Pour un parquet national du numérique et une 33ème chambre correctionnelle de la cybercriminalité ?

Actualité législative publié le **16/10/2019**, vu **1409 fois**, Auteur : Droit de la sécurité informatique

Les données et les intrusions informatiques vont sans nul doute représenter le contentieux de demain pour lequel nous ne disposons actuellement que de trop peu de moyens et d'expertises.

Les données et les intrusions informatiques vont sans nul doute représenter le contentieux de demain pour lequel nous ne disposons actuellement que de trop peu de moyens et d'expertises. Il convient dans ces conditions et sans tarder de réfléchir à l'évolution du contentieux lié au numérique. Ainsi qu'il est souligné à juste titre, « *c'est avant tout une question de conduite du changement, de sensibilisation, qui permettra d'insuffler une culture du numérique* ».

Plus de 300 000 ordinateurs touchés dans 150 pays différents, 45 hôpitaux empêchés de fonctionner en raison de la paralysie de leur système informatique entrainant le report d'interventions chirurgicales et le déroutement d'ambulances, l'usine Renault de Douai à l'arrêt, la Deutsche Bahn, FedEx et Telefonica également touchés...Tel est le résultat de l'attaque informatique « WannaCry » du 12 mai 2017.

Quelques semaines plus tard, le 27 juin 2017, à nouveau un écran noir et une demande de rançon en lettres rouge. Le *ransonware* « Petrwrap » se diffusait dans les serveurs des banques ukrainiennes et russes, touchant entre autres un transporteur maritime international ainsi que plusieurs grandes entreprises françaises.

Ce qui est particulièrement frappant et doit nous alerter dans ces évènements, c'est la régularité à laquelle ils commencent à survenir, la vulnérabilité des sites exposés - aussi sensibles que des centrales nucléaires, des hôpitaux ou des cabinets d'avocat -, la différence entre des virus dont le mode opératoire pourrait nous paraître similaire (tantôt rançon, parfois simple sabotage...), la désorganisation et la panique qu'ils créent démontrant notre inexpérience à y faire face.

Combien d'années seront-t-elles nécessaires pour nous rendre compte de l'importance pris par le numérique dans nos vies ? Combien d'attaques informatiques révélées, de réseaux en lignes démantelés suffiront à nous en faire prendre pleinement conscience ?

Cet article a pour objectif d'interpeller les pouvoirs publics et l'ensemble des acteurs concernés afin de réfléchir dès aujourd'hui aux modalités d'organisations collectives pour lutter contre ces nouvelles menaces, aujourd'hui peu maîtrisées, mais qui deviendront à n'en pas douter notre quotidien de demain.

La cybercriminalité va se « démocratiser » (I). La question de la création d'un parquet national du numérique se pose avec insistance, ainsi qu'à terme celle d'une 33ème chambre correctionnelle dédiée à ces contentieux (II). Devant l'urgence de cette situation, l'ensemble des acteurs doivent

engager dès à présent une consultation collective afin de déterminer comment adapter notre système judiciaire pour apporter une réponse pénale efficace (III).

I. - LA CYBERCRIMINALITÉ, AU CŒUR DU CONTENTIEUX DE DEMAIN

A. La cybercriminalité va se démocratiser

Rien qu'en France, on dénombre 4 165 cyberattaques en 2016 (1) , soit en moyenne une cyberattaque toutes les deux heures. Pour cause, la cybercriminalité est une activité lucrative. En témoigne, l'emblématique affaire *Silk Road*, le plus grand site de vente de drogues au monde qui aurait généré en trois ans un trafic évalué à 1,2 milliard de dollars avec des commissions de l'ordre de 80 millions de dollars. (2)

Ses facettes sont multiples puisque la cybercriminalité va de l'escroquerie aux vols de données en passant par l'usurpation d'identité. Elle renvoie également à la pédopornographie, la diffusion de contenus illicites ou malveillants, l'atteinte aux systèmes de traitements automatisés des données, la contrefaçon, l'espionnage de sociétés ou encore la saturation de sites internet d'entreprises et d'institutions et de particuliers.

Cette activité délictuelle n'a de cesse de prospérer : rien qu'en un an, elle progressé de 67 %. Son coût pour l'économie globale est estimé entre 375 et 575 milliards de dollars (3) . Et encore, ces chiffres relèvent peut être de l'euphémisme, la plupart des victimes restant parfois dans l'ignorance ou préférant ne pas communiquer sur un sujet qui leur donnerait mauvais presse. Selon une étude d'IBM, à l'horizon 2020, les pertes liées aux seules failles de sécurité informatique pourraient ainsi atteindre 3 500 milliards de dollars (4) .

La cybercriminalité, sous tous ses aspects, est un phénomène qui prend de l'ampleur. A l'heure où l'ensemble de notre économie est mise en données - en témoigne l'augmentation du nombre d'objets connectés estimés à 20 milliards en 2020 contre 6 milliards en 2016 (5) - le risque réside dans la démocratisation de cette délinquance, risque d'autant plus grand si un sentiment d'impunité persiste. De l'agriculture jusqu'à l'éducation en passant par l'industrie lourde, la quasi-totalité de nos activités et interactions seront reliées à un système d'information, et, partant, vulnérables aux intrusions et piratages.

Ce constat est inquiétant et les contremesures gouvernementales proposées insuffisantes. Comme le relevait déjà Myriam Quéméner, experte en matière de lutte contre la cybercriminalité pour le Conseil de l'Europe : « *Au-delà des quelques tentatives de la région parisienne, le bilan général révèle un déficit de sensibilisation et de connaissance à tous les niveaux, qui minore la gravité de cette nouvelle forme de délinquance et contribue au manque d'efficacité constaté globalement* ». De toute évidence, il n'a pas encore été pris réellement conscience des enjeux et des dangers de la cybercriminalité. (6)

Cette nouvelle forme de délinquance fait fi des frontières et ne peut être appréhendée qu'à travers son aspect transnational de sorte que la première nécessité réside dans la mise en place d'une coppération internationale efficace. Elle présente en outre un degré de complexité rendant nécessaire une spécialisation pointue des acteurs et des outils afin de mieux comprendre les mécanismes sous-jacents employés, comme dans le cas d'emploi de processus d'anonymisation par le navigateur TOR (*The Onion Router*) ou de demandes de rançon en bitcoin.

Dans l'affaire *Silk Road,* les avocats de Ross Ulbricht ont remis en cause plusieurs aspects de l'enquête, en particulier le comportement de deux agents fédéraux qui auraient tenté d'extorquer et faire chanter le prévenu. Cette affaire complexe avait en effet conduit en août 2015 à la condamnation de Shaun Bridges, membre des services secrets américains, lequel avait plaidé coupable après avoir détourné plus de 800.000 dollars en devise électronique bitcoin alors qu'il enquêtait sur « la route de la soie ». quelques mois plus tard, Carl Mark Force, un agent de la

DEA (*Drug Enforcement Authority*) avait été condamné à 78 mois de prison pour extorsion de fonds et blanchiment d'argent dans cette même affaire.

Fermé par le FBI en novembre 2014, *Silk Road* proposait entre d'autres, d'après l'accusation, des faux papiers, et des services de tueurs à gage. Ross Ulbricht étant notamment poursuivi pour avoir commandité cinq assassinats dans son entourage. Dans un arrêt récent du 31 mai 2017, une cour d'appel de New York a considéré qu'Ulbricht était le fondateur du site, opérant sous le pseudonyme « *Dread Pirate Roberts* », et l'a condamné à la réclusion criminelle à perpétuité.

Ce qui n'a pas empêché de nouvelles plateformes criminelles de voir le jour. En 2015, Agora, Alphaby et Nucleus proposaient ainsi quotidiennement près de 650 000 annonces (7) : « *Les échanges effectués sur ces marchés noirs généralistes témoignaient aussi de la montée rapide en compétences des pirates informatiques : les produits digitaux (logiciels, malware) et leurs guides d'utilisation associés permettaient au premier venu d'acquérir un certain niveau de connaissances et de revendre le fruit de ses activités illégales (données volées) sur ces mêmes plateformes.* » (8)

Cette affaire complexe et l'actualité récente soulignent les spécificités inhérentes aux technologies, et la nécessité de former les prochaines générations d'enquêteurs, de juges et d'avocats pour en appréhender toutes les subtilités.

B. Etats de lieux de l'arsenal français en matière de cybercriminalité

Si les agendas français en matière de cybersécurité et de cyberdéfense semblent bien définis, aucune stratégie d'ensemble n'a encore été suffisamment établie en matière de lutte contre la cybercriminalité, pourtant placée parmi les trois priorités de l'Union inscrites à l'agenda européen de sécurité publié le 28 avril 2015 (9) .

En France, la stratégie de cybersécurité est définie par l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), rattachée au secrétariat général de la Défense et de la sécurité nationale. (10) La ligne de conduite en matière de cyberdéfense est également définie avec le secrétariat général de la Défense et de la sécurité nationale, placé directement sous l'égide du Premier ministre, avec notamment l'élaboration d'un « Livre blanc » publié le 29 avril 2013. (11) En revanche, s'agissant de la cybercriminalité, aucune réforme générale et cohérente n'a encore été entreprise. Traitée comme une problématique parmi d'autres, elle devrait au contraire faire l'objet d'une stratégie spécifique, définie par plusieurs ministères (Intérieur, Défense, Justice, etc.).

La France n'est pas totalement dépourvue dans ce domaine puisqu'elle dispose déjà d'un arsenal juridique et de plusieurs services spécialisés. Néanmoins ceux-ci souffrent d'un manque de coordination, et l'absence d'une politique nationale. En l'état, nos Parquets peuvent compter sur le soutien de services de police, de gendarmerie et de douane dont nous présenterons succinctement les principaux pour mémoire :

- **OCLCTIC** (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) créé en 2000, cet Office est le point de contact unique national dans les échanges internationaux avec Interpol, Europol et le G8H24. (12)

- **ANSSI** (Agence Nationale de Sécurité Informatique) créée en juillet 2009, cette agence veille à détecter et à réagir en cas d'attaques informatiques en particulier sur les réseaux d'Etats et d'opérateurs sensibles (Décret nº 2009-834 du 7 juillet 2009). Elle est désormais chargée, depuis la loi du 18 décembre 2013, de recueillir les déclarations des entreprises chargées d'opérations d'importance vitale (OIV) victimes d'incident de sécurité, auxquelles elle peut imposer des mesures de sécurité. (13)

- **DLCC** (Division de lutte contre la cybercriminalité), créée le 29 avril 2014 et rattachée au Service technique de recherches judiciaires et de documentation (STRJD) de la Gendarmerie nationale. Elle jouit d'une compétence nationale en matière d'infractions liées à la cybercriminalité.

- Une cellule « cyberdouane » compte une vingtaine d'employés. (14)

- **BEFTI** (Brigade d'enquête sur les fraudes et les technologies de l'information) créée en 1994 et composée d'une trentaine d'agents exerçant des missions de prévention et d'assistance auprès des services d'enquête ainsi que d'élucidation des délits et crimes en lien avec la cybercriminalité. Située au sein de la Préfecture de Police de Paris, elle est compétente pour Paris et la petite couronne.

Les plaintes pénales déposées suite à une intrusion informatique ou un vol de données n'aboutissent que trop rarement à la condamnation de leurs responsables. Par ailleurs, du fait du manque de moyens, la priorité est donnée aux attaques touchant les acteurs de premiers plan (sites sensibles, entreprises cotées), or les attaques viseront demain de plus en plus d'acteurs, y compris de petites et moyennes taille, pour laquelle une réponse pénale efficace devra être assurée.

Force est de constater que nous disposons actuellement en France que de trop peu d'enquêteurs spécialisés et de moyens alloués à la lutte contre cette nouvelle forme de criminalité (15) . Tous les acteurs de la société citoyens, grands groupes, associations, collectivités, petites et moyennes entreprises seront concernés. Notre politique pénale doit prioriser les infractions causant les plus grands troubles à notre collectivité, la cybercriminalité en fait partie, à n'en pas douter.

C. Cybercriminalité, une notion floue

La notion de cybercriminalité peut s'avérer floue parce qu'elle ne répond à aucune qualification juridique précise et qu'aucun texte ne la définit. La seule occurrence dans un code se trouve à l' article 694-32 du Code de procédure pénale déterminant la liste des infractions pour lesquels le mandat d'arrêt européen de l'article 695-23 du même Code peut être exécuté sans le contrôle de la double incrimination.

Seuls deux textes internationaux évoquent explicitement la cybercriminalité dans leurs intitulés : la Convention de Budapest sur la cybercriminalité du 23 novembre 2001, et son protocole additionnel du 28 janvier 2003.

Avant de créer un pôle juridictionnel spécialisé en la matière, il conviendrait préalablement de s'accorder sur les affaires qu'il pourrait être amené à traiter. En effet, de nombreux dossiers auront demain une composante numérique, sans pour autant devoir faire l'objet d'une étude particulière par des acteurs spécialisés.

Dans une communication du 22 mai 2007, la Commission européenne énonçait que « *la cybercriminalité devait s'entendre comme des infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'informations ou contre ces réseaux et systèmes* ». L'ANSSI vise également les « *actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un crime ou d'un délit, ou les ayant pour cible* ». La cybercriminalité regrouperait ainsi toutes les

infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet.

En 2014, le pôle d'évaluation des politiques pénales de la Direction des affaires criminelles et des grâces avait réalisé une extraction de la table NATINF (NATure d'INFractions), recensant l'ensemble des infractions définies par la norme française, afin de mieux cerner les types d'infractions concernées par la cybercriminalité. Au total, 248 NATINF étaient recensés. Il s'agit d'infraction rattachée à la cybercriminalité, soit par leur objet, soit parce que leur mode de commission est qualifié par la loi comme une circonstance aggravante.

Si une définition de la notion était trouvée, elle n'emporterait pas nécessairement compétence du Parquet spécialisé en la matière. Seules les affaires présentant un degré de complexité technique ou factuelle important devraient lui être dévolues.

Par ailleurs, l'enjeu majeur d'un Parquet du Numérique serait celui de sa coordination avec les différents services spécialisés déjà existants. Fréquemment, le numérique est un moyen permettant à la grande délinquance organisée de blanchir l'argent par exemple ou de financer des réseaux terroristes : quel serait alors l'acteur compétent ? La question de la centralisation d'une juridiction spécialisée, et de la compétence concurrente avec d'autres juridictions se posera nécessairement.

II. SUR L'OPPORTUNITÉ D'UN PARQUET NATIONAL DU NUMÉRIQUE ET D'UNE 33ÈME CHAMBRE CORRECTIONNELLE DE LA CYBERCRIMINALITÉ

Les spécificités du numérique sont à l'heure actuelle trop peu connues des magistrats. Il conviendrait pourtant de se prémunir contre ce contentieux inédit de masse qui risque, sous peu, d'aggraver l'engorgement des juridictions. L'efficacité de la lutte contre la cybercriminalité est également conditionnée par la mise en place d'une coordination efficace des actions envisagées.

A. Une juridiction spécialisée pour le contentieux numérique complexe

La création d'un Parquet spécialisé dans le numérique permettrait assurément de répondre aux problématiques posées par les infractions propres aux réseaux électroniques, notamment les attaques visant les systèmes d'information, le déni de service et le piratage ainsi que celles commises à l'aide des réseaux de communication électroniques et de systèmes d'information lorsque celles-ci atteignent un certain degré de complexité ou constituent des atteintes particulièrement graves. Son niveau élevé de spécialisation et les outils de haute technologie qui lui seraient confiés permettraient par exemple d'identifier les auteurs ayant recours à des processus de chiffrement et de récolter des preuves rendues plus difficiles à obtenir par des technologies avancées.

L'idée d'une juridiction dédiée au contentieux du numérique n'est pas complétement nouvelle. En 2006 déjà, le rapport Lasbordes préconisait la création d'une juridiction spécialisée (16) . La même idée était reprise par le rapport Bockel du 18 juillet 2012, lequel prévoyait en « *Priorité nº 3 : Introduire des modifications législatives pour donner les moyens à l'ANSSI d'exercer ses missions et instituer un pôle juridictionnel spécialisé à compétence nationale pour réprimer les atteintes graves aux systèmes d'information* ». (17)

Ce rapport détaillait en page 95 ce projet : « *Enfin, pour reprendre l'une des préconisations du rapport Lasbordes, il semblerait utile d'instituer un pôle juridictionnel spécialisé et centralisé pour réprimer les atteintes graves aux systèmes d'information. Les pôles spécialisés ont fait la preuve de leur efficacité, qu'il s'agisse de la lutte contre le terrorisme ou de la lutte contre le blanchiment. Compte tenu de la complexité des atteintes graves aux systèmes d'information, qui nécessitent souvent de passer par l'entraide internationale, il semblerait utile de disposer de magistrats spécialisés, spécialement formés à ces questions, regroupés au sein d'un pôle centralisé, ce qui permettrait également de renforcer la coopération entre les services spécialisés de la police et de la gendarmerie et la Justice* ».

En d'autres termes, comme il a déjà pu l'être justement rappelé : « *Il faudra aussi dans un souci d'efficacité que toute la « chaîne pénale » soit spécialisée, c'est à dire parquet, instruction et juridiction de jugement. Par contre, pour les affaires courantes d'escroqueries par Internet, pédophilie par Internet et affaires moins complexes, on pourrait prévoir d'institutionnaliser le réseau des magistrats « cyber référents » bénéficiant d'une formation obligatoire au plan national tant au niveau du parquet que du siège*. » (18)

L'excellent rapport de référence du magistrat Marc Robert préconisait en février 2014 de substituer au traitement local un traitement centralisé, « *seul de nature à permettre d'effectuer les recoupements nécessaires et de saisir ensuite, et de manière utile, le parquet compétent* » (19) . L'auteur suggérait ainsi de doter le Parquet de Paris d'une compétence concurrente en matière de cybercriminalité d'une certaine gravité.

Plus récemment, lors de la consultation publique réalisée en octobre 2015 en vue du projet de loi pour une République Numérique, le CNNum proposait de créer « *un parquet numérique spécialisé sur les questions de contenus illicites en ligne* » (20) . Néanmoins, le champ de compétence matérielle du projet apparaissait très limité puisque se cantonnant aux contenus haineux sur Internet. Cette proposition n'a donc pas été retenue.

A défaut d'un pôle juridictionnel dédié, il convient toutefois de remarquer l'effort de spécialisation initié en France. Depuis septembre 2014, le pôle financier du Parquet de Paris est divisé en deux sous-pôles : l'un dédié à la protection des personnes, l'autre à la cybercriminalité du fait de son omniprésence en matière d'infractions économiques et financières, comprenant deux magistrats (21) .

Ces transformations organisationnelles se sont accompagnées de nombreux renforcements législatifs en la matière (voir notamment Loi nº 2014-1353 du 13 nov. 2014 renforçant les dispositions relatives à la lutte contre le terrorisme ; Loi nº 2015-912 du 24 juillet 2015 relative au renseignement ; Loi nº 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale). Pour autant, cet effort se fait de manière désordonnée comme le souligne Marc Robert : « *L'efficacité recherchée dans la lutte contre la cybercriminalité aurait sans doute mérité une loi-cadre englobant tous les aspects de cette lutte et mettant en exergue une stratégie d'ensemble*». (22)

Ces évolutions apparaissent à l'évidence insuffisantes, surtout lorsqu'on les compare aux solutions préconisées par d'autres pays européens. En Espagne, par exemple, il existe un Procureur Général en charge de la cybercriminalité, placé directement auprès du Procureur Général de l'Etat. (23) Il coordonne la lutte contre la cybercriminalité et bénéficie de l'aide de 70 parquetiers réunis au sein d'un parquet spécifique dédié à ce type de criminalité. (24)

En France, les JIRS (Juridictions interrégionales spécialisées) commencent timidement à traiter la matière, sauf pour les parquets des TGI dans le ressort des Cours d'appel de Paris et Versailles dans lesquels il existe des magistrats référents, mais pas de services spécialisés (25) . Des

exemples de spécialisation existent pourtant dans d'autres domaines comme le Parquet National Financier. Après quatre ans d'existence, il convient de tirer un premier bilan de cette juridiction afin de constater s'il serait ou non opportun de répliquer l'expérience pour les affaires numériques présentant un certain niveau de complexité, et nécessitant ainsi un degré de spécialisation particulier.

B. S'inspirer du Parquet National Financier (PNF)

Le contexte général de la cybercriminalité est similaire en plusieurs points à celui qui entourait la matière économique et financière avant la création du Parquet National Financier. Revenons un instant sur les raisons à l'origine de la création de ce dernier, devenu un acteur incontournable du paysage judiciaire.

Présenté pour la première fois par la garde des Sceaux à l'occasion du Conseil des ministres du 7 mai 2013 (26) , le projet de loi organique visant à la création d'un Parquet National Financier était motivé par les constats suivants :

- Le coût du manque à gagner résultant de la fraude fiscale et de l'évasion fiscale pour la France s'élevait à une somme comprise entre 40 et 80 milliards (27) (et 1 000 milliards au niveau européen (28)).

- L'aggravation et la complexification de la délinquance économique, laquelle s'apparente de plus en plus à la « *criminalité organisée "classique"*, *la dissémination des actifs des délinquants, le recours à des montages opaques de plus en plus complexes impliquant une multiplicité de flux et d'intervenants au niveau international, rendent les investigations particulièrement délicates à mener*». (29)

- L'absence d'interlocuteur précisément déterminé au niveau national et international ce qui rend les opérations d'entraide internationale difficiles, confirmant le constant selon lequel « *trop souvent, les frontières constituent autant de muraille protectrice de la criminalité internationale* ». (30)

- La spécialisation insuffisamment assurée des magistrats, alors même que l'Union européenne appelle, dans sa directive en préparation à l'époque des débats parlementaires, les Etats membres à demander « *aux personnes responsables de la formation des juges, des procureurs, de la police ainsi que du personnel de justice et des autorités compétentes intervenant dans les procédures et enquêtes pénales de dispenser une formation appropriée*». (31)

- L'insuffisance des moyens humains, techniques et financiers. Les chiffres avancés par le Ministre de la Justice à l'occasion de la présentation du projet de loi le 20 juin 2013 devant l'Assemblée nationale étaient alarmants (32) : 37 enquêteurs spécialisés avaient quitté les brigades spécialisées en quatre ans, entre 2008 et 2011 ; en 2011, seulement 9 instructions relatives à des infractions financières et économiques étaient en cours au pôle d'instruction de Paris contre plus d'une centaine en 2003 ; 11 magistrats étaient en exercice au sein de la section financière de Paris en 2007, seulement 8 en 2011.

Ces cinq principales observations se retrouvent en matière de cybercriminalité. A titre de comparaison, le coût en France en matière de fraude informatique est estimé à 3,7 milliards d'euros en 2016 (33) . Les raisons qui ont motivé la création du PNF sont les mêmes que celles qui doivent conduire à la création d'un Parquet dédié aux infractions du numérique (34) .

En effet, le PNF présente des avantages indéniables : la concentration des moyens et la spécialisation des magistrats ont amélioré le traitement des infractions économiques et financières d'un point de vue aussi bien temporel que qualitatif puisque le PNF jouit d'une approche globale et nationale, ce qui assure par là même une conduite pénale nationale plus homogène et cohérente,

et d'une expérience non négligeable en raison de l'unicité du type de délinquance traité.

Les magistrats peuvent par ailleurs se concentrer sur les seules enquêtes économiques et financières dévolues au PNF car ils échappent aux contraintes chronophages qui pèsent sur les parquets de droit commun, à savoir le traitement en temps réel ou les permanences, il en résulte un temps d'enquête réduit.

Le PNF donne de la visibilité à la politique de lutte contre la fraude fiscale et la délinquance économique et financière ; le Procureur national financier est une « *incarnation de la lutte contre la grande délinquance*» (35) . Il est aussi l'interlocuteur privilégié en matière de coopération internationale, ce qui a eu pour conséquence une bien meilleure entraide avec les autres Etats.

Cependant, bien qu'une autonomie des moyens dédiés à la lutte contre la grande fraude fiscale et la grande délinquance économique et financière ait été entérinée, les moyens effectivement mis en œuvre ne sont pas à la hauteur de ce que l'étude d'impact de la loi prévoyait puisque l'effectif devait se monter à 22 magistrats du parquet pour un maximum de 8 dossiers par membre alors qu'à l'heure actuelle seuls 15 magistrats du parquet sont rattachés au PNF pour 400 affaires (soit plus de 26 par membre). Ils ne sont épaulés que par 4 assistants spécialisés et 10 fonctionnaires.

Enfin, en plus des services d'enquêtes spécialisés déjà existants, des directions interrégionales ou services régionaux de police judiciaire, de la sous-direction des affaires économiques et financières de la préfecture de police de Paris, des sections de recherche de la gendarmerie nationale ou du service national de douane judiciaire, le PNF peut faire appel au nouvel office créé par le décret nº 2013-960 du 25 octobre 2013, à savoir l'office central de lutte contre la corruption et les infractions financières et fiscales (OCLCIFF) (36) , qui constitue son « bras armé ».

Alors que la « criminalité informatique » fait partie au même titre que le blanchiment d'argent et la corruption de la liste des dix « *domaines de criminalité particulièrement grave revêtant une dimension transfrontière résultant du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes* » énumérés par l'article 83 du TFUE , le parallèle pourrait être tentant de créer un Parquet National du Numérique (PNN), travaillant de concert avec l'OCLCTIC.

C. A terme, la création de la 33ème chambre correctionnelle dédiée à la cybercriminalité

Il pourrait également être envisagé à terme de créer une 33ème Chambre correctionnelle spécialisée et exclusivement dédiée au jugement des infractions instruites par le Parquet National du Numérique (PNN), à l'image de la 32ème Chambre correctionnelle, dédiée aux affaires émanant du PNF.

En effet, la 32ème Chambre correctionnelle n'avait pas été initialement envisagée par les projets de loi relatifs au Procureur national financier et à la délinquance économique et financière. Cette nouvelle chambre correctionnelle a pourtant rapidement vu le jour à la suite de l'entrée en vigueur de ladite loi.

Le 9 septembre 2014, à l'occasion de son discours d'installation, le nouveau Président du Tribunal de grande Instance de Paris, Monsieur Jean-Michel Hayat, a fait part de souhait de voir se créer une 32ème chambre correctionnelle : « *nous disposerions d'un audiencement distinct et non commun, permettant ainsi d'éviter la concurrence des urgences. Une telle création permettrait, d'une part, au parquet de Paris de bénéficier d'un désencombrement salutaire, d'autre part au parquet national financier de disposer de plages d'audiencement immédiates, dès que les premières procédures arriveront au début 2015, en phase de jugement* ».

Si le contentieux émanant du PNF était au départ insuffisant à alimenter à lui seul la 32ème Chambre, ce n'est désormais plus le cas. Selon le Président du TGI de Paris, cette nouvelle

Chambre a permis de juger ces affaires dans un délai raisonnable (le délai entre l'ordonnance de renvoi et l'audience sur le fond état en moyenne de trois mois et dix-huit jours (37)) et de désengorger les autres chambres correctionnelles. (38)

Nous avons présenté dans la première partie de cet article les raisons qui nous incitent à penser que le nombre de dossiers de cybercriminalité augmentera significativement dans les prochaines années. Voilà pourquoi il faut réfléchir dès à présent à une politique pénale spécifique en la matière, ce qui passe tout d'abord par la définition des modalités d'une spécialisation de toute la chaine : de la phase d'enquête au jugement. Cette réflexion devra nécessairement s'opérer au niveau national afin notamment de choisir le mode opératoire. A cet égard, quelques premières questions seront introduites ci-après en guise d'ouverture.

III. SUR LA NÉCESSITE D'UNE CONSULTATION PUBLIQUE

Afin de créer une filière judiciaire numérique, plusieurs questions doivent être débattues, notamment sur le type de spécialisation à proposer aux magistrats et la proportion qui devrait être concernée ; sur la centralisation ou la décentralisation d'un tel parquet ; sur la possibilité de mettre en œuvre un parquet au niveau européen.

A. La spécialisation des magistrats

A l'heure actuelle, la formation des magistrats en matière de cybercriminalité est quasi inexistante. Si des formations diplômantes de longue durée sont peu à peu mises en place, comme un DU Cybercriminalité (39) , des cycles approfondis d'études de la criminalité organisée cybercriminalité ou encore un stage de 5 jours à l'OCLCTIC, il n'existe pas de formation initiale complète pour les auditeurs de justice. C'est déjà le cas s'agissant des infractions économiques et financières puisque l'ENM fournit aux auditeurs de justice une formation en rapport avec ce domaine. Cependant, cette formation, aussi bien théorique que pratique, reste légère puisqu'elle représente désormais 11 demi-journées de formation (contre 8 avant 2016) sur 31 mois de formation (40) . L'ENM propose par ailleurs, depuis 2013, des cycles approfondis d'études en droit de l'entreprise (CADDE) pour les magistrats traitant de dossiers économiques et financiers ainsi qu'un stage collectif de 5 jours au sein de l'AMF (41) .

Au stade de la formation continue, le Procureur national financier veille à fournir aux magistrats des connaissances solides, raison pour laquelle a été conclue en 2016 une convention entre l'AMF, l'ENM et le PNF prévoyant le suivi d'une formation dispensée par l'AMF (42) . L'on peut espérer qu'une formation similaire soit mise en place avec la CNIL ou l'ANSSI.

Il n'existe cependant pas de spécialisation prévue par la loi de sorte que le choix des magistrats incombe au Procureur général et au Premier Président de la Cour d'appel de Paris après avis du Président et du Procureur de la République du TGI de Paris. Les magistrats choisis présentent tout de même un lien avec les matières traitées : à titre d'exemple, un magistrat du parquet était auparavant au SNDJ, un autre à l'AMF.

B. Trop de centralisation, un risque pour une défense large du territoire ?

De manière isolée, quelques cas de compétence spécifiques ont déjà été prévus par le législateur. A titre d'exemple :

- Les JIRS bénéficient d'une compétence concurrente en matière de STAD de « *grande complexité* » (article 704 1º du code de procédure pénale).

- Le Parquet de Paris jouit d'une compétence concurrente en cas de cyberattaques en lien avec une entreprise terroriste (Article 706-16 du code de procédure pénale).

- En cas d'infractions constituant des atteintes aux intérêts fondamentaux de la nation au sens de l' article 411-1 du code pénal, une compétence spéciale est reconnue au profit de plusieurs juridictions (Bordeaux, Lille, Lyon, Marseille, Metz, Paris, Rennes, Cayenne et Toulouse, articles 697 et 702 du code de procédure pénale). (43)

Ainsi, concernant des escroqueries commises par le biais d'outils informatiques, un auteur préconise que soit aussi consacrée une compétence concurrente au niveau du TGI de Paris afin de centraliser non pas le contentieux mais l'information, les critères d'attribution devant résider dans la complexité de l'infraction ou de la sophistication des moyens à déployer (44) . En effet, il serait sans doute peu viable de percevoir la cybercriminalité comme un contentieux relevant uniquement de la juridiction parisienne.

La difficulté de la question réside dans la spécificité des infractions liées à la cybercriminalité qui, bien que réalisées en un point, peuvent toucher de nombreuses victimes en un même temps ce qui implique non pas nécessairement une compétence nationale du parquet parisien mais un traitement national préalable à la saisine d'un parquet (45) .

La question de la nature d'un nouveau Parquet se pose aussi : Parquet National, comparable en tous points au PNF, extension et renforcement des JIRS ou encore Parquet dématérialisé ? A titre de comparaison, les débats parlementaires autour de la création du PNF se sont concentrés autour de son utilité. Le Sénat avait par exemple rejeté le projet dans la mesure où ce nouvel acteur allait entrainer une confusion entre les différents parquets. Il était également reproché au projet de prévoir le rattachement de ce nouveau Procureur au Procureur général de la Cour d'Appel de Paris et non au Procureur de la République de Paris, « *lequel est déjà chargé de la gestion de contentieux nationaux*». (46) Les opposants au projet préféraient « *l'extension des pouvoirs des juridictions interrégionales spécialisées avec la création d'un procureur adjoint spécialisé dans la fraude fiscale complexe*». (47)

Si la loi organique a finalement été adoptée, les règles de compétence demeurent pourtant toujours aussi complexes. A titre d'exemple, le PNF dispose tout d'abord d'une compétence exclusive pour la poursuite des infractions boursières, alors qu'elle dispose ensuite d'une compétence concurrente à celle des tribunaux de grande instance de droit commun et des JIRS (juridiction interrégionales spécialisées) pour la poursuite de certaines infractions. Une distinction est faite selon la grande complexité ou non de la procédure.

C. Parquet National versus Parquet européen du Numérique

Le 17 juillet 2013, la Commission européenne proposait la création d'un Parquet européen spécialisé en matière économique et financière. Ce nouveau parquet n'a pas pour objectif de constituer un « *simple instrument procédural* (48) » mais un instrument de coopération entre les Etats membres ayant choisi de participer à sa création. Ainsi, ce Parquet européen n'ambitionne pas de remplacer l'OLAF (Office européen de lutte anti-fraude) qui continue d'exercer ses missions d'enquête (49) , de coordination et d'assistance.

A l'image de ce Parquet ou de l'OLAF, il doit être créé un organe européen coordonnant les actions des parquets nationaux (qui viendrait compléter l'action seulement préventive exercée par le réseau Insafe). Il est primordial d'avoir une politique pénale cohérente au sein de l'Union européenne dans la mesure où la cybercriminalité dépasse souvent et facilement les frontières, l'infraction étant commise à distance.

L'institution de cet organe s'inscrirait dans la politique menée par la Commission européenne, à laquelle adhère le Conseil de l'Union européenne, afin de lutter contre la cybercriminalité, qui vise notamment au renforcement de la sécurité des réseaux et des systèmes d'information (50) .

CONCLUSION

Les données et les intrusions informatiques représentent le contentieux de demain pour lequel nous ne disposons actuellement que de trop peu de moyens et d'expertises. L'urgence nous commande dès à présent de réfléchir à l'évolution du contentieux lié au numérique. C'est avant tout une question de conduite du changement, de sensibilisation, qui permettra d'insuffler une culture du numérique. Anticiper cette évolution dès maintenant est primordiale afin de disposer demain de parquetiers, de services d'enquêtes disposant des connaissances et des moyens nécessaires pour aborder les affaires de cybercriminalité.

Cela nécessite de faire de l'éducation numérique pour les juges et les auxiliaires de justice une priorité (51) . Cela nécessite de définir une politique pénale nationale en matière de cybercriminalité dotée de réels moyens. Créons une délégation interministérielle, placée sous l'autorité du Premier Ministre, afin de définir et impulser une stratégie. Engageons un débat collectif sur ces enjeux, avec les Barreaux, les Ordres, le Conseil National de la Magistrature, et les cabinets des différents ministères concernés.

(1)

The Global State of Information Security Survey 2017 - octobre 2016 http://www.pwc.fr/fr/publications/cybersecurite/gsis-2017.html

(2)

Silk Road Creator Ross Ulbricht Loses His Life Sentence Appeal, Andy Greenberg , Wired, 31 mai 2017 <www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-lifesentence-appeal/>

(3)

Cybercriminalité : l'insuffisante prise de conscience des pouvoirs publics, 19 mai 2017, <www.lefigaro.fr/vox/societe/2017/05/19/31003-20170519ARTFIG00272-cybercriminalite-l-insuffisante-prise-de-conscience-des-pouvoirs-publics.php>

(4)

Cost of Data Breach Study, IBM Study, 2017 <www-935.ibm.com/services/fr/fr/it-services/security-services/cost-of-data-breach/>

(5)

<www.stuffi.fr/20-8-milliards-dobjets-connectes-en-2020/>

(6)

Quéméner M., Le rôle préventif de la justice en matière de cybersécurité, IP/IT 2016 p. 12

(7)

Etude CEIS, juin 2015

(8)

Petit A., Visite guidée du Darkweb criminel, D. IP/IT 2017, p. 86

(9)

Latournerie J.-Y., Cybermenaces et protection des entreprises : une priorité de l'état, D. IP/IT 2016 p. 8,

(10)

<www.interieur.gouv.fr/content/download/101310/797848/file/Lutte-contre-les-cybermenaces.pdf>

(11)

<www.ssi.gouv.fr/uploads/IMG/pdf/2011 02_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf>

(12)

Réseau regroupant les pays signataires de la Convention de Budapest sur la cybercriminalité du 23 novembre 2001

(13)

Daoud E. et Peronne G., Cyberattaques : la lutte s'intensifie, AJ Pénal 2015, p. 396

(14)

Quéméner M., La coopération entre les organes de lutte contre la cybercriminalité. Pour une stratégie globale de « cybersécurité » française, RLDA 2013/87

(15)

Latournerie J.-Y., Cybermenaces et protection des entreprises : une priorité de l'état, D. IP/IT 2016 p. 8, « *lutte contre la cybercriminalité [ ] mobilise aujourd'hui plus de 600 enquêteurs spécialisés des services de police et de gendarmerie* »

(16)

Rapport Lasbordes, janvier 2006 <www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048.pdf> « *Axe 5. Accroître la mobilisation des moyens judiciaires • Reconnaître la spécificité des contentieux liés aux systèmes d'information. • Aggraver les peines prévues au code pénal en matière d'atteinte à la SSI. • Introduire une exception au principe d'interdiction de la rétro-conception dans le code de la propriété intellectuelle pour des motifs de sécurité. • Assurer la sensibilisation des magistrats et des forces de sécurité par la formation initiale et continue. • Constituer un pôle judiciaire spécialisé et centralisé de compétence nationale. • Renforcer les coopérations internationales.* »

(17)

Bockel J.-M., La cyberdéfense : un enjeu mondial, une priorité nationale, <www.senat.fr/rap/r11-681/r11-681.html>.

(18)

Voir. note 15

(19)

Robert M., Protéger les internautes - Rapport sur la cybercrimianlité », Groupe de travail interministériel sur la lutte contre la cybercriminalité, févr. 2014

(20)

Le Gouvernement avait alors jugé que : « *Il existe déjà un service d'enquête spécialisé PHAROS, qui permet de détecter de caractériser efficacement des contenus illicites pour ensuite transmettre les dossiers aux parquets. Il conviendrait néanmoins de davantage sensibiliser les parquets sur ces questions spécifiques et de favoriser une plus grande réactivité de leur part. Il est prévu dans le plan de lutte contre le racisme et l'antisémitisme de rendre les sanctions plus efficaces et plus pédagogiques afin que les personnes qui diffusent des contenus illicites puissent prendre conscience de la teneur de leurs actes et connaître les risques qu'elles encourent en diffusant des discours de haine* ».

(21)

Molins F., Juridictions interrégionales spécialisées - L'action des juridictions interrégionales spécialisées », Cahiers de droit de l'entreprise, 2015, nº 5, dossier 28

(22)

Robert M., Cybercriminalité : les nouvelles réponses législatives, AJ Pénal 2016 p. 412

(23)

Voir note 20.

(24)

D'autres inspirations pourraient être tirées de la « task force » des Pays-Bas réunissant différents acteurs tels que la police, le Parquet et des banques, ou du « Cybercrime Reduction Partnership » en Grande-Bretagne, lieu d'échange entre acteurs gouvernementaux, judiciaires et universitaires sur les questions relatives à la cybercriminalité.

(25)

Seul le parquet du TGI de Paris est doté d'une section spécialisée en matière de cybercriminalité, regroupant des magistrats et des assistants spécialisés, compétente aussi bien pour les atteintes aux S.T.A.D. (système de traitement automatisé de données) que pour les escroqueries et fraudes aux cartes bancaires. Voir Robert M., Protéger les internautes - Rapport sur la cybercrimianlité,

Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, p. 41 : « *enfin, sur le plan judiciaire, seul le parquet de Paris dispose d'une section spécialisée dans la lutte contre la cybercriminalité : la section dite S2 dédiée à "la lutte contre la délinquance astucieuse et la cybercriminalité", qui comprend un pôle cybercriminalité composé de plusieurs magistrats et d'un assistant spécialisé ; elle a à connaître, notamment, de l'essentiel des atteintes aux S.T.A.D. commises à l'encontre des administrations comme des entreprises ayant leur siège à Paris (en l'état, le parquet de Paris est saisi de 600 affaires de cette nature, dont 16 ont donné lieu à saisine de la JIRS) ; quant aux escroqueries et fraudes aux cartes bancaires, elles sont aussi traitées par la même section, qui peut ainsi, les concernant, bénéficier du soutien du pôle spécialisé. Les affaires poursuivies au titre des STAD relèvent ensuite de la compétence de deux chambres correctionnelles dont les membres se sont formés à cet effet* »

(26)

Conseil des ministres du 7 mai 2013, <http://discours.vie-publique.fr/notices/136001059.html>

(27)

Rapport du syndicat national Solidaires Finances Publiques, « Evasions et fraudes fiscales, contrôle fiscal », janvier 2013 <http://archives. solidairesfinancespubliques.fr/gen/cp/dp/dp2013/120122_ Rapport_fraude_evasionfiscale.pdf>

(28)

L'évasion fiscale en chiffres, Le portail de l'économie, des Finances, de l'Action et des Comptes publics, <https://www.economie.gouv.fr/facileco/evasion-fiscale-chiffres-france-europe<

(29)

Circulaire du 23 janvier 2014 relative à la présentation de la loi nº 2013-1117 en date du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière

(30)

Hirtzlin O. et Pinçon et Levarques C., LPA, 28 avril 2014, nº 84.

(31)

Directive 2014/57/UE relative aux sanctions pénales applicables aux abus de marché.

(32)

AN, deuxième séance du jeudi 20 juin 2013, <www.assemblee-nationale.fr/14/cri/2012-2013/20130278.asp>

(33)

<www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_ v3.pdf>

(34)

Le projet de loi était également motivé par la volonté de *Prévenir et détecter le plus en amont possible* la commission d'infractions : il ne s'agissait pas de pallier un vide juridique puisque des textes répressifs existaient déjà mais de contenir le phénomène le plus en amont possible et de le poursuivre jusqu'à son terme ou comme le dit la Garde des sceaux « *il ne s'agit plus de répondre, de réagir, mais bien de mettre en œuvre une politique pénale qui vise, sinon à éradiquer la fraude et la corruption, du moins à les rendre plus difficiles, plus risquées, socialement stigmatisantes et financièrement très coûteuses* », AN, deuxième séance du jeudi 20 juin 2013, <www.assemblee-nationale.fr/14/cri/2012-2013/20130278.asp>

(35)

Rapport de la Commission mixte paritaire, AN nº 1296 et 1297, p. 7.

(36)

Selon la circulaire du 31 janvier 2014, « *cet office est chargé, dans son domaine de compétence, de mener des enquêtes judiciaires à la demande des autorités judiciaires ou d'initiative, d'assister, à leur demande, les services de la police nationale et les unités de la gendarmerie nationale dans le cadre des enquêtes qu'ils diligentent, d'animer et de coordonner, à l'échelon national et au plan opérationnel, les investigations de police judiciaire et les recherches, d'effectuer ou de poursuivre des investigations à l'étranger, de suivre et d'exploiter tout dispositif de signalements, et enfin, de recueillir et de centraliser tout renseignement ou information à des fins opérationnelles ou documentaires* ».

(37)

Hayat J.-M.,La compétence nationale du TGI de Paris, Droit fiscal 2016, nº 238, 495

(38)

Grâce également aux choix de recourir aux procédures de CRPC et de composition pénale.

(39)

Quéméner M., précité, p. 12

(40)

<www.enm.justice.fr/?q=formation-initiale-francais>

(41)

<www.enm.justice.fr/?q=formation-continue-francais<

(42)

Houlette E., l'action du parquet national financier, Joly Bourse, nº 02, p. 154.

(43)

QE nº 88952, 22/09/20 - ordre public - terrorisme - djihad. lutte et prévention. - Thierry Lazaro - Justice, Publication au JO AN 17 mai 2016 :

(44)

Quéméner M., Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme, D. IP/IT 2016, p. 431

(45)

Robert M., Cybercriminalité : les nouvelles réponses législatives, AJ Pénal 2016 p. 412

(46)

,Zarka J.-C. Fraude fiscale et procureur financier : opposition persistante au Sénat, D. 2013, p. 2341.

(47)

Précité.

(48)

Kuhl L. RSC 2017, p. 41.

(49)

A ce titre, l'OLAF est chargé d'enquêter conjointement avec les autorités nationales, de collecter des preuves ou d'intervenir à la demande d'une autorité nationale.

(50)

Chopin F., Les politiques publiques de lutte contre la cybercriminalité, AJ Pénal 2009, p. 101

(51)

Basdevant A., qu'est-ce que le tout numérique que promet Emmanuel Macron ? », LePoint.fr, 29 avr. 2017 <www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/qu-est-ce-que-le-tout-numerique-que-promet-emmanuel-macron-29-04-2017-2123624_56.php>