Techniques d'enquête numérique judiciaire : les défis d'une survie dans la modernité

Par Floran VADILLO
Chercheur associé à l'IRM (Université de Bordeaux)
Ancien conseiller auprès du garde des Sceaux

Généralement, lorsque nous songeons aux techniques de pointe en police judiciaire, se bousculent dans nos esprits les relevés d'empreintes, les tests ADN, voire, pour les plus technophiles, les écoutes téléphoniques ou « interceptions judiciaires », ou encore l'analyse comportementale prédictive. Rares sont ceux qui évoquent les *IMSI catchers* (1), les chevaux de Troie informatiques, la géolocalisation téléphonique ou par balisage… que l'on croit plutôt l'apanage des services de renseignement.

De fait, les techniques d'enquête de la police judiciaire française font figure de parent pauvre politique, industriel et médiatique. Pour s'adapter aux nouvelles formes ou aux nouvelles manifestations de la criminalité, pour assurer leur modernisation ou leur acclimatation à l'environnement numérique, elles sont donc désormais confrontées à trois défis quasi vitaux : un défi ontologique face à la concurrence tant politique que technologique de la police administrative ; un défi juridique et jurisprudentiel ; un défi technologique de modernisation et conduite de projets.

Une âpre concurrence politique et technologique

Dans notre système institutionnel, il existe une *summa divisio* entre police judiciaire et police administrative, comme le rappelle avec constance le Conseil constitutionnel : à la première incombe « la constatation d'une infraction pénale particulière, […] la recherche de ses auteurs, […] le rassemblement de preuves », tandis qu'à la seconde échoient « la protection de l'ordre public pour faire cesser un trouble déjà né, fût-il constitutif d'infraction, et […] la prévention des infractions (2) ».

Pareille séparation est supposée induire une complémentarité, le Conseil constitutionnel y a longtemps veillé, octroyant néanmoins un net avantage à la police judiciaire en matière de capacités d'investigation (et notamment d'ingérence dans la vie privée des individus concernés par une enquête) dans la mesure où le contrôle de l'autorité judiciaire semblait apporter en contrepartie toutes les garanties nécessaires.

De fait, à partir des années 2000, le législateur a pris soin d'offrir à la police judiciaire un cadre juridique des plus modernes, notamment dans le domaine technologique grâce à la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité défendue par Dominique Perben, alors garde des Sceaux. En effet, si la loi du 10 juillet 1991 avait fondé le régime juridique des interceptions judiciaires, le texte de 2004 a introduit dans le Code de procédure pénale d'utiles techniques spéciales d'enquête à l'instar de la surveillance physique humaine, l'infiltration ou la sonorisation. Par la suite, la loi du 14 mars 2011 d'orientation et de programmation pour la

(1) Matériel d'interception permettant de recueillir les numéros IMSI (immatriculation de la carte SIM) et IMEI (immatriculation du téléphone lui-même).
(2) « Commentaire de la décision n°2005-532 DC du 19 janvier 2006 », in *Les Cahiers du Conseil constitutionnel,* Cahier n°20.

performance de la sécurité intérieure a ajouté la captation de données informatiques, disposition que la loi du 13 novembre 2014 a modernisée tout en introduisant dans notre droit les enquêtes sous pseudonyme pour tenir compte du champ offert par les communications électroniques, et en particulier les réseaux sociaux. Entre-temps, la loi du 28 mars 2014 a également fixé un cadre à la géolocalisation téléphonique ou par balisage. Enfin, la loi du 3 juin 2016 a permis l'usage d'*IMSI catchers* pour la captation tant de métadonnées que de communications.

Ce cadre, bâti au gré des textes de loi votés en raison de lacunes ou de condamnations (*cf. infra*), mais aussi en imitation d'exemples étrangers (notamment états-uniens), se distinguait par sa modernité et une complétude d'autant plus aisément atteinte que les activités de police administrative ne bénéficiaient d'aucun fondement juridique (seules les interceptions administratives étaient autorisées par la loi précitée de 1991).

Cependant la prégnance du phénomène terroriste a lentement sapé cette avance, d'un point de vue tant législatif que technologique. En effet, la nécessité d'empêcher tout acte terroriste d'être perpétré a remis en selle une police administrative jusqu'alors délaissée. Confrontés à l'impact social et médiatique d'un attentat, les responsables politiques ont préféré superposer les dispositifs et entretenir une concurrence afin de se prémunir contre toute accusation de n'avoir pas suffisamment œuvré [(3)].

La première entaille remonte à la loi du 23 janvier 2006 [(4)], laquelle a ajouté au maigre arsenal des services de renseignement la possibilité de recueillir des données de connexions téléphoniques à des fins de géolocalisation. Dans les années qui ont suivi, sont venus principalement s'adjoindre des droits de consultation de fichier avant que la loi de programmation militaire du 18 décembre 2013 n'autorise la géolocalisation en temps réel et, surtout, avant que la loi du 24 juillet 2015 ne vienne doter les services de renseignement d'un cadre juridique complet et moderne. Pensée comme un texte d'équilibre avec les activités de police judiciaire [(5)], cette loi a établi une parité que les différentes législations votées après les attentats de novembre 2015 (en particulier les lois de reconduction de l'état d'urgence) ont profondément et durablement déséquilibrée.

Un tel déséquilibre s'est révélé d'autant plus aigu que les services de renseignement ont bénéficié d'investissements techniques et technologiques tout à fait considérables (dès 2008), leur permettant non seulement de mettre en œuvre les moyens juridiques offerts par la loi, mais également de développer de très fortes compétences en matière de déchiffrement et de lutte informatique. De même, le Groupement interministériel de contrôle (GIC), service du Premier ministre chargé de mettre en œuvre les interceptions administratives, est rapidement devenu un centre technologique d'importance.

À l'inverse, la police judiciaire n'a jamais bénéficié ni des structures, ni des moyens idoines pour mettre en œuvre l'intégralité des dispositions votées. Pourtant, le service interministériel d'assistance technique (SIAT) de la DCPJ [(6)] ou l'Institut de Recherche criminelle de la Gendarmerie

(3) L'explication de cette bascule mériterait de plus amples développements dans la mesure où la législation antiterroriste s'est bâtie, de 1986 à 1996, sur la prévalence du judiciaire au point de déborder la *summa divisio* évoquée plus haut au profit de celui-ci. Mais la double compétence (administrative et judiciaire) du service de renseignement intérieur (DST, DCRI puis DGSI) et l'utilisation du renseignement par les responsables politiques comme preuve de leur implication dans la lutte contre le terrorisme ont favorisé la mutation décrite.

(4) Loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(5) L'auteur de la présente contribution a beaucoup œuvré à cette législation auprès de Jean-Jacques Urvoas, président de la Commission des Lois de l'Assemblée nationale et rapporteur du projet de loi relatif au renseignement. Le lecteur pourra notamment consulter : Floran VADILLO, « Une loi relative aux services de renseignement : l'utopie d'une démocratie adulte ? », note n°130 de la Fondation Jean Jaurès, 17 avril 2012, 20 p.

(6) Direction centrale de la Police judiciaire, au sein de la Direction générale de la Police nationale.

nationale (IRCGN) recueillent en leur sein des profils experts qui pourraient donner la pleine mesure de leur talent. À titre d'illustration de ce retard accumulé en dépit du cadre législatif, la captation de données informatiques adoptée en 2011 n'a pour l'heure jamais été mise en œuvre faute d'investissements et de structure porteuse [7].

Les écueils du droit

Au-delà de la concurrence politique et technologique de la police administrative, les techniques d'enquête numérique judiciaire doivent également subir les évolutions juridiques et jurisprudentielles, internes ou externes, qui constituent autant d'à-coups souvent brutaux et nocifs.

Il s'agit d'ailleurs d'un sujet fondateur en ce domaine puisque la loi du 10 juillet 1991 – la première du genre – n'a été adoptée qu'à la suite d'une condamnation de la France par la Cour européenne des droits de l'Homme [8] qui venait s'ajouter à des arrêts de la Cour de cassation dans le même sens [9]. Dans le même ordre d'idées, la législation de mars 2014 relative à la géolocalisation judiciaire avait été rendue nécessaire par un arrêt de la Cour de cassation sanctionnant le défaut de base légale [10].

En effet les ingérences dans la vie privée, même sous le contrôle de l'autorité judiciaire, doivent répondre à des critères stricts tels que la prévisibilité du droit, l'intelligibilité de la loi et l'existence de garanties suffisantes (nature de l'ingérence, durée, conditions de recevabilité de la preuve…). Les techniques d'enquête numérique judiciaire souffrent donc de cette construction sédimentaire, au gré des besoins, des censures ou des lacunes. L'instabilité du droit les régissant s'avère préjudiciable. À ce titre, alors que la loi du 3 juin 2016 avait considérablement modifié le régime d'emploi de ces techniques, la future loi de programmation pour la Justice procédera à de nouvelles modifications. Il aura sans doute manqué une loi-cadre permettant d'unifier les régimes procéduraux pour simplifier le cadre d'emploi et favoriser une plus grande sécurité juridique sans s'exposer à l'obsolescence technique (autant d'objectifs poursuivis par la loi relative au renseignement adoptée en 2015).

Et si le droit national s'avère déterminant, il ne doit pas faire oublier l'importance primordiale des normes européennes. Le récent arrêt de la Cour de Justice de l'Union européenne du 21 décembre 2016 [11] l'a rappelé cruellement, lui qui a jeté un trouble sur les durées de conservation par les opérateurs téléphoniques et les motifs d'accès des données de connexion. Il rend nécessaire l'adoption d'une nouvelle directive actuellement en cours de préparation.

De même, seul le droit européen permettra d'éviter que les géants du numérique (notamment Facebook ou Google) ne se soustraient aux cadres juridiques nationaux en matière de réquisition judiciaire en arguant un conflit de normes et la seule applicabilité du droit états-unien. Trop souvent, ces entreprises choisissent les réquisitions auxquelles elles acceptent de déférer (notamment celles en lien avec la pédopornographie et le terrorisme), alors que cette liberté d'appréciation ne

(7) Pour remédier à cette situation, les ministères de la Justice et de l'Intérieur, après plusieurs mois de travail, étaient parvenus à un accord en mars 2017 afin de structurer l'offre étatique de « logiciels espions » au profit de la police judiciaire. Le texte issu de ce consensus prévoyait la création du Service technique national de captation judiciaire chargé de développer et de mettre à disposition des enquêteurs des solutions informatiques. Après de longs mois d'attente, il vient enfin d'être publié, *cf.* arrêté du 9 mai 2018
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036887904&dateTexte=&categorieLien=id
(8) CEDH, 24 avril 1990, Huvig et Kruslin c/ France.
(9) Cour de cassation, Assemblée plénière du 24 novembre 1989, affaire Baribeau, ou Cour de cassation, Chambre criminelle, du 13 juin 1989.
(10) Cour de cassation, criminelle, Chambre criminelle, 22 octobre 2013.
(11) CJUE 21 décembre 2016, « Tele2 ».

leur appartient pas. Il est donc nécessaire de prévoir, au niveau européen, des dispositifs contraignants ou statutaires permettant la bonne tenue des enquêtes judiciaires [12].

Les techniques d'enquête numérique judiciaire méritent donc une réflexion juridique globale, qui s'inscrive à l'échelle nationale et européenne, afin de leur garantir une réelle effectivité et une plus grande sécurité.

Relever le défi technologique

Le défi le plus évident réside dans la capacité à suivre les évolutions technologiques, pour ne plus les subir avec fatalité et, surtout, ne pas accumuler un retard trop important (lequel légitimerait le recours exclusif aux services de police administrative qui déséquilibrerait notre système judiciaire et le droit de la preuve).

En ce domaine, les techniques d'enquête numérique judiciaire doivent se confronter à trois évolutions majeures.

La première procède de la généralisation du chiffrement des communications électroniques. Protection indispensable de la vie privée contre laquelle rien ne doit être fait pour l'entraver ou créer des failles (les « portes dérobées ») dans lesquelles s'engouffreraient services de renseignement étrangers ou réseaux criminels, cette pratique constitue néanmoins un frein majeur à la conduite des enquêtes. À titre d'exemple, 80 % des interceptions de données sont aujourd'hui chiffrées, réduisant considérablement la capacité des enquêteurs à collecter du renseignement utile aux procédures judiciaires.

Il s'avère donc capital d'offrir aux juges judiciaires la possibilité d'accroître leur capacité d'accès à des données en clair. En ce sens, la loi du 13 novembre 2014, puis celle du 3 juin 2016 ont offert aux magistrats la capacité de recourir au centre technique d'assistance (CTA) de la DGSI [13] afin de disposer de moyens de déchiffrement plus robustes que ceux proposés par certaines entreprises. Toutefois, ces premiers efforts doivent maintenant ouvrir une réflexion juridique plus vaste autour de la mise à disposition des capacités étatiques de déchiffrement au profit du judiciaire (cadre d'autorisation et de contrôle, recevabilité de la preuve, préservation de la confidentialité, y compris en procédure).

Enfin, il paraît déterminant de mettre en œuvre les dispositions relatives aux « chevaux de Troie » judiciaires qui permettent de contourner le chiffrement des données en communiquant aux enquêteurs celles directement saisies sur le terminal avant leur envoi.

La deuxième évolution tient au traitement et à la conservation de la donnée de masse : le cadre juridique relatif aux techniques d'enquête numérique, l'existence de nombreux fichiers, la massivité des sources ouvertes ont aujourd'hui considérablement restreint le caractère stratégique de l'acquisition des données (sous réserve de la question du déchiffrement). Néanmoins, ces facteurs ont également souligné avec acuité la problématique de la gestion de la donnée de masse à des fins analytiques. Trop de temps humain est consacré à des résultats insatisfaisants ; toutes les données ne sont pas exploitées, toutes les perspectives ne sont pas explorées.

(12) Dans une autre publication, nous avons suggéré 1) d'obliger les entreprises concernées à disposer d'un réservoir de clés de chiffrement que pourraient solliciter les magistrats pour mettre au clair les données d'un individu faisant l'objet d'une surveillance ; 2) de conférer le statut d'opérateur de communications électroniques à certaines entreprises (WhatsApp, Hangouts, Messenger, Skype…) afin de pouvoir pratiquer des interceptions judiciaires ; 3) d'accroître considérablement les sanctions en cas de refus de déférer à des réquisitions judiciaires, notamment grâce à des amendes proportionnelles au chiffre d'affaires de l'entreprise concernée *in* « Projet de loi Collomb : l'injustifiable agonie de nos droits », *L'Hétairie*, note n°2, 22 septembre 2017
https://www.lhetairie.fr/projet-de-loi-collomb

(13) Article 230-2 du Code de procédure pénale.

Alors que les services de renseignement évoluent peu à peu sur cette question (acquisition récente d'une solution Palantir par la DGSI, ou projet Artémis initié par le ministère des Armées), la police judiciaire ne pourra faire l'économie d'actions sur ce point. Cela supposera naturellement des partenariats industriels avec des entreprises offrant toutes les garanties de l'indispensable souveraineté numérique (sujet à la fois stratégique et juridique au regard des exigences de l'administration de la preuve). Tout délai dans la prise de décision se traduit immanquablement en un retard technologique dirimant.

Naturellement, le traitement de cette donnée de masse soulève la question sensible de sa conservation. Or, le droit actuel de la preuve ne permet pas de sélectionner les données pertinentes. Cela suppose, soit de développer des capacités de stockage dignes des meilleurs réseaux sociaux, ce qui s'avère hors de portée et source de dysfonctionnements conséquents (à l'instar de ceux subis pour cette raison par la Plateforme nationale des interceptions judiciaires, la PNIJ), soit de faire évoluer le droit pour que, d'un commun accord avec les parties, seules les données pertinentes soient conservées.

Enfin, la troisième évolution est liée aux dysfonctionnements étatiques dans la conduite des grands projets technologiques. Comme le reconnaît Henri Verdier, directeur de la DINSIC : « Nous manquons cruellement, au sein de l'État, de grands chefs de projet, de personnes ayant une culture de production numérique. Nous sommes devenus malhabiles pour acheter, parce que l'on ne sait plus très bien spécifier, négocier ou encadrer nos fournisseurs. Nous devons donc travailler sur les ressources humaines pour réintégrer de nouveaux profils, pour réapprendre la conception et le pilotage de projets [14]. » Par conséquent, l'État doit s'armer, non pour réinternaliser massivement certaines fonctions, mais pour tenir son rang face aux industriels et au progrès technologique.

Cette préoccupation a motivé la création de l'Agence nationale des Techniques d'Enquête numérique judiciaire (ANTENJ) en avril 2017 [15]. Confiée à un magistrat jouissant d'une solide expérience de la criminalité organisée mais également des services enquêteurs, cette agence a bénéficié d'efforts budgétaires conséquents pour constituer un centre de compétences au sein du ministère de la Justice et un interlocuteur crédible pour les services de police judiciaire et les industriels. Elle a vocation à incarner l'un des acteurs majeurs des évolutions, notamment technologiques, de ce champ stratégique.

Pour que s'opère l'œuvre de justice, cette dernière doit disposer des moyens nécessaires, en particulier dans la conduite des enquêtes. Or les progrès technologiques offrent tout à la fois une fabuleuse opportunité d'efficacité et un péril majeur si le retard actuel devait s'accentuer.

Le sujet s'avère d'une complexité absolue tant il mêle considérations politiques, stratégiques, juridiques et technologiques. Il convoque imagination et réactivité, un esprit critique qui ne confine pas à la désespérance, mais aussi une certaine idée de l'État. Car il s'agit d'offrir à la police judiciaire le Bertillon [16] du XXIe siècle.

(14) VERDIER H. : « Le vrai sujet : faire advenir l'État d'après la révolution numérique », *Chronik*, 19 décembre 2017. https://chronik.fr/henri-verdier-vrai-cest-de-faire-advenir-letat-dapres-revolution-numerique.html

(15) Décret n°2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires.

(16) Alphonse Bertillon (1853-1914), fondateur en 1882 du premier laboratoire de police d'identification criminelle, créateur de l'anthropométrie judiciaire (« système Bertillon ») adopté dans toute l'Europe, puis aux États-Unis, et utilisé en France jusqu'en 1970.