأمن المعلومات «جيسيك»»، إنترنت الأشياء 2017» ، دبي، 21 ايار / مايو 2017.

– التقرير المعد من قبل الجمعية العامة للأمم المتحدة حول «تعزيز وحماية الحق في حرية الرأي والتعبير»، مجلس حقوق الإنسان، الدورة الثالثة والعشرون، 2015.

– تقرير حول «حق الخصوصية في لبنان»، معد من قبل منظمة تبادل الإعلام الإجتماعي، الخصوصية الدولية، جمعية الإتصالات التقدمية، 2015.

• Rapports

– Cyberlex et CECYF، Rapport sur “ la procédure pénale face aux évolutions de la cybercriminalité et du traitement de la preuve numérique”، 242018 / 1 /.

– Rapport de Délégation ministrielle aux industries de sécurité et à la lutte contre les cybermenaces – État de la menace، janv 2017.

المحتوى: