"La lutte contre la cybercriminalité"

08/11/2019

Discours de Monsieur François Molins, procureur général près la Cour de cassation, en ouverture du colloque "*La lutte contre la cybercriminalité*" organisé par la Compagnie des experts agréés par la Cour de cassation.

Mesdames, Messieurs,

La société connaît aujourd'hui une phase de transformation numérique de grande ampleur et l'ensemble de nos systèmes sont de plus en plus interconnectés.

Attaques informatiques contre les systèmes d'information d'entreprises ou d'institutions, vols de bases de données afin d'obtenir une rançon, espionnage, financement d'organisations terroristes par du crowdfunding, escroqueries en ligne : la délinquance a investi l'espace cyber. Les menaces peuvent provenir d'Etats, d'entreprises privées ou d'organisations criminelles. Certaines opérations relèvent d'une nouvelle forme de cybercriminalité organisée. Aussi, les attaques informatiques ne constituent plus un simple risque conjoncturel, mais sont devenues systémiques, comme l'ont démontré les attaques WannaCry et NotPetya en 2017.

Pour faire face à l'acuité de ces menaces, aux risques encourus, et à l'évolution de la cybercriminalité, l'adaptation des moyens de lutte doit être permanente et l'implication de l'ensemble de la chaîne des acteurs institutionnels et privés doit être recherchée.

La cybersécurité constitue un enjeu crucial, que ce soit pour nos concitoyens qui doivent pouvoir réaliser leurs démarches administratives et utiliser leurs smartphones en toute sérénité ; pour les entreprises qui doivent pouvoir pratiquer leurs activités sans risquer un espionnage industriel ou un blocage de leurs chaînes de production ; ou encore pour l'État qui doit être en capacité de protéger ses données les plus sensibles, de garantir l'intégrité de ses systèmes d'information, et tout simplement d'assurer sa souveraineté.

Je souhaiterais, à l'occasion de l'ouverture de ce colloque organisé par la Compagnie des experts agréés par la Cour de cassation, rappeler quelques-uns des enjeux majeurs de la lutte contre la cybercriminalité, tout en soulignant que son renforcement doit garantir à la fois le respect des droits fondamentaux et des libertés publiques, et la protection de l'ordre public en général, et de l'ordre public numérique en particulier.

Les enjeux sociétaux

Les attentats terroristes des trois dernières années ont mis en exergue le recours de plus en plus important aux technologies de l'information et de la communication dans la diffusion de propos provoquant ou faisant l'apologie du terrorisme, et dans la préparation des actes terroristes.

La lutte contre les contenus illicites constitue notamment un défi à plusieurs titres. Il importe de poursuivre les efforts de retrait rapide et durable des contenus radicaux. La propagation sur les grandes plateformes numériques américaines de contenus relevant du discours de haine reste un enjeu de taille. Par ailleurs, la viralité de l'information sur les réseaux sociaux interroge, tant en matière de désinformation que d'enfermement cognitif des usagers.

La criminalité sur le darkweb est extrêmement diversifiée :

- Le premier agrégat de crimes et délits regroupe les trafics de stupéfiants et d'armes.
- On peut également évoquer les infractions liées à la délinquance économique et financière qui représente le tiers des plaintes enregistrées, avec notamment le vol et le recel de données de carte bancaires (dit carding), ainsi que le trafic de fausse monnaie et de faux documents. Moins spectaculaires que les trafics précédemment évoqués, ces infractions touchent néanmoins un nombre plus important de victimes.
- Enfin, toujours présents sur le web de surface via les réseaux peer to peer, les pédophiles déplacent progressivement leur activité sur le darkweb, dont le caractère technologique ne constitue plus un obstacle.

Sur Internet, les trafics illicites sont facilités par trois mécanismes : les forums de discussion, le darknet et les cryptomonnaies. Il a par ailleurs également été constaté une utilisation de plus en plus accrue des outils de chiffrement et d'anonymisation sur Internet, ce qui soulève des questions techniques, juridiques et opérationnelles dans la lutte contre la criminalité et le terrorisme, et rend l'accès à la preuve numérique délicat.

Les enjeux économiques

Le cyberespace est devenu un lieu de confrontation. Les attaques à l'encontre des systèmes informatiques de l'État, des organismes publiques, des entreprises ou des citoyens sont quotidiennes, sans que l'on puisse toujours en saisir l'origine et en comprendre les motivations.

Les attaquants informatiques à l'encontre d'entreprises peuvent conduire aussi bien à des opérations très ciblées qu'à des actions massives et indiscriminées. Ces atteintes, qui peuvent être motivées par l'appât du gain, le sabotage,

l'espionnage ou l'ingérence économique, ont des incidences financières et réputationnelles considérables.

Les cyberattaques peuvent ainsi constituer un vecteur d'ingérence économique efficace. Elles peuvent permettre de capter une technologie ou un savoir-faire, d'acquérir une information stratégique, d'effectuer un chantage ou d'exiger une rançon. Elles peuvent avoir pour but de déstabiliser un acteur économique, une autorité de régulation ou un groupe de consommateurs, souvent à des moments choisis stratégiquement (dans un contexte de fusion-acquisition, de congés, de publication d'un bilan, etc.).

Pour se protéger, les entreprises disposent de deux principaux outils complémentaires : la prévention et le transfert de risque par le biais de l'assurance, dont la couverture du risque cyber commence à se développer. Aucun secteur économique n'est à l'abri. Les secteurs bancaire et financier constituent des cibles de choix pour les hackers, en raison des flux monétaires générés et des données sensibles de leurs clients. Il en est de même du secteur de la santé, très producteur de données.

L'émergence d'attaques directes contre les réseaux bancaires et de paiement, notamment pour prendre le contrôle de distributeurs automatiques ou pour transférer directement des fonds, apparaît dans un contexte déjà sensible. Les virus bancaires persistent, les logiciels malveillants ciblant les points de vente poursuivent leur développement et le système de traitement des opérations bancaires internationales SWIFT subit régulièrement des attaques. Il est essentiel de veiller à ce que la confiance en ces systèmes ne soit pas entamée.

Les enjeux judiciaires et juridiques

Il importe que la justice s'adapte face à un contentieux complexe, qui nécessite des magistrats spécialisés. La technicité des infractions de cybercriminalité demande en effet un investissement important : la formation est un élément-clef, au moins aussi déterminant que la question des moyens financiers, tels que les frais de justice pour les expertises informatiques par exemple.

Cette spécialisation s'est manifestée notamment au parquet du tribunal de grande instance de Paris par la création en 2014 d'une section F1 en charge de la cybercriminalité. La spécialisation va de pair dans ce contentieux avec une certaine centralisation.

Cette section a en effet une compétence exclusive :

- lorsque les faits visent des systèmes informatiques étatiques, institutionnels et de sociétés privées considérées comme des opérateurs d'importance vitale pour le bon fonctionnement de l'Etat (dans les domaines de l'énergie ou de la santé par exemple), et qui porteraient atteinte aux intérêts fondamentaux de la Nation.
- Sa compétence s'étend également aux affaires dans lesquelles les victimes sont dispersées sur l'ensemble du territoire national. Il s'agit dans ce cas de phénomènes massifs et sériels nécessitant, pour la bonne conduite de l'enquête, un parquet centralisateur (dans le cas par exemple d'attaques par « rançongiciels »).
- La section F1 du parquet de Paris est enfin compétente lorsque les informations portées à sa connaissance proviennent d'autorités policières ou judiciaires étrangères.

Le partage de l'information est par ailleurs essentiel. Au mois de juin dernier a eu lieu la première réunion des magistrats « cyberréférents » des parquets généraux et des parquets sur l'état de la cybercriminalité en France et son traitement judiciaire. Il s'agit d'un nouveau réseau de magistrats spécialisés qu'il est important d'intensifier.

Le ministère de la Justice doit en outre veiller à l'adaptation constante des textes législatifs et réglementaires aux évolutions technologiques et comportementales en matière de cybercriminalité, de façon à renforcer l'efficacité des moyens d'investigation et des dispositifs de prévention, tout en cherchant à trouver le juste équilibre entre d'une part, la

sauvegarde de l'ordre public, la prévention et la répression des infractions et d'autre part, le respect des libertés individuelles.

Face à la persistance de la menace terroriste, la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a étendu les techniques spéciales d'enquêtes, notamment celles qui comportent en elles-mêmes une dimension numérique (l'enquête sous pseudonyme, la captation de données informatiques et le recours à l'IMSI catcher) ou qui peuvent être mises en oeuvre au moyen de communications électroniques (comme l'infiltration), à certaines infractions relevant des atteintes aux intérêts fondamentaux de la Nation. Il s'agit d'infractions de nature criminelle, comme par exemple l'intelligence avec une puissance ou une organisation étrangère en vue de susciter des actes d'agression contre la France, ou le sabotage. Cette loi a permis également la captation des données informatiques échangées par le biais de réseaux sans fil (comme le wifi).

Pour lutter efficacement contre les menaces actuelles ou émergentes, notamment contre les atteintes aux systèmes de traitement automatisé de données, il apparaît également nécessaire de développer d'autres approches en matière d'investigations : par exemple, l'extension du champ d'application de la technique d'enquête sous pseudonyme est souhaitable. C'est un enjeu majeur de l'efficacité des enquêtes face aux évolutions des modes opératoires criminels sur le darknet.

Les enjeux internationaux

La dimension internationale de la cybercriminalité implique également de faciliter la coopération au niveau européen et international afin de renforcer les moyens de lutte contre ce phénomène.

Au niveau européen

Les enquêtes sur la cybercriminalité exigent inévitablement des services de police et des autorités judiciaires qu'ils coopèrent et coordonnent les mesures d'instruction avec des autorités de ressorts différents. Eurojust est l'organe clef de la coopération judiciaire européenne, par la création et le renforcement de partenariats avec tous les États membres et l'ensemble des institutions, organes et agences de l'Union européenne.

La cyberattaque NotPetya (du nom du logiciel malveillant utilisé) en juin 2017 a mis en lumière l'importance d'une réponse coordonnée immédiate face à des attaques de grande envergure, révélant ainsi la valeur ajoutée de l'engagement précoce d'Eurojust et d'Europol. En effet, dans les heures qui ont suivi l'attaque, les autorités judiciaires françaises ont ouvert une enquête criminelle et ont demandé l'assistance d'Eurojust. Des enquêtes parallèles ont été lancées dans plusieurs autres pays dans le monde. La coordination a concerné 10 Etats membres ainsi que l'Ukraine. Une ECE a été établie en décembre 2017 pour garantir la collecte en temps opportun des éléments de preuve électroniques et la coordination des efforts d'enquête dans les pays participants, afin de surmonter les différences entre les divers cadres juridiques.

Au niveau international

La convention du Conseil de l'Europe sur la cybercriminalité, signée le 23 novembre 2001 à Budapest, reste à ce jour le seul instrument international contraignant en matière de lutte contre la cybercriminalité. Un deuxième protocole additionnel à cette convention est en cours de rédaction depuis septembre 2017, et envisage de simplifier la coopération judiciaire entre les 63 pays adhérents à la convention et de faciliter la coopération directe avec les fournisseurs de

services sur Internet des autres pays membres. Sont notamment étudiés de meilleures possibilités d'accès transfrontalier aux données par les services d'enquête, un cadre simplifié pour les demandes d'entraide judiciaire concernant les données d'abonnés et une formalisation des procédures d'urgence. Les travaux dans ce cadre prévoient d'ores et déjà d'assurer une cohérence avec les travaux en cours dans le cadre de l'Union européenne.

L'initiative menée par l'Alliance mondiale Cyber (GCA) depuis 2015 est une autre illustration de l'utilité de la coopération internationale, associant les organismes institutionnels et les entreprises privées. Il s'agit d'une organisation internationale, partenaire notamment du parquet de New-York et du ministère de la Justice français, dont l'effort est intersectoriel et vise à éradiquer le risque cyber. Elle développe des solutions concrètes qui améliorent la sécurité du numérique, et les met à la disposition du public. Les premiers efforts ont notamment aidé à lutter contre le risque de phishing.

A titre de conclusion, le colloque qui se tient aujourd'hui est l'occasion de rappeler que la lutte contre la cybercriminalité est l'un des grands défis actuels pour la justice.

De nombreuses questions restent ouvertes :

- Le débat relatif au chiffrement des données reste complexe, la protection des données à caractère personnel devant être garantie inconditionnellement et la lutte contre la criminalité devant s'adapter aux nouveaux usages pour protéger les français.
- Les conséquences de l'arrêt Tele2 de la CJUE de décembre 2016 sont encore très incertaines, d'autres arrêts devant intervenir, alors que la conservation et l'accès aux données nécessaires aux enquêtes constitue un enjeu de premier plan.

Le colloque d'aujourd'hui permettra de dresser un panorama complet des enjeux, des menaces et des réponses à apporter à la cybercriminalité, et de montrer que la cybersécurité est une question primordiale en terme de protection des citoyens, et doit être au cœur de l'action de l'Etat.

Colloques | Discours

Procureur général

Par François Molins