Nouveaux enjeux : la « cybersécurité »

Entretien avec Xavier LEONETTI, substitut placé, cour d'appel d'Aix-en-Provence, ancien responsable de la sécurité économique et de la cyberprévention à la DGGN

Vous êtes l'auteur d'un *Guide de Cybersécurité* : quelle a été votre approche pour étudier ce phénomène ?

Internet fait désormais partie de nos vies. Tous les jours, à chaque instant, nous sollicitons cet assistant multifonction afin de répondre aux questions les plus diverses ou dans le but de gérer nos tâches quotidiennes (rendez-vous, démarches administratives, réservations de sorties…). La vie sans le numérique ne paraît donc plus possible. Mais à quel prix ? Il semble que la vague du progrès numérique nous submerge, entraînant notre abandon à ces nouveaux dieux du quotidien.

Or, plus de 90 % des 70 000 cyberinfractions recensées en 2015 par l'Observatoire national de la délinquance et des réponses pénales (ONDRP) sont des escroqueries et des attaques financières. C'est-à-dire qu'à l'image de l'économie réelle qui repose sur la confiance, l'économie souterraine se nourrit de la confiance que l'escroc crée au préjudice de sa victime. La particularité de l'espace cyber est que les internautes font preuve d'une crédulité excessive.

En effet, il apparaît que dans l'espace virtuel les individus font preuve d'une négligence plus importante que dans le monde réel.

Ainsi, imagine-t-on des personnes distribuer sur la voie publique des prospectus décrivant leurs habitudes illustrés par des photos de leur vie intime ? Non, pourtant, des millions d'internautes le font chaque jour sur Facebook. De même, si une personne vêtue d'un uniforme « Orange » ou « SFR » abordait les passants en leur demandant leur numéro de carte bleue, obtiendrait-elle satisfaction ? Sans doute pas. Malheureusement, sur internet, cette pratique (dite de « phishing ») fait plusieurs milliers de victimes tous les mois.

Cet ouvrage répond donc à la finalité de démystifier l'espace cyber, expliquant de manière pratique et concrète comment s'en prémunir. Par ailleurs, j'ai souhaité réaliser une présentation des principaux outils disponibles en matière de cybersécurité, en veillant à guider le citoyen néophyte dans cette jungle d'acteurs.

À quelles formes de menaces la société du numérique nous expose-t-elle ?

Il existe trois grandes catégories d'infractions cybercriminelles observées :

• La première est relative aux infractions liées aux systèmes d'information et de traitement automatisé des données (STAD). Il s'agit par exemple, d'intrusions sur un serveur informatique, ou de piratage de données.

• La seconde catégorie regroupe les infractions liées aux formes de criminalité « traditionnelles » qui utilisent les nouvelles technologies de l'information et de la communication (NTIC) comme de nouveaux modes opératoires. Ainsi, un véhicule volé qui était précédemment revendu via les annonces gratuites de la presse, est aujourd'hui vendu par l'intermédiaire de sites internet spécialisés dans la vente de particuliers à particuliers.

• La troisième catégorie est constituée par les infractions commises par internet rela-

Guide de cybersécurité. L'Harmattan, 2015

Prix de l'Institut national des hautes études de la Sécurité et de la Justice

tives à la dignité ou à la personnalité et les atteintes sexuelles commises par ce même biais. Ces infractions traditionnelles connaissent aussi une nouvelle vie sur le web, au moyen notamment de l'anonymat offert par internet.

La société numérique fait également peser un risque sur le fonctionnement des États eux-mêmes et en particulier sur les démocraties où la liberté des échanges accroît les possibilités de piratage et d'intrusion. Ces derniers mois, les États-Unis ont été confrontés à des suspicions de piratages informatiques pendant la campagne électorale présidentielle. Cette situation unique dans l'histoire politique américaine nous enseigne que les acteurs de la vie publique et politique doivent très tôt acquérir des réflexes d'hygiène et de sécurité numérique. À défaut, les informations qu'ils détiennent se trouvent susceptibles d'être interceptées ou modifiées par des tiers ou des puissances étrangères.

On peut ainsi imaginer en France le piratage des listes électorales détenues sur les serveurs informatiques des mairies. Il s'agirait moins de compromettre que de désorganiser un scrutin permettant alors de créer un doute sur la sincérité des élections. Dans un contexte de défiance vis-à-vis des autorités publiques et politiques, ce risque est réel d'autant que les scrutins sont de plus en plus nombreux (dernièrement à Notre-Dame des Landes par exemple).

C'est pourquoi une démarche particulière de prévention à destination des partis politiques a été initiée à l'automne 2015 par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Dispose-t-on d'indicateurs statistiques fiables pour évaluer aujourd'hui ces menaces ?

L'étude des formes de cybercriminalité se révèle parcellaire car elle dépend de la performance des outils de comptage utilisés par l'administration. Or, en la matière, les différents services de l'État utilisent chacun des grilles d'analyse et de comptage différentes. Il s'agit d'un véritable « château Kafkaïen ».

Par exemple, s'agissant de l'utilisation du logiciel « Cassiopée », l'application est déjà interconnectée avec celle de la gendarmerie et bientôt avec celle de la police. Cependant, les critères de « Cassiopée » ne sont pas identiques à ceux utilisées par la police et la gendarmerie, si bien qu'il n'existe pas de continuité statistique entre les ministères de l'Intérieur et de la Justice. C'est d'ailleurs ce que relevait le Premier ministre, en octobre 2014, à l'occasion du séminaire de rentrée des auditeurs de l'INHESJ et de l'Institut des hautes études de la défense nationale (IHEDN) : « les systèmes d'information des forces de sécurité d'une part, et de la justice d'autre part, sont structurellement incapables de communiquer ».

De surcroît, il convient de ne pas oublier qu'une partie des faits statistiques sont traités en dehors du système pénal. Par exemple, le groupement d'intérêt économique des cartes bancaires peut être amené à traiter de phénomènes cybercriminels dans le cadre de solutions de conflits à l'amiable.

Enfin, le « chiffre noir » de la cybercriminalité est l'un des plus élevés, souvent parce que les personnes physiques ou morales visées ignorent les faits. En effet, une entreprise met en moyenne 229 jours pour découvrir la menace dont elle fait l'objet.

Le droit pénal appréhende-t-il de manière adaptée ces nouvelles formes de délinquance ?

Jamais, sans doute, le prédateur n'a été aussi près de sa victime puisque au moyen des smartphones et des objets connectés il est partout et constamment avec elle, et peut-être demain en elle, avec le recours à des organes ou prothèses connectés.

Jamais aussi le délinquant n'a été aussi loin de son juge, ne serait-ce qu'en raison des frontières juridiques et de la lenteur de la coopération judiciaire comparée à la vitesse des transactions sur la Toile. Néanmoins, l'arsenal pénal permettant de réprimer les comportements délinquants s'est particulièrement étoffé, notamment depuis l'adoption de la loi dite « LOPPSI 2 » du 14 mars 2011.

Les atteintes aux systèmes de traitement automatisé de données (« STAD », art 323-1 à 323-7 c. pén.) permettent de réprimer les nouveaux types d'infractions. Ainsi, l'accès ou le maintien frauduleux dans un STAD (art. 323-1, al. 1er) permet de réprimer le phishing qui consiste à soutirer des informations personnelles à des internautes en leur envoyant un courriel usurpant l'identité d'une banque ou d'un site marchand (voir par exemple, TGI Paris, 2 sept. 2004). De même, s'agissant de la participation à un groupement de pirates (art. 323-4) : lorsque des participants n'ignoraient pas que les informations échangées avaient pour finalité de commettre des atteintes au système informatique d'accès à Canal plus, leur participation à l'entente est pénalement répréhensible (T. corr. Carpentras, 25 juin 2004).

En matière de traitement de données à caractère personnel, l'article 226-16 du code pénal permet de sanctionner la mise en ligne du nom d'une personne au sein du contenu rédactionnel d'un site web, qui est un traitement automatisé de données nominatives au sens de l'article 5 de la loi

de 1978 et qui nécessite la déclaration à la CNIL du site web concerné.

Comment la lutte contre la cybercriminalité s'organise-t-elle au niveau international ?

Au niveau européen, plusieurs organisations ont en charge des missions de cybersécurité. En particulier le Centre de criminalité en haute technologie d'EUROPOL qui a pour mission de mener des actions de coordination, de soutien opérationnel, d'analyse stratégique et de formation. De même, le Centre européen de lutte contre la cybercriminalité (EC3) centralise l'expertise et l'information, soutient les enquêtes criminelles et promeut les solutions à l'échelle de l'union européenne se concentrant sur les activités illicites en ligne menées par des organisations criminelles.

Le 2 avril 2014, une opération coordonnée par INTERPOL a permis d'interpeller 58 personnes impliquées dans un réseau criminel responsable d'affaires de « sextorsion ». Cette affaire fait suite au suicide de Daniel PERRY, un adolescent écossais victime d'une tentative de chantage sur internet.

De l'autre côté de l'Atlantique, aux États-Unis, dès janvier 2014, le président Barack OBAMA déclarait que « maintenant, nos ennemis recherchent la capacité de saboter nos réseaux, nos institutions financières et notre système de contrôle aérien. Nous ne pouvons rester sans rien faire et dans quelques années, se demander pourquoi nous n'avons pas agi pour contrer ces menaces réelles pour notre sécurité et notre économie ». Dans ce contexte, le DHS (« Department of Homeland Security ») a recruté, à lui seul, plus de 500 personnes en 2012 pour améliorer la protection des États-Unis contre les attaques cyber.

Au niveau national, quelles sont les principales structures dédiées à la prévention des infractions et à la recherche de celles-ci ?

Au cours de l'année 2013, j'ai pu participer aux travaux engagés par le ministère de l'Intérieur visant à renforcer et mieux coordonner les moyens d'actions en matière de prévention et de lutte contre la cybercriminalité. À cette occasion, j'ai pu constater la diversité et la qualité des compétences publiques en la matière.

Il convient de souligner que la police et la gendarmerie nationales disposent de cyberenquêteurs dont la spécialité croît selon le niveau d'infraction. Par exemple, la police nationale s'est récemment dotée d'une sous-direction de lutte contre la cybercriminalité. De même, au sein du Pôle judiciaire de la gendarmerie nationale, la division de lutte contre la cybercriminalité (DLCC) dispose de compétences uniques en matière de cybercrime destinées à appuyer les unités locales. Par ailleurs, l'action de la gendarmerie se trouve renforcée de l'apport du réseau de la réserve citoyenne cyberdéfense placée sous l'autorité du ministère de la Défense. À leurs côtés, la direction générale de la sécurité intérieure (DGSI) dispose de compétences spécifiques notamment s'agissant de cyberradicalisation ou de lutte contre le cyberespionnage.

Rappelons d'ailleurs que les articles 706-102-1 à 706-102-6 du code de procédure pénale créent une nouvelle catégorie de technique d'enquête relative aux captations des données informatiques. Il s'agit d'un dispositif ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre. En outre, s'agissant de la consultation des données personnelles à distance par des enquêteurs, la Cour de cassation, dans un arrêt du 6 novembre 2013, a retenu qu'il s'agit d'une « simple mesure d'investigation et non d'une perquisition distincte exigeant une nouvelle décision (d'un) magistrat ».

Au sein du ministère de la Défense, le centre d'analyse et de lutte informatique défensive (CALID) opère une veille et une analyse des nouvelles cybermenaces et assure également la cyberprotection des opérations extérieures de la France.

Enfin, du point de vue interministériel, l'Agence nationale de sécurité des systèmes d'information (ANSSI) créée en 2009 édicte les règles de sécurité des systèmes d'information de l'État et joue le rôle de gardien des « opérateurs d'importance vitale ».

Pensez-vous que l'office du juge soit différent par rapport à ces menaces que vous identifiez bien comme étant, pour partie, des infractions « classiques » en droit pénal ?

L'office du juge doit intégrer le cyberespace, à la fois comme la matière de son action, mais également comme un outil de travail et d'accompagnement dans sa prise de décision.

En premier lieu, l'espace cyber opère de perpétuelles mutations des champs infractionnels. Citons notamment l'apparition des monnaies virtuelles. Ces dernières sont des moyens de transaction permettant d'effectuer des paiements en ligne. Ainsi, contrairement à une devise officielle, une monnaie virtuelle n'est pas l'incarnation de l'autorité de l'État ou d'une banque centrale. C'est pourquoi, au cours du mois de juillet 2014, une plate-forme de bitcoins a été démantelée en Midi-Pyrénées dans le cadre d'une enquête diligentée par la division économique et financière de la gendar-

merie nationale. Plus de 200 000 euros de bitcoins ont été saisis à la suite de mouvements suspects constatés sur les réseaux numériques.

Ensuite, le monde virtuel révolutionne l'office du juge en ce qu'il conduit à revoir la nature même des modes d'enquête, de poursuite et de procès. En particulier, les réseaux sociaux sont parfois considérés comme étant de véritables adjoints de sécurité. Ainsi, sur la toile, plusieurs plates-formes de signalement des comportements suspects voire infractionnels se sont développés. On se souvient à cet égard de l'affaire du lanceur du chat survenue en 2014, au cours de laquelle un adolescent s'était filmé en train de maltraiter l'animal.

Ce dossier a permis d'illustrer la complémentarité possible entre les internautes et les services de police. Pour autant, il convient de rappeler que dans plus de 90 % des cas, les traques conduites par des internautes justiciers se soldent par un échec et le web ne doit pas devenir un Far West où chacun règle ses comptes et tente de faire la loi.

Par exemple, certains groupes de militants, tels que les « Anonymous » (dont n'importe qui peut se prévaloir), se mêlent de nombreuses causes sous prétexte de lutter contre les injustices. Mais, souvent, ils peuvent se tromper de cible et lyncher la mauvaise personne. Ainsi, dans le Missouri (États-Unis), à la suite de la mort de Michael BROWN lors d'une intervention policière, Anonymous a publié sur Twitter, l'identité du policier que le groupe pensait être à l'origine de l'homicide du jeune homme. Anonymous s'est trompé d'identité, dévoilant le nom d'un policier nullement concerné par cette affaire.

Ainsi, comme le souligne Myriam QUÉMÉNER, magistrate et conseiller juridique auprès du préfet de police de Paris en charge de la cybersécurité, « lutter efficacement contre la cybercriminalité est un enjeu majeur pour les années à venir. Cette démarche est indissociable de l'amélioration de la connaissance des nouveaux vecteurs d'information tel qu'internet et les réseaux numériques ».

L'organisation judiciaire est-elle, selon vous, adaptée au traitement des infractions numériques ?

En septembre 2014, les services du parquet de Paris ont été réorganisés afin d'être plus efficaces dans le traitement des dossiers financiers, de cybercriminalité et de santé publique. Désormais, le parquet financier de Paris comporte un pôle cybercriminalité (« section F1 ») au sein de la division économique, financière et commerciale. Le parquet de Paris demeure cependant le seul à disposer d'une section spécialisée dans la lutte contre « la délinquance astucieuse et la cybercriminalité ». Cette section traite plus particulièrement des dossiers d'atteintes aux systèmes de traitement automatisé de données commises à l'encontre des services de l'État et des entreprises situés à Paris.

Les juridictions interrégionales spécialisées (JIRS) ont à connaître de nombreux cas de cybercriminalité, de même que plusieurs cours d'appel qui ont désigné au sein de leurs effectifs des magistrats référents pour les questions de cyberterrorisme.

Enfin, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a reconnu à tout juge d'instruction la possibilité de décider de la captation à distance des données informatiques, dans le cadre des dispositions spécifiques relatives à la criminalité et à la délinquance organisée.

L'enjeu est donc de maintenir le processus de spécialisation judiciaire amorcé avec la création d'un pôle spécialisé au sein du parquet de Paris. Comme nous l'avons vu, les cybermenaces sont multiples, complexes et diffuses et recommandent de ce fait la création de structures adaptées et spécialisées.

De surcroît, nous faisons face à une délinquance de masse, où les infractions sont ventilées « façon puzzle » sur l'ensemble du territoire.

Par conséquent, le regroupement des infractions (au niveau des JIRS par exemple) doit permettre d'étoffer un dossier permettant par la suite de rendre plus légitime le recours à une coopération internationale.

10 CONSEILS DE « CYBER-BON SENS »

1. « Fermer sa porte »
Il convient de bien choisir son pare-feu et son anti-virus. À l'image du monde réel, l'utilisation d'une porte blindée réduit les risques de cambriolage.

2. « Ne pas laisser traîner ses clefs »
Selon l'étude Privacy Index 2014, 62 % des internautes ne modifient pas régulièrement leur mot de passe (71 % en France).

3. « Ne pas laisser entrer un inconnu »
Il convient de ne pas télécharger de logiciel inconnu et de ne pas ouvrir de pièces jointes provenant d'une personne inconnue.

4. « L'habit ne fait pas le moine »
Dans ce cas, il s'agit de ne pas répondre aux appels/courriels imitant ceux d'un organisme officiel qui demandent de transmettre des coordonnées bancaires.

5. « Ne pas croire tout ce que l'on dit »
Vérifier le texte d'une information afin de détecter les fausses nouvelles et les rumeurs.

6. « Ne pas se précipiter »
Très souvent la cyberattaque joue sur le fait que les internautes consultent rapidement leurs courriels et cliquent trop vite sur un lien, lequel renvoie vers un faux site web.

7. « Payer en toute sécurité »
Utiliser une solution technique de paiement en ligne, de type e-carte bleue ou paiement par solution « 3DSecure ».

8. « Pour vivre heureux, vivons cachés »
Sans devenir un inconditionnel du secret, une certaine discrétion est recommandée sur les réseaux sociaux.

9. « Rester vigilant »
Pour cela, il convient de se sensibiliser aux cybermenaces et de signaler les comportements suspects et les contenus illicites sur la toile.

10. « En cas de problème appeler à l'aide »
Trop souvent les victimes d'attaques n'osent pas se signaler ou déposer plainte soit parce qu'elles ont honte de leur crédulité, soit parce qu'elles pensent que cela ne servira à rien.

Au cœur de la Justice

www.union-syndicale-magistrats.org

USM.Magistrats / @USM_magistrats

Appli USM disponible sur GooglePlay et Apple Store

L'Union Syndicale des Magistrats, créée en 1974, est le syndicat de magistrats majoritaire et apolitique qui a recueilli 70,8 % des voix aux élections professionnelles en 2016. Elle se bat au quotidien pour assurer l'indépendance de la Justice, défendre les intérêts moraux et matériels des magistrats et contribuer au progrès du droit et des institutions judiciaires afin de promouvoir une justice accessible, efficace et humaine.

USM
UNION SYNDICALE DES MAGISTRATS

Revue de l'Union Syndicale des Magistrats - 18, rue de la Grange Batelière - 75009 Paris
Tél. : 01 43 54 21 26 - Email : contact@union-syndicale-magistrats.org