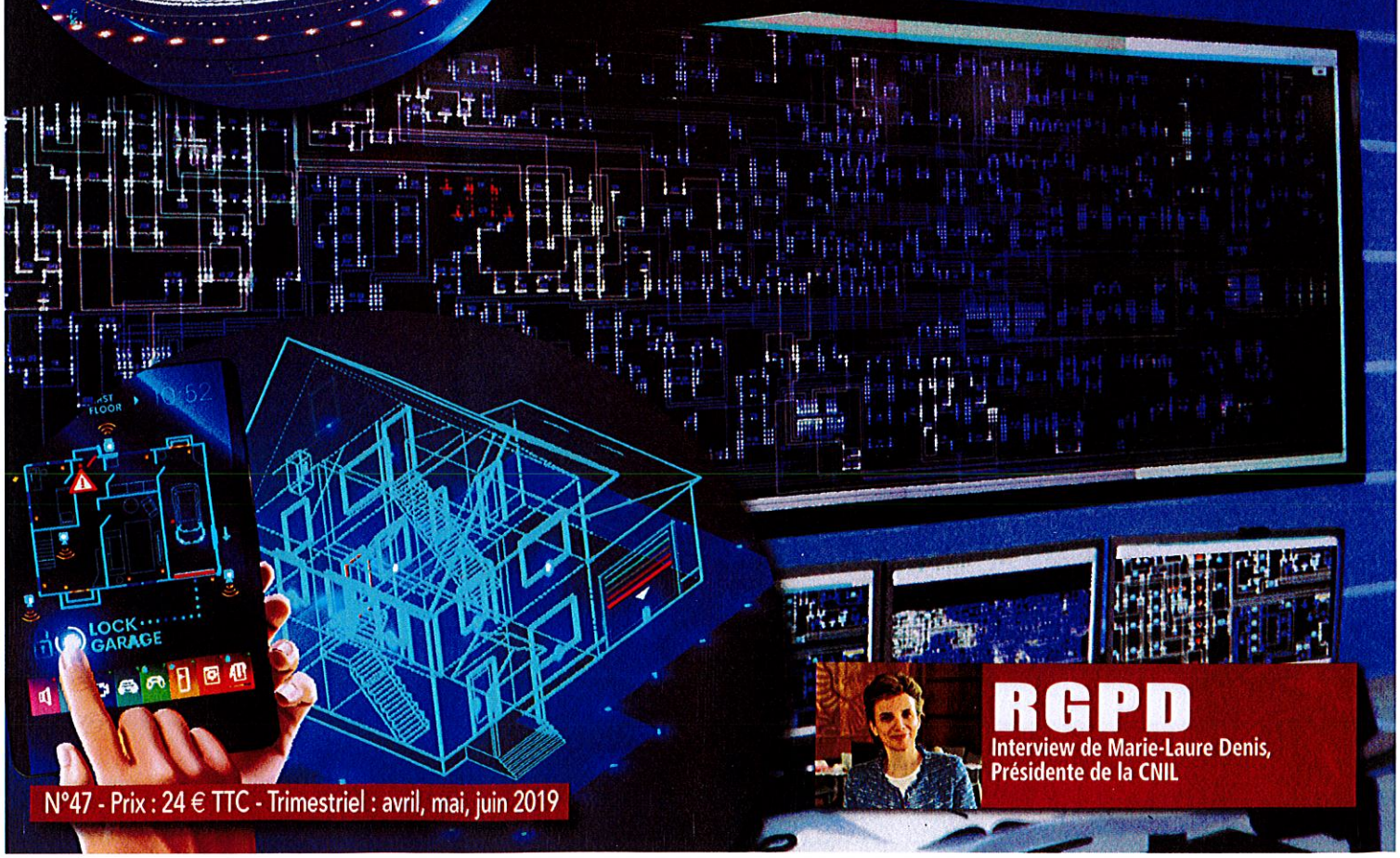
Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

SOC

TECHNOLOGIES & SÉCURITÉ



RGPD

Interview de Marie-Laure Denis, Présidente de la CNIL

N°47 - Prix : 24 € TTC - Trimestriel : avril, mai, juin 2019

QUAND LA JUSTICE S'INTÉRESSE À VOTRE SMARTPHONE

Par Olivier Iteanu, Avocat à la Cour,
Chargé d'enseignement à l'Université de Paris I Sorbonne

Selon l'observatoire des marchés des communications électroniques en France, un organisme créé au sein de l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), le nombre de cartes SIM[1] en service en France s'élève à 75,6 millions au 31 décembre 2018. Cela donne l'ampleur du phénomène téléphone mobile et de son petit frère évolué le smartphone. Ce dernier est partout et tout le temps dans nos vies, toutes générations, toutes activités légales et… illégales confondues. Immanquablement, les smartphones sont aussi devenus des outils très performants pour les délinquants. On peut commettre des délits avec un smartphone, comme par exemple un accès frauduleux à un système[2], mais le plus souvent l'appareil sert à préparer l'infraction ou à la faciliter. La Justice française a alors mis en place ces dernières années un dispositif très complexe et très complet pour intégrer le smartphone dans la besace des enquêteurs chargés d'élucider des délits ou des crimes. Nous le passons en revue.

PAS QUE LES GAFAM, ET LE RGPD ?

On a beaucoup écrit et parlé sur les GAFAM et leur appétit de data. Cette appétence ne s'est pas limitée au Web et les smartphones les intéressent aussi. Ce phénomène est d'autant plus prégnant que l'équipement se diffuse, les capacités de stockage de ces petits appareils se développent, en même temps que le nombre de services offerts. Immanquablement, tous les éditeurs des applications pour smartphones cherchent alors à accéder aux données de leurs utilisateurs, devenues un véritable or noir aujourd'hui. Les autorités publiques ont pris acte de cette situation, à commencer par les autorités américaines. Aidées par l'omniprésence dans le monde des entreprises technologiques américaines, notamment en Europe, elles ont mis en place un partenariat public-privé, plus ou moins imposé, pour capter les données collectées par leurs nouveaux « associés ». Edward Snowden, l'informaticien, ancien employé de la CIA et de la NSA, s'est fait l'écho de ce partenariat d'un nouveau genre, en juin 2013, en révélant notamment l'existence d'un programme spécial, appelé PRISM. Depuis 2013, les choses n'ont non seulement pas changé, mais on peut dire que, du point de vue des utilisateurs, elles se sont aggravées. Dernièrement, en mars 2018, c'est même une Loi d'un genre nouveau aux effets extraterritoriaux qu'a votée le congrès américain : le CLOUD ACT. En clair, l'objectif est d'obtenir des prestataires de cloud sous juridiction américaine, quel que soit le lieu de stockage des données de leurs clients à travers le monde, la transmission de toutes données (« any records ») aux autorités de poursuites fédérales ou locales américaines. Mais revenons au smartphone. La troisième évolution des dispositifs de surveillance est l'instauration de dispositifs légaux dans les Lois locales et ici dans le Code pénal et le Code de procédure pénale français, qui donnent à la Justice et à la police des pouvoirs d'enquêtes étendus sur le smartphone. La différence avec les GAFAM est double. D'une part, ces dispositifs de surveillance sont légaux. Tout acte de surveillance décidé par un officier de police judiciaire, un magistrat du Parquet ou un Juge d'instruction sera donc à un moment ou un autre connu de la personne concernée. De ce fait, obligatoirement à cet acte de surveillance correspond un recours possible devant un juge qui a la possibilité de rétracter ou d'annuler la décision de surveiller à la demande la personne concernée. D'autre part, ces actes de surveillance sont encadrés par des règles connues, qui sont des conditions posées à leur légalité. Par exemple, la géolocalisation d'un smartphone exige une autorisation écrite préalable du Procureur pour une durée limitée de 15 jours. Le juge d'instruction, quant à lui, peut l'autoriser pour une durée maximale de 4 mois, éventuellement renouvelables.

Enfin, ces mesures sont légitimes, car il s'agit de prévenir ou d'élucider des infractions, c'est-à-dire d'identifier des auteurs ou des complices pour les renvoyer devant la Justice et les faire condamner. Il s'agit aussi de donner aux victimes une possibilité de recours contre les auteurs ou complices d'infractions ayant causé le préjudice. Des actes qui sont donc nécessaires dans tout État de droit. Et le RGPD dans tout ça, direz-vous ? Car ces actes de surveillance vont aboutir à des collectes d'informations susceptibles d'identifier des personnes physiques, c'est-à-dire des données à caractère personnel. Le règlement européen entré en application le 25 mai 2018 s'applique à ces actes de surveillance. Or, l'article 6 c) dudit règlement prévoit bien que la collecte est licite, dès lors qu'elle est prévue par la Loi, ce qui est notre cas. Il n'est donc nul besoin du consentement des personnes concernées puisque la Loi prévoit cette collecte et ce traitement. On comprendrait d'ailleurs difficilement qu'il faille obtenir le consentement de personnes soupçonnées de délits ou de crimes pour mener une enquête à leur encontre…

UNE FOISON DE MESURES SUR LE SMARTPHONE

Quand on en fait le recensement, on s'aperçoit que le Code pénal et le Code de procédure pénale renferment un nombre impressionnant de mesures qui concernent le smartphone. Nous allons tenter de les classer et de les énoncer. A titre préalable, il faut savoir qu'une enquête de police et de Justice représente schématiquement trois cas. Dans un premier temps, l'enquête préliminaire qui est l'enquête ordinaire menée par la police avec le Parquet pour déterminer la vérité, généralement suite à une plainte. En d'autres termes, la Justice s'interroge sur la réalité d'une infraction dont on lui a rapporté l'existence ou dont elle a eu connaissance. Vient ensuite l'enquête dite de flagrance, en cas d'urgence dictée par une situation qui nécessite une action rapide de la police. Enfin, il y a l'enquête menée par le juge d'instruction, juge judiciaire, qui instruit et donc enquête. On peut dire schématiquement que chacune de ces enquêtes a ses règles au regard des investigations menées sur un smartphone. Ces investigations sont de quatre types, à commencer par l'identification. Il s'agit ici de connaître l'identité du titulaire d'une ligne téléphonique ou d'une carte SIM. Le policier adresse à l'opérateur concerné une demande d'identification et celui-ci répond. C'est l'acte le plus simple en apparence et le moins formel, car le moins intrusif dans la vie des personnes. La seconde consiste à localiser ou à géolocaliser un appareil. La localisation des smartphones dans la législation est relativement récente, avec une Loi de 2014. Dans ce cadre, les services de police sont capables de solliciter des opérateurs pour deux types d'interventions : soit suivre un individu en temps réel avec un système dit de triangulation des antennes relais activées par l'appareil, soit effectuer un bornage, qui consiste à localiser un téléphone dans le passé. Ce bornage peut permettre de présumer que la personne se trouvait à tel endroit géographique à une date donnée, ce qui peut constituer une information importante pour l'enquête. La troisième mesure est la plus médiatique, c'est la perquisition informatique[3], car oui, à l'instar d'un local, un smartphone peut faire l'objet d'une perquisition. Évidemment, cela signifie que l'investigation va amener à prendre connaissance de contenus ou de données. C'est donc un acte très intrusif. C'est pourquoi, en enquête préliminaire, que nous avons qualifié d'enquête ordinaire, l'officier de police ne peut procéder à cette fouille sans l'accord préalable de l'intéressé. Bien évidemment, cette fouille pose la question du chiffrement et déchiffrement, à laquelle la police américaine, en l'occurrence le FBI, s'était heurtée dans un bras de fer qu'elle avait mené avec Apple en 2014. Disons simplement qu'au-delà des difficultés pratiques auxquelles la police française va souvent se heurter, les acteurs du secteur numérique étant la plupart du temps étrangers, il existe un dispositif légal qui permet de réquisitionner les personnes qualifiées pouvant déchiffrer un contenu, l'ensemble de ces dispositions se trouvant dans le Code de la sécurité intérieure. Enfin, la police et la Justice se réservent la possibilité d'intercepter les conversations téléphoniques. C'est la bonne vieille écoute téléphonique qui a laissé place à l'interception, elle-aussi très encadrée par la Loi pénale.

En conclusion, comme on le voit dans ce tour rapide, on est loin du vide juridique lorsqu'il s'agit du smartphone dans la Loi pénale française. Reste que les délinquants sont prévenus et qu'il y a toutes les chances qu'ils prennent leur disposition en conséquence. La partie de gendarmes et de voleurs n'est donc pas terminée et on souhaite, pour notre État de droit, que le gendarme trouve toutes les solutions et parades. ■■■

LEGAL BRIEFING

When Justice takes a look at your smartphone

By Olivier Iteanu, Avocat à la Cour, Lecturer at the University of Paris I Sorbonne

According to the observatory for electronic communications markets in France, an organisation created within the Regulatory Authority for Electronic Communications and Posts (ARCEP), there were 75.6 million SIM cards[1] in use in France as of 31 December 2018. This indicates the scale of the mobile phone phenomenon as a whole and of its prodigious sibling the smartphone. The latter is ubiquitous: at all times, whatever the age, for all types of activities, legal and otherwise.

Inevitably smartphones have also become very powerful tools for criminals. One can commit crimes with a smartphone, such as fraudulently accessing a system[2], but more often the device is used to prepare an offence or to facilitate one. In recent years French Justice has set up a thoroughly comprehensive and complex system to allow investigators, responsible for elucidating misdemeanours or crimes, access to smartphones. Let us take a closer look at this.

[1] Excluding M2M cards for IoT
[2] Art. L 323-1 of Penal Code : "Fraudulently accessing or deliberately remaining in all or part of an automated data processing system is punishable by two years' imprisonment and a 30,000 euro fine."

[1] Hors cartes MtoM pour objets connectés
[2] Art. L 323-1 du Code pénal : « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.* »
[3] Art. 57-1 et 76-3 du Code de procédure pénale