Sécurité globale

N° 15, nouvelle série [N° 41 de la série originale]

Sécurité globale

Editions ESKA
12, rue du Quatre-Septembre - 75002 Paris
Tél. : 01 42 86 55 65 - Fax : 01 42 60 45 35
Site : www.eska.fr

RECOMMANDATIONS AUX AUTEURS

Le comité de rédaction de la revue est ouvert à toute proposition d'article.

Les auteurs sont priés de respecter les lignes directrices suivantes quand ils préparent leurs tapuscrits :

- ✔ Les articles ne doivent pas dépasser 40 000 signes (notes et espaces comprises).
- ✔ Les articles doivent êtres inédits. Si justifié par un intérêt éditorial précis, la rédaction accepte néanmoins les versions longues et étayées d'articles préalablement parus.
- ✔ Deux résumés, l'un en français, d'une dizaine de lignes maximum et un autre, en anglais, de la même importance, doivent être fournis avec le manuscrit, accompagnés de la qualité et la liste des dernières publications de l'auteur.
- ✔ Une bibliographie sommaire peut éventuellement être jointe aux articles.
- ✔ Les auteurs feront parvenir leur article par Internet à l'adresse suivante : agpaedit@wanadoo.fr en format MS Word (.doc ou .rtf) ; Times New Roman 11 justifié, interlignes simples.
- ✔ Les auteurs doivent joindre dans un fichier séparé portant mention de l'ensemble de leurs contacts : courriel, adresse postale et le cas échéant numéro de téléphone.
- ✔ L'article doit être présenté de la manière suivante : titre en Times 14, suivi, à chaque fois à la ligne, du prénom et du nom de l'auteur, de sa qualité (notice biographique), du résumé français/anglais et du corps du texte.
- ✔ Les auteurs sont invités à structurer leurs analyses par intertitres afin de faciliter la lecture.
- ✔ Lors de la remise de l'article à la rédaction les fichiers Word doivent être titrés de la façon suivante : NOM (de l'auteur en majuscules) – titre (de l'article en minuscules).
- ✔ Tous les tableaux, graphiques, diagrammes et cartes doivent porter un titre et être numérotés en conséquence et sourcés s'ils ne constituent une œuvre originale. Toutes les figures doivent être transmises séparément en fichiers jpeg ou pdf d'une résolution suffisante (idéal 300 dpi) et leurs emplacements doivent être clairement indiqués dans le texte.
- ✔ Réduire au minimum le nombre de notes, et les placer en notes de fin selon le système de référencement Word.
- ✔ Tous les textes qui ne correspondraient pas aux critères linguistiques standards et aux exigences de rigueur critique seront renvoyés aux auteurs pour adaptation.
- ✔ Une attention particulière devra être portée à la ponctuation : guillemets français, majuscules accentuées (État, À partir de, Égypte, etc.) et à un usage modéré des majuscules conformément aux règles typographiques.

Référence : Collectif, *Lexique des règles typographiques en usage à l'imprimerie nationale*, Imprimerie Nationale, Paris, 2002.

Les articles signés expriment la seule opinion de l'auteur et ne sauraient engager la responsabilité de la revue.

Sécurité Globale | N°15, nouvelle série | N°41, série originale

Revue trimestrielle | © Editions ESKA 2018

ISSN : 1959-6782 • ISBN : 978-2-7472-2837-4 • CPPAP : 0921 T 90246

Imprimé en France

Sommaire

N°15

DOSSIER
Cybermonde : état des lieux, perspectives, risques et périls

Chroniques et rubriques

Cybermonde

État des lieux, perspectives, risques et périls

Dossier rassemblé et préparé sous l'autorité de Mme **Myriam Quéméner**. Magistrate, elle fut sous-directrice de la justice pénale générale à la Direction des affaires criminelles et des grâces ; substitut général à la Cour d'appel de Paris ; conseiller juridique du préfet chargé de la lutte contre les cyber-menaces. Mme Quéméner est aujourd'hui Avocat général près la Cour d'appel de Paris & expert ès-cybercriminalité au Conseil de l'Europe.

Pour une lutte plus efficace contre la cybercriminalité

Myriam Quéméner
Avocat général près la Cour d'appel de Paris, docteur en droit

La cybercriminalité[1] est par nature une criminalité organisée, internationale qui abolit les frontières par le biais des réseaux numériques. Le cyberespace offre un champ numérique sans limite, des outils désormais facilement accessibles ainsi qu'une multiplication des victimes potentielles ce qui a pour effet de renforcer la nocivité du phénomène criminel. Par ailleurs, les défis en termes de sécurité des systèmes d'information sont croissants, d'une part compte tenu de l'aggravation des cybermenaces[2], et, d'autre part en raison du recours toujours plus important à des systèmes abritant des données personnelles souvent sensibles. La cybersécurité est aussi l'un des enjeux majeurs du XXIe siècle et figure d'ores et déjà à l'agenda du législateur européen et la lutte contre la cybercriminalité[3] est désormais au coeur des priorités des gouvernants.

Des cyberenjeux de taille

Les normes pénales peinent parfois à s'adapter à la cybercriminalité car, outre les problématiques découlant du caractère transnational des enquêtes et des poursuites, les technologies en évolution perpétuelle génèrent pour les criminels de nouveaux modes d'action.

Les données numériques constituent désormais un réel enjeu de pouvoir entre les États qui veulent s'assurer le contrôle sur celles qui circulent sur leur territoire, et entre les entreprises privées qui fournissent les réseaux qu'elles empruntent. Véritables richesses immatérielles, l'intérêt qu'elles suscitent reflète les transformations que connaît la géopolitique à l'ère numérique : remise en cause des frontières physiques nationales, affirmation d'acteurs privés et non étatiques, « numérisation » des conflits revendications de souveraineté sur le cyberespace, attaques informatiques.

Maîtriser la donnée suppose de connaître ses moyens et ses conditions de production, ses canaux de transmission, et son mode et son lieu de stockage[4]. La donnée, créatrice de valeur et de pouvoir « fait le lien entre

espaces physiques et numériques » Les données et leur maîtrise reconfigurent les rapports de force au plan stratégique et économique et donnent lieu à de nouvelles représentations de souveraineté.

On assiste aussi au développement de « cyberparadis » sortes d'états aux législations faibles voire inexistantes, l'inadaptation des outils juridiques traditionnels parce que trop longs à mettre en œuvre[5] alors que la preuve numérique est éphémère, rend plus difficile l'identification des cybercriminels. Lorsqu'il s'agit d'attaques contre les systèmes de traitements automatisés de données comme les attaques en déni de service distribué, piratages informatiques notamment, particulièrement celles lancées depuis l'étranger.

La dimension internationale de la cybercriminalité[6] implique d'harmoniser les législations nationales ou à tout le moins, de faciliter la coopération au niveau européen et international afin de renforcer les moyens de lutte contre ce phénomène. Les poursuites judiciaires peuvent se heurter ou être ralenties par le caractère international de cette criminalité.

Lorsque les prestataires ne sont pas établis dans l'Union européenne il convient d'avoir recours à une demande d'entraide pénale internationale. La mise en œuvre de ces procédures peut être rendue encore plus complexe en cas de localisation des données de ce prestataire au sein de multiples pays. Cela peut alors susciter d'autres questions tenant à la localisation des données et à la détermination des juridictions territorialement compétentes pour y accéder.

Les enjeux sont très forts et il ne faut pas négliger leurs aspects géopolitiques et stratégiques avec l'émergence de législation extraterritoriale risquant de porter atteinte à l'Europe comme *le* Clarifyng Lawful Overseas use of data Act *ou Cloud act*. S'il est vrai que *le Cloud Act*[7], adopté par le congrès américain le 23 mars 2018 prévoit que les données ne pourront être transférées que dans des cas limitativement énumérés (poursuite et prévention d'infractions graves, identification précise des informations demandées et de la personne en cause, etc.), il convient d'être vigilants.

Ainsi, à la compétition géopolitique entre les pays les plus puissants, se superpose également un affrontement dans le cyberespace, dans un curieux mélange de défense de la souveraineté nationale et de recherche de l'extraterritorialité la plus large. Il convient de ne pas négliger la menace de la captation des données par un oligopole d'entreprises utilisant leur position dominante pour faire obstacle à de nouveaux acteurs. En dehors de ces aspects, il existe aussi des extraterritorialités « rampantes », liées aux technologies numériques et dont l'exemple le plus spectaculaire est celui des États-Unis.

Face à ce phénomène, la France réagit et construit une législation protectrice d'une part de ses systèmes d'information avec la

directive Network information security (NIS) transposée en France en février 2018 et d'autre part de ses données personnelles avec le Règlement Général sur la Protection des Données (RGPD) qui a une dimension extraterritoriale en imposant à toutes les entreprises des mesures pour protéger les données personnelles. La législation européenne s'inscrit dans une démarche de souveraineté, à commencer par celle de chacun sur ses données à caractère personnel.

Progrès et perspectives

L'Union européenne s'est dotée de dispositifs de coopération policière et judiciaire facilitant la lutte contre l'insécurité. L'Union européenne a en effet très tôt perçu les enjeux entourant la cybercriminalité. C'est donc en ce sens qu'elle a mis en place en janvier 2013 le centre européen de lutte contre la cybercriminalité au sein d'Europol[8] (l'office européen de Police). Ce centre aussi appelé EC3 (pour *European Cyber-Crime Center*) a donc pour objectif principal de lutter contre la cybercriminalité.

Au niveau des textes, rappelons tout d'abord que la convention dite de Budapest du Conseil de l'Europe sur la cybercriminalité signée le 23 novembre 2001 et ratifiée en France le 19 mai 2005 demeure l'instrument international contraignant de référence en matière de lutte contre la cybercriminalité.

Un deuxième protocole additionnel à cette convention[9] est en cours de rédaction depuis septembre 2017 qui envisage des mesures visant à simplifier la coopération judiciaire entre les 56 pays adhérents à la convention et à faciliter la coopération directe avec les fournisseurs de services sur Internet des autres pays membres. Sont notamment étudiées 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.

Ces travaux sont en cohérence avec ceux réalisés dans le cadre de l'Union Européenne et la conclusion de ce projet est attendue pour 2019.

Dans le cadre de l'Assemblée générale des Nations Unies, la Commission pour la prévention du Crime et la Justice pénale a été chargée de constituer en 2011 un groupe intergouvernemental d'experts (IEG), dédié à la rédaction d'une étude approfondie sur le phénomène de la cybercriminalité. Ce groupe a rendu son rapport en 2013 ; il a été mis en évidence une division de la communauté internationale sur l'opportunité de compléter ou non le cadre juridique existant.

Les débats mettent en évidence des divergences importantes sur les instruments juridiques internationaux à utiliser dans la lutte contre la cybercriminalité. Une majorité d'États, dont la France, se sont montrés réticents à un nouveau texte juridique international, se prononçant en faveur de

l'utilisation de la Convention de Budapest comme base juridique pour la lutte contre la cybercriminalité.

L'une des solutions passe par à notre sens par l'élaboration d'un véritable droit de la cybersécurité[10] cohérent et non plus éparpillé dans de multiples codes et textes.

La décision d'enquête européenne (DEE)

La directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale[11] présente l'intérêt d'unifier le droit européen de la recherche de la preuve. La décision d'enquête européenne remplace l'ensemble de ces procédures et apparaît ainsi comme un élément d'une indispensable simplification des procédures[12]. Elle constitue une avancée significative dans le domaine de la coopération judiciaire en fournissant un instrument plus conforme au niveau d'ambition juridique de l'Union européenne et aux défis de la criminalité auxquels elle est confrontée.

Cet outil devrait s'affirmer comme essentiel pour lutter efficacement en Europe contre la criminalité dont la dimension transnationale ne cesse de se développer. Il doit également être l'occasion de favoriser un traitement plus systématique de la criminalité dans ses différentes facettes notamment économique et financière.

Nouvelle directive relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces

La Commission européenne entend se doter de moyens supplémentaires capables de répondre aux cyberattaques. Selon elle, le cadre juridique actuel relatif à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (décision-cadre 2001/413/JAI, 28 mai 2001) n'étant plus en phase avec les défis et les évolutions technologiques d'aujourd'hui, elle propose d'adopter des mesures efficaces en matière de « cyber dissuasion » et de répression par le droit pénal *via* une nouvelle directive.

En outre, la directive[13] proposée élargira le champ des infractions relevant de la cybercriminalité en y incluant les transactions effectuées par le biais des monnaies virtuelles. Elle introduira également des règles communes relatives au niveau des peines pour une durée minimale allant de deux ans à cinq ans pour les plus élevées. Par ailleurs, elle clarifiera la portée de la compétence juridictionnelle des États membres en ce qui concerne ces infractions et garantira les droits des victimes de la cybercriminalité.

Enfin et en renforçant la coopération en matière de justice pénale à l'échelle européenne, la directive aura pour objectif de faciliter l'accès transfrontalier aux preuves électroniques. En ce sens, la Commission présentera au mois d'octobre 2018 les ré-

sultats de ses réflexions sur le rôle du cryptage dans les enquêtes pénales.

Le projet de directive et de règlement e-evidence

La Commission européenne a présenté le 17 avril 2018 un projet de directive et un projet de règlement sur l'accès aux preuves électroniques en matière pénale qui devront être adoptés par le Conseil de l'Union européenne et par le Parlement européen. Aujourd'hui, les autorités répressives sont souvent tributaires du bon vouloir des prestataires de services à leur remettre les preuves dont elles ont besoin. L'objectif est de procurer une sécurité juridique aux entreprises et aux prestataires de services en appliquant des règles identiques pour ordonner la fourniture de preuves électroniques.

Ces textes prévoient notamment de créer une injonction européenne de production : cela permettra à une autorité judiciaire d'un État membre de demander des preuves électroniques (telles que des courriels, des SMS ou des messages échangés dans des applications) directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données ; ce prestataire sera alors tenu de répondre dans un délai de 10 jours, et dans les 6 heures en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire).

Empêcher l'effacement de données au moyen d'une injonction européenne de conservation : cela permettra à une autorité judiciaire d'un État membre de contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données afin que ladite autorité puisse demander ces informations ultérieurement par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production.

Les nouvelles règles garantissent une solide protection des droits fondamentaux, comme l'intervention d'autorités judiciaires et des exigences supplémentaires pour l'obtention de certaines catégories de données. Elles comportent également des garanties concernant le droit à la protection des données à caractère personnel. Les prestataires de services et les personnes dont les données sont demandées bénéficieront de plusieurs garanties, parmi lesquelles la possibilité, pour le prestataire de services, de demander un examen si, par exemple, l'injonction constitue une violation manifeste de la charte des droits fondamentaux de l'Union européenne.

Contraindre les prestataires de services à désigner un représentant légal dans l'Union : afin que tous les prestataires qui proposent leurs services dans l'Union européenne soient soumis à des obligations identiques, même si leur siège est situé dans un pays tiers, les nouvelles règles leur imposent de désigner un représentant légal

dans l'Union pour la réception, le respect et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres à des fins de collecte de preuves en matière pénale.

La compétence des acteurs institutionnels

Les officiers de police judiciaire se spécialisent, les douaniers aussi et progressivement les magistrats doivent suivre cette voie. La création en septembre 2014 de la **section F1 du parquet de Paris** spécialisé en cybercriminalité, ainsi que la récente **compétence nationale concurrente**[14] **de la juridiction parisienne en matière d'attaques informatiques** (atteintes aux STAD) facilitent la coordination dans le traitement de la cybercriminalité[15]. Ainsi, il ressort que la compétence concurrente en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) peut être appréhendée à travers plusieurs critères objectifs, parfois cumulatifs comme la pluralité d'auteurs ou de victimes. La technicité des moyens employés ou du mode opératoire mis en place (affaire « Mirai » ; attaque de type « Black box » visant des DAB ; forum de cybercriminels sur un Darknet…) ; La dimension nationale ou transnationale des faits ou de l'infrastructure (les demandes d'entraides pénales internationales vers la Chine et la Russie sont fréquentes en ce domaine ; coordination requise en lien avec les structures que sont EUROPOL, EUROJUST et INTERPOL) ; La qualité des victimes de la cyber-attaque (STAD mis en oeuvre par l'Etat, mais aussi par les OIV, ou des systèmes informatiques liés à des personnalités de premier plan…), le service d'enquête étant alors fréquemment la DGSI, bénéficiant de l'expertise technique de l'ANSSI.

Cependant les effectifs restent insuffisants et les formations doivent être obligatoires désormais pour les magistrats tant du siège que du parquet ayant en charge ces « cyberprocédures ».

En outre, n'oublions pas qu'en 2020, le parquet européen[16] sera une réalité, ouvrant ainsi la voie d'une coopération renforcée que 20 États (bientôt 21 les Pays-Bas rejoignant l'entente à l'été 2018) se sont engagés à concéder une partie de leur souveraineté afin de lutter plus efficacement contre les atteintes aux intérêts financiers de l'Union européenne. Mais le Règlement n° 2017/139 du 12 octobre 2017 et la directive « PIF » (n° 2017/1371 du 5 juillet) sont loin de régler toutes les difficultés. L'évolution du parquet européen sera observée non seulement par les États membres qui ne font pas encore partie de la coopération renforcée, mais aussi à l'international car il constitue un mécanisme très innovant de lutte contre les fraudes massives qui privent chaque année les États de milliards d'euros de recettes fiscales. Il n'est pas à exclure à moyen terme une extension du champ de compétence à des formes de criminalité en lien avec le numérique. Or, le succès ou l'échec de l'institution dépendront en grande partie du contenu des textes de transposition de la

directive, qui doivent être adoptés avant le 6 juillet 2019.

La coopération public/privé

Dans la mesure où la preuve des cyberattaques ne peut se faire sans le recours au secteur privé qui en détient souvent des éléments déterminant, la lutte contre ce fléau implique un renforcement des échanges avec aussi bien les géants de l'Internet qu'avec les opérateurs. Par exemple, un accord vient d'être conclu entre Orange et Europol portant sur le partage de connaissances sur les différentes cybermenaces, symbolisé par un échange des informations sur l'état et la menace sur les réseaux, mais aussi les tendances en matière de cybercriminalité. L'opérateur français a accepté de transmettre à Europol des indicateurs qu'il peut voir passer sur ses réseaux, comme la fraude, les spams ou les cyberattaques mobiles et bancaires. A travers cette action, Orange, qui est présent dans sept pays européens comme opérateur de télécommunications, espère offrir à ses clients et aux utilisateurs du monde entier « *un Internet plus sûr* ». Leurs efforts conjugués ont pour but de créer un cyberespace plus sûr pour tous les acteurs de l'Union européenne : citoyens, gouvernements et entreprise.

On peut citer l'opération récente hors norme « *black* Hand » menée à l'initiative des douanes qui a démantelé l'une des plus importantes plateformes illégales actives en France sur le « dark web ».

Pour conclure provisoirement, les axes d'amélioration en matière de lutte contre les cybermenaces impose une accélération des processus de l'élaboration de la norme juridique face à la rapidité de l'évolution des fonctionnalités du numériques. Les pistes de travail doivent se concentrer d'une part sur les processus d'accès à la preuve numérique qu'il convient de normaliser dans un objectif de sécurisation juridique et d'autre part sur l'identité numérique afin de pouvoir identifier les auteurs de ces actions malfaisantes.

Notes

[1] M. Quéméner et Y. Charpenel, Cybercriminalité. Droit pénal appliqué, Paris : Economica, coll. Pratique du droit, 2010, p. 7

[2] Ministère de l'Intérieur, rapport relatif à l'état de la menace liée au numérique en 2018 .www.interieur.gouv.fr

[3] Veille de W. Roumier, Justice pénale dans le cyberespace, Droit pénal n° 7-8, Juillet 2017, alerte 48

[4] M. Quéméner, le droit face à la disruption numérique, LGDj 2018

[5] 10 mois en moyenne pour les demandes d'entraide pénale internationales (CRI ou MLAT – Mutual Legal assistant Treaty - pour les USA), délai maximum de réponse à une décision d'enquête européenne (European Investigative order) fixé à 120 jours.

[6] Dossier : Cybersécurité, cybercriminalité : quelles réponses stratégiques et juridiques ? Dalloz IP/IT/Dalloz IP/IT 2018. 158 — 19 mars 2018

[7] G. Mathias, A. Alfer, Conséquences du Cloud Act pour les européens ? Revue expertises Juin 2018

[8] Office européen de police

[9] P. Berthelet, aperçu de la lutte contre la cybercriminalité dans l'Union européenne, RSC 2018 p. 59

[10] T. Douville, L'émergence d'un droit commun de la cyber-sécurité, Recueil Dalloz ? D. 2017. 2255 — 16 novembre 2017

[11] https://eur-lex.europa.eu

[12] T. Cassuto, La directive concernant la décision d'enquête européenne en matière pénale – AJ pénal 2014. 338

[13] Dalloz actualité 25 septembre 2017, Communiqué de la Commission européenne, 19 sept. 2017, IP/17/3193

[14] Loi du 3 juin 2016

[15] Par exemple sur le traitement des rançon-giciels (dépêche DACG du 10 mai 2017 n°2017/0058/MI2C).

[16] Dossier : Parquet européen : c'est parti ! – AJ pénal 2018. 275

Le Darknet est-il une zone de non droit ?

Adel Jomni
Enseignant-chercheur, Université de Montpellier

"Le vice, toujours sombre, aime l'obscurité."
Nicolas Boileau / Epitre VIII

1. Du monde visible au monde invisible

Bien souvent le Darkweb est décrit comme la « face cachée d'Internet »[1] par analogie avec la partie émergée d'un iceberg[2]. Le Web est composé essentiellement de trois parties :

1.1. Le Clear Web

C'est la partie émergée de l'iceberg. Elle est connue sous le nom de « Clear Web» ou « Web visible ». C'est le contenu véhiculé par l'Internet et accessible via les moteurs de recherche classiques de type Google, Yahoo, Bing, etc.

Les moteurs de recherche utilisent des « web crawler » ou « robot d'indexation » afin d'identifier automatiquement toutes les pages du web, de les indexer et de les référencer. Les ressources indexées par le robot sont analysées par des algorithmes afin d'optimiser leur « *référencement* », ce qui permet d'améliorer la pertinence des recherches effectuées avec le moteur de recherche.

1.2. Le DeepWeb (ou toile profonde)

Au-delà du « Clear Web », on retrouve des pages (ou sites) web non-indexables par les robots des moteurs de recherche. Ces pages constituent le « DeepWeb ou *toile profonde* ». C'est la « *partie de la toile qui n'est pas accessible aux internautes au moyen des moteurs de recherche usuels* »[3]. Cette partie représente, selon les estimations, environ 90% du contenu total d'Internet[4].

1.3. Darknet / Darkweb

Un Darknet (appelé Internet clandestin[5]) est un *ensemble de réseaux distribués de type F2F (Friend to Friend) conçus pour assurer l'anonymat des utilisateurs.* Les Darknets ne constituent pas un réseau physiquement distinct, mais bien des protocoles de transmission qui fonctionnent au sein de réseaux existants[6]. Ces protocoles ont volontairement été créés afin d'échapper à tout référencement par des robots d'indexation, et le plus souvent pour préserver l'anonymat des internautes.

1.4. Fonctionnement du Darknet

Le fonctionnement du *Darknet* repose sur trois facteurs essentiels[7] :

- l'usage de l'infrastructure Internet ;
- l'existence de protocoles spécifiques permettant la constitution de « sous-réseaux » non indexables ;
- des architectures décentralisées de type « *peer to peer* » ou « *mix net* » afin de partager du contenu, le plus souvent anonymement.

Il existe une multitude de *Darknets* comme *GNUnet, Freenet,* I2P, *Retroshare,* mais le plus connu et le plus populaire des *Darknets* reste le réseau *Tor* (The Onion Router) qui utilise la racine « *.onion* ». Le réseau *Tor* permet d'anonymiser les flux de connexions TCP/IP afin de rendre non-identifiable l'origine d'une session de navigation Web ou de messagerie instantanée. Cet anonymat est garanti par le routage complexe des données "en oignon", c'est-à-dire en utilisant un cryptage par couches successives.

Cependant, l'anonymisation du flux n'est pas suffisante, car l'application peut potentiellement transmettre des informations annexes permettant d'identifier la personne : c'est pourquoi les équipes en charge du projet *Tor* ont également développé un navigateur Web dédié à ce Darknet intitulé « *Tor Browser* [8]», ainsi que d'autres applications spécialement conçues pour préserver l'anonymat de leurs usagers[9].

Le Darkweb constitue le contenu publié sur cette infrastructure qui est le Darknet. C'est un ensemble de sites internet non référencés par les moteurs de recherche traditionnels et s'appuyant sur un réseau crypté. La majorité des sites du Darkweb utilisent le système de cryptage de Tor. Souvent la notion de Darkweb est utilisée pour désigner aussi le Darknet.

2. Le Darknet confronté au droit

Historiquement, le Darknet a été conçu pour créer un réseau sécurisé à destination des agences gouvernementales, des opposants politiques en danger, des lanceurs d'alertes, des militants, des journalistes. C'est bien l'enjeu initial de la naissance de ce type de réseau.

L'anonymat quasi total du Darknet l'a transformé en un lieu idéal pour exercer des activités illégales. Dans une étude réalisée en 2016 sur plus de 2 700 sites consul-

tables à partir du *Darknet*, les chercheurs Daniel MOORE et Thomas RID ont avancé que « seulement » 57% du contenu était illicite[10]. Ce pourcentage avancé est cependant à relativiser dans la mesure où le contenu présent sur le *Darknet* est très difficilement quantifiable : par exemple de nombreux sites hébergeant des contenus illicites ne sont ouverts que durant quelques heures avant d'être fermés, puis répliqués à nouveau et accessibles via un lien différent.

2.1. Le monde virtuel de l'économie souterraine

L'activité criminelle sur le *Darknet* est devenue très professionnelle. C'est un véritable marché guidé par la demande. Le crime s'y est organisé en adaptant la qualité et la diversité de ses offres de service. On parle même de plateforme « *Crime-as-a-Service* ». Il est possible de retrouver sur le Darknet :

- des sites sur lesquels les pirates publient des informations personnelles et confidentielles d'individus ou d'entreprise (*doxing*) ;
- de nombreuses « boutiques » permettant d'acheter des cigarettes de contrebande, des faux papiers (passeports, cartes d'identité, cartes SNCF...), des faux médicaments, de la fausse monnaie (euros, livres, dollars...), des armes... ;
- des sites de dons à des organisations terroristes ;
- de la pédopornographie ;
- des services de « *Hack-as-a-Service* » offrant des virus prêts à l'emploi (RAT, Trojans, DDoS) ;
- des forums de conseil en piratage et des sites d'échanges entre criminels.

2.2. Développement des cryptomarchés

De nombreuses places de marché proposant des moyens de paiement cryptographiques se trouvent sur le *Darknet*, ce sont des « *cryptomarchés* ». Parmi ces places de marché, on trouve des « marchés noirs » proposant divers produits illicites.

Sur ces cryptomarchés, il est impossible de connaître son interlocuteur et aucun recours de l'acheteur n'est possible en cas de problème relatif à la transaction. Afin de limiter ces risques, les acheteurs ont recours à des « tiers de confiance », appelés également *escrows*, afin de jouer un rôle d'intermédiaire dans la transaction. Il s'agit en quelque sorte de la mise sous séquestre d'une somme d'argent qui ne sera versée au vendeur qu'au moment de la réception de la livraison par l'acheteur. En cas de litige, ces *escrows* sont également en charge d'une sorte de procédure de médiation. Parfois, certains vendeurs jouissant d'une bonne réputation exigent une procédure de finalisation anticipée appelée « *Finalize Early* ».

Le processus d'achat est le suivant[11] :

- ouverture d'un compte sur la plate-forme de vente visée. On utilise naturellement une adresse mail anonyme ;
- anonymisation de ses Bitcoins à travers un Bitcoin mixer ;

- passation de commande. Les échanges directs avec le vendeur se font par messagerie anonyme chiffrée ;
- approvisionnement de son compte Bitcoins auprès du service *escrow* ;
- réception de la commande généralement envoyée par circuit postal classique. De l'avis général, les vendeurs montrent une grande expertise dans leur capacité à conférer à leurs envois un aspect anodin;
- déblocage des fonds auprès de *l'escrow* ;
- évaluation du vendeur sur le site. La réputation de ce dernier étant essentielle afin d'attirer la confiance des autres acheteurs.

2.3. Absence de vide juridique pour le Darknet

Tous les systèmes d'information grâce auxquels fonctionnent les réseaux Internet, et tous les sites Internet quels qu'ils soient, sont assimilés à des systèmes de traitement automatisé de données, plus communément appelés « STAD »[12]. Cette qualification juridique n'a d'effet que pour qualifier les atteintes perpétrées sur ces STAD (maintien frauduleux, extraction...).

L'état actuel du droit ne consacre pas de régimes spécifiques propres aux différents « réseaux » d'Internet (Clearweb, Deepweb, Darkweb). Les technologies déployées derrière ces réseaux, qui constituent le support de l'information permettant sa publication en ligne, sont transparentes aux yeux du législateur français pour la qualification d'infractions pénales, sauf quelques exceptions. On parle du principe de « neutralité technologique ».

Nombres d'actes répréhensibles pénalement sont déjà commis au quotidien sur le *Clearweb* (pédopornographie, recel...). On retrouve de tels actes sur le *Darkweb*, à la différence près que ce type de réseau est plus propice à l'illicéité grâce à l'anonymat qu'il propose.

On peut cependant relever que l'usage d'un logiciel d'anonymat peut devenir illicite, alors que son utilisation n'est pas en soi répréhensible. C'est ainsi le cas lorsque ce type de logiciel est utilisé pour masquer l'identité d'un individu postant des articles faisant l'apologie du terrorisme. Une telle publication étant de base réprimée par l'article 421-2-5 du Code pénal, le fait d'entraver l'efficacité des procédures permettant de remonter jusqu'à cet individu, via notamment un logiciel d'anonymat, est condamné par l'article 421-2-51 du même code.

Pour apprécier la licéité ou l'illicéité d'un site Internet, il convient d'en étudier surtout le « *contenu* », c'est-à-dire l'ensemble des informations présentes sur le site, plutôt que le « *support* », c'est-à-dire la technologie utilisée pour mettre le site Internet en ligne. Le contenu d'un site Internet peut s'apprécier au regard de deux biais : le contenu relatif à une obligation formelle (les mentions légales), et le contenu « libre » publié par un individu.

2.3.1. La licéité du contenu formel

Concernant le contenu formel, il est intéressant d'évoquer le cas des sites Web proposant des services de « *commerce électronique* » au sens de l'article 14 de la loi pour la Confiance dans l'Économie Numérique (dite « LCEN ») du 21 juin 2004[13]. Ces sites doivent se soumettre à des obligations d'information spécifiques en plus de respecter les principes issus du droit général encadrant la réalisation de leurs transactions. Parmi ces informations on retrouve notamment, au titre des articles 6 et 19 de la LCEN, les noms et prénoms des personnes physiques proposant le service, ou à défaut la raison sociale de la personne morale, l'adresse où cette personne est établie, son adresse électronique, ainsi que ces coordonnées téléphoniques permettant de rentrer en contact avec elle, le numéro d'inscription au RCS ou son régime d'autorisation.

Sur le Darkweb, ces services de commerce électronique connus sous le nom de « cryptomarchés », utilisant des cryptomonnaies dans leurs transactions, sont aussi soumis aux obligations d'information prévues par la LCEN.

2.3.2. La licéité du contenu « libre »

Le contenu libre représente l'ensemble du contenu posté à l'initiative du créateur de la page web, et parfois même des internautes. En reprenant l'exemple des cryptomarchés évoqués précédemment, il convient de rappeler à titre liminaire le grand principe issu du code civil selon lequel : « *il n'y a que les choses qui sont dans le commerce qui puissent être l'objet des conventions* »[14]. En d'autres termes, les choses « hors commerce » (drogues, images pédopornographiques...) ne peuvent pas faire l'objet d'une vente, d'un échange ou de toute autre transaction.

En guise d'exemple, en matière de terrorisme, le code pénal sanctionne différents comportements comme : le fait de procéder à des infractions informatiques en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur[15], de participer au financement d'une telle entreprise[16], le fait d'adresser à une personne des offres ou des promesses afin qu'elle participe à un groupement terroriste, le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures prévues à l'article 6-1 de la LCEN ou à l'article 706-23 du code de procédure pénale[17].

L'exemple cité ci-dessus n'est pas isolé. En effet, en matière de vente de stupéfiants, le code pénal réprime également le fait : de diriger ou d'organiser un groupement ayant pour objet l'importation, l'exportation, le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicite de stupéfiants[18].

Le démantèlement récent (juin 2018), par la Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED) de la plateforme "Black Hand" très active dans le Darknet (environ 3 000 membres y sont inscrits en France) et très prisée par les trafiquants en tous genres de produits et services illicites (stupéfiants, armes, faux papiers, données bancaires volées, etc), illustre bien la mobilisation des services d'enquêtes pour interpeller et poursuivre les administrateurs et toutes les personnes qui participent au développement de ce genre de plateformes illégales. Quatre suspects ont été déferrés devant les magistrats de la juridiction interrégionale spécialisée du Parquet de Lille. Ils ont été mis en examen pour plusieurs délits comme l'association de malfaiteurs, le trafic de stupéfiants, l'escroquerie, le trafic de faux documents administratifs, etc.

En juillet 2017, Alphabay l'une des plus importantes plateformes illégales sur le Darknet (plus de 250 000 annonces, 200 000 membres, et 40 000 vendeurs, entre 600 000 et 800 000 dollars de revenus par jour[19]) a été mise hors ligne au terme d'une enquête menée conjointement par les autorités américaines et des polices européennes. Satisfait de ce "coup de filet", le procureur américain Jeff Sessions a déclaré[20] : "*Inutile de vous cacher sur le Darknet, nous vous retrouverons et nous vous traduirons en justice*". Rob Wainwright, directeur d'Europol ajoutait[21] : "*Les forces de l'ordre ont envoyé un message clair aux criminels : nous avons les moyens d'identifier les lieux et les acteurs de la criminalité et de mettre fin à leurs actes, y compris sur le Darknet*".

En février 2015, Ross Ulbricht, citoyen américain, est reconnu coupable de sept chefs d'accusation dont blanchiment d'argent, trafic de stupéfiants, entreprise criminelle et piratage informatique. Il a été condamné à la réclusion à perpétuité[22] pour avoir créé une plateforme de trafic de drogue sur le Darknet (environ 18 millions de dollars de revenus). *« L'anonymat présumé du darknet n'est pas un bouclier protégeant des arrestations et des poursuites »*, a fait valoir le procureur fédéral de Manhattan, Preet Bharara.

Cette liste d'exemples non limitative et l'analyse des dispositifs juridiques actuels, applicables au Darknet, montrent d'abord la détermination des équipes d'enquête nationales et internationales pour poursuivre et arrêter les responsables des plateformes illicites présentes sur cette partie sombre de l'Internet ; ensuite, l'absence de vide juridique pour réprimer les infractions qui y sont commises. Le Darknet est par conséquent bien loin d'être une zone de non-droit.

Notes

[1] V. en sens le dossier consacré au Darknet dans la revue Dalloz IP/IT de Février 2017.

[2] D. Shestakov, Sampling the National Deep Web, *in* Database and Expert Systems Applications pp 331-340, 2011

[3] Avis de la Commission d'enrichissement de la langue française publié au Journal Officiel du 26 septembre 2017 - Numéro 225, la toile profonde (Deepnet) l'avis de la Commission d'enrichissement de la langue française publié au Journal Officiel du 26 septembre 2017 - Numéro 225, la toile profonde (Deepnet)

[4] C. Sherman, G. Price, *The Invisible Web: Uncovering Information Sources Search Engines Can't See*, 2001

[5] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035638782&dateTexte=&categorieLien=id

[6] P. Biddle, P. England, M. Peinado, B. Willman, *The Darknet and the Future of Content Protection, in Digital Rights Management*, 2003

[7] S. Mansfield-Devine, *Darknets*, in Computeur Fraud & Security, Vol. 2009, Issue 12, Décembre 2009

[8] Moyen le plus accessible au réseau Tor sans connaissances avancées en informatique . Il existe d'autres outils comme Tor2web, PirateBrowser

[9] « *The Tor Project FAQ* », sur trac.torproject.org

[10] D. Moore et T. Rid, *Cryptopolitik and the Darknet*, in The Darkness Online, 2016

[11] J-Ph RENNARD, Darknet : mythes et réalités, ELLIPSES 2016

[12] Art. 323-1 et s. C. pén. (STAD), Décision-cadre n° 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information & Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information (système d'information), TGI de Paris, 12e Ch, *Blogmusik | Anthony C. et autres*, 17 décembre 2010 (site Internet)

[13] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

[14] C.Civ art. 1128 anc., C.Civ art. 1162

[15] C. pén. art. 421-1, al. 2

[16] C. pén. art. 421-1, al. 6 et 7, art. 421-2-2 et art. 421-2-3

[17] C. pén. art. 421-2-5-1

[18] C. pén. art. 222-34

[19] Selon Nicolas Christin, professeur de sciences de l'informatique à l'université Carnegie Mellon.

[20] https://www.youtube.com/watch?v=DtWy_uF0SCM

[21] https://www.youtube.com/watch?v=k2FI45hdlXs

[22] « Le fondateur de Silk Road reconnu coupable de sept chefs d'accusation » [archive], sur Le Monde, 4 février 2015

NIS : vers un cadre harmonisé pour la cybersécurité ?

Garance Mathias
Avocat à la Cour - Associée Fondateur Mathias Avocats

L'actualité des dernières années a été marquée par la multiplication des attaques informatiques et des incidents de sécurité majeurs touchant tous types d'acteurs et affectant l'économie. Selon des chiffres publiés par la Commission européenne[1] en septembre 2017, depuis le début de 2016 plus de 4 000 attaques par rançongiciel (ou ransomware) ont eu lieu chaque jour à travers le monde, soit une augmentation de 300 % par rapport à 2015. La Commission relève également que 80 % des entreprises européennes ont été affectées en 2016. L'impact économique de la cybercriminalité a été multiplié par cinq entre 2013 et 2017, et pourrait encore être multiplié par quatre d'ici 2019.

La cybersécurité est aujourd'hui un point de préoccupation inévitable pour tous les acteurs économiques. Ainsi, le Parlement européen et le Conseil de l'Union européenne ont adopté le 6 juillet 2016[2] la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « Directive SRI » ou bien « Directive NIS ». A noter qu'avant l'adoption de la directive dite NIS, aucun cadre commun n'était prévu et les enjeux de cybersécurité étaient traités à l'échelle nationale.

Par cette directive, l'Union européenne vise à renforcer la cyber-résilience des réseaux en Europe en instaurant un cadre commun harmonisé. Chaque Etat membre devra par ailleurs désigner une ou plusieurs autorités nationales et mettre en place une stratégie pour gérer les cyber menaces. L'adoption de cette directive a également constitué une première étape dans la stratégie européenne de cyberdéfense.

Les nouvelles obligations en matière de sécurité

La directive définit deux notions importantes, à savoir les opérateurs fournissant des services essentiels et les fournisseurs de services numériques. Par « *opérateur fournissant des services essentiels* », les institutions européennes entendent toute entreprise qui joue un rôle important pour la société et l'économie, et qui évoluerait dans les secteurs suivants : l'énergie (électricité, pétrole et gaz), les transports (aérien,

ferroviaire, par voie d'eau et routier), les services bancaires (établissements de crédit), les infrastructures de marchés financiers (plateformes de négociation, contreparties centrales), la santé (prestataires de soins de santé) ou encore l'eau (fourniture et distribution d'eau potable)[3]. Les trois critères d'identification de ces opérateurs sont la fourniture d'un service essentiel au maintien d'activités sociétales et/ou économiques critiques ; la fourniture de ce service étant tributaire des réseaux et des systèmes d'information ; et tout incident aurait un effet disruptif important sur la fourniture dudit service.

Quant aux « *fournisseurs de services numériques* », il s'agit notamment des prestataires de cloud, des moteurs de recherche ou encore des plateformes en ligne comme Amazon. La directive oblige chaque Etat membre à s'assurer que ces acteurs économiques prennent toutes mesures techniques et organisationnelles appropriées dans le cadre d'une politique de gestion de risques. Ces mesures ayant vocation à éviter autant que possible ou à tout le moins réduire les conséquences des éventuels problèmes de sécurité. En cas d'incident ayant un impact significatif sur la continuité de services de ces opérateurs, ces derniers devront les notifier aux autorités désignées, répondre à leurs demandes d'information et se conformer à leurs instructions.

Le niveau de sécurité mis en œuvre par ces acteurs devra être proportionnel aux risques potentiels qu'ils rencontrent dans le cadre de leur activité. Il s'agit donc de prendre en compte des facteurs de risques tels que la continuité de service, la sécurité logique et physique des infrastructures ou encore leur degré de conformité aux standards internationaux en matière de sécurité. Cependant, dans le cas des « *fournisseurs de service numérique* », ces exigences ne devraient pas être applicables aux microentreprises et aux petites entreprises[4].

Outre les obligations imposées aux « *fournisseurs de service numérique* » et aux « *opérateurs de services essentiels* », chaque État membre devra également adopter une stratégie nationale en matière de sécurité des réseaux. A ce titre, des objectifs stratégiques et des mesures politiques et réglementaires concrètes devront être définies et régulièrement actualisées. Les États membres devront également veiller à disposer de CSIRT[5], afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et assurer une coopération efficace au niveau de l'Union.

Une loi de transposition

La loi de transposition du 26 février dernier reprend les définitions de la directive sans changement significatif. Le décret n°2018-384 du 23 mai 2018[6] clarifie et précise certains éléments du régime juridique des opérateurs de services essentiels.

Quant aux « *fournisseurs de services numériques* », la directive est laconique à leur sujet. Dans ce contexte, constitue un ser-

vice numérique « *tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services* »[7]. Trois types d'activités sont concernés : les places de marché en ligne, les moteurs de recherche et les services d'informatique en nuage. Ce dernier domaine peut paraître flou. Il vise la fourniture d'un « *service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées* »[8].

La liste des fournisseurs de services numériques ne sera pas établie par décret. Il reviendra donc aux acteurs de s'identifier comme tels et de se conformer à leurs nouvelles obligations. A noter que les microentreprises et petites entreprises sont exclues par la directive de la qualification de fournisseurs de service numérique.

En France, certains acteurs connaissent déjà des obligations légales en matière de cybersécurité. C'est notamment le cas des Opérateurs d'importance vitale (OIV), qui sont soumis à des obligations strictes en matière de cybersécurité pour ce qui concerne leurs systèmes d'information d'importance vitale sous le contrôle de l'ANSSI. Le législateur français a en conséquence fait un choix : les opérateurs potentiellement concernés par ces qualifications, mais qui connaissent déjà des obligations au moins équivalentes en matière de sécurité, sont exclus du champ d'application des nouvelles mesures.

Ainsi, la loi exclut explicitement les Opérateurs d'importance vitale, mais également les prestataires de service de confiance issus du règlement eIDAS du 23 juillet 2014[9], les opérateurs de télécommunications pour leurs activités liées à l'exploitation de réseaux de communication électronique ou à la fourniture de service de communication électronique, ainsi que tout opérateur faisant déjà l'objet d'une norme sectorielle lui imposant des mesures de cybersécurité d'un niveau au moins équivalent à celui prévu par la loi.

Des sanctions pour les acteurs réfractaires

La loi de transposition du 26 février précitée prévoit des sanctions pour les acteurs qui n'auraient pas respecté les obligations mises à leur charge.

La non-déclaration des incidents de sécurité exposera les opérateurs de services essentiels à 75 000 euros d'amende contre 50 000 euros pour les fournisseurs de service numérique. Le non respect des règles de sécurité ou l'absence de mesure de sécurité sera passible de 100 000 euros d'amende pour les opérateurs de services essentiels et 75 000 euros d'amende pour les fournisseurs de service numérique. Enfin, en cas d'obstacle aux contrôles de l'ANSSI, les opérateurs de services essentiels s'exposent à 125 000 euros d'amende, contre 100 000 euros pour les fournisseurs de service numériques.

Vers une stratégie globale de sécurité des réseaux

La France doit en outre adopter une stratégie nationale en matière de sécurité des réseaux. Cette stratégie est en cours d'élaboration. Le 12 février 2018, le secrétaire d'État auprès du Premier Ministre chargé du numérique a présenté officiellement la revue stratégique de cyberdéfense[10].

Fruit de six mois de concertation, le texte effectue un état des lieux de la menace cybernétique en France et formule une série de propositions stratégiques visant à améliorer la position française. Cette position s'exprimera notamment dans la loi de programmation militaire pour 2019/2025[11]. Le projet de loi se place dans la continuité de la loi de programmation militaire pour 2014/2019 et accorde une place importante à la cyberdéfense.

Pour conclure, force est de constater que le dispositif législatif en matière de cybersécurité s'enrichit et tend à permettre aux différents acteurs économiques de se prémunir des attaquer et de disposer de moyens pour riposter.

Notes

[1] Communiqué de presse de la Commission européenne en date du 19 septembre 2017, faisant suite au discours annuel sur l'état de l'Union de Jean-Claude Juncker du 13 septembre 2017 et se concentrant sur les questions de cybersécurité abordées dans le discours. http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm

[2] JOUE du 19.07.2016, Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et qui est entrée en vigueur en août 2016.

[3] L'annexe II de la directive comprend des catégories d'acteurs pouvant être qualifiés d'opérateurs fournissant des services essentiels.

[4] Article 16-11 de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

[5] Centres de réponse aux incidents de sécurité informatique, également connus sous la dénomination de centres de réponse aux urgences informatiques (CERT).

[6] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

[7] Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, JORF n°0048 du 27 février 2018, texte n°2, Article 10, 1°.

[8] Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, JORF n°0048 du 27 février 2018, texte n°2, Article 10, 2°, c).

[9] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[10] "Revue stratégique de cyberdéfense", 12 février 2018.

[11] Loi de programmation militaire 2019-2025 : textes officiels. Accessible à l'adresse URL : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-projet-de-loi/loi-de-programmation-militaire-2019-2025-textes-officiels.

Nouvelles perspectives dans la lutte contre la cybercriminalité

Thomas Cassuto
Magistrat, Docteur en droit, Vice-Président de l'Institut Présaje

Introduction

163 zetaoctets[1], soit le nombre de données numériques produites en 2017[2]. 15 milliards d'objets connectés dans le monde. Ces deux chiffres sont à rapporter au coût estimé de la cybercriminalité pour l'économie mondiale en 2017, soit 400 milliards d'euros[3].

Les cybermenaces, dont la cybercriminalité, constituent un défi majeur à double titre. Elles font peser un risque sur les infrastructures critiques, vitales au bon fonctionnement de la Nation, et dont les capacités de résilience sont mises à rude épreuve. Elles mettent également en péril la démocratie. En effet, les données personnelles sont exploitées pour influencer collectivement les individus afin d'orienter leurs choix politiques. Les risques pour la démocratie sont d'autant plus forts que la manipulation de l'opinion s'effectue à l'insu des individus et à l'instigation de puissances étrangères.

Ce n'est pas une nouveauté, la cybercriminalité procède à la fois de la criminalité organisée et de la confrontation de cyberpuissances. Certains conflits actuels le confirment. Ainsi, la frontière entre cyberguerre et cybercriminalité se trouve floutée. Dans ce contexte, d'un point de vue judiciaire, l'amélioration de la lutte contre la cybercriminalité repose sur le renforcement de la sécurité des réseaux, des outils juridiques et des capacités opérationnelles.

1. Renforcer la sécurité des réseaux

La loi du 6 janvier 1978 informatique et libertés a instauré un certain nombre d'obligations à la charge des personnes procédant au traitement des données per-

sonnelles. Le non respect de certaines de ces obligations, en particulier les manquements à la sécurité ou la collecte et le traitement illicites de données personnelles sont sanctionnées par les articles 226-16 et suivants du Code pénal.

La loi de 1978, texte vivant et évolutif, a préfiguré l'élaboration d'un droit européen. Désormais, le droit de l'Union européenne fixe dans les traités le droit à la protection des données personnelles et codifie les modalités de protection de ce droit. Par plusieurs décisions, la Cour de justice de l'Union européenne (CJUE) a définitivement consacré en pratique ce droit fondamental[4].

Dernières étapes en date, le Règlement général relatif à la protection des données personnelles[5] (RGPD) et la Directive « police »[6] qui l'accompagne constituent le cadre général de la protection des données personnelles. Parallèlement, la Commission a présenté le 10 janvier 2017 un projet de Règlement « vie privée et communications électroniques »[7]. Ces normes trouvent également un écho dans plusieurs conventions du Conseil de l'Europe.

Dans ce contexte normatif en ébullition, les acteurs des réseaux, fournisseurs d'accès, plateforme, moteurs de recherche, éditeurs, doivent être placés face à leurs responsabilités. La lutte contre différentes formes de cybercriminalité passe incontestablement par une sécurité des réseaux physiques et virtuels administrés par des entreprises mondialisées. Il est donc urgent de sanctionner systématiquement et avec vigueur les manquements de ces entreprises à leur obligations nées du droit européen de la protection des données personnelles. À cette occasion, il serait opportun d'étendre à ce type d'infractions le champ d'application de la convention d'intérêt judiciaire prévue par l'article 41-1-2 du code de procédure pénale[8] en incluant, outre une amende, l'obligation de se soumettre à un contrôle renforcé de la CNIL.

En second lieu, il faut admettre que la cybercriminalité profite largement des manquements des principaux acteurs des réseaux d'informations, qu'il s'agisse de manquements involontaires à leurs obligations ou d'une compromission à des fins commerciales, par exemple par la commercialisation illicite des données personnelles. A cet égard, la transmission de données personnelles par un réseau social à une société ayant procédé à des profilages à des fins électorales[9], ou encore des entreprises chinoises, dans un pays où l'Etat procède à une collecte massive des données personnelles, notamment biométriques[10], constitue une défaillance majeure qui constitue une forme de cybercriminalité. Ces dérives doivent être pénalement sanctionnées conformément au droit européen applicable notamment lorsque les données personnelles ont transité par le sol européen ou concernent des ressortissants européens.

La sécurité des données personnelles n'est pas seulement une question de liberté individuelle dès lors que le *big data*, or noir de l'IA, peut être utilisé à des fins criminelles ou pour altérer la démocratie. À cet égard, l'information et les garanties des droits des individus doivent encore être améliorées.

2. Renforcer les outils juridiques

L'évidence s'impose d'elle même : la cybercriminalité est une criminalité organisée à dimension et vecteurs transnationaux. Elle suscite une coordination et une coopération d'acteurs multiples dans les domaines techniques, financiers, sociaux, etc. C'est donc à l'échelle internationale qu'il convient de renforcer les outils et de les transposer avec efficacité au niveau national.

À cet égard, la Convention du Conseil de l'Europe sur la cybercriminalité[11], dite Convention de Budapest, fait office de principal instrument international du fait qu'elle a été ratifiée par des États non membres dont notamment les États-Unis, le Canada, le Japon, l'Australie, le Sénégal, etc. Son adoption en 2001 est malheureusement datée. Cette Convention peine à intégrer les évolutions technologiques et l'arrivée de nouveaux acteurs. Elle souffre également du fait que la Russie ne l'a pas signée et que la Chine y est opposée, ces deux pays estimant que la Convention serait trop orientée sur la répression. En toute hypothèse, cet instrument doit encore être modernisé, dans le cadre d'un troisième protocole, afin de définir de nouvelles infractions, renforcer la sécurité des réseaux et étendre la responsabilité à de nouveau acteurs[12].

Au niveau européen, le RGPD constitue le cadre général imposé à ceux qui procèdent au traitement de données personnelles. Il est toutefois nécessaire de renforcer les moyens d'action visant à réprimer la cybercriminalité qui cible ces données. À cet égard, la Directive relative à la décision d'enquête européenne[13] met en œuvre le principe de reconnaissance mutuelle pour le recueil de preuve. Toutefois, les délais qu'elle impose, drastiquement réduits par rapport à ceux observés en matière d'entraide pénale classique, demeurent trop importants pour lutter contre la cybercriminalité, singulièrement lorsque des fraudes financières générant d'importants mouvements de fonds en de brefs délais sont en cause.

La mise en place d'équipes communes d'enquête[14] doit être facilitée afin de garantir la structuration et le déploiement de ces équipes intégrées en des temps très courts. La possibilité de les faire travailler à distance doit y contribuer. Leur constitution pourrait être encouragée entre services spécialisés en matière de lutte contre la cybercriminalité.

La décision d'enquête européenne devrait être utilement complétée par le projet de Règlement présenté le 21 décembre 2016 concernant la reconnaissance mutuelle des décisions de gel et de confiscation[15], dont

l'adoption pourrait permettre de suivre et de contrer les opérations financières frauduleuses produites par les cybercriminels et les priver ainsi de leurs profits.

Demain le procureur européen[16] devra être en mesure de disposer des capacités de lutter contre la cybercriminalité qui, sous différentes formes, trouve un terrain de prédilection dans la fraude aux intérêts financiers de l'UE.

C'est dans ce contexte que la Commission européenne a présenté, le 17 avril 2018 une proposition de règlement[17] relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, d'une part, et une proposition de directive[18] établissant des règles harmonisées en matière de désignation de représentants légaux chargés de collecter les preuves dans le cadre d'une procédure pénale. Ces propositions visent à faciliter l'accès des autorités judiciaires nationales aux preuves électroniques notamment en imposant aux détenteurs de ces données de répondre directement à l'autorité requérante. Le projet de règlement, mettant en œuvre le principe de reconnaissance mutuelle, doit permettre d'ordonner la transmission de données en moins de 10 jours, voire moins de 6 heures en cas d'urgence vers l'Etat requérant à la demande de celui-ci. Il prévoit également une injonction de conservation, permettant d'empêcher l'effacement de données permettant de contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données en vue de leur transmission ultérieure. Ces mesures apparaissent également comme une réponse à la promulgation le 23 mars 2018 du « cloud Act » américain, lui-même adopté en réaction à l'affaire Microsoft ayant donné lieu à une décision d'une cour d'appel énonçant qu'en vertu du *Stored Communications Act* de 1986 ne s'appliquait qu'aux données stockées aux Etats-Unis et n'a pas d'effet extraterritorial[19].

L'objectif des deux propositions de la Commission, au demeurant indispensables pour lutter efficacement contre la cybercriminalité, est ici de pouvoir obtenir directement de la part de tout représentant dans l'UE des données détenues ou administrées par toute personne, y compris lorsque ces données auront été transmises hors UE, aux USA par exemple[20].

Parallèlement, à l'échelle européenne, il est nécessaire d'actualiser les règles minimales communes relatives à la définition des infractions afin de les adapter aux nouvelles formes de cybercriminalité. Cette harmonisation a minima doit favoriser la reconnaissance mutuelle des mesures d'enquête et prévenir les difficultés liées à la double incrimination. La Directive 2013/40/UE[21] y contribue. Elle devra être adaptée pour tenir compte de nouvelles formes de fraude telles que les traitements illicites de données personnelles, le recours à la cryptologie ou le refus illicite de révéler une clef de

cryptage, ou encore les fraudes liées à la technologie de la chaîne de blocs.

Au plan national, le législateur adapte régulièrement la définition des infractions afin de tenir compte des évolutions. Sur le plan de la procédure pénale, il semble toutefois nécessaire de rationaliser les règles afin réduire le temps entre la prise de décision et l'accès aux données utiles. Ainsi, l'économie générale des règles relatives à la perquisition informatique, aux réquisitions, à la saisie de données informatiques, au décryptage au moyen de procédés de défense nationale, de géolocalisation ou de captations de données informatiques[22] doit être simplifiée afin de garantir leur efficacité au quotidien. Il est également urgent que l'État se dote des outils techniques permettant la mise en œuvre de ces dispositions, en particulier celles des articles 706-102-1 et s. du code de procédure pénale relatives à la captation des données informatiques et s'attache au développement, sur le fondement des articles 230-6 et s. du même code, des fichiers permettant l'analyse systématique des faits et données recueillies.

3. Renforcer les moyens capacitaires

Cela sonne comme une évidence. Face à une criminalité qui ne cesse de se développer, l'adaptation d'un arsenal législatif est nécessaire mais pas suffisant.

En premier lieu, il est urgent de renforcer les moyens matériels et humains ainsi que la formation des services spécialisés en matière de cybercriminalité que ce soit au niveau national ou régional et ce, en lien avec EUROPOL qui a développé un centre d'expertise dans ce domaine. Ces services doivent accueillir des compétences transversales et établir ou renforcer des partenariats avec des chercheurs et les principaux acteurs du net, en particuliers les acteurs publics. De plus, la lutte contre la cybercriminalité nécessite une innovation rapide et permanente destinée à élaborer des solutions techniques face des problématiques en constante évolution qui doit conduire à rapprocher enquêteurs et chercheurs.

En second lieu, il est également nécessaire d'inventer un système de greffe électronique pour stocker et conserver les pièces à conviction numériques afin de réduire la gestion physique d'un matériel encombrant, tant en terme de nombre d'unités informatiques ou de stockage que de volume de données. Par ailleurs, il est désormais acquis que les développements de l'intelligence artificielle auront un impact dans la sphère pénale. De nouvelles formes de criminalité vont apparaître tels que les drones autonomes armés[23] ou impliqués dans la logistique de trafics. L'intelligence artificielle fait déjà l'objet de détournements et la menace que son utilisation détournée infiltre l'ensemble des réseaux est croissante.

Il convient, face à cette menace et plus généralement compte tenu de l'augmentation exponentielle des données numériques pro-

duites, de développer des capacités et des applications de l'intelligence artificielle dédiées au traitement des données de masse, à la lutte contre toutes les formes de criminalité, notamment la cybercriminalité. En effet, nous postulons qu'à brève échéance, seule l'intelligence artificielle résoudra des problématiques criminalistiques liées au détournement de l'intelligence artificielle[24].

Le développement de ces capacités devra s'appuyer sur un solide partenariat public – privé – université. A cet égard, il importe d'étendre la capacité de mettre en œuvre, dans un cadre strict et selon des règles d'emploi bien définies, des moyens de cyberdéfense dès lors que certaines formes de cybercriminalité seraient à même de menacer la souveraineté nationale, l'intégrité du territoire ou nos infrastructures vitales.

Conclusion

La lutte contre la cybercriminalité constitue par définition la forme de criminalité qui nécessite de la part des autorités la plus grande capacité d'adaptation et d'évolution. Constituant une menace par ses finalités, ses moyens ou ses contenus, la cybercriminalité engendre une menace contre les intérêts vitaux de la Nation.

Depuis plusieurs années, la lutte contre la cybercriminalité fait l'objet d'une attention particulière et les moyens ont été développés. Reste que l'évolution de cette forme de criminalité, dont se sont emparées de nombreuses organisations terroristes, nécessite un renforcement de la protection des réseaux et des données personnelles ainsi qu'une accélération du développement des moyens capacitaires et des compétences.

Cette lutte doit s'inscrire également dans le contexte de la construction à grande vélocité d'un droit transnational lié aux technologies de l'information et de la communication.

Notes

[1] 163 milliards de teraoctets.

[2] Le chiffre double tous les 18 mois.

[3] Communication de la Commission européenne.

[4] Arrêt C-135-12 du 13 mai 2014, Google ESPAGNE consacrant le droit à l'oubli sur le fondement du droit à la protection des données formulée par la Charte européenne des droits fondamentaux ; Arrêt C-162/14 du 6 octobre 2015, Maximilien Schrems contre Data Protection annulant le Safe Harbor établi avec les USA en vertu de la Directive 95/46/CE.

[5] Règlement (UE) 2016/679 du 27 avril 2016.

[6] Directive 2016/680/UE du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[7] COM(2017) 10 final.

[8] Instauré par la loi du 9 décembre 2016.

[9] « Le «scandale Facebook» pousse Cambridge Analytica à la faillite », Le Figaro, 2 mai 2018.

[10] « Données personnelles : Facebook les a partagées avec des groupes chinois », Le Figaro, 6 juin 2018.

[11] Convention du 23 novembre 2001 entrée en vigueur le 1er juillet 2004.

[12] Un second protocole relatif à la lutte contre le terrorisme est toujours en cours d'élaboration.

[13] Directive 2014/41/UE, transposée par l'ordonnance 2016-1636 du 1er décembre 2016. V. Thomas Cassuto « La Directive concernant la Décision d'enquête européenne » AJ Pénal Dalloz juillet – août 2014, pp. 338.

[14] Décision-cadre 2002/465/JAI du 13 juin 2002.

[15] COM(2016) 819 final.

[16] Art. 86 du TFUE, Règlement 2017/1939/UE mettant en œuvre une coopération renforcée concernant la création du Parquet européen.

[17] COM (2018) 225 final.

[18] COM (2018) 226 final.

[19] V. Sylvie Peyrou, « Le projet de règlement « E-evidence » (preuves électroniques) présenté par la Commission européenne : un « Cloud Act » européen », http://www.gdr-elsj.eu

[20] En ce qui concerne les USA, il existe un accord cadre, l'EU-US PRIVACY SHIELD, entré en vigueur le 1er août 2016, qui prévoit un dispositif de certification et d'autocertification pour les entreprises qui procèdent au transfert de données personnelles vers les USA. Ce mécanisme souffre de nombreuses limites.

[21] Directive du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre.

[22] V. notamment articles 57-1, 77-1-1, 99-5, 230-1, 230-32, 706-102-1 et suivants du code de procédure pénale.

[23] Les systèmes armés létaux autonomes (SALA) suscite désormais d'intenses travaux au sein de la Conférence du désarmement. Cf. l'intervention du Représentant permanent de la France du 15.11.2017, https://cd-geneve.delegfrance.org.

[24] V. Thomas Cassuto « Justice et intelligence artificielle », Revue l'ENA hors les murs, juin 2018.

La nécessité d'un ministère public présent en ligne

Gordon Choisel
Doctorant à l'Université Paris 2 Panthéon-Assas
Chargé d'enseignement aux universités du Mans et de Paris Sud

« Le maintien de l'ordre public dans une société est la loi suprême »[1]

Le 25 novembre 2017, le président de la République déclarait vouloir « traquer, réguler les contenus inacceptables auxquels nos enfants ont parfois accès et qui construisent [leurs] comportements »[2].

Face à « une imbrication de plus en plus forte des activités en ligne et hors ligne »[3], la volonté présidentielle s'inscrit dans la nécessité de protéger aussi efficacement « l'harmonie du corps social »[4] dans les rapports virtuels que dans les rapports réels. En effet, Internet ne saurait être un lieu neutre : comme tout lieu où les hommes vivent en société, il faut des règles canalisant leur activité et s'opposant au règne de la violence et de l'arbitraire[5]. Ainsi, en affirmant qu'il est « à titre personnel, le garant [que] partout, le droit doit passer »[6], le président a rappelé que la banalisation d'actes répréhensibles en ligne ne peut qu'entraîner une multiplication d'actes équivalents dans la réalité. De même, Internet permet la diffusion de messages, explicites ou non, qui ont un impact sur les rapports physiques[7]. Autrement dit, le respect de l'ordre public en ligne est une condition de sa préservation hors ligne.

Malheureusement, Internet apparaît comme un lieu où l'effectivité du droit[8] est mise à mal et où les États sont condamnés « à une négociation permanente »[9]. Dans ce contexte, la cybercriminalité[10] ne peut que continuer de développer, surtout « si un sentiment d'impunité persiste » [11]. Or, la délinquance en ligne la plus courante n'est pas visée par les récentes évolutions législatives qui ne se sont attachées qu'aux expressions les plus dramatiques de la cybercriminalité[12]. Dès lors, il convient de réfléchir aux modalités d'une lutte efficace contre la cy-

berdélinquance afin de garantir un respect général de l'ordre public en ligne.

Bien qu'il existe des difficultés liées au cadre juridique d'Internet (I), des solutions déjà applicables pourraient être complétées assez facilement (II).

Les obstacles s'opposant à un respect de l'ordre public en ligne

Transposant la directive 2000/31/CE du 8 juin 2000, la LCEN a mis en place une exonération de responsabilité du fait des contenus pour les fournisseurs d'accès et les hébergeurs[13]. Ainsi, ces intermédiaires techniques ne sont tenus d'aucune obligation de surveillance des informations dont ils permettent la transmission. Leur responsabilité ne peut donc être engagée que s'ils refusent de retirer des données ou d'en rendre l'accès impossible à partir du moment où ils en ont eu connaissance ou suite à une notification en bonne et due forme. Partant leur seule obligation est de retirer un contenu illicite (*take down*) dès qu'ils ont connaissance de l'illicéité, sans aucune obligation d'en empêcher la remise en ligne (*stay down*)[14]. Ce faisant, la participation des hébergeurs à la préservation des droits et à la protection de l'ordre public, semble minime alors même que leur modèle économique est fondé sur une monétisation de l'analyse du comportement des internautes face aux contenus diffusés[15].

Dès lors, dans un environnement où les intermédiaires techniques n'assurent quasiment aucun contrôle[16], la délinquance a pu largement proliférer.

Ainsi en est-il des plateformes illégales de *streaming* ou de téléchargement qui utilisent des films ou séries piratés comme produits d'appel pour vendre leur audience à des régies publicitaires diffusant des publicités illégales (pornographie, escroqueries, jeux non agréés, etc). Autrement dit, ces sites ont un modèle économique entièrement fondé sur l'illégalité et s'inscrivant dans un écosystème ouvertement délinquant auquel participent des régies publicitaires et des annonceurs. Pourtant, peu de poursuites sont engagées malgré l'existence manifeste d'infractions.

Ainsi, bien que le respect sur Internet de l'article 227-24 du *Code pénal* semble techniquement impossible[17] et juridiquement délicat[18], le « faible nombre de poursuites »[19] sur son fondement interroge. En effet, de nombreux sites diffusent de la pornographie ou redirigent vers de tels sites sans aucune restriction d'accès alors que la précocité comme les conséquences de l'exposition des plus jeunes à ces contenus ne cessent d'être dénoncées.

De même, ces plateformes recourent massivement à la contrefaçon sans être réellement inquiétées. Certes la mauvaise conception de la répression de la contrefaçon en ligne[20] est à l'origine d'une prolifération de la contrefaçon commerciale sur

Internet[21]. Mais il n'est pas normal que les ayants droit assurent seuls la poursuite des contrefacteurs et de leurs complices.

Pourtant, des solutions existent qui permettent dès aujourd'hui d'assurer un meilleur respect de l'ordre public en ligne. Bien évidemment, des compléments législatifs ou réglementaires garantiraient une meilleure effectivité des poursuites.

Les solutions permettant un respect de l'ordre public en ligne

À côté de la possibilité d'engager la responsabilité des prestataires techniques pour une absence de passivité, la jurisprudence européenne a explicitement reconnu l'existence d'une obligation de diligence. Ainsi, la responsabilité civile d'un hébergeur peut être engagée « s'il a eu connaissance de faits ou de circonstances sur la base desquels un *opérateur économique diligent* aurait dû constater l'illicéité [...] et, dans l'hypothèse d'une telle connaissance, n'a pas promptement agi »[22]. Dès lors, l'opérateur « qui connaît un fait illicite perpétré par quelqu'un avec lequel il est en relation contractuelle et sur lequel il a un pouvoir de droit ou de fait, mais qui s'abstient de tenter d'y mettre fin, devrait engager sa responsabilité »[23]. De même, les instruments de *soft law* permettraient aussi l'engagement de la responsabilité des intermédiaires : si une charte implique l'engagement des signataires « d'adopter une démarche relativement active [...] le juge pourra [...] en déduire l'existence d'une norme de comportement, de référence, celle d'un "bon père de famille numérique" »[24]. Ainsi, « le juge [pourrait] se saisir afin de contrôler *a posteriori* la loyauté des pratiques commerciales de ces différents acteurs »[25], voire « leur imposer [...] de s'impliquer de façon plus marquée, c'est-à-dire au delà de ce que les textes leur imposent »[26].

Mais la possibilité d'engager la responsabilité civile des intermédiaires techniques ne doit pas être exclusive d'une meilleure réponse pénale.

Le blocage ou le déréférencement d'un site internet est une compétence exclusive du juge civil en référé ou sur requête[27] et ne constitue pas une peine pénale. À l'exception de la provocation à des crimes et délits d'une particulière gravité et de leur apologie[28], le ministère public n'est pas explicitement chargé d'interrompre la réalisation d'un délit en ligne en requérant le blocage ou le déréférencement d'un site délinquant. Cependant, l'article 423 du *Code de procédure civile* lui permet expressément « [d'] agir pour la défense de l'ordre public à l'occasion des faits qui portent atteinte à celui-ci » puisque sa « mission [est] de défendre les intérêts de la société et de veiller au maintien de l'ordre public »[29].

Ainsi, le parquet pourrait d'ores et déjà participer à la lutte contre la cybercriminalité en demandant le blocage et le déréférencement de nombreux sites multidélinquants.

Toutefois, aucun parquet n'a engagé une telle procédure. Plus encore, en matière de terrorisme et de pédopornographie, les dispositifs existants sont apparus insuffisants au législateur qui a instauré une possibilité de blocage administratif des sites[30]. Face à une délinquance en ligne plus ordinaire mais extrêmement présente, le gouvernement souhaite confier à une autorité administrative indépendante la police du *net*[31]. Or, parce qu' « Internet, espace de droit, l'est comme espace de droits »[32], la place du juge judiciaire doit rester première. À cette fin, plusieurs évolutions sont envisageables.

Tout d'abord, suivant un principe de concentration et spécialisation de la justice pénale face à la criminalité complexe[33], la création d'un parquet national numérique – ou *a minima* d'une section spécialisée à compétence nationale – serait une réelle avancée[34]. Cela permettrait de répondre plus efficacement et rapidement à une délinquance à la pointe de l'évolution technologique. Mais ce choix devrait s'inscrire dans une politique pénale volontariste exprimée dans des instructions générales non équivoques.

En outre, la création d'un *référé pénal* pourrait faciliter le travail du ministère public pour qui le recours au juge civil n'est pas forcément évident lors d'une procédure pénale[35]. Ainsi, face à « [des] circonstances litigieuses appelant une réponse sans retard de la part d'un juge »[36], le blocage et le déréférencement pourraient être ordonnés par le juge des libertés et de la détention, sur simple requête du procureur de la République. Mais ici encore une volonté politique est nécessaire pour porter cette réforme procédurale.

Ainsi, une présence effective du ministère public en ligne semble indispensable pour lutter efficacement contre la cyber-délinquance. Si les outils juridiques existent, il apparaît urgent d'offrir à la Justice les moyens matériels de les employer.

Notes

[1] J.-É.-M. Portalis, *Discours préliminaire du premier projet de Code civil.*

[2] E. Macron, *Discours à l'occasion de la Journée de lutte contre les violences faites aux femmes*, Palais de l'Élysée, 25 novembre 2018 (disponible sur www.elysee.fr).

[3] Conseil d'État, *Étude annuelle 2014 – Le numérique et les droits fondamentaux*, p. 133.

[4] F. Terré, *Introduction générale au droit*, 15e éd., coll. « Précis », Dalloz, 2015, p. 1.

[5] F. Terré, *op. cit.*, pp. 2 et 8.

[6] E. Macron, *op. cit.*

[7] V. entre autres le reportage *Les réseaux de la haine*, réalisé en 2014 par Rokhaya Diallo et Mélanie Gallard, diffusé sur *LCP* le 1er juin 2014 : http://www.lcp.fr/emissions/160200-les-reseaux-de-la-haine.

[8] Sur la manière dont le processus judiciaire est quotidiennement entravé : M. Robert, *AJ Pénal* 2016, p. 412

[9] M. Robert, art. cit. Dans le même sens, Conseil d'État, *Étude annuelle 2014*..., *op. cit.*, p. 134 ; A. Bensamoun, C. Zolynski, « La promotion du droit négocié en propriété intellectuelle : consécration d'une conception dialogique du droit », *D.* 2011, p. 1773.

[10] « Le terme de "cyberdélinquance" serait plus juridiquement exact, mais la notion de "criminalité" recouvre, au plan international, toutes les infractions, indépendamment de leur gravité » (M. Robert, *Rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité – Protéger les internautes*, févr. 2014, p. 10, n. 3).

[11] A. Basdevant, « Pour un parquet national du numérique et une 33e chambre correctionnelle de la cybercriminalité ? », *RLDI* n° 139, juill. 2017, p. 38. Selon un récent rapport, « la cybercriminalité est pour partie une délinquance de masse » (DMISC, *État de la menace liée au numérique en 2018*, mai 2018).

[12] P. Berthelet, « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne », *RSC* 2018, p. 59.

[13] Article L. 32-3-3 du *Code des Postes et Télécommunications* et article 6 I. de la LCEN. Sur la distinction en les régimes de l'article 6 I. de la LCEN et de l'article L. 336-2 du *Code de la propriété intellectuelle* : J. Larrieu, Ch. Le Stanc, P. Tréfigny, *D.* 2016, 2141, II. B.

[14] Civ. 1ère, 12 juill. 2012, n° 11-15.165, n° 11-13.666 et n° 11-13.669. Cependant, la LCEN autorise une « surveillance ciblée et temporaire demandée par l'autorité judiciaire » (art. 6 I.-7, al. 2).

[15] Conseil supérieur de la propriété littéraire et artistique, *Rapport de la mission sur la révision de la directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*, décembre 2014, p. 55.

[16] Certaines initiatives des hébergeurs vont néanmoins dans ce sens (par ex. le *Content ID* et les *Trusted Flagger* de *Youtube* ou le déréférencement et les pénalités appliquées par *Google* aux sites signalés comme contrefaisants par les ayants droits). Sur l'article 13 de la proposition de directive 2016/0280, v. F. Herpe, « *Value gap* : vers un rééquilibrage au bénéfice des ayants droit », *Juris art etc.* 2017, n° 47, p. 34.

[17] « Aucun filtrage n'est réalisable qui permettrait de garantir qu'un site reste inaccessible aux mineurs » (A. Lepage, « Pédopornographie et contenus nocifs pour les mineurs sur internet : même combat ? », *AJ Pénal* 2015, p. 399).

[18] Il faut concilier « protection des mineurs et préservation de la liberté d'expression à l'égard des majeurs » pour qui l'accès à des contenus pornographiques doit demeurer possible (A. Lepage, « Pédopornographie... », art. cit.).

[19] A. Lepage, obs. ss TGI Nîmes, 4 févr. 2014, *Comm. com. électr.* 2014, comm. 66.

[20] V. M. Vivant : « Au-delà de l'HADOPI : penser la contrefaçon », *RLDI* 2009, n° 51, p. 3 ». Pour cet auteur, « Il y a des manières de faire (et en l'occurrence de légiférer) qui ne sont tout simplement pas acceptables » (*ibid.*). Cf. M. Vivant, « Internet, piratage et contrefaçon – Trois questions à M. Vivant », *D.* 2009, n° 26, p. 1808. ».

[21] Une meilleure appréhension de sa dimension transfrontalière et de la difficile identification de ses auteurs auraient peut-être permis de trouver un régime adapté à la contrefaçon d'œuvres en ligne. Par exemple en réfléchissant à une pénalisation opportune de la contrefaçon à partir d'une juste qualification de cette dernière. V. M. Vivant, J.-L. Bruguière, *Droit d'auteur et droits voisins*, 3e éd., coll. « Précis », Dalloz, 2015, n° 1085 et 1098.

[22] CJUE, Gde. Ch., « L'Oréal c/ *eBay* », n° C-324/09.

[23] P.-Y. Gautier, « De l'éventuel "rôle actif" des opérateurs internet dans la réalisation du dommage (qualifications de responsabilité civile) », *D.* 2011, p. 2054. L'auteur se fonde sur « une complicité de nature civile avec ses particularités : ainsi, alors qu'on sait qu'en droit pénal la complicité par abstention n'est point punissable, il n'en est pas de même en matière civile, dans le cas où l'opérateur avait le devoir d'agir, ce que les Anglo-Saxons appellent le *duty of care* ».

[24] A. Bensamoun, C. Zolynski, « Lutte contre la contrefaçon sur internet : les sources de l'implication des prestataires techniques », *RLDI* 2011/75, n° 2494, pp. 59-65. D'ailleurs, « la Cour de cassation [...] a déjà admis qu'une simple obligation morale pouvait être qualifiée d'obligation civile » (*ibid*.).

[25] A. Bensamoun, C. Zolynski, « La promotion du droit négocié... », art. cit. Dans le même sens, C. Castets-Renard, art. cit.

[26] A. Bensamoun, C. Zolynski, « Lutte contre la contrefaçon sur internet... », art. cit. D'ailleurs, « on voit apparaître en jurisprudence une obligation, à la charge de l'hébergeur, de veiller à ce que le trouble ne se reproduise plus sur le modèle du *take and stay down* américain, et ce sans toujours requérir la collaboration de l'ayant droit » (*ibid*.)

[27] Cet article trouve son fondement dans le fait que « si la personne lésée s'est vue reconnaître par l'art. 6 I.-5 le droit de requérir de l'hébergeur implanté en France le retrait de données "manifestement" illicites, une telle disposition s'avérait sans portée lorsque l'hébergeur était implanté à l'étranger » (M. Robert, *Rapport...*, *op. cit.*, p. 195).

[28] Articles 50-1 de la *Loi du 29 juillet 1881 sur la liberté de la presse* et 706-23 du *Code de procédure pénale*.

[29] *Dictionnaire de l'Académie française*, 9e éd., V° « Ministère ». Cf. F. Molins, *Répertoire de droit pénal et de procédure pénale*, Dalloz, V° « Ministère public ».

[30] *Loi n° 2014-1353 du 13 novembre 2014* (v. M. Quéméner, *AJ Pénal* 2015, p. 32).

[31] É. Macron évoquait le CSA (*op. cit.*).

[32] M. Vivant, *al.*, *Le Lamy Droit du numérique*, Éd. Lamy, 2017, 1937.

[33] Création de la section antiterroriste du Parquet de Paris en 1987 et du Parquet national financier en 2013.

[34] Cf. A. Basdevant, art. cit.

[35] V. M. Robert, *Rapport...*, *op. cit.*, p. 190, n. 157.

[36] N. Cayrol, *Répertoire de procédure civile*, Dalloz, V° « Référé civil », n° 1.

Le secret des affaires, outil de protection des actifs numériques

Olivier de Maison Rouge

Avocat – Docteur en droit
Auteur : « Penser la guerre économique », Va Press, 2018
« Le droit du renseignement », LexisNexis, 2016
« Le droit de l'intelligence économique », Lamy, 2012
A paraître automne 2018 : « Cyberisques », LexisNexis
Vice-président de la Fédération européenne des experts en cybersécurité
Rapporteur du groupe de travail de transposition de la directive sur le secret des affaires près Ministère de l'Economie & des Finances

La directive (UE) n°2016/943 du 8 juin 2016 relative aux savoir-faire et informations économiques non divulgués (secrets d'affaires) a contribué à donner corps à une référence juridique de protection de l'innovation stratégique au travers d'une définition harmonisée, en complément des règles relatives à la sécurité des systèmes d'information et des données personnelles. Elle a depuis lors été intégrée dans le droit français non sans débats houleux.

Pour Aristote Onassis « *Le secret des affaires est de savoir quelque chose que personne d'autre ne sait* »[1]. On pourrait encore affirmer que le secret des affaires est un savoir-faire à ne pas faire savoir. Il en est ainsi des secrets de composition du Coca-Cola ou du Nutella, toujours imités, mais jamais égalés, permettant à leur titulaire de préserver leur modèle économique à l'instar de la fabrication de la Chartreuse, célèbre liqueur des pères éponymes[2].

Au-delà de ces secrets issus de l'industrie alimentaire, il convient au préalable de convenir que l'économie a depuis lors enregistré une mutation profonde dans sa substance. La transformation numérique en est la dernière illustration. Ainsi, il est patent que la globalisation des échanges a modifié en profondeur la valeur de l'entreprise. La dématérialisation de l'économie rend plus diffus aujourd'hui ce qui constitue le patrimoine d'une entreprise : ses hommes, mais aussi leurs idées, leurs savoir-faire, les

connaissances stratégiques, leurs réseaux relationnels et commerciaux, leurs méthodes de gestion, les créations numériques, son patrimoine informationnel, c'est-à-dire un ensemble de pratiques non brevetées, résultant de l'expérience, et testées.

Or, l'utilisation croissante et les rapides progrès des nouvelles technologies de l'information fragilisent ce patrimoine malgré l'amélioration des moyens de défense technique. C'est pourquoi une protection juridique adaptée à cette couche informationnelle s'avérait indispensable, l'atteinte et la révélation d'un tel patrimoine immatériel pouvant parfois générer des conséquences dévastatrices irréparables. En conséquence, la protection associée à ces nouveaux savoirs-faires se devait d'évoluer pour les embrasser et par là-même assurer un nouveau cadre favorable à l'innovation. C'est dans ce contexte que le secret des affaires a pris corps, outil de sécurité des actifs stratégiques tout à la fois agile et robuste.

I. Le secret des affaires s'inscrit dans un mouvement de sécurité numérique

Le vrai secret est une connaissance que son détenteur rend délibérément inaccessible. (...)

Le secret, suivant le cas, interdit de connaître, de prouver, de diffuser ou de reproduire l'information qu'il protège voire de la modifier, comme lorsqu'un mot de passe empêche le sabotage de données informatiques.[3]

Face à l'émergence aussi soudaine que rapide des géants du numérique et des acteurs du *big data*, il a été récemment sanctuarisé le primat de la protection des données personnelles précédemment instaurée en France dès 1978 sous l'autorité de la CNIL qui a depuis lors servi de modèle au reste de l'Europe[4]. De même, l'ANSSI[5] est devenue une référence française présente au cœur de la cybersécurité ; il faut encore relever que le SISSE, créé le 29 janvier 2016[6], a pour sa part mission de participer à « la défense de la souveraineté numérique ».

En outre, dans ce même souci de limiter l'accès à des données sensibles, la France a défini certains modes de protection, notamment physiques et logiques, conférant aux entreprises utilisatrices un droit à restriction de la diffusion des informations. Ce sont les Zones à régime restrictif (ZRR)[7] et les Opérateurs d'importance vitale (OIV)[8], qui sont des cadres juridiques spécifiques et contraignants, permettant aux personnes morales privées de sécuriser, sous le contrôle de l'État et sur autorisation des ministères[9], un périmètre donné, en raison, notamment, de la nature des données traitées au cœur de ces citadelles informationnelles[10].

Depuis 5 ans, l'Europe a accompagné ce mouvement et l'a amplifié, en intégrant la cybersécurité des données personnelles :

- La directive 2013/40 relative aux attaques contre les systèmes d'information ;
- Le règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance ;
- Le règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- La directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (NIS).

A contrario, déniant la légitime protection des informatives privations des entreprises, et ce bien que la jurisprudence européenne – sous le visa de l'article 8 CESDH – les aient consacrées, les informations économiques non divulguées n'étaient toujours pas consacrées. Il a donc fallu l'adoption de la directive 2016/943 du 8 juin 2016 pour y remédier.

Dans cet esprit, le secret des affaires – en ce qu'il revêt la confidentialité des informations économiques non divulguées – permet de renforcer la compétitivité de l'entreprise et de s'inscrire dans un acte d'affirmation de stratégie. Plus prosaïquement, il s'agit de préserver l'avantage concurrentiel de son titulaire dans une économie largement ouverte, dématérialisée et exposée aux risques contemporains.

La source d'inspiration de ce projet de directive trouve son origine dans l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) qui est une annexe au Traité de Marrakech du 14 avril 1994, instituant l'Organisation Mondiale du Commerce (OMC). Il n'est pas inutile de rappeler que les principes directeurs de cet organisme tendent à la libre circulation des marchandises, au niveau mondial.

Précisément, se voulant l'exception au principe affirmé, l'accord ADPIC crée une catégorie de droits dérogatoires échappant à cette dérégulation. Ce faisant, l'OMC vise nommément la protection des renseignements économiques non divulgués qu'elle range parmi les droits assimilés à la propriété intellectuelle liée au commerce.

II. La protection d'un actif immatériel stratégique

Le texte instaure une norme juridique unifiée afin « d'étalonner » cette notion constituée de R&D, *« de savoir-faire et d'informations commerciales non divulguées »* pour en reprendre le titre de la directive.

Les secrets d'affaires seraient ainsi identifiés sous trois conditions cumulatives :

(i) non connus du grand public, c'est-à-dire tenus secrets ;

(ii) ayant une valeur commerciale, parce que secrets ;

(iii) et faisant l'objet de mesures spécifiques destinées à les garder confidentiels.

Sous cette définition commune et harmonisée, le secret des affaires est présenté comme un outil supplémentaire permettant de renforcer la préservation des actifs informationnels de l'entreprise.

La protection des informations essentielles est désormais assurée en amont par la confidentialité renforcée, rendant indisponible une information par nature volatile, et *a posteriori* par le juge qui doit préserver le secret.

Ce socle juridique faisait jusqu'à présent défaut en droit car, sauf à s'intégrer à un logiciel, un algorithme n'est pas protégé par le droit. En effet, le droit de la propriété intellectuelle couvre davantage des inventions de nature industrielle et/ou artistique, mais ne recouvre pas l'innovation numérique qui en est absente en tout ou partie. Le droit des logiciels est d'ailleurs un droit récent, davantage considéré comme un droit connexe du droit d'auteur. De même, le droit des producteurs de bases de données, qui pouvait être le cadre juridique des informations stratégiques, est trop restreint et mal appliqué. C'est pourquoi une protection juridique adaptée à ce patrimoine de la connaissance stratégique s'avérait indispensable.

Sur la notion de valeur commerciale, selon le législateur français, il faut entendre, pour son détenteur, « un élément de son potentiel scientifique, technique, de ses intérêts économiques ou financiers, de ses positions stratégiques ou de sa capacité concurrentielle »[11] mais recouvre également les procédés, techniques, formules, algorithmes, cahiers de laboratoires, R&D, organigramme, business plan, concept, ... conformément à la Directive qui recherchait la protection de « l'économie de la connaissance » en vue de constituer »[12].

En revanche, à la différence des droits de propriété intellectuelle, son titulaire ne dispose pas de titre délivré par l'INPI, mais doit s'assurer de sa protection afin de conserver son monopole par nature précaire. En cela, pour le vice-Président de l'OMPI[13], « *ce type de protection ne nécessite pas de procédure d'enregistrement auprès de l'administration : il s'applique de facto au sein de chaque entreprise (...) qui plus est, le secret d'affaires permet de protéger un volume d'informations bien plus important que ne le permet un brevet* ».

Ce faisant, le droit français a donc opté pour un outil agile, simple d'utilisation, peu onéreux et tout à la fois robuste, répondant aux préoccupations légitimes des start-uppers et entrepreneurs de l'industrie du futur, à condition de mettre en œuvre des mesures de sécurité spécifiques.

La loi envisage d'en assurer largement la protection contre l'obtention, la divulgation et l'utilisation illicites et notamment :

- la juridiction saisie pourra ordonner des mesures d'interdiction, notamment provisoires ;

- il sera possible de solliciter des mesures dites “correctives” se traduisant notamment par l’interdiction d’importation de produits fabriqués en violation de secrets d’affaires ;

La procédure judiciaire, souvent présentée comme étant un mode de collecte d’informations confidentielles, pourra être aménagée au moyen de mécanismes permettant d’assurer la préservation des secrets d’affaires :

(i) Création d’un périmètre de confidentialité pour les parties (avocats, experts, témoins).

(ii) Restriction dans l’accès aux pièces produites au cours de la procédure.

(iii) Restriction dans l’accès aux audiences.

(iv) Jugement élagué de l’énonciation des secrets d’affaires.

En matière de réparation des dommages, outre le préjudice constaté, le juge pourra également tenir compte des conséquences économiques négatives telles que le manque à gagner ou les bénéfices réalisés par le contrevenant.

Innovation juridique majeure, le secret des affaires présente donc une matrice opérationnelle pertinente en matière de sécurité numérique des actifs immatériels qui reste désormais à déployer au sein de l’entreprise, où, au-delà de la contrainte, il s’agit davantage de faire œuvre de pédagogie et de sensibilisation pour permettre à tout salarié d’avoir conscience de protéger son outil de travail et son emploi comme l’énonce Roger-Pol DROIT « sans le secret des affaires, c’en serait fini de l’industrie, des services, de l’économie »[14].

Notes

[1] Cité par François Forestier, *Aristote Onassis, l’homme qui voulait tout*, Éditions de la Loupe (2006)

[2] On pourrait encore ajouter l’élaboration de certaines bières trappistes

[3] François-Bernard et Edith HUYGHE, *Histoire des secrets*, Hazan, 2000

[4] A ce titre, il faut se souvenir que la loi informatique et liberté, qui peut paraître très avant-gardiste à l’heure où l’ordinateur domestique n’était pas répandu ; en réalité, le législateur a voulu s’opposer à un projet gouvernemental de fichage électronique national dénommé « Safari ». Clin d’œil de l’histoire, le RGPD applicable 40 ans plus tard vise à freiner l’ingérence électronique des GAFAM (Pour Google, Apple, Facebook, Amazon et Microsoft), Apple ayant son moteur de recherches dénommé « Safari » ...

[5] Agence Nationale de Sécurité des Systèmes d’Information

[6] D. n°2016-66, Art. 2 3°

[7] décret n°2011-1425 du 2 novembre 2011, arrêté du 3 juillet 2012 et la circulaire n° 3415/SGDSN/AIST/PST du 7 novembre 2012.

[8] Article R. 1332-1 et s. du Code de la défense en application de l’article 22 de la Loi de Programmation militaire (LPM) n°2013-1168 du 18 décembre 2013

[9] Sous l’autorité d’un Haut fonctionnaire de défense et de sécurité (HFDS)

[10] Depuis, la Directive (UE) 2016/1148 du 6 juillet 2016 dite NIS a instauré un niveau élevé commun de sécurité des réseaux et des systèmes d'information transposée par la loi du 23 février 2018

[11] Expose des motifs, proposition de loi déposée à la Présidence de l'Assemblée Nationale le 19 février 2018

[12] Directive, préambule 1)

[13] Pooley James, « Le secret d'affaires : un droit de propriété intellectuelle méconnu », in OMPI magazine, juin 2013

[14] In « Dangereuse transparence », Les Echos, 26 octobre 2011

Une excursion (guidée) au Far-West numérique

Xavier Raufer

Introduction

La criminologie parcourt désormais deux univers – distincts mais qui toujours s'observent, se copient et souvent s'entremêlent : le *physique* et le *numérique*. Or si – certes inquiétante – la criminalité du monde physique, terrorisme inclus, est vaguement sous contrôle, le chaos numérique est à présent déchaîné, la société humaine étant loin même de concevoir le danger réel qu'il présentera demain. A grands traits :

- Les pires cyber-attaques n'entraînent quasiment jamais de ripostes donc, s'amplifient et s'aggravent,
- A ce jour, les grandes puissances mondiales n'ont pas conçu de moyen efficace pour contrer les pires attaques ; puissances incapables même de définir une agression numérique et de quand elle constitue un acte de guerre. Elles n'arrivent même pas à décider ensemble du licite/interdit dans le cybermonde ! Sauf pédopornographie (et encore) nulle norme/règle impérative n'existe de fait dans le cyberespace. Le président Macron a dit "Nous devons être forts et avoir des règles claires" – or la société humaine y est faible et le chaos y règne.

Bref, tout ce qui a été tenté pour réguler le cyberespace n'a pas empêché qu'il devienne, *dixit* le président Obama, un chaotique et anarchique "*wild wild west*", où sans grand risque, chacun peut piller et agresser à sa guise.

Or en France, cette inquiétante réalité tend à disparaître derrière une autosatisfaction de façade. Dans ses rapports, notre appareil officiel de lutte contre les cyber-menaces semble content de lui. Tous ces textes semblant d'ailleurs issus d'un même moule :

- D'abord une brève introduction, généraliste et bienséante, sur le désordre du cybermonde, évitant prudemment les précisions gênantes et éléments qui fâchent.
- Ensuite, la proclamation de Grands Principes et Nobles Valeurs avertissant le genre humain et le cybermonde qu'ils

devront désormais se plier aux normes, règles, besoins, us et coutumes de l'administration française.

- Enfin l'essentiel : érection d'un harmonieux et géométrique Parthénon textuel voué (à 30%) à affronter le problème et (à 70%) à magnifier le périmètre et l'emprise de l'administration en cause. Lisons la récente "Revue Stratégique de cyberdéfense" (168 pages, février 2018). Que dit-elle de l'ennemi, du pirate, de l'Etat hostile qui infiltre, espionne ou sabote ; de l'agent étranger, du mafieux ? Rien. Le sabotage, le vol, l'espionnage et la déstabilisation, certes ; des risques et vulnérabilités, bien sûr – mais l'attaquant ? Au détour d'une phrase, glisse parfois au loin un agaçant gêneur, sans plus ; sinon, la France affronte une menace fantôme.

A la fin de la "Revue", 77 références, notes, sources, etc. : rien sur les acteurs de la cybercriminalité, pirates ou autres. La "Revue" est captive de ce que la phénoménologie nomme "sphère du calculable", où "seul compte ce qui SE compte". D'où nos questions : à ignorer l'ennemi, comment "construire la paix et la sécurité du cyberespace international" ? Comment "anticiper", "prévenir", "détecter" des attaques, si on ignore QUI regarder, surveiller ; si l'on néglige la NATURE de la cyber-menace ?

Précisons : "Protection de nos systèmes d'information" – contre qui ? "Posture active de découragement et de réaction... Souveraineté numérique" – face à qui ? "Réponse pénale efficace" – qui incarcérer ? "Prévention... Anticipation... Détection... Attribution... Réaction : comment faire, sans adversaire identifié et connu ?

Certes, des services veillent à nos intérêts fondamentaux. D'abord, la DGSI dont on apprend qu'elle "muscle ses capacités d'enquêtes cyber" (*Le Monde*, 5/06/2018), en envisageant un "service *technique* national de captation judiciaire, STNCJ". Mais affronter les cyber-prédateurs n'est-il qu'affaire *technique* ? Car s'il y a des "cyber-attaques croissantes en nombre, en intensité et en sophistication", n'est-ce pas du fait de cyber-attaquants, qu'il est crucial de nommer, d'exposer ? Les ordinateurs-outils-criminels, n'obéissent-ils pas à des bandes ou réseaux de pirates de chair et d'os, criminels, terroristes, hybrides, qu'il faut repérer et infiltrer ? Sinon, n'est-on pas dans la cyber-défense platonique ?

Enfin, cet irénisme face aux cyber-bandits n'est pas spécifique à la France, mais affecte toute l'Union européenne, qui veut bien sûr instaurer un marché digital commun à ses pays-membres. Pour le "mois de la cyber-sécurité en Europe" d'octobre 2015, l'organisme dédié de l'UE, l'ENISA (*European Union Agency for Network and Information Security*) publie une liste de 40 enseignements et diplômes, au total 375 cours différents, dispensés dans la plupart des pays de l'UE[1]. Leurs thèmes ? Là encore, que du calculable : sécurité des réseaux, systèmes, ordinateurs et logiciels... Sciences informatiques et forensiques... Cryptographie... Audit et sécurité des Techniques de

l'information et de la communication... Management et sécurité de l'information... Protocoles de sécurité en informatique, etc. Qui est l'ennemi (numérique) ? Où est-il ? Que fait-il aujourd'hui et que fera-t-il demain ? Rien d'annoncé – rien de consistant sur les pirates, espions ou saboteurs. On combat des nuées.

Oublier l'ennemi n'est pas la démarche de cette étude. Avec pour devise "Droit aux choses mêmes" (Edmund Husserl), en route pour le territoire ennemi.

Prologue – L'homme de *Silicon Valley* – fragile ô combien 2

"Sans patrie ni frontières" – étrange retour du rêve kominternien. Dans le kaléidoscope post-hippie californien de *Silicon Valley* la bonne vie est sans attaches, mobile, flexible, fluide. Anarchisme égotiste pour gosses de riches à la Ayn Rand – mythe libertarien du transitoire, de la mobilité et du MOI absolu. Rêve puéril – ne t'ennuie jamais ; fuis la routine ; fais ce que veux. Vivre en tribu, en néo-chasseurs-cueilleurs : six mois en bureau partagé à Berlin... L'été *(lequel ?)* au Chili dans une caravane... Le reste, dans une "couveuse" pour "jeunes pousses" de New York. Concevoir aujourd'hui un logiciel pour une banque au Myanmar... Demain lancer une marque nouvelle en Arabie saoudite. Globe-trotters-entrepreneurs mondialisés, nouveau royaume des élus ? En fait, proies rêvées pour réseaux criminels, pirates, services spéciaux avides de piller cet aimable monde numérique, défendu par d'aveugles "flocons de neige", clones de Peter Pan et éternels ados.

Démons et merveilles de la *Silicon Valley*

D'abord ceci : qui a su s'extraire de ce que la phénoménologie nomme "sphère des évidences courantes" est tout, sauf étonné de la domination des "titans du tech'" ci-après dépeinte. Bien au contraire, il s'en est convaincu, notamment en lisant ceci (prophétie remontant à 1966, voici cinquante-deux ans)... "Nous méditons sur la phénomène du gouverner. Le phénomène est justement devenu aujourd'hui, à l'ère de la cybernétique, si fondamental qu'il met en cause et détermine toutes les sciences de la nature et le comportement de l'homme... Que les sciences de la nature et notre vie soient aujourd'hui dominées dans une mesure croissante par la cybernétique n'est pas un hasard, mais est prédéterminé dans l'histoire de la naissance de la science et de la technique moderne"[3].

Dans notre monde un peu éloigné de la philosophie, les institutions, services, coordinations, états-majors, etc., instaurés pour combattre les nuisances numériques adhèrent bien plutôt à une logique d'ingénieur – les nôtres, en France, pareil. N'envisageant que des contraintes et besoins objectifs, l'ingénieur ne se pose d'usage que les seuls problèmes qu'il sait résoudre. Au cœur de sa logique, la newtonienne théorie d'un mécanisme impeccable ; affecté cependant de pannes ou avaries qu'il suffit de réparer

pour en restaurer la perfection technique. Pour l'ingénieur, le cybermonde est dans l'idéal une vertueuse et fiable horloge ; des nuisibles en perturbant les rouages, il faut les réparer pour qu'après, tout aille bien.

Or si bien sûr, une roulette du casino est *par construction* truquée au détriment du joueur, les meilleurs techniciens du monde ne pourront rendre "vertueuse" une machine dont la norme est de tricher. Cela, les (par ailleurs) fort compétents cyber-ingénieurs peinent à le réaliser. Foncièrement honnêtes, ils occultent le fait que le cybermonde ne procède pas d'une pure et virginale Création visant, comme le prétend une propagande intéressée, à "rendre le monde meilleur" à le "rendre plus ouvert et connecté", pour le délivrer de ses actuelles misères et afflictions. Bien plutôt, ce cybermonde est d'origine le fief de cyniques et libertaires titans, dont l'unique objectif est d'amasser les milliards, dans l'absolu dédain du crime, du piratage et du pillage éhonté des données privées de leurs clients.

Exagération ? Non : d'emblée, ces frappants exemples de la vraie nature du GAFA *Facebook*, les autres (Google Apple, Amazon) ne valant guère mieux :

- A ses débuts, un journaliste demande à Mark Zuckerberg, Pdg de *Facebook*, pourquoi le public lui confierait toutes ses données privées. Limpide réponse du libertarien assumé Zuckerberg "*They trust me – dumb fucks*" ("les pauvres cons me font confiance").
- Dans le *New York Times international* du 28 avril 2018, photo du siège social de *Facebook*, à Menlo Park (Cal.). Clairement lisible, l'adresse – que l'entreprise à bien sûr librement choisie elle-même – "*1, Hacker Way*", 1 allée des pirates. Au cas où les choses ne seraient pas assez claires...
- Début 2018, toujours sur *Facebook*, un expert découvre quelque 120 forums et groupes de discussion (± 300 000 – bien, *trois cent mille* – participants au total) consacrés au cyber-crime, au piratage, proposant à tout un chacun des logiciels et outils d'intrusion ou de vol numérique ; au vu et au su de tout le monde. Pourquoi se planquer sur le *Dark Web* ? Facebook est si accueillant...

Les formidables titans du net ont une idéologie et une pratique de pirates : là est le fondement de toute la cyber-criminologie. Commençons donc par là notre étude, en incitant nos lecteurs à bien ouvrir les yeux.

Des titans du techno-capitalisme, plus puissants que des Etats-nations

Ce que nous décrivons ci-après ne concerne pas des entreprises innovantes jouissant d'un succès bien mérité, mais bien plutôt des monopoles en ligne, lancés dans une impitoyable "*uberisation*" du monde.

Du seul fait des GAFA, la bourse américaine est en croissance continue depuis désormais 9 ans. De janvier à juin 2018, 50% des profits réalisés par les entreprises

de l'indice *Standard & Poors 500* proviennent de Facebook, Alphabet (Google), Apple, Amazon et Netflix.

En août 2018, la capitalisation de Apple (fondé en 1976) dépasse les mille milliards de dollars. Voici vingt ans, Apple n'était qu'une entreprise moyenne concevant des ordinateurs haut de gamme.

Facebook avait 100 millions de clients en 2008, 2,1 MILLIARDS en 2018. Facebook capte 77% du trafic mondial des réseaux sociaux sur téléphones portables.

Amazon avait 17 000 salariés en 2007, 542 000 en 2017 ; la MOITIÉ du *e-commerce* mondial passe par ses méga-serveurs.

Apple et Google fournissent le *software* (logiciels, applications, etc.) de 99% des *smartphones* du monde. Google détient 81% du marché mondial des moteurs de recherche sur Internet.

Sur tout dollar de publicité en ligne, Facebook et Google en raflent 59 cents. Ces deux sociétés captent par ailleurs 63% de la publicité digitale diffusée aux Etats-Unis. Croissance du chiffre d'affaires de la publicité digitale en 2017 : 89% au profit des deux mêmes.

La GAFA-idéologie : celle du renard dans le poulailler

Une récente étude (*NYTi* – 18/10/2017, cf. sources) révèle les opinions politiques de 600 influents patrons et hauts cadres du *high-tech* américain (1/3, de la Silicon Valley & environs). Comme prévu, ils sont massivement libertaires, pour une dérégulation absolue et une immigration totalement libre (besoin d'esclaves à bon marché...). Evidemment aussi, ils sont farouchement hostiles à tout contrôle étatique et pour une capacité de licencier sans limites : l'entrepreneur doit être parfaitement libre sur son marché. Le sociétal ne leur coûtant rien, ces sommités en suivent ardemment toutes les modes : stupéfiants et avortements libres, glorification LGBT, etc.

Côté *business*, ces patrons et hauts cadres du *high-tech* sont nettement moins sympa-progressistes. Ainsi, la fiche de chacun des deux milliards et plus d'usagers de *Facebook* contient une centaine de données : race (censée ne pas exister), sexe (censé céder à la "fluidité"), revenu, surface financière, prix de la résidence principale, famille ou pas, parent d'adolescent (s) ou non, crédits, pratique du Ramadan (!), véhicules, achetés quand. Vendues à des fins publicitaires, ces intrusives "*Ad Preferences*" rapportent à *Facebook* de un à trois milliards de dollars chaque trimestre.

Derrière le chatoyant mirage post-Hippie-tous-égaux-et-frères, la manipulation au millimètre – dans l'obscurité absolue, la "transparence", c'est pour les niais – de toutes ces données privées extorquées à plus de deux milliards de clients, abonnés, etc., dote les GAFA de la plus formidable concentration de pouvoirs coercitifs de

l'histoire du monde. Dès à présent, ces GAFA colonisent l'humanité connectée : salons, chambres à coucher, salles à manger, cuisines, bureaux – jusque dans vos poches.

L'inceste des "Libertaires" GAFA avec le Pentagone, la CIA, etc.

Amazon a créé le *cloud* de la communauté américaine du renseignement ; *Microsoft* a suscité le *cloud* "*Azure Government Secrets*" (à usage du gouvernement fédéral, des Etats, du Pentagone, etc.) ; *Google* pilote le projet d'intelligence artificielle du Pentagone, etc. Quel comique a dit "neutralité du Net" ?

Une poigne de fer sur les médias et l'information planétaire

> "Jamais neutre, la technologie est toujours empreinte des valeurs de ses créateurs. Dans le cas des crypto-monnaies à base *Blockchain*, ces valeurs sont libertariennes et mécanistes ; la confiance y repose sur des règles algorithmiques, les normes des Etats et autres régulateurs y sont vues avec suspicion et hostilité". *(New York Review of Books*, 18/01/2018, cf. sources).

Quelques individus anonymes décident désormais de comment la planète s'informe, consomme, communique ; *Facebook* est le vrai "rédacteur en chef de la Terre" ; 45% des Américains s'informent cette plateforme ; 70%, sur *Facebook+Google*, deux entreprises privées contrôlant ainsi le paysage informatif de milliards de terriens. Une preuve de plus de la justesse du jugement de Karl Marx & Friedrich Engels (*L'idéologie allemande*, Ed. sociales, Paris 1962) : "Les pensées de la classe dominante sont aussi les pensées dominantes de chaque époque ; autrement dit, la classe qui est la puissance *matérielle* dominante de la société, en est aussi la puissance dominante *spirituelle*"[4].

L'absolu dédain des GAFA pour le crime et la sécurité des gens

(*NYTi* – 20/12/2017 – cf. sources) Sur 324 hectares, un grand quartier de Toronto (Canada) est à restructurer. "*Sidewalk labs*" (l'atelier de remodelage urbain de *Google*) s'y met. Socle de son projet, le mantra bobo-libertaire friction = mauvais, diversité = bon, fluidité = meilleur encore. Le quartier sera neutre en carbone ; propreté, recyclage, suivi du bruit et de la pollution y dépendront de dispositifs *high-tech*. Les taxis et les livreurs ? Des robots. Autour des immeubles modulaires, trottoirs et rues seront chauffés par des réseaux d'avant-garde y faisant fondre la neige.

L'exaltant futur est là, à la portée de la main. Sauf qu'en même temps, Toronto subit une sévère crise criminelle. Puisqu'il s'agit de *Google*, que le lecteur y recherche "Toronto Crime" : par dizaines, articles et études l'édifieront. Mais comme tout *Silicon Valley, Google* dédaigne la criminalité et la sécurité des gens. Aveuglé par la calculabilité, ne s'étant pas consulté lui-même, Google ignore – ou méprise – que devant

ses "immeubles modulaires" et sur ses "trottoirs chauffants", gisent des cadavres troués de balles. Une agaçante "friction" parmi d'autres, sans doute.

Derrière les mirages du néo monde, de classiques turpitudes

Sous le *gospel* de l'avenir splendide de l'humanité numérisée, une réalité moins reluisante : les techno-titans du jour agissent comme les bons vieux capitalistes d'hier : aliénation du personnel par voie d'ingénierie sociale ; faveurs sexuelles extorquées par chantage à l'emploi ou au fric ; ignorance des filous et escrocs de son genre.

• *Silicon Valley fait "suer le burnous"* – (*NYTi* – 6/09/2017 – cf. sources) fascination pour les "jouets pour adultes"... apologie de la richesse, limite lavage de cerveau... Apostolat de l'addiction au travail... Le *Burnout* suicidaire, expérience extatique... "Tu veux t'offrir ton avion perso ?" : facile : 18 heures de travail par jour ; ni vacances, ni soirées, ni dîners en ville ; ni copains, ni famille ni enfants, ni jeunesse ni sommeil. T Shirt populaire à *Silicon Valley* : "*9 to 5 is for losers*". Tout pour briller auprès des titans du *Tech* et de leurs cours. Marche ou crève – quelle importance ? Des milliers de juvéniles gogos affluent chaque année dans la *Valley*. La propagande y pourvoit.

• *Puritanisme et "diversité", pour la galerie* – En surface, les élites de *Silicon Valley* adhèrent à toutes les inclusives "valeurs" du jour : droits des LGBT (etc.), "diversité", antiracisme, féminisme, veganisme, etc. Dans la *Valley* qui enfreint cette écrasante idéologie est exclu du numérique Éden. Surface disons-nous, car là encore, sous les mirages du néo-monde persistent les pires abus du vieux – même, rien n'a changé depuis le "*sport fucking*" des années 1970. (*CBS News* – 10/02/2018 ; *Vanity Fair* – 2/01/2018, cf. sources). Sous la pudibonde surface de la *Silicon Valley*, de récentes enquêtes dévoilent la culture de la partouze imprégnant ces *Boy's Clubs* où cohabitent PDG, banquiers d'affaires, dirigeants du *high-tech*, de l'immobilier, de la publicité, etc. Le week-end, ces titans au mental de paléo-*hippies* "invitent" leurs employées, ou celles de *start-up* adjacentes, à des soirées sexe-drogues-pouvoir dans de discrètes villas ou suites d'hôtels. Or si vous travaillez dans la *Valley*, comment refuser des "invitations" lancées par qui régit votre avenir ? Quel public enfin, pour ces secrètes orgies ? Deux fois plus de jeunes femmes que d'hommes mûrs – tous blancs-hétérosexuels. La "Diversité", c'est pour la revue de presse.

• *Cyber-arnaques, arnaques quand même* – Madoff dans le *high-tech* ? Avec tous les *datas*, la "transparence" et les cyber-contrôles ? Impossible ? Non. Juvénile *self-made-woman,* Elisabeth Holmes avait fondé et dirigeait la *start-up* Theranos, vouée à révolutionner les tests sanguins. Un laboratoire au bout d'une épingle, grâce à sa technologie "Edison" : cent tests à l'instant avec une goutte de sang. Pour les systèmes américains de santé (*Medicare, Medicaid*),

des centaines de millions d'économies. Monts et merveilles : le banc-de-sardines médiatique s'embrase : couverture de *Fortune Magazine*... de *Forbes*... du *Time*... L'une des femmes les plus riches et influentes du monde ! Coqueluche des médias ! Henry Kissinger au conseil de Theranos ! Des fonds de capital-risque déversent 900 millions de dollars sur la start-up-miracle. Crédulité, jobardise, aveuglement – tout était faux. *Silicon Valley*, médias, investisseurs, clients – tous bernés. A l'ancienne.

Cyber-conflits, présents et futurs

A présent, ce qu'on appelle "cyber-conflits" tient plutôt de la Guerre froide numérique : non-déclarée ; perturbations insidieuses-indirectes ; course aux armements, au cas où. Mais par rapport à la Guerre froide bipolaire, les acteurs ont changé. Voici aujourd'hui la Corée du nord et sa cyber-armée de ± 6 000 pirates, capables de voler (ou récupérer) les armes numériques offensives de la NSA et de les bricoler, pour piller des banques mal protégées (pour les fins de mois) ; ou de saboter les ordinateurs des contempteurs du"Grand Leader". Dans un monde parlant toujours plus de détecter et de prévenir, notons au passage que nul méfait de Pyongyang n'a jamais été ni décelé, ni prévu par quiconque, la cyber-expertise planétaire pataugeant bien plutôt des mois entiers avant de vaguement entrevoir la lumière.

Ces épisodes montrent cependant que le cyber-conflit est idéal pour la stratégie asymétrique : bon marché, d'usage anonyme, lucratif même – et dangereux pour les infrastructures des pays développés. Insistons sur ce point, rarement abordé par notre évasive cyber-défense, en dépeignant l'état d'un pays moderne, peu après un *blitzkrieg* réussi sur ses infrastructures énergétiques critiques. Celles-ci étant désormais à 100% informatisées, le pays est débranché, effondré, avant même le premier coup de feu :

- Effacement de données cruciales,
- Pillage d'informations sensibles,
- Paralysie d'infrastructures critiques,
- Capacités militaires atteintes,
- Plus d'électricité au bureau ni à la maison,
- Plus de services télécom, de téléphones portables ni d'Internet,
- Plus de services d'urgence ni de sécurité civile,
- Plus de trains ni de métros,
- Panne des dispositifs hospitaliers et de santé publique,
- Plus de feux de trafic,
- Plus de réseaux financiers, cartes de paiement ni distributeurs de billets,
- Plus d'essence dans les stations,
- Comptes en banque inaccessibles,
- Plus de contrôle des barrages hydrauliques, éoliennes, fermes solaires, etc.,
- Arrêt des usines de traitement des eaux & ordures (ménagères, industrielles),
- Plus d'appels possibles à la police (d'où, émeutes et pillages de masse),
- Plus de réfrigérateurs ni de chaînes d'approvisionnement des grandes surfaces alimentaires (nourriture épuisée en une semaine),

Selon un expert "Pour de tels hackers, nous sommes Bambi dans les bois". Au minimum, les Etats-Unis, la Russie et la Chine sont capables de telles attaques – face auxquelles la riposte est impossible aujourd'hui : dans le cybermonde, la dissuasion n'existe pas.

Et quand désormais, des pirates sont détectés dans un réseau critique, ils n'en fuient plus comme naguère en refermant poliment "la porte" derrière eux : ils s'incrustent et ripostent ; les experts décrivent ici l'équivalent cyber des combats de tranchées, de corps-à-corps à l'arme blanche. (Mai 2018, rapport, *Office of the US Director of national intelligence*). Sur ces cyber-attaques stratégiques, trois exemples actuels :

– Administration fédérale des Etats-Unis, bureau des personnels (*Office of Personnel Management*, OPM) : tout fonctionnaire fédéral a son dossier numérique (formulaire SF 86) contenant... toute sa vie : liste de tout étranger rencontré à l'âge adulte, parents, conjoint (s), enfants... famille... tous ceux avec qui l'intéressé a un lien, licite ou non... dossier médical et financier. Or en juin 2015, l'OPM annonce que 21 millions (bien, *millions*) de ces dossiers SF86 ont été piratés. Par qui ? Euh... les Chinois peut-être.

- Août 2017, Arabie saoudite – une cyber-attaque sur l'usine pétrochimique d'un grand groupe international échoue du fait d'un "bug" mineur. Ciblant les contrôles des fonctions fondamentales de l'usine, cet attentat numérique sophistiqué supposait une connaissance pointue de ses plans et schémas. L'idée n'était pas de saboter l'usine, mais de la faire sauter, comme par accident ("format Bhopal"). Or l'architecture (Schneider Electric) de cette usine est analogue à quelque 18 000 autres dans le monde (nucléaire, pétrochimie, traitement des eaux, gaz, chimie lourde, etc.).

- Du nom de ECDIS (*Electronic Chart Display*) un logiciel commun sur la flotte de commerce (cargos, tankers, etc.) peut, par piratage à distance, truquer de quelques 300 mètres (taille et emplacement) la localisation GPS des navires voisins. ECDIS alimentant l'alarme-collision de l'*Automatic Identification System*, un tel cyber-sabotage sur divers navires proches paralyse, et vite, tout espace maritime resserré comme la Manche.

Cyber-pirates et piratages, aujourd'hui et demain

> *"Notre monde virtuel, qu'il soit le système d'information de l'entreprise, un réseau industriel ou tout simplement votre ordinateur familial, n'a jamais été aussi vulnérable, attaqué de toutes parts, sans que nous voyons une atténuation de ce phénomène"* Interview d'un expert ès-cybersécurité, SDBR – 3/04/2018.

A l'origine du désastre, la NSA

Pour la commission d'enquête du Congrès, c'est une débâcle absolue – le pire séisme de toute l'histoire américaine du renseigne-

ment. "*Tailored Access Operations*", la division la plus secrète de la NSA chargée de tout l'offensif-intrusif dans les systèmes informatiques cibles, est pénétrée jusqu'au cœur, éventrée. Les pirates *Shadowbrokers* (commission d'enquête *dixit*) savent tout ou presque des opérations secrètes de la NSA – alors que Washington ne sait rien sur eux – ni d'ailleurs sur l'ampleur du vol, 18 mois après le début d'une enquête interne. Brillants pirates ? Taupes ? Les deux ensemble ? Nul ne sait. Or *Shadowbrokers* a volé à la NSA toutes ses cyber-armes conçues pour percer toute paroi coupe-feu sous Windows, Linux, etc.

Que la CIA ne ricane pas trop : son centre de cyber-renseignement est aussi pénétré, ses document secrets étant ensuite livrés en masse à *Wikileaks* – par qui ? Analogue ignorance. Puis ces cyber-armes de la NSA ("*Eternal Blue*", "*Double Pulsar*", etc.) filent (vendues ? Livrées en douce ?) chez des pirates de Chine, de Russie ou de Corée du Nord – sans doute peu hostiles à leurs propres services officiels. Enfin, ces pirates bricolent de virulents logiciels de rançon (*Wannacry*, *NotPetya*, etc.) qui, dès mai 2017, ravagent le monde numérique, millions d'ordinateurs bloqués, etc.

Selon le méga-assureur américain AIG, très présent dans la couverture des cyber-risques d'entreprises, les attaques par logiciels de rançon (*Wannacry*, etc.), avec probables ingérences étatiques, explosent de + 26% en 2017 ; AIG estimant que le préjudice mondial de *Wannacry* atteint les 8 milliards de dollars.

Au Royaume-Uni, l'observatoire "*National Fraud & Cybercrime Reporting Center*" signale au printemps 2017 (et les attaques *Wannacry*), une explosion des cyber-fraudes en ligne, laissant la profession de la sécurité numérique clairement désarmée : + 63% de ces signalements émanant des entreprises et commerces.

Aujourd'hui, demain : fondamentaux du piratage

Pour les experts, le terme "cybercriminalité" recouvre diverses infractions, au premier rang desquelles :

- Les vols d'identité (réelles, d'individus bien vivants du monde physique),
- Conception-usage d'"identités synthétiques" de personnages factices, crédibles pour les contrôles des entités ciblées par les pirates.
  Ces deux types de fraude identitaire permettent une foule de vols, d'escroqueries, etc.,
  Préjudice pour les banques des Etats-Unis, environ 2 milliards de dollars/an.
- Les logiciels de rançon conçus pour "kidnapper" (encoder) les données d'une entreprise, d'un ministère, d'une mairie, etc. et les libérer contre rançon en crypto-monnaie.
- Intrusions digitales diverses visant une cible (entreprise, etc.), en vue d'espionnage, chantage, compromission, acte de concurrence déloyale, etc.

Pour des experts académiques britanniques, ce *e-commerce* criminel a désormais ses méga-serveurs, type *Amazon* ou *Facebook* illicites, leur chiffre d'affaires mondial frôlant les 1 500 milliards de dollars/an (niveau du PNB de la Russie). Ainsi, disent ces experts, si ce "cyber-capitalisme noir" était un pays, il serait au 13e rang mondial du classement par PNB.

Sur ces méga-serveurs opérant d'usage sur *le Dark Net*, une clientèle toujours plus vaste acquiert aisément des stupéfiants, armes, munitions, explosifs, outils de piratage, services illicites, avis experts de pirates et formations à la fraude en ligne.

Bons *managers*, les méga-serveurs criminels consacrent environ 300 milliards de dollars par an à améliorer leurs sites et supports techniques, à fluidifier leurs échanges-clientèle, à optimiser leur "expérience-client", etc. Sur ces 1 500 milliards de dollars :

- Commerce noir (marchés illicites en ligne) : 860 milliards de dollars ($md.)
- Piratage, vol de propriété intellectuelle, etc. : 500 $md.
- Espionnage – vente de données pillées : 160 $md.
- Vente d'outils de piratage, de sabotage, etc. : 1,6 $md.
- Rançons obtenues par "*ransomware*" : 1 $md. (etc.).

Pas résolu à ce jour, le gravissime problème de l'identité numérique

A ce jour, n'existe nul équivalent digital *universel* du passeport. Prouver son identité en ligne ? Impossible – car comme nous le répétons sans trêve, les libertaires "puissances configuratrices" du Net ont tout misé sur la connectivité et la communication et dédaigné la sécurité. La fluidité ! Le reste, on verra plus tard, ou jamais. Dans le monde physique, l'authentification repose sur la connaissance, ou la reconnaissance. Et dans le monde numérique ? *Quid* si le document original a été volé, perdu ou falsifié ? Et les fameuses "questions de sécurité" (nom de jeune fille de sa mère, etc.) ? *Google* fixe à 74% le taux d'oubli des réponses. Résultat, nulle technologie n'est à présent satisfaisante : simple, claire, incassable et fonctionnant sur tous systèmes d'exploitation, ordinateurs et *smartphones*.

ÉTATS-UNIS – (*Javelin identity fraud report 2018*, cf. sources) Enquête de victimation, novembre 2017 : 6,6% des consommateurs américains ont récemment subi une fraude identitaire, + 8% sur l'enquête de 2016. Préjudice total (vols, fraudes, réparations, rachats, etc.) de la fraude identitaire pour tous usagers d'internet : 16,8 milliards de dollars.

GRANDE-BRETAGNE, 175 000 cas connus de fraude identitaire en ligne en 2017 (2007-2017 : explosion de + 175% des cas connus).

Vulnérabilités : l'oubli du facteur humain

Perdu entre le calculable, les écrans et des normes d'habilitation au secret métastasant sans contrôle, Washington oublie le crucial facteur humain. Ainsi, l'enquête sur le pillage des cyber-armes secrètes de la NSA a (au moins) révélé les exactions d'un des employés du service, pochard mythomane ayant, au fil des ans, "emprunté" à TAO *(Voir plus haut)* une masse inouïe de fichiers secrets : en *bytes*, 5 fois le volume de TOUS les ouvrages de la Bibliothèque du Congrès (la plus importante du monde).

Documents ensuite retrouvés sur des disques durs, entre la boîte à gants de sa voiture (qu'il conduisait ivre) et la cabane du fond de son jardin. Pour les administrations et entreprises, le facteur humain concerne (données 2016) 28% des attaques : dissimulation d'incidents de sécurité informatique ; personnel mal informé, négligent ou soudoyé (les criminologues disent "technicien dévoyé") ; *phishing*, ingénierie sociale malveillante, etc.

Explosion du piratage des omniprésents téléphones portables

Des centaines de failles de sécurité ou logiciels de piratage ("malware") sont régulièrement découvertes dans le système *Android*. Suite à une intrusion-éclair, le propriétaire perd le contrôle de son portable, donc de son compte de banque ou de crypto-monnaies, vidé au profit du pirate, qui peut aussi y trouver des documents compromettants ou photos intimes et soumettre le piraté à un juteux chantage.

Récemment, quelques piratages spectaculaires...

EQUIFAX : société de gestion d'emprunts et crédits, environ 840 millions de clients au monde dont 91 m. d'entreprises. Piratage de ± 150 millions de dossiers (nom, référents financiers, adresse, date de naissance, mots de passe, questions de sécurité, *toutes* les coordonnées financières de l'intéressé, etc.).

YAHOO : *tous* ses quelque trois milliards de comptes email piratés.

SEC : *Securities and exchange commission*, la puissante commission américaine de contrôle des opérations boursières ; des millions d'*emails* confidentiels piratés, permettant ensuite de frauduleuses manipulations de cours (délits d'initié, etc.).

DELOITTE (*Big Four,* audit, expertise comptable et *consulting* juridique, risques, etc.) : conseille ses clients sur le piratage, mais est lui-même piraté (± 5 millions d'emails volés).

VINGCARD : serrures et clés électroniques de dizaines de milliers d'hôtels du monde, donc de millions de chambres d'hôtel. Système déjà piraté, nul ne semblant savoir en quelle ampleur et gravité.

Risques et péril des crypto-monnaies

Il ne s'agit pas ici de retracer l'histoire des monnaies numériques, ni d'expliquer la technologie qui les fonde, mais de montrer comment et à quelle vitesse les plus belles inventions du cybermonde sont dévoyées à usage criminel. D'abord ce rappel : ces crypto-monnaies ne sont ni assurées ni régulées ; les transactions opérées en *Bitcoin*, *Ethereum*, *Ripple*, *Monero*, *Zcash*, *Dash*, etc., sont irréversibles et in-traçables.

Le yo-yo des crypto-monnaies

Que "valent" ces devises numériques ? Strictement, ce qu'en dit leur marché, de sommets vertigineux en insondables abîmes. A sa première cotation le 16 août 2010, le *Bitcoin* "vaut" 0,07 cents (du dollar US). Le 17 décembre 2017, ce *Bitcoin* "valait" 20 000 dollars ; fin décembre 2017, la "bulle *Bitcoin*" "valait" 140 milliards de dollars, (niveau de capitalisation du groupe Coca-Cola). Fin juin 2018, le *Bitcoin* "vaut" 6 500 dollars (- 53% de janvier à juin 2018). Des crises géopolitiques expliquent bien sûr pour part ces montagnes russes. Mais les facteurs criminels comptent aussi. Ils sont de deux types :

- Les pirates pillent tant et plus ces fragiles plateformes d'échange des crypto-monnaies ; contrairement au système *Blockchain* ("technologie de stockage et transmission sécurisée d'informations sans organe central de contrôle") lui, incassable.
- Ces crypto-monnaies sont un notoire outil criminel (rançons, blanchiment, règlement de livraisons de stupéfiants, etc.).

Les plateformes d'échange des crypto-monnaies, cible des pirates

– De leur origine à mars 2015, 1/3 des plateformes d'échange *Bitcoin* ont été piratées ; la moitié de celles piratées ont ensuite fermé ;

– De 2010 à 2016, 4 milliards de dollars ont été piratés sur des plateformes de crypto-monnaies. Récemment :

. *Décembre 2017*, la coopérative (slovène ?) de minage de *Bitcoin NiceHash* est piratée de 80 millions de dollars ($m.) en crypto-monnaies ;

. *Janvier 2018*, la plateforme japonaise *CoinCheck* est piratée de 530$m. en crypto- monnaies ;

. *Juin 2018,* la plateforme sud-coréenne *CoinRail* est piratée de 37 $m. en crypto- monnaies ;

. *Fin juin 2018,* la plateforme sud-coréenne *Bithumb* (6e *trader* au monde en la matière) est piratée de 27$m. en crypto-monnaies.

Les crypto-monnaies, outils du blanchiment de l'argent du crime

Selon Europol, quelque 100 milliards d'euros (€md.) d'argent criminel sont blanchis chaque année dans l'Union européenne, dont 4% du total, quelque 5,5 €md. grâce aux crypto-monnaies. Phénomène devant lequel les polices sont impuissantes.

– La Grande-Bretagne compte désormais une centaine de Distributeurs Automatiques de *Bitcoins*, etc, connectés à des plateformes d'échanges de crypto-monnaies, genre distributeurs de billets ; chacun de ces "*DA-Bitcoins*" a de dix à vingt clients par jour. Or selon une enquête, 80% des clients des "*DA-Bitcoins*" sont des *dealers*, spéculateurs – ou les deux ensemble. Les commerçants gérant ces "*DA-Bitcoins*" décrivent des défilés d'individus "puant le hasch à dix mètres" multipliant par liasses de billets de 50 £ sterling, les transactions de 10 000 à 15 000 £.

– Au Japon, la Yamaguchi-Gumi, principale fédération yakuza, blanchit environ 270 millions de dollars de 2016 à 2018, par multiples petits virements en Monero, ZCash, etc. Ce n'est toutefois qu'une part minime du chiffre d'affaires des Yakuza (trafic de stupéfiants chimiques, prêts usuraires, racket immobilier, arnaques boursières, etc.) estimé à quelque 6 milliards de dollars par an.

– Des gangs colombiens experts ès-blanchiment *high-tech,* réexpédiaient chez eux des millions d'euros du blanchiment de la cocaïne dans l'Union européenne, via une plateforme Bitcoin finlandaise. Quasiment le même jour, un système sophistiqué transférant d'Europe à des banques de Bogota, les euros convertis en pesos colombiens.

France : l'état de la menace numérique

Diverses sources informent sur l'état de la cybercriminalité dans notre pays. Modes de calculs différents, populations étudiées variables ; malgré tout, domine l'idée que la France n'est pas épargnée – loin de là – par les cyber-prédateurs (Pays les plus affectés par le cyber-crime : 1 – Etats-Unis, 2 – France, 3 – Russie) et que les choses vont plutôt en s'aggravant.

– Enquête cadre de vie et sécurité publiée en 2017 – victimation en 2016 et perceptions de la sécurité (INHESJ + ONDRP) : Débit frauduleux sur un compte bancaire : 2010, ± 500 000 victimes (1,8% de la population française) ; 2016, ± 1 210 000 victimes (4,3% de la pop. fr.). 34% de ces débits frauduleux, moins de 100 € ; 18%, plus de 1 000 €.

– Délégation ministérielle aux industries de sécurité et à la lutte contre les cyber-menaces (DEMISC, signalements à la gendarmerie), 63 500 dossiers en 2017 regroupant 320 000 victimes, + 32% sur 2016. Ces dossiers concernent toutes les plaintes liées au cyberespace et aux Nouvelles Technologies de l'Information et de la Communication :

escroqueries et fraudes (67% du total), usurpations d'identités, usage de logiciels de rançon, piratage téléphonique, vols de données personnelles (adresse e-mail, mots de passe, identifiants bancaires), extorsions par faux support technique et cyber-ingérences diverses, pédopornographie, apologie du terrorisme.

Conclusion

Tant que la nature prédatrice des GAFA échappera aux ingénieurs en cyber-sécurité, leur travail – tactiquement utile – reviendra stratégiquement à poser des rustines sur un Zodiac qu'un sadique s'amuse à crever et la cyber-sécurité restera largement cosmétique. Or cette cyber-sécurité est ardemment souhaitée par une opinion planétaire toujours plus informatisée et connectée. Un expert le souligne (*Communication et Influence*, avril 2018, cf. sources) "Il existe bel et bien une demande émanant des populations du monde entier, de retour aux structures établies et à un ordre commun qui permette d'endiguer la fluidification générale et de revenir à une stabilité dont les peuples ont la nostalgie".

Dans la société de l'information, cette entreprise passe prioritairement par une régulation du cybermonde. Comment faire ? L'auteur propose une démarche diagnostic-traitement :

DIAGNOSTIC – La cybercriminalité ne régressera pas par plus encore de haute-technologie, mais par volonté politique. Dans le domaine cyber, une fuite en avant type blindage-canon provoquerait un désastre pire encore que l'inepte guerre *high-tech* en Irak.

TRAITEMENT – Comme jadis la société de l'automobile conçut le code de la route, celle de l'information doit en créer un, ensuite imposé par une puissante coalition mondiale (pays du G20 par exemple). Plus ou moins vite, cette normative superstructure numérique s'imposera mondialement. Comme le code de la route vaut pour tout véhicule, luxueux ou modeste, ce code numérique ciblera les titans du net, financiers-filous, etc., qui aujourd'hui pillent impunément le cybermonde et exploitent ses usagers.

* * *

ANNEXES

1. Cybercrime, les grandes dates

[Voir *MalwareBytes*, cf. sources]

DÉCENNIE 1960

- Premiers piratages de lignes de téléphone (*Phone Phreaking*),

- "Val Smith" (pseudo) se sert d'un ordinateur pour falsifier des données et extorquer à son employeur le remboursement de notes de frais indues.

DÉCENNIE 1970

- (1976) Dan B. Parker publie "Crime by Computer".

DÉCENNIE 1980

- (1981) Ian Murphy "Captain Zap", premier *hacker* condamné pour avoir piraté les systèmes informatiques de facturation d'ITT,

- (1986) Loi aux Etats-Unis "Computer fraud and abuse (CFA) act",

- (1988) Premier logiciel malicieux ("Morris Worm") à se répandre aux Etats-Unis ; son concepteur, Robert Tapan Morris, est le premier condamné au titre du CFA.

DÉCENNIE 1990

- (1990) Los Angeles, Kevin Poulsen est arrêté pour avoir piraté les lignes téléphoniques d'une radio locale ; pour y gagner les prix des concours radiophoniques),

- (1994) Un *hacker* russe pirate $ 100 millions à la Citibank,

- (1996) Matthew Bevan et Richard Price commettent le premier grand piratage (détecté) d'ordinateurs militaires américains.

DÉCENNIE 2000

- (2000) Virus Love Bug depuis les Philippines ; 50 millions d'ordinateurs infectés en dix jours ; dommages : de 5 à 8 milliards de $.

- (2000) Première opération massive de déni de service (DOS) de "Mafia Boy" ; fermeture-crash de eBay et Amazon ; dégâts : 1,7 milliard de $.

- (2003) Consommation et commerce par Internet se généralisent ; les consommateurs privés sont toujours plus touchés par le *Spam* et le *Phishing*,

- (2007) DOS massif de sites officiels estoniens ; des officiels russes suspectés.

DÉCENNIE 2010

- (2010) Etats-Unis+ Israel : implantation dans des systèmes nucléaires iraniens du virus Stuxnet,

- (2014) Sony Pictures, piratage massif des "Guardians of Peace" ; des officiels nord-coréens suspectés,

- (2016) Elections présidentielles aux Etats-Unis : les interférences et manipulations d'officiels russes suspectées,

- (2017) les rançon-giciels WannaCry et NotPetya provoquent d'énormes dégâts sur internet.

2. Cybercrime : un diagnostic lucide du Parlement européen

[Résolution du 3/10/2017, cf. sources]

"- La cybercriminalité augmente en intensité, en complexité, et en ampleur ; la cybercriminalité déclarée dépasse la criminalité traditionnelle dans certains pays de l'Union européenne ; elle s'étend à d'autres domaines de la criminalité tels que la traite des êtres humains ; l'utilisation des outils de chiffrement et d'anonymisation à des fins criminelles se développe, les attaques à l'aide de "rançongiciels" sont plus nombreuses que celles posées par les logiciels malveillants classiques, tels que les chevaux de Troie,

- Le nombre d'attaques visant les serveurs de la Commission a augmenté de 20% en 2016 par rapport à 2015,

- Les dispositifs connectés à l'internet des objets, comme les réseaux intelligents, les réfrigérateurs connectés, les voitures et les instruments ou outils médicaux, sont souvent moins bien protégés que les dispositifs traditionnels connectés à l'internet et constituent donc une cible idéale pour les cybercriminels,

- Les lignes entre la cybercriminalité, le cyber-espionnage, la guerre informatique, le cyber-sabotage et le cyber-terrorisme sont de plus en plus floues ; la cybercriminalité peut cibler les individus, des entités publiques ou privées, et couvrir un large éventail d'infractions, y compris les atteintes à la vie privée, les abus sexuels commis en ligne contre des enfants, l'incitation publique à la violence ou à la haine, le sabotage, l'espionnage, la criminalité financière et la fraude, comme la fraude aux paiements, le vol et l'usurpation d'identité, ainsi que l'atteinte illégale à l'intégrité des systèmes,

- Un nombre considérable d'actes de cybercriminalité ne font l'objet d'aucune poursuite et demeurent impunis,

- Lien de plus en plus étroits entre terrorisme et criminalité organisée."

3. Le syndrome de Pinocchio : l'univers enchanté (?) des startups

Comme tant d'autres jeunes cyber-fans, Mathilde Ramadier a subi l'attraction des *startups*. Les fruits ont-ils tenu la promesse des fleurs ? Euh... [Extraits de son livre "*Bienvenue dans le nouveau monde...*", Premier Parallèle éditeur, 2017 – cf. sources].

"... En vérité, les startups s'arment d'une véritable novlangue destinée à dissimuler la loi de la jungle dans la brume du *cool*. Comme toutes les langues, elle n'est pas seulement un liant, un outil de communication, elle déploie également tout un imaginaire autour d'elle, apporte de nouveaux signifiants qui contribuent à bâtir des repères communs... mais qui peuvent aussi faire croire à des choses qui n'existent pas. Derrière l'utopie riche de promesses humanistes vendue par la startup-sphère, se cache en réalité un ultralibéralisme, une concurrence féroce et la pulvérisation de tout ce qui pourrait s'apparenter de près ou de loin à quelque chose de durable [...]

(Les managers) Super rapides, flexibles, increvables, perfectionnistes, ces nouveaux aventuriers de l'ère de la data n'ont plus ni dieu ni maître, mais une nouvelle langue commune et en l'occurrence, un seul mot à la bouche : l'innovation. La présence, même symbolique, de leur Mecque lointaine, la Silicon Valley, finit d'ancrer le sentiment d'appartenance à l'entreprise, qu'on appelle désormais "famille" [...]

La lointaine Silicon Valley, portée au pinacle, est toujours citée en exemple, comme une divinité que personne n'a jamais vue. le rêve promis n'est rien d'autre qu'un cauchemar [...]

Après tout, il est bien réconfortant de penser qu'une révolution est en marche dans notre époque houleuse et que des jeunes gens courageux et sympas bousculent l'ordre établi pour nous sauver de tout ce qui ne fonctionne pas dans notre société ! La novlangue des startup veille avec soin à ce que le message se diffuse largement, avec la complicité d'autres acteurs – parmi eux l'Etat et de nombreux médias [...]

Les solutions que la startup-sphère nous promet – à la crise, au chômage, à l'ennui, à la répétition du même et à la désuétude, à la vieillesse, à la laideur, etc., se basent elles aussi sur un leurre : on ne peut prétendre déjà vivre dans le nouveau monde avant de l'avoir véritablement bâti. Les startups sont donc des entreprises "révolutionnaires" financées par des "business angels", dirigées par des "rock stars" et alimentées par des "treasure hunters". Hou hou ! On redescend sur terre deux minutes ? L'atterrissage est douloureux, je sais.

4. Dark Web : un catalogue de la "Manufacture d'armes et d'outils du cybercrime"

[Armor Black Market Report 2018, cf. sources]

Monétarisation du piratage sur le Dark Web – Outils criminels à vendre, tarifs et prix, au début 2018 :

- Outil de déni de service (DOS) à louer : $ 10 l'heure ; $ 200 la journée entière,
- Outil de piratage basique (*Disdain Exploit Kit*) à louer : $ 80 la journée, $ 500 la semaine, $ 1 400 le mois ; en plus, vidéos ou cours de soutien à l'utilisation (ou au piratage) : de $ 100 à $ 150 par mois,
- Achat d'un "Cheval de Troie" numérique : de $ 3 000 à $ 5 000,
- Outil de piratage d'un compte Internet : ± $ 13 ; d'un outil de vol de mots de passe ; $50,
- Attaque en déni de service (une semaine) : de $ 500 à $ 1 200,
- Outils de piratage de DAB (Distributeurs automatiques de billets) : de $ 700 à $ 1 500,
- Tutoriaux de piratage : de $ 5 à $ 50,

Marché des cartes de paiement piratées

- (à l'unité) Visa/Mastercard, Etats-Unis : de $ 7 à 10 ; Europe : de $ 15 à 30,

- (à l'unité) American Express, Etats-Unis : de $ 10 à 12 ; Europe : de $ 15 à 35,
- "*FULLZ*" (carte de paiement plus données personnalisées, haut-de-gamme) :
  . (à l'unité) Visa/Mastercard, des Etats-Unis : de $ 35 à 50 ; d'Europe : de $ 70 à 100,
  . (à l'unité) American Express, des Etats-Unis : $ 35 ; d'Europe : idem,

Marché des accès à des comptes en banque ou analogues, approvisionnés

(Bank of America, JP Morgan-Chase, Wells Fargo, Paypal, etc.) :

- Avec $ 3 000 sur le compte : $ 300,
- Avec $ 20 000 et + sur le compte : $ 1 000,

Marché des identités volées

Ensemble : nom-prénom, adresse, n° de tel., de sécurité sociale, de compte bancaire, date de naissance, CV professionnel et des crédits en cours, casier judiciaire : de $ 40 à 200,

Marché des comptes de réseaux sociaux

(L'unité) : $ 13

Comptes Instagram piratés : (1000) $ 15 ; (2 500) $ 25 ; (5 000) $ 40 ; (10 000) $ 60,

Marché des programmes de fidélité piratés

- Compagnies aériennes (Etats-Unis) : 1 compte 50 000 miles, $ 100 ; 100 000 miles, $ 150 ; 150 000 miles, $ 200,
- Compagnies aériennes (Europe) : 1 compte 25 000 miles, $ 35 ; 100 000 miles, $ 90 ; 150 000 miles, $ 120,
- Chaînes d'hôtels : 50 000 points, $ 75 ; 150 000 points, $ 140.

Sources et références

• *Presse, sites, médias*

New York Times International (Ci-après NYTi) - 4/08/2018 "Rise of tech's megacompanies"

NYTi - 6/07/2018 "To hackers, we're Bambi in the woods"

Les Numériques - 21/06/2018 "Marché des cryptomonnaies : la fin des illusions ? Dévissages et piratages en série"

Le Figaro - 20/06/2018 "Les cybermenaces deviennent un phénomène de masse en France"

Les Echos - 20/06/2018 "Cette nuit en Asie : nouvelle alerte sur le Bitcoin après le braquage de la plateforme coréenne Bithumb"

National Public Radio - 19/06/2018 "Journalist warns cyber attacks present a perfect weapon against global order"

Dark Reading - 14/06/2018 "Four faces of fraud: identity, fake identity, ransomware and digital"

BFM - 11/06/2018 "Le Bitcoin retombe sous les 7 000 dollars après un nouveau braquage"

BBC News - 7/06/2018 "Ship hack risks chaos in English channel"

Le Monde - 5/06/2018 "La DGSI muscle ses capacités d'enquêtes cyber"

RT - 3/06/2018 "World saw worst year ever for data breaches and cyberattacks in 2017 - report"

Dark Reading - 1/06/2018 "Cybercrime is skyrocketing as the world goes digital"

CBS News - 20/05/2018 "Was the media duped by Elisabeth Holmes ?"

The Register (UK) - 17/05/2018 "Biometrics: better than your mother's maiden name - good luck changing your body if your info is stolen"

BTC Manager - 16/05/2018 "Japan's biggest newspaper reports 30 Billion Yen was laundered through crypto-exchanges"

Reuters - 11/05/2018 "Apple is almost a $ 1 trillion company, but watch out for Amazon"

Voice of America - 11/05/2018 "National security division focuses on combatting cyberthreats"

NYTi - 28/04/2018 (Photo du siège de Facebook à Menlo Park, Cal)

NYTi - 21/04/2018 "Silicon Valley and the Pentagon"

Europol - 9/04/2018 "Illegal network used cryptocurrencies and credit cards to launder more than € 8 Million from drug trafficking"

Rolling Stone - 3/04/2018 "Can we be saved from Facebook ?"

Communication et Influence - avril 2018 "Olivier Kempf "Guerre informationnelle et jeux d'influence dans le cyberespace"

NYTi - 16/03/2018 "Cyberattack on Saudi plant had deadly goal"

Javelin Identity Fraud Report - March 2018 - "Survey Data Collection"

Armor - March 2018 - "The Black Market Report, a look inside the Dark Web"

Business Insider - 12/02/2018 "Criminals in Europe are laundering $ 5,5 Billion of illegal cash through cryptocurrency, according to Europol"

NYTi - 12/02/2018 "A.I. picking up some biases from the real world"

CBS News - 10/02/2018 "Brotopia explores the roots of Silicon Valley's sexism problem"

Computer Business Review - 25/01/2018 - Cybercrime statistics: hackers still having an online fraud frenzy"

NYTi - 23/01/2018 "Seeking an elusive cure for cyber attacks"

New York Review of Books - 18/01/2018 "Bitcoinmania"

Vanity Fair - 2/01/2018 "Oh my god, it's so fucked up - Inside Silicon Valley's secretive orgiastic dark side"

MalwareBytes - décembre 2017 "Une brève histoire du cybercrime"

Daily Mail - 4/12/2017 "Teenagers reeking of drugs deposit wads of £ 50 notes in Bitcoin cash points"

NYTi - 15/11/2017 "Leaks shake agency to its core"

Financial Times - 30/10/2017 "Washington appears to have fallen out of love with Silicon Valley "

NYTi - 20/10/2017 "Vision of a world according to Google"

NYTi - 18/10/2017 "Silicon Valley is not your friend"

NYTi - 17/10/2017 "North Korea wreaks havoc with its corps of hackers"

Parlement européen - 3/10/2017 - Résolution - texte adopté "2014-2019 : lutte contre la cybercriminalité"

NYTi - 8/09/2017 "Tech giants, liberal but with a twist"

NYTi - 6/09/2017 "In Silicon Valley, 9 to 5 is for loosers"

Security Defense Business Review - 5/09/2017 "La menace dans le cybermonde de 2017"

NYTi - 23/08/2017 "Phone numbers let hackers into wallets"

New York Review of Books - 22/12/2016 "They have, right now, another you"

• *Ouvrages*

"Cybermonde et nouvelles menaces", Alain Establier & Xavier Raufer, MA Editions, 2018,

"Bienvenue dans le nouveau monde - comment j'ai survécu à la *coolitude* des startups", Mathilde Ramadier, Premier Parallèle ed. 2017,

"Survivre à la guerre numérique", François Levieux, Eric Meillan, Jean Picollec ed. 2017,

"Cyber-criminologie", Xavier Raufer, CNRS Editions, 2015.

Notes

[1] Allemagne, Autriche, Bulgarie, Chypre, Espagne, Finlande, France, Grande-Bretagne, Grèce, Hongrie, Irlande, Italie, Luxembourg, Norvège, Pays-Bas, Pologne, Portugal, Roumanie, Suède, etc.

[2] Lire d'urgence le splendide "Beyond the map, Unruly enclaves, ghostly places, emerging lands and our search for new utopias" Alastair Bonnett - University of Chicago Press - 2018.

[3] Martin Heidegger (avec Eugen Fink) Séminaire "Héraclite", hiver 1966-1967, Gallimard, 1973.

[4] K. Marx et F. Engels disent aussi dans le *Manifeste du parti communiste* (1847) : "Que démontre l'histoire des idées, si ce n'est que la production intellectuelle se transforme avec la production matérielle ? Les idées dominantes d'une époque n'ont jamais été que les idées de la classe dominante".

Chroniques & Rubriques

PROFONDEUR STRATÉGIQUE - 1

La sortie de prison des djihadistes : le défi date des années 2000, réponses incertaines

Olivier Giras

"Olivier Giras" est le nom de guerre d'un acteur chevronné de l'antiterrorisme, côté terrain.

Sans surprise, alors que s'écrit cet article, un nouvel attentat survenu à Liège vient endeuiller l'Europe. Depuis la défaite de l'Etat Islamique en Syrie et en Irak, le front se trouve plus que jamais devant nos écoles et nos cafés et l'ennemi, bien identifié, au cœur de nos frontières.

Si le pire n'est jamais certain, la libération prochaine, dans ce contexte, de 20 détenus radicalisés inquiète fort. Le procureur Molins avertit l'opinion : « On court le risque majeur de voir sortir de prison, à l'issue de leur peine, des gens pas du tout repentis, risquant même d'être plus endurcis encore, du fait de leur séjour en prison ». La Garde des Sceaux minimise cependant les risques « Autant o*n ne peut maintenir en prison quelqu'un qui a terminé sa peine, autant nous sommes en mesure de le suivre de manière extrêmement étroite pour que, dès lors qu'il y a le moindre écart, il puisse à nouveau être judiciarisé* ».

La libération de détenus radicalisés

La question de l'impact potentiel de la libération de détenus aurait dû être posée dès les années 2000 lorsque des djihadistes libérés de prison ont propagé leur idéologie mortifère nourrissant l'ambition combattante de nos égorgeurs d'aujourd'hui. A travers quelques exemples tragiques, tentons de comprendre les conséquences de ces libérations :

Les filières dites « Tchétchènes »

En 2006, vingt-cinq personnes étaient jugées pour avoir constitué en France un ré-

seau de recrutement de combattants islamistes pour le Caucase et préparé un attentat à l'arme chimique. De nombreux produits nécessaires à la confection de bombes sales avaient été découverts en perquisition. Revenons sur les agissements post libération de trois des principaux protagonistes M, B et S.

Risquant d'être torturés en Algérie, la Cour européenne des droits de l'Homme avait refusé l'extradition de S et B. Ils avaient alors été assignés à résidence en France.

Dès lors, S continuait à diffuser son idéologie, donnant des interviews à la presse locale, assurant notamment que « *les attentats-suicide ayant une dimension économique sont le meilleur moyen de lutte pour les islamistes* ». Puis échappant à son contrôle judiciaire, il fuit vers la Syrie où il devient l'un des chefs de Jund al-Aqsa, groupe djihadiste proche du Front al-Nosra, branche syrienne d'Al-Qaïda. Il a finalement été tué par une frappe américaine.

B a demandé l'asile aux autorités helvètes qui lui ont refusé. Extradé vers la France, il a été condamné à 14 mois de prison ferme le 27 juin 2017 pour avoir violé son assignation à résidence. Il sera libéré en 2018.

M, lui se livre à un prosélytisme salafiste à travers notamment un blog et des vidéos sur YouTube. Ses propos, toujours à la limite du répréhensible, désignent les nombreux ennemis de l'Islam *« Parmi les plus grands ennemis de l'Islam, il y a les loges franc-maçonnes (...) les chevaliers croisés, (...) les juifs (...) ont toujours utilisé la sorcellerie, comme moyen de détourner et nuire aux croyants ».*

La désignation d'ennemis conspirateurs qui stigmatise et brime le musulman est un levier de recrutement puissant pour les Salafistes. Le chômage, le délaissement des banlieues, la cause Palestinienne seront autant d'éléments sur lesquels le recruteur s'appuiera dans sa tâche. L'individu recruté, la diffusion de croyances moyenâgeuses en la sorcellerie viendront s'ajouter à une discipline de vie intenable en Occident : parler à des mécréants ou regarder une femme peuvent vous réincarner en porc ou vous faire brûler dans la douleur éternelle des flammes de l'enfer...

D'opérationnel djihadiste, M est devenu une sorte de recruteur de la cause. Son passé et les nombreux articles sur lui confirment à ses adeptes la pureté et la solidité de son engagement. Son aura ne sera que plus grande.

Ces croyances en la sorcellerie et dans l'incarnation du Mal au 21e siècle pourraient prêter à sourire si nous ne savions pas que la promesse d'être sauvé de l'Enfer en s'attaquant aux ennemies de l'Islam est le carburant de tout candidat au martyr. Celui-là même qui sans aucun doute a animé les assassins du Bataclan ou de Nice.

Des attentats de 1995 à Ansar al-Fath

SB a été jugé et condamné à 10 ans de prison pour sa participation aux attentats de 1995 à Paris. Il aurait notamment recruté Khaled Kelkal et était responsable de l'implantation des réseaux du G.I.A. en Europe.

Lors de sa sortie de prison en 2003, suite à une remise de peine, son réseau formé d'anciens codétenus recrutés en prison va financer de la cause islamiste et notamment la guerre en Irak. Son réseau Ansar Al Fath (NDR : Les partisans de la victoire) rackettait des prostituées dans le bois de Boulogne. Interpellé et jugé, il sera condamné à 15 ans de prison pour le financement de la cause terroriste et pour des projets d'attentats sur le territoire notamment dans le métro et à l'aéroport d'Orly. Il sera libéré en 2020...

Chérif Kouachi

Orphelin très tôt de parents algériens, Chérif Kouachi est élevé en foyer. Au début des années 2000, il est endoctriné par FB, chef d'un groupe Salafiste. Interpellé peu avant de partir faire le djihad en Irak il remercie les enquêteurs de lui avoir sauvé la vie en l'empêchant de partir combattre en Irak. Son repentir est alors sans doute véritable.

En prison, Kouachi fait connaissance de DB. Cet algérien déchu de sa nationalité française est détenu en France depuis son retour d'Afghanistan, où Al Qaïda l'aurait mandaté pour créer des cellules opérationnelles en France et en Europe. La faiblesse d'esprit de Kouachi fait de lui une proie facile et un nouveau candidat au martyre. La suite, hélas, nous la connaissons. DB, lui, devrait être libéré cet été et expulsé vers l'Algérie.

Larossi Abballa

Lors de son interpellation en 2011, les enquêteurs retrouvent en perquisition un agenda avec une liste de commissariats et de lieux touristiques des Yvelines, des cibles potentielles. L'enquête révèle d'inquiétants échanges : « *Crois-tu vraiment qu'ils ont besoin de nous là-bas au Pakistan ? Allah avec sa volonté nous donnera les moyens de hisser le drapeau ici, en France* », « *Faut commencer le taff* », « *j'ai soif de sang. Allah m'est témoin* ». Il est aussi établi qu'il avait participé fin 2010 - début 2011 à des entraînements militaro-religieux et sportifs dans des parcs du Val-d'Oise et de Seine-Saint-Denis. Lors d'une équipée plus discrète dans les bois de Cormeilles-en-Parisis (Val-d'Oise), le groupe s'entraînait à égorger des lapins...

Des faits punis seulement de 3 ans de prison, 6 mois avec sursis, alors que la France vient de subir les attentats de M. Mehra. Abballa ressort libre de l'audience, ayant déjà purgé l'intégralité de sa peine en détention provisoire. La suite : il assassine deux policiers à leur domicile, devant leur petit garçon.

Le traitement des individus radicalisés à leur sortie de prison

Si la solution de l'internement préventif des individus les plus radicalisés tient de l'OVNI juridique, il faut aussi se garder de croire que la surveillance généralisée des détenus libérés est une solution miracle.

L'internement préventif

Des difficultés constitutionnelles et la ratification de plusieurs traités internationaux nous interdisent l'internement préventif d'individus radicalisés et libérés à l'issue de leurs peines de prison. En outre, plusieurs éléments permettent de douter de son efficacité.

L'appréciation de la dangerosité des profils nouvellement libérés est faite par un magistrat de l'ordre judiciaire qui, sans preuve formelle de leur dangerosité, n'osera pas mettre en œuvre cette mesure. Nous avons déjà vu les limites de l'exercice avec les peines-plancher. Ces dernières, vendues comme une réponse au traitement de la délinquance ont été peu appliquées par des magistrat,s parfois réticents à énoncer des peines d'emprisonnement mais surtout contraints par un système judiciaire et carcéral à bout de souffle. Difficile en effet pour l'autorité judiciaire d'incarcérer des individus, même avec un nouveau cadre légal, en l'absence de création par l'exécutif de places de prison.

Toujours sur cette évaluation des profils, n'oublions pas que ceux-ci peuvent évoluer vers le pire et très vite. La pratique de la dissimulation et la faiblesse de ces profils rendent l'exercice d'évaluation fort périlleux et peu fiable dans le temps. Fatalement, des erreurs surviendront. Enfin, nul n'imagine que cet internement hors cadre infractionnel pourra durer dans le temps. Le rétablissement des lettres de cachet n'est pas pour demain.

La surveillance

S'agissant du suivi des djihadistes libérés, la ministre de la Justice confie à son collègue de l'Intérieur un défi impossible. Le service de renseignement pénitentiaire va délivrer une sorte de « bon de livraison » à ses homologues de la DGSI. Charge à ces derniers de trouver 500 nouveaux agents disponibles chaque année pour suivre les 20 nouveaux libérés annuels. Gardons en tête à cet égard les 2000 milliards d'euros de dette du budget de l'Etat... Outre les aspects logistiques, la surveillance de ces individus se heurte à plusieurs réalités : la quantité, la facilité du mode opératoire et la technique.

- *La quantité*

Créer une échelle de priorité permettant aux policiers de suivre seulement ce que les journalistes appellent le haut du panier est illusoire. Quand bien même nous serions en Corée du Nord, nul service de renseignement n'est capable de sonder l'esprit humain. La nature humaine est imprévisible, encore plus chez les radicalisés qui sont pour la plupart des esprits fort influençables.

La radicalité de leur pratique religieuse, la crainte de l'enfer pour tous les péchés qu'ils ont commis, résonnent avec la faculté d'être sauvé en mourant en martyr. « La mort, je l'aime comme vous aimez la vie » nous mettait en garde déjà Mohamed Mehra. L'ensemble agissant comme un accélérateur du passage à l'acte rarement prévisible.

• *La facilité du mode opératoire*

La facilité du mode opératoire (couteau, voiture...) rend le passage à l'acte quasi- indétectable. Nous sommes loin des éléments préparatoires à un attentat à la bombe, un braquage ou un trafic de drogue pour lesquelles divers actes permettent de caractériser et criminaliser un imminent passage à l'acte. La plupart des éléments apparaissent après la commission de l'acte. Comment détecter un individu sortant de chez lui avec un couteau ou avec sa voiture ?

• *Les techniques de surveillance*

Deux types de surveillances existent, devant être conjointement réalisées pour être efficaces : les surveillances technique et physique.

La surveillance des communications sur Internet est rendue difficile par l'utilisation de logiciel tel que *Tor* (anonymisation du surf sur Internet), préconisée notamment dans la revue Dar-Al-Islam. En outre, on peut souscrire un abonnement téléphonique depuis un Tabac sans présenter de carte d'identité et utiliser ainsi son abonnement Data pour surfer anonymement sur Internet. Nous sommes loin de l'abonnement à la boutique France Telecom, et de la traçabilité qu'elle permettait.

Certains djihadistes, comme les trafiquants ou les braqueurs, changent de téléphone plusieurs fois par semaine et empruntent celui de collègues, amis, familles pour leurs appels sensibles. En parallèle, rédiger une demande de commission rogatoire technique demandant à un magistrat la mise sur écoute d'une ligne téléphonique exige des pages de justifications. Le combat est inégal. En outre des applications type *Telegram* ou *What'sapp* disposent des clés de chiffrement de la société éditrice de la solution, rendant inaudible la conversation pour des enquêteurs.

La surveillance physique n'est pas plus facile. Opérer des filatures dans ces quartiers justement appelés les « territoires perdus de la République » est quasi-impossible. Les éléments exogènes à la cité sont filtrés - même parfois accompagnés. Inévitablement, la surveillance de ces individus semble un pari difficile à tenir et chaque échec sera vu par le citoyen français comme une erreur de stratégie du gouvernement.

Quelles solutions à ce cauchemar ?

L'expulsion systématique des étrangers ou des binationaux

La question de la déchéance de nationalité et de l'expulsion des étrangers condamnés pour des faits de terrorisme doit être de

nouveau examinée par le Législateur sous l'impulsion du gouvernement. Cette question doit être abordée sans passion mais avec la conscience, conférée par le passé proche, que tout individu libéré pourrait commettre un attentat ou, plus passivement, recruter de nouveaux salafistes, vivier des candidats au martyre. Chaque attentat commis par un binational récidiviste affaiblira à nouveau la position de l'exécutif jusqu'à l'intenable. Un éventuel attentat à la charge émotionnelle trop intense provoquera un séisme peut-être lourd de conséquences.

Des accords interdisant la torture ou la peine capitale pour les déchus renvoyés dans leurs pays ou l'aide à la construction de lieux d'accueil spécialisés faciliteraient l'exécution de ces expulsions. Ces accords pourraient être validés au niveau supranational par la C.E.D.H. De plus, la plupart des pays ayant alors donné leur accord n'étant pas laïques, seront beaucoup plus légitimes et aptes que nous à tenter une déradicalisation.

Le traitement judicaire des djihadistes et l'individualisation de la peine

Le Rapport Arpaillange des années 80 expliquait que : *« La sanction pénale est censée à la fois punir, intimider, éliminer ou neutraliser au moins provisoirement, amender et resocialiser le délinquant, tout en exerçant un effet de dissuasion sur ses imitateurs éventuels. Ces diverses fonctions ne sont en réalité guère compatibles ; Les tribunaux prononcent des mesures qui ne sont bien souvent ni intimidantes, ni rééducatrices. Les tribunaux n'osent plus punir, ils n'ont pas les moyens de traiter, de telle sorte que ce mélange des genres rend l'intervention judicaire équivoque, parfois aberrante et finalement peu efficace...* ».

L'éminent pénaliste Jean-Claude Soyer précisait qu'avec le Nouveau Code Pénal « *il n'existe plus symboliquement, de peine minimale, ni de circonstances atténuantes. Le juge répressif n'est donc plus tenu que par le maximum légal et théorique qui, placé très haut le plus souvent, lui laisse en fait un pouvoir discrétionnaire. Lequel évoque, ô paradoxe, un adage d'Ancien Régime : "Toutes peines sont arbitraires en ce royaume"* ».

Pour le terrorisme, l'individualisation de la peine par le magistrat devrait être réduite. Un individu ne peut être coupable de participer légèrement à un attentat. Participer de près ou de loin à une entreprise ayant auparavant assassiné des enfants dans des écoles, tué des familles entières à Nice ou des passants, rend complice et comptable de tout acte revendiqué par ces entités terroristes. Nulle mansuétude ne peut dès lors conduire à aménager la peine. Un *quantum* minimum de la peine devra être défini, le juge gardant bien sûr son pouvoir d'appréciation de la culpabilité de l'individu. Un homme dont la volonté est de terroriser la nation ne devrait pas pouvoir sortir après seulement 3 ans de prison.

Un droit d'exception réservé aux seuls groupes terroristes internationaux à l'évidente nocivité doit être créé. En revanche, d'autres moyens de s'assurer de l'innocuité du suspect doivent être imaginés pour ceux qui, temporairement, ont subi l'influence d'un recruteur. Car pour ceux-là, une courte peine de prison est contre-productive. Cependant bâtir un tel système trouve ses limites avec un Etat endetté de 2 000 milliards d'Euros et une administration judiciaire et pénitentiaire aux personnels dont l'abnégation n'a d'égale que la pauvreté de leurs moyens.

Le développement de nouveaux moyens de preuve issu du droit anglo-saxon

La certitude d'une peine exemplaire doit être associée à la possibilité de prouver de manière irréfutable la culpabilité de l'individu. Le pragmatisme anglo-saxon permet aux enquêteurs de disposer d'outils aussi redoutables qu'efficaces. La provocation à l'infraction est interdite dans notre Droit européen et français car l'administration de la preuve est considérée comme déloyale et fait obstacle à un procès équitable. « *Les coups bas sont interdits, les simples ruses de guerre ne le sont pas* » disait le Doyen Carbonnier.

La chambre criminelle de la Cour de cassation a récemment rappelé le principe en jugeant loyal un stratagème visant à interpeller un malfaiteur. En effet, le procédé utilisé par des enquêteurs se présentant comme acheteurs potentiels d'un véhicule en réponse à une annonce, et donner rendez-vous au voleur pour l'appréhender, n'est pas un stratagème ou une machination dès lors qu'il ne vise pas à provoquer l'auteur à commettre l'infraction mais seulement à l'interpeller. De fait, l'infraction de recel était constituée avant que les policiers ne contactent les receleurs. Dès lors, nous sommes loin de l'agent infiltré au cœur d'un réseau, le manipulant pour le confondre.

En vertu du même principe de loyauté dans l'administration de la preuve, l'immunité légale et totale pour des individus exprimant un repentir permettrait de désorganiser les structures terroristes actives sur notre sol. La vulnérabilité et l'influençabilité de ces individus permettent de les manipuler pour en faire des "martyrs", pourquoi ne pas utiliser ces faiblesses pour défendre la nation ?

De même, récompenser la remise d'information permettant d'incriminer de futurs auteurs d'attentats serait efficace dans des cités où l'argent est un élément Ô combien structurant. Dans cette guerre particulière, l'usage de quelques *ruses* strictement encadrées ne paraît pas illégitime, dès lors qu'elles permettent d'éviter des bains de sang.

PROFONDEUR STRATÉGIQUE - 2

Seine-Saint-Denis : la "misère sociale", vraiment ?

Xavier Raufer

Pour homogénéiser et clarifier les comptes publics européens (et mieux taxer ensuite les Etats-membres...) Eurostat (L'Insee de l'Union européenne) exige désormais que lesdits Etats-membres intègrent à leur PIB (Produit intérieur brut, "thermomètre" mesurant la richesse nationale), leurs transactions illicites estimées : travail au noir, argent des contrebandes d'alcool et de tabac ; narcotrafic et prostitution - toutes activités économiques certes illégales mais quand bien même, commerces effectifs de biens et services, (définition classique : "Transaction de libre choix, par accord mutuel des parties impliquées").

Pour l'Insee, qui a longtemps ergoté sur l'aspect volontaire de ces commerces (addiction des toxicomanes, prostituées contraintes...), tout cela fait environ 3 milliards d'euros par an, de 3 à 4% du PIB français.

Regardons maintenant ce qu'il en est de nos voisins : pire des Etats-membres historiques de l'Union européenne, l'économie illégale contribue pour environ 12% à la richesse nationale d'une Italie, de longue date adepte de la *combinazzione*.

Imaginons maintenant que la Seine-Saint-Denis est, dans une France par ailleurs mieux régulée, une sorte d'Italie interne et "redressons"-là donc dans une similaire proportion : alors que le misérabiliste discours de Borloo & co. nous prétend le "9/3" aux tréfonds de la misère, on réalise que cette pauvreté est plutôt artificielle.

Car bien sûr, la comptabilité publique dont use la France officielle n'intègre nullement les compensatoires trafics illicites.

Voici donc (pour 2010, derniers chiffres publiés permettant comparaison) les dix départements français au taux de pauvreté

(apparent) le plus élevé : Seine-Saint-Denis, Aude, Pyrénées Orientales, Corse, Gard, Vaucluse, Pas-de-Calais, Ardennes, Hérault, Creuse.

Cherchons maintenant à savoir quel est *aujourd'hui* le PIB officiel de la Seine-Saint-Denis. Pas simple à trouver : depuis une décennie *(pourquoi ?)* l'Insee ne publie plus les PIB de l'Ile-de-France par départements, mais en un bloc, au seul niveau régional. Cependant, après enquête, il nous est dit que l'Insee fournit quand même chaque année à Eurostat des données détaillées à l'échelle départementale et là, on finit par repérer des chiffres précis et assez récents, dans d'immenses tableaux Excel bourrés de chiffres minuscules.

Ces derniers chiffres Eurostat remontent à 2014 (et quand on les totalise, ils sont cohérents avec ceux, globaux, de l'Insee en mars 2017) :

Hauts-de-Seine : ± 154 milliards (ci-après Md.) d'€
Seine-Saint-Denis : ± 59 Md.€
Val-de-Marne : ± 54 Md.€
Yvelines : ± 53 Md.€
Essonne : ± 47 Md.€
Seine-et-Marne : ± 40 Md.€
Val-d'Oise : ± 34 Md.€.

Redressons maintenant le PIB de six des sept départements de l'Île-de-France des + 3% de l'économie illicite-criminelle (proportion valant pour la France entière).

Par ailleurs, sans aller jusqu'aux 12% de l'Italie, corrigeons modestement la "zone grise" de Seine-Saint-Denis de +10% : on obtient ainsi le réaliste PIB suivant :

Hauts-de-Seine : ± 159 Md.€
Seine-Saint-Denis : ± 65 Md.€
Val-de-Marne : ± 56 Md.€
Yvelines : ± 55 Md.€ ;
Essonne : ± 48 Md.€ ;
Seine-et-Marne : ± 41 Md.€
Val-d'Oise : ± 35 Md.€.

De loin, la Seine-Saint-Denis est ainsi le second département le plus riche d'Ile-de-France, sachant que le PIB des Hauts-de-Seine est artificiellement gonflé par le quartier de la Défense, où maints grands groupes ont leur siège social et paient donc taxes, impôts, etc. Pour conclure : bien sûr, la partie invisible de la fortune du "9-3" irrigue surtout ses fameux quartiers sensibles, ceux de la "Politique de la Ville".

La Seine-Saint-Denis, département misérable ? Encore un bobard-Borloo.

Faits & Idées

Xavier Raufer & Stéphane Quéré

Régulièrement, *Sécurité Globale* propose des chiffres et données récents, collectés par sa base documentaire internationale. Vérifiés et recoupés, ces faits couvrent tout le champ du crime, du terrorisme, plus tout élément contextuel pertinent. D'où l'objectif et le nom de cette chronique : donner aux lecteurs des *faits*, pour qu'ils aient (plus et mieux encore) des *idées* ; ce, pour enrichir notamment le débat criminologique.

• Faits & données criminels à l'échelle mondiale

Ici, les faits et données d'envergure mondiale ; au minimum, transcontinentale.

PIRATERIE MARITIME[1]

2017 :

- Indonésie, 43 actes violents en mer (1 attaque avec enlèvement ; 5 tentatives d'attaque ; 33 incidents à l'ancre ou au port).
- Nigeria : 36 attaques de navires.
- Somalie, golfe d'Aden : 9 attaques de navires.

1er trimestre 2018 :

- Nigeria : 22 attaques de navires.
- Indonésie : 9 attaques de navires dans les eaux territoriales du pays.

CONTREFAÇONS[2]

Contrefaçons dans le E-Commerce mondial - montant des ventes de produits contrefaits en 2017 (estimation) environ 30 milliards de dollars US (md$). Par ailleurs, nul ne semble vraiment connaître le volume et les montants du E-Commerce en tant que tel, ce qui interdit tout calcul proportionnel. Les marques estiment leur préjudice (2017, ventes en ligne) à environ 322 md$; tout type de vente, physique, classique ou numérique, préjudice mondial de 1 200 md$. En ligne, les biens contrefaits les plus vendus sont : produits de luxe, vêtements, chaussures, cosmétiques, sacs à main...

Contrefaçons dangereuses - faux médicaments : dans 95 pays du monde, la malaria affecte environ 3,2 millions de gens. En Afrique en 2016, la malaria a fait quelque 445 000 morts, dont 70% d'enfants de moins de cinq ans. Du fait de médicaments invalides (contrefaits, faux ou mal dosés), ± 200 000 personnes meurent par an, dont ± 115 000 en Afrique sub-saharienne. Selon une étude de 2012, l'Asie du Sud-Est et l'Afrique absorbent ensemble environ 1/3 de tous les médicaments invalides fabriqués au monde.

VILLES LES PLUS DANGEREUSES AU MONDE (2017)[3]

(Dangereuses, du fait de leurs taux d'homicides). Sur ces 50 villes, 42 sont dans l'aire Amérique latine + Caraïbes. Brésil : 17 villes/50 ; Mexique : 12 villes/50 (5 en 2015) ; loin derrière, les Etats-Unis et l'Afrique du Sud.

[9e Etude de l'ONG Mexicaine *Consejo Ciudadano para la Seguridad Publica y la justicia penal*]

cf. tableau 1 (p. 85).

• Faits & méfaits de la DGSI (Davos-Goldman-Sachs-Idéologie)[4]

Voici la réalité sur une mondialisation de fait conduite au profit des seuls plus riches, en une logique d'économie de rente, où la fortune s'accroît du seul fait qu'on est riche au départ. Signal inquiétant, la dernière année où des inégalités type 2017 furent constatées entre capital et travail fut... 1913.

Etats-Unis 1 : (*Tax Policy Center*) : lois fiscales décrétées par Donald Trump (notamment, baisse de l'impôt sur les sociétés de 35% à 20%) ; en 2027, 90% du bénéfice de ces mesures ira aux 20% des Américains les plus riches.

Taux d'imposition le plus élevé dans les décennies 1960 et 1970 : + de 70% ; taux maximal sous Trump : 37%.

En 2017, les 20 Américains les plus riches possèdent ensemble une fortune supérieure à celle, cumulée, des 50% d'Américains les plus modestes (ils sont 152 millions).

En 1774, les 1% des revenus les plus élevés percevaient 8,5% de la richesse annuelle produite. En 2012, ces 1% des revenus les plus élevés percoivent 19,3% de la richesse annuelle produite.

En 1895, les 6% des Américains les plus riches possèdent 66% de la richesse nationale.

En 2017, les 10% des Américains les plus riches possèdent 77% de la richesse nationale.

En 1928, les 10% des Américains les plus riches captaient 46% de la richesse produite

Tableau 1.

Ville	% d'homicides (+/-)	nombre d'hom.	population
1-Los Cabos, Mexique	111,4/100 000	365	328 245 hab.
2-Caracas, Venezuela	111,2 ...	3 387	3 050 000 ...
3-Acapulco, Mex.	106,7 ...	910	854 000
4-Natal, Brésil	102,6 ...	1 378	1 344 000
5-Tijuana, Mex.	100,8 ...	1 897	1 890 000
6-La Paz, Mex.	84,8 ...	259	306 000
7-Fortaleza, Brésil	83,5 ...	3 270	3 920 000
8-Ciudad Victoria, Mex.	83,4 ...	301	361 000
9-Ciudad Guayana, Ven.	80,3 ...	728	907 000
10-Belem, Br.	71,4 ...	1 743	2 242 000
11-Vitoria da Conquista, Br.	70,3 ...	245	349 000
12-Culiacan, Mex.	70,1 ...	671	958 000
13-Saint-Louis, USA	65,9 ...	205	312 000
14-Maceio, Br.	64 ...	658	1 030 000
15-Cape Town, S.Af.	62,3 ...	2 493	4 005 000
16-Kingston, Jamaïque	59,8 ...	705	1 181 000
17-San Salvador, Salvador	59,1 ...	1 057	1 790 000
18-Aracaju, Br.	58,9 ...	560	952 000
19-Feira de Santana, Brésil	58,8 ...	369	628 000
20-Ciudad Juarez, Mex.	56,2 ...	814	1 449 000
21-Baltimore, USA	55,5 ...	341	614 700
22-Recife, Br.	55 ...	2 180	3 970 000
23-Maturin, Ven.	54,5 ...	327	600 100
24-Guatemala City, Gua.	53,5 ...	1 705	3 190 000
25-Salvador, Br.	51,6 ...	2 071	4 016 000
26-San Pedro Sula, Hond.	51,2 ...	392	766 000
27-Valencia, Ven.	50 ...	784	1 580 000
28-Cali, Colombia	49,6 ...	1 261	2 543 000
29-Chihuahua, Mex.	49,5 ...	460	930 000
30-Joao Pessoa, Br.	49,2 ...	554	1 127 000
31-Ciudad Obregon, Mex.	49 ...	166	339 000
32-San Juan, Puerto Rico	48,7 ...	169	348 000
33-Barquisimeto, Ven.	48,3 ...	644	1 336 000
34-Manaus, Br.	48,1 ...	1 024	2 131 000
35-Distrito Central, Hond.	48 ...	588	1 225 000
36-Tepic, Mex.	47,1 ...	237	504 000
37-Palmira, Col.	46,7 ...	144	309 000
38-Reynosa, Mex.	42 ...	294	702 000
39-Porto Alegre, Br.	41 ...	1 748	4 270 000
40-Macapa, Br.	40,3 ...	191	475 000
41-New Orleans, USA	40,1 ...	157	391 500
42-Detroit, USA	39,7 ...	267	673 000
43-Mazatlan, Mex.	39,4 ...	192	489 000
44-Durban, S.-Af.	38,2 ...	1 396	3 662 000
45-Campos dos Goytacazes, Br.	37,6 ...	184	491 000
46-Nelson Mandela, S.-Af.	37,6 ...	474	1 264 000
47-Campina Grande, Br.	37,3 ...	153	411 000
48-Teresina, Br.	37,1 ...	315	851 000
49-Votoria, Br.	36,1 ...	707	1 961 000
50-Cucuta, Col.	34,8 ...	290	834 000

par an (hors rétribution du capital). De 1951 à 1982, cette captation a cru de + 32%.

De 1979 à 2008, Les 10% des Américains les plus riches ont perçu 100% du bénéfice issu de la croissance des revenus ; les 90% d'autres ont vu leurs revenus diminuer.

Ploutocratie : en 2012, fortune moyenne des membres du Congrès des Etats-Unis : ± 1m$; fortune moyenne des ménages du pays : 56 335 $.

Etats-Unis 2 : salaires des patrons et des salariés - un écart qualifié de "grotesque" par un économiste de l'Université Cornell (l'étude n'inclut pas les salariés à temps partiel, sinon, le verdict serait pire encore) :

- Gain annuel moyen (2017) des 200 Pdg les mieux payés des Etats-Unis : 17,5 m$, + 17% sur le gain moyen de 2016 ; ratio : 275/1. Et la "diversité", valeur soi-disant cardinale du capitalisme américain ? Tous ces 200 personnages sont des hommes blancs d'âge mur. Clairement, "diversité" = piège à gogos.
- En 1979, les Pdg des grands groupes américains gagnaient en général 30 fois plus que le salaire moyen de leurs employés. En 2013, c'est TROIS CENT fois plus.
- En 2017, le Pdg de Walmart a gagné 22,2 millions de dollars (m$). Salaire moyen annuel d'un employé de Walmart : $ 19 177. Cet employé devra donc travailler plus d'un millénaire pour égaler un an de gain de son patron (cash, actions, etc.).
- En 2017, Le Pdg de "Live Nation" (*show-biz*, concerts) a gagné 70,6 m$, au salaire moyen, un de ses employés doit travailler 2 893 ans pour atteindre ce montant.
- En 2017, Le Pdg de Time Warner (médias, etc.) a gagné 49 m$, au salaire moyen, un de ses employés doit travailler 651 ans pour atteindre ce montant.

Encore, ces sociétés sont-elles publiquement cotées en bourse et tenues à un minimum de clarté et de décence. Dans les sociétés privées (*hedge funds*, etc.) les écarts sont dix fois plus obscènes encore. En 2017, le Pdg du *hedge fund* Blue Crest Management a ainsi gagné 2 md$.

Grande-Bretagne : selon un rapport du parlement (*House of Commons Library*), il y a eu en 2017 un nouveau milliardaire tous les deux jours. La fortune des 1% les plus riches du monde a cru en moyenne de 6% par an. (Pour les 99 autres % ayant un capital, cette croissance n'a été que de 3%/an). Si la tendance se poursuit, par pur effet "boule de neige", ce 1% du sommet contrôlera en 2030 64% de la fortune mondiale. Début 2018, fortune estimée totale du 1% le plus riche : 140 000 md$; en 2030, 305 000 md$.

Sondage suite à ce rapport :

- Qui aura le plus de pouvoir en 2030 : les super-riches (34% de oui) ; les gouvernements nationaux (28% de oui).
- Quelles conséquences à cette ploutocratie du sommet ? La corruption (41% oui) ; la vassalisation des gouvernements (oui, 43%).

Etude (*Institute for Fiscal Studies*) sur les jeunes Britanniques des classes moyennes (25 à 34 ans), au revenu moyen pour leur tranche d'âge, les 20% du milieu, possédant leur propre logement ou maison. Ils étaient :

- 65% en 1995-1996 et
- 27% en 2015-2016.

Rapport sur les inégalités mondiales (WID 2018) - FRANCE : En 2014, Insee, le PIB français est de 2 132,4 md€ ; le Revenu national brut est de 2174,5 md€.

- En 2014, les 10% des Français gagnant le plus d'argent captent 32,6% du revenu national avant impôt ; les 1% des Français gagnant le plus d'argent en captent 10,8%.
- En 2014, les 10% des Français les plus riches possèdent 55,3% du patrimoine national ; les 1% des Français les plus riches en possèdent 23,4%.

Encore et toujours, la piraterie bancaire : en février 2018, la filiale californienne de la Rabo bank (d'Utrecht, Pays-Bas) est condamnée à 369 m$ d'amende, pour avoir blanchi par centaines de millions de dollars l'argent de cartels mexicains de la drogue. Initiée en 2013, l'enquête montre que, de 2009 à 2012, Rabo bank a accepté sans contrôle ces sommes énormes, ce sur les comptes de clients suspects, déjà signalés par les autorités fédérales des Etats-Unis.

• La criminalité, par continents

Ici, les faits et données, classés par continent.

Afrique[5]

(Etude OCDE + Banque mondiale + Banque africaine de développement).

- Données portant sur l'Afrique en général : 13% des enlèvements contre rançon (connus) y sont commis ; fraudes sur Internet en Afrique ou à partir de l'Afrique : préjudice en 2017, environ 12,7 md$; piraterie maritime dans les eaux africaines : préjudice annuel estimé de 565 m$ à 2 md$.
- 15 pays de l'Afrique de l'Ouest : aide publique au développement pour la zone : par an, ± 25 md$. Parmi les activités criminelles majeures dans la région :
- Trafic de stupéfiants (teansit vers l'Europe de la cocaïne d'Amérique latine, surtout),
- Extraction illégale de minéraux,
- Trafic des êtres humains,
- Contrefaçons diverses,
- Enlèvements contre rançon,
- Piraterie maritime,
- Cyber-crime.

Chiffre d'affaires criminel pour la région, environ 50 md$/an. Les revenus d'origine criminelle représentent ± 3,6% du PIB des pays de la région, cumulés.

Afrique du sud (*South African Police Service* - statistiques criminelles calculées à la Britannique, à cheval sur deux ans, de l'été 2016 à l'été 2017 par exemple).

Infractions enregistrées été 2016-été 2017 (suivies ou pas de condamnations) : - 1,8%. Mais les homicides augmentent depuis 5 ans consécutifs. Assassins et victimes sont d'usage de jeunes hommes enrôlés dans des gangs. En 2016-2017, il y a eu 40 000 vols à main armée de plus que 5 ans plus tôt (2012-2013).

Asie - Pacifique[6]

Triangle d'Or (confins de la Birmanie-Thaïlande-Laos) : Le pavot et l'héroïne y sont supplantés par la production/vente en gros de Ya Ba, fort toxique mélange de metamphétamine et de caféïne, consommable sous forme de cachets ou de poudre (crystal meth, ou ya-ice). En mars 2018, 700 kilos de ya ice de grande pureté ont été saisis au nord de la Thaïlande. Au Bangladesh, de janvier à mars 2018, 5,3 millions de cachets de Ya Ba ont été saisis par les autorités. Depuis l'implantation de cette drogue dans la région (vers 2007) le trafic de Ya Ba a explosé (multiplié par 40 !).

Corée du Sud : en 2016 (selon la police) le pays comptait 383 bandes et gangs, ayant ensemble 47 251 membres (quelle précision !). Cette année-là, 3 160 individus, appartenant à 44 gangs, ont été arrêtés. Ces bandes sont surtout implantées à Séoul, dans le port de Busan et dans les provinces de Gyeonggi et Gyeongsang.

Moyen Orient[7]

Royaume d'Arabie Saoudite (KSA) : statistiques criminelles officielles (seulement fournies en pourcentage), année 2017 : homicides : - 6,5% ; crimes d'honneur : - 14,5% ; vols : - 2% ; Vols à main armée + vols avec violence ("robberies") : - 10,5%.

Amériques

• *Amérique du Nord*

Canada[8]

De 2013 à 2016, les infractions avec usage illicite d'une arme à feu ont cru de 3%. Et les homicides par armes à feu ont cru, ces mêmes années, de + 66%.

Etats-Unis[9]

Les armes à feu dans le pays - (rapport du *National Institute of Justice*) les citoyens américains possèdent à titre privé quelque 310 m. d'armes à feu. Dernier décompte mondial, en 2008, il y avait quelque 650 m. d'armes à feu privées sur la planète. 40% des habitants des Etats-Unis ont une arme ou vivent dans un foyer en possédant une ou plusieurs. 66% des possesseurs d'armes à feu en ont plusieurs. Au total et selon l'OCDE, en 2010, un Américain est 51 fois plus à risque d'être tué par arme à feu qu'un Britannique.

Effet du laxisme ? Pas sûr : de tous les Etats-Unis, la métropole disposant des lois les plus sévères sur la détention et le port d'armes est Chicago, où il y a eu environ 4 000 tués et blessés par balles en 2017...

Homicides par armes à feu dans le pays : ± 13 000 par an en moyenne, soit, 4,5/100 000 habitants (hors homicides commis par la police). Tous homicides confondus : 5,4/100 000. Là-dessus, les tueries de masse font 2% des homicides en général (et 4,5% des hom. par arme à feu, moyenne 2015-2018).

Par comparaison : Canada, 0,5/100 000 ; France, 0,2/100 000. Moins de 20 ans tués par balle aux Etats-Unis en moyenne, ± 2 650 par an ; ± 900 par suicide, ± 1 500 par homicide; en plus dans cette tranche d'âge, environ 15 000 blessés/an.

Données de l'année 2015 - Il y a eu cette année-là 36 252 morts par arme à feu , environ 22 000 suicides et 12 979 homicides (là-dedans, 248 morts de moins de 14 ans et 4 140 de 15 à 24 ans), en outre, 489 accidents mortels de tir et ± 500 tués dans des échanges de tirs avec la police.

Suicides par arme à feu - aux Etats-Unis, ils sont huit fois supérieurs à la moyenne des autres Etats développés. de 1999 à 2015 (*National Center for Injury Prevention*) il y a eu 313 641 suicides (réussis) par arme à feu.

Mortalité pré-hospitalisation - De 2008 à 2017, en dix ans, 4 fois plus de blessés par balles meurent avant d'atteindre l'hôpital, étant, soit touchés par plus de balles, soit, de plus près. De 2007 à 2014, "échantillon" de 36 297 victimes, mortes avant l'hôpital : 88% blessés par balles, 12%, arme blanche.

Criminalité violente : après une baisse régulière sur 20 ans (1995-2015), le crime violent a augmenté de + 7% et 2015-2016 (mais semblerait baisser en 2017). Les victimes d'homicides dans la période récente sont en grande partie de jeunes Noirs (FBI-UCR, *Uniform Crime Report*). Homicides de Noirs :

- En 2014 : 6 095,
- En 2015 : 7 039,
- En 2016 : 7 881, 50% des homicides de l'année (les Noirs sont 12,1% de la population américaine au recensement de juillet 2016). La plupart de ces victimes noires sont tuées par d'autres jeunes Noirs d'âge analogue ; d'usage lors de guerres de gangs.

Homicides par villes des Etats-Unis, les 20 pires

(FBI-UCR + *Chiefs of Police Association* - avril 2018)

cf. tableau 2 (p. 90).

Homicides à Chicago, Milwaukee, Louisville : doublement sur 2014-2016.

A Chicago, 5 circonscriptions de police regroupant 8% de la population urbaine, concentrent 32% des homicides. Deux de ces circonscriptions, Burnside et Fuller

Tableau 2.

Rang	Ville	% homicides
1	Saint-Louis	64,6/100 000
2	Baltimore	55,2/100 000
3	New Orleans	40,4/100 000
4	Detroit	39,7/100 000
5	Cleveland	33,4/100 000
6	Kansas City	31,7/100 000
7	Memphis	26,9/100 000
8	Newark	25,9/100 000
9	Chicago	23,8/100 000
10	Cincinnati	23,8/100 000
11	Philadelphia	20,2/100 000
12	Milwaukee	19,8/100 000
13	Tulsa	18,7/100 000
14	Pittsburgh	18,2/100 000
15	Stockton	18/100 000
16	Indianapolis	17,7/100 000
17	Washington	17,3/100 000
18	Nashville	17,2/100 000
19	Oakland	17,2/100 000
20	Atlanta	17/100 000

Park, ont des taux d'homicides à la Salvadorienne : 100/100 000.

ÉTATS-UNIS & TUERIES DE MASSE[10]

Les tueries de masse récentes les plus meurtrières (par nombre de victimes)

cf. tableau 3.

En 2017, il y a eu 589 morts lors de tueries de masse (définition : 4 tués ou plus dans l'espace public).La fréquence de ces tueries s'accrôit (FBI) entre 2000 et 2013 ; 70% de ces tueries étant commises en moins de cinq minutes.

Les tueurs de masse

24 fois plus d'hommes que de femmes ; 85% de moins de 44 ans ; milieux modestes, individus solitaires ou isolés et socialement aliénés : pas vraiment un profil précis...

Tueries de masse et pathologies mentales

1 Américain sur 5 souffre de problèmes psychologiques récurrents (80 m. de personnes, dont 48 m..de troubles sévères et ± 19 m. en soin psy.) mais ces Américains

Tableau 3.

Date	Lieu, etc.	Morts & bless.
Octobre 2017	Mandalay Bay resort, Las Vegas	58 m. ± 500 b.
Juin 2016	Pulse, Orlando Fl.	49 m.
Avril 2007	Virginia Tech, Blacksburg campus, Va.	32 m. 17 b.
Décembre 2012	Sandy Hook school, Newton, Ct.	27 m.
Novembre 2017	Rural Texas Church	26 m. 19 b.
Octobre 1961	Luby's Cafeteria, Killeen, Tx.	23 m. 27 b.
Juillet 1984	McDonalds San Ysidro, Ca.	21 m.
Août 1966	University, Austin, Tx.	17 m. 30 b.
Février 2018	Marjory Stoneman Douglas High School, Parkland Fl.	17 m. 14 b.
Décembre 2015	Centre social, San Bernardino, Ca.	14 m.
Août 1986	Bureau de poste, Edmond, Ok.	14 m.
Avril 1999	Columbine High School, Littleton, Co.	13 m. 24 b.
Novembre 2009	Fort Hood Tx.	13 m. 32 b.
Avril 2009	Centre pour immigrés, Binghamton, Ny.	13 m. 4 b.

psychologiquement fragiles n'ont commis ces dernières années que 3% des crimes violents connus. De plus, ces cas pathologiques courent 2,5 fois plus de risques d'être victimes de violences que les sains d'esprit.

(*National Center for Health Statistics NCHS*) de 1999 à 2015 , 1% des 198 760 homicides par arme à feu ont été commis par un cas pathologique avéré - mais une autre étude du NCHS arrive à 5% de tels cas. Et sur 235 tueries de masse étudiées dans la dernière décennie, 22 des tueurs étaient ces cas pathologiques.

Une autre étude (de 2009 à 2016) montre que 34% des tueries de masse sont le fait d'individus interdits de possession ou d'achat d'armes à feu (âge... condamnations... toxicomanie... pathologie mentale avérée..., etc.). Selon *L'American Psychiatric Association*, un Américain court cependant 15 fois plus de risque d'être tué par le foudre, que par un malade mental.

Au total, une grande confusion : selon les paramètres de départ et les définitions choisies, de 25% à 60% des tueurs de masse souffrent plus ou moins gravement d'une pathologie (shizophrénie paranoïaque, troubles bipolaires, dépression) ; ou ont subi des violences, familiales ou autres ; pouvant expliquer l'épisode violent.

Tueries de masse et lieux d'enseignement

(Gun Violence Archive) Depuis la tuerie à l'école de Sandy Hook (décembre 2012), les Etats-Unis ont connu 273 fusillades dans des écoles. (*Washington Post*, mars 2018) en

18 ans (2000-2018) 187 000 éleves ont été confrontés à la violence armée dans des écoles primaires ou secondaires du pays ; moyenne : 10 tueries par an. De 2000 à 2018, il y a eu 22 tueries dans les *écoles* (hors universités) des Etats-Unis (hors affrontements entre bandes) - plus que durant tout le XXe siècle, où 60% des tueurs dans les écoles étaient des 11-18 ans, au XXIe siècle, ils sont 77% de cette tranche d'âge.

Episode armé dans des écoles, janvier-février 2018, avec morts ou blessés

cf. tableau 4 (ci-dessous).

Mexique[11]

Selon le Secrétaire d'Etat (mexicain) aux droits humains, Il y a dans des tombes collectives, morgues, hôpitaux, services de police scientifique, etc., environ 35 000 corps non identifiés ; par ailleurs dans le pays, plus de 30 000 plaintes sont en cours pour disparition inexpliquée.

Sondage : 77% des hab. des 55 plus grandes villes du pays se sentent en insécurité.

Homicides - En 2017, 25 339 hom. ; au 1er trimestre 2018 (sur mêmes mois 2017- + 20% d'hom. : Jan 2018, 2 549 hom., fev. 18, 2 389, mar 18, 2 729 ; total du trimestre, 7 667 hom., le plus meurtrier de l'histoire du pays. En 2016, 60% des homicides du pays étaient le fait du crime organisé ; en 2017, ce taux est de 75%.

Homicides de 2015 à 2016 : + 25% ; de 2016 à 2017 : + 23%.

Taux d'homicides :
2014 : 13,4/100 000
2016 : 16,5/100 000
2017 : 20,2/100 000

Depuis l'entrée en fonction (déc. 2012) du président Enrique Pena Nieto, il y a eu 104 583 homicides connus. Pour TOUT le mandat de son prédecesseur Felipe Calderon, 102 859.

Tableau 4.

Date	Lieu	Morts & blessés
14/02/2018	Parkland Fl. MSD High School	17 m. 14 b.
5/02/2018	Prince George County, Md.	1 b.
1/02/2018	Salvador Castro Middle School, L.A. Ca.	2 b.
23/01/2018	Benton Ky. Marshall County High School	2 m. 18 b.
22/01/2018	New Orleans La. Net Charter High School	1 b.
22/01/2018	Italy tx. high School	1 b.
10/01/2018	Sierra Vista, Ar. Colorado elementary school.	1 m.

• *Amérique latine, généralités sur le crime*[12]

En 2016, il y a eu dans le monde quelque 560 000 morts violentes (guerres : 18% du total ; homicides, 68%, etc.). A eux seuls, 7 pays d'Amérique latine provoquent 25% des homicides mondiaux. L'étude sur "Les 50 villes les plus dangereuses du monde" [voir plus haut]. Or les 2/3 de ces villes sont dans 3 pays latino-américains : Brésil, Mexique, Venezuela". Au total, l'Amérique latine compte 8% de la population mondiale et il s'y produit 38% des homicides connus. Au plan économique, cette criminalité violente est désastreuse : elle coûte au continent environ 236 md$ par an (environ $300 par an, pour chaque habitant de la région).

Taux d'homicides impressionnants de certains pays latino-américains en 2017 :
- Venezuela : 89/100 000
- Salvador : 60/100 000 (début 2015 : 104/100 000 hom, 95% jamais élucidés)
- Jamaïque : 56/100 000
- Honduras : 43/100 000
- Brésil : 30/100 000

Colombie[13]

La guerre civile a duré 52 ans dans le pays (1964-2016) et provoqué 220 000 morts.

Homicides en 2017 : 11 781 (c'était trois fois plus à l'apogée de la guerre civile, en 1998) ; 2016 : 12 252.

Il y avait à Cali, en 1994, 124/100 000 homicides ; quatre fois plus qu'à New York en son apogée meurtrière. Il y en a en 2017 24/100 000, au plus bas depuis 42 ans.

Depuis le début de 2018, guerre dans la métropole de Medellin, entre deux méga-gangs, "Oficina de Envigado" (la structure criminelle originale de Pablo Escobar fin de la décennie 1970, toujours bien vivace) et une milice anti-guérilla nommée "Autodefensas Gaïtanistas de Colombia" ou "Los Urabenos". Homicides dans la ville au 1er trimestre 2018 : + 24% sur les mêmes mois de 2017. Et le téléphérique qui mettait en pamoison les bobo-journalists et urbanistes ? On l'a arrêté, il se faisait tirer dessus.

Europe

Ici, les faits et données, classés par pays de l'Europe (sauf la France).

Allemagne[14]

Cerains types de crimes montent en Allemagne, fin 2017 et début 2018, tandis que d'autres baissent :
- *Rhénanie Nord-Westphalie* : plus de 500 attaques à l'arme blanche commises au 2e semestre 2017 ; Leipzig, ces mêmes attaques, + 300% en 2017. Berlin : 7 attaques à l'arme blanche par jour.
- Plus généralement en Allemagne, la criminalité connue telle que publiée par le BKA (police fédérale) :

Infractions en général 5,76 m. en 2017 ; 6,11 m. en 2016, soit - 9,6% en un an, la plus forte baisse en 25 ans. ATTENTION ! Chaque entrée illicite sur le sol allemand étant une infraction, toute baisse du nombre de clandestins après l'inondation migratoire de 2015 fait automatiquement baisser - de façon parfaitement factice - le nombre des infractions contenues dans la statistique.

Homicides : 785 en 2017 : + 3,2%

Infractions violentes en 2017 : - 2,4%

Cambriolages : 116 540 connus, - 23% sur 2016 (151 540 ; 167 136 en 2015 ; 80% de ces cambriolages ne sont jamais élucidés).

Vols toutes catégories : 2,09 m. en 2017 (-11,8% sur 2016).

- Vols à l'étalage : - 6,6%
- Pickpockets : - 22,7%
- Vols de véhicules : - 8,6%

Belgique[15]

(Fédération belge des finances) De 2007 à 2017, les braquages de banques en Belgiques sont tombés de 127 (10 braquages par mois) à 11 (un par mois) ; soit - 90%.

Grande-Bretagne-1 données criminelles

Faits criminels commis dans tout le Royaume-Uni (UK)

Agression à l'arme blanche d'oct. 2016 à sept 2017 : 37 443, + 21%.

Agression à l'arme à feu d'oct. 2016 à sept 2017 : 6 694.

Faits criminels commis dans l'ensemble England-Wales (E+W)[16]

(E+W) en 2017, agressions à l'arme blanche, + 22% ; à l'arme à feu, + 11%.

Hospitalisations pour blessures à l'arme blanche (2012-2017), + 13%.

Cambriolages : (E+W) d'oct. 2016 à sept. 2017 : 261 915 (connus) : + 32% sur oct. 2015 à sept. 2016. 90% des cambriolages jamais élucidés - une infraction sans risque. Sur 17 082 arrestations pour cambriolage aggravé (avec arme), 20% de - de 18 ans.

Faits criminels commis dans le grand Londres[17]

Agression à l'arme blanche, d'oct. 2015-sept 2016 à oct. 2016-sept 2017 : + 23%.

Tués à l'arme blanche à Londres du 1/01/2018 au 12/04/2018 : 44 individus, dont 33 identifiés ; 5 femmes ; 20 au minimum issus de minorités visibles extra-européennes.

Hospitalisations pour blessures à l'arme blanche (2012-2017), + 17%.

Homicides dans le grand Londres (hors attentats) de 2014 à 2017 : + 40% en 3 ans.

Total des homicides dans le grand Londres pour 2017 : 116 (hors attentats).

Homicides, janvier-mars 2018 (arme à feu, arme blanche, dont 11 adolescents) : 55, + 25% sur jan-mar 2017 (13) - jan-

mar 2018 New York City : 54 hom. (total hom NYC 2017 : 292).
Vols à l'arraché sur deux-roues, grand Londres, 2017 : 23 000 - 63 par jour.

Autres faits criminels significatifs[18]

(*Retail Crime Survey* - activités criminelles affectant le commerce) doublement en 2017 (sur 2016) des violences physiques contre des personnels de vente ; désormais 6 cas sur 1 000 vols. Le commerce britannique emploie 10% des salariés du pays. Le coût financier direct du crime sur le commerce en 2017 est de £ 700 m. (€ 785 m., + 6% sur 2016).

Criminalité dans les campagnes britanniques (*UK Assurances-NFU-Mutual*) de janvier à mars 2018, + 13% de vols et cambriolages) ; dont des vols de tracteurs retrouvés de la Lituanie à Chypre-Turc. Plus des 4X4, des véhicules tout-terrain et du matériel agricole.

Grande-Bretagne-2 laxisme et bienséance[19]

The Guardian (grand quotidien de gauche britannique) 27/04/2018 "Dans certains quartiers de Londres et d'autres métropoles, être un jeune homme noir est un mortel péril, en soi et pour soi".

Comment susciter ex-nihilo une crise criminelle majeure, ce dans un pays où la criminalité baissait depuis quinze ans ?

1 - La soi-disant "droite" de Mme Theresa May, alors ministre de l'Intérieur pétrifiée devant le qu'en dira-t-on médiatique, capitule devant la bienséance et l'antiracisme-monochrome, en fait, talisman protecteur des bandits issus des minorités visibles.

2014 : sous peine de sanctions décrète Mme May, les policiers ont désormais interdiction de fouiller un suspect sans "soupçons sérieux" motivé. La police entend le message : fouiller les racailles = racisme. Donc, finis les contrôles des *BAME Black - Asians Minorities Ethnic* - jeunes Africains ou Pakistanais formant de 70 à 80% de l'effectif des gangs prédateurs des métropoles. Contrôles et fouilles tombent au plus bas depuis 17 ans.

(*England+Wales, E+W*) - 2010 Arrestations pour possession d'arme : 13 833,

2017 Arrestations pour possession d'arme : 7 794.

Résultat immédiat : Infractions violentes constatées (*E+W*) en 2016 : 1 033 719 ; en 2017 : 1 229 260. Et - amusante coïncidence - les agressions par arme blanche (armement favori des gangs) sont en 2017 au plus haut depuis 8 ans.

Celui qui désormais s'indigne de la criminogène bienséance est un Noir, d'origine jamaïquaine, M. Trevor Phillips, ami politique de Tony Blair et directeur de la (fort officielle) Commission pour l'égalité raciale et les droits humains. M. Phillips parle clair

"Soyons francs : ceux qui poignardent et sont poignardés ne sont pas de jeunes Blancs du Surrey ; criminels et victimes sont d'usage de jeunes Caribéens des ghettos. Il faut rétablir le *stop and search* ciblé là où c'est utile - les minorités raciales des ghettos elles-mêmes l'exigent". Selon M. Phillips, rien de "raciste" à dire que la vague criminelle est raciale et concerne les ghettos - mais la bienséante classe politique a peur de le dire.

2 - Bonne libérale, Me May massacre les budgets et effectifs de la police.

De 2011 à 2017, le budget annuel de la Metropolitan Police (*Scotland Yard*) a perdu 690 m. d'€. D'octobre 2017 à mars 2018, *Scotland Yard* perd encore 646 emplois policiers.

(*E+W*) : en 2009, à leur apogée, quand le crime baissait depuis 1995, les effectifs policiers étaient de 144 353. Au 30/09/17, il en reste 121 929 - au plus bas depuis 20 ans. Moins 22 424 policiers dans les rues (-14%) de sept. 2009 à sept. 2017.

Policiers armés E+W : mars 2010 : 6 976 ; mars 2017 : 6 278.

3 - Dans le même temps, la justice en rajoute dans le laxisme

En théorie, tout individu de 16 ans et plus, arrêté pour la 2e fois en possession d'une arme blanche, prend six mois de prison ferme. Or sur le total de tels individus supposés filer en prison pour un semestre,

- En 2017, 2 016 d'entre eux coupent purement et simplement à la prison,
- En 2016, ils étaient 1 891 dans ce cas.

... Libres, bien sûr, de continuer leur carrière criminelle et poignarder leurs semblables.

Italie[20]

(Eléments contextuels) L'économie souterraine en Italie : de 2012 à 2015, le travail "au noir" (emplois illégaux) a augmenté de + 6,3% ; dans le même temps 462 000 emplois légaux ont disparu dans le pays. En 2017, le pays comptait ainsi quelque 3,3 m. de travailleurs illicites dont les salaires sont de ± 54% plus bas que dans l'emploi légal, pour l'industrie ; et de 36% plus bas, dans l'agriculture. Par régions :

Calabre : ± 9,9% d'emplois illégaux
Campanie : ± 8,8%
Sicile : 8,1%
Pouilles : 7,6%

On voit que, sans doute pas par hasard, le phénomène touche d'abord le *Mezzogiorno* mafieux.

Pays-Bas[21]

Il y a un conte de fée néerlandais : tout va bien, la dépénalisation du cannabis est un succès, la criminalité baisse, les Pays-Bas sont un modèle de l'approche en douceur des affaires illicites. Regardez ! en 2017 (sur 2016) les infractions connues (93 020) ont encore baissé de - 5% à Amsterdam ; moins de tout, moins de braquages, de vols à la tire, de cambriolages, etc. La nuit du nouvel

an 2015, il y avait eu 550 cambriolages ; nouvel an 2017, 475, etc.

Ecoutons maintenant les syndicats de policiers, bien moins optimistes ; pour eux, l'appareil statistique néerlandais voit très mal - voire pas du tout, les "crimes invisibles" commis dans les quartiers hors-contrôle : guerres entre *dealers*, trafics d'armes, blanchiment - même certains homicides-règlements de comptes commis par des tueurs à gages, surtout dans les milieus marocain et surinamais.

Plus largement ces policiers (syndicat NPB) pensent que le gouvernement les délaisse et que de ce fait, la police néerlandaise est submergée, insuffisante, dépassée : taux moyen de résolution des affaires de 1 sur 5 ; informatique caduque, demandes d'aide spécialisée (filatures, informatique, criminalistique) accordées une fois sur trois, etc. Les bandits le savent : en 2017, ces policiers ont subi de leur part 9 101 agressions physiques ou verbales (injures, menaces, coups, environ 25 par jour) - 197 plaintes de policiers pour tentative d'homicide.

Pour les syndicalistes des services judiciaires, les citoyens finissent par ne plus porter plainte, trouvant cela inutile du fait de la non-réaction policière ; les chiffres publiés par le service officiel de comptage WODC étant politisés, enjolivés et ne dépeignant pas la réalité, plus sinistre.

Preuve par la drogue ? Selon EMCDDA (l'organisme anti-drogues de l'Union européenne, UE) l'étude des eaux usées de villes de 19 pays de l'UE pour y trouver des traces de stupéfiants issues des urines des égouts (consommation ou fabrication...), montrent qu'Amsterdam est au 1er rang européen pour la cocaïne et l'ecstasy, et Eindhoven N°1 pour les amphétamines. Or pour qu'on use de ces drogues et qu'on les rejette en urinant, il faut bien d'abord qu'elles aient été vendues, ou produites, sur place...

Par ailleurs, 50% de la cocaïne importée en Europe arrive à Rotterdam (Europol).

Conclusion : la police néerlandaise se dit incapable de combattre l'économie souterraine - ses moyens et effectifs actuels lui permettant seulement de cibler 1 gang sur 9. Elle dit tout cela dans un rapport de l'Association néerlandaise des chefs de police fondé sur 400 interview de collègues. Le rapport contient des révélations explosives :

- Il manque 2 000 enquêteurs à la police du pays.
- Chaque année, la justice néerlandaise néglige ou ignore 3,5 millions des infractions à elle transmises.
- Les criminels enrichis par le narcotrafic investissent impunément l'économie légale (tourisme, immobilier, hôtellerie) et se font des amis dans la classe politique.
- 80% des agressions de gens fragiles (âge, handicap, etc.) échappent à la police et à la justice.

Bref conclut le rapport, les Pays-Bas "deviennent un narco-Etat" - affirmation qui tranche sur l'irénisme officiel...

France[22]

Suicides dans les forces de l'ordre

Policiers suicidés : 2011, 43 ; 2012, 43 ; 2013, 40 ; 2014, 55 ; 2015, 44 ; 2016, 39 ; 2017, 51 ; 2018 (jan-avril), 17.

Gendarmes suicidés : 2011, 32 ; 2012, 32 ; 2013, 23 ; 2014, 22 ; 2015, 25 ; 2016, 25 ; 2017, 17 ; 2018 (jan-avril), 17.

Vols à la tire

(Domaine dans lequel le chiffre noir est énorme, 1 sur 4 = dépôt de plainte) 753 000 plaintes en 2017 dont environ 3m. en réalité, soit dans les faits, en France métropolitaine, 344 vols à la tire par heure, ± 5 par minutes.

Fraudes à la carte bancaire

2 millions de ces usages frauduleux de carte bancaire en France, en 2016.

France – 2 – Sondages sur les affaires de sécurité et d'environnement international périlleux[23]

(2017-2018) Ces dix-huit derniers mois, les Français sont mécontents de leur sécurité et le montrent régulièrement, dans maintes enquêtes et sondages.

Enquêtes cadre de vie, Ile de France : victimations (vols & tentatives, véhicules, deux-roues, dans les véhicules, vandalisme, cambriolages (lieux divers), agressions (sexuelles, par proche, tout-venant, vols avec et sans violences, etc.)

Vicitmations (toutes atteintes confondues : 2011, 43% de la population en général ; 2017, 47,8% de la pop. (ayant subi agression, vol de biens du ménage, ou autre, de 2014 à 2017)

Agressions tout type, subie : 5,7% en 2011 ; 6% en 2017 (580 000 Franciliens concernés, 2017)

Vols sans violence subis : 5,6% en 2011 ; 10,5% en 2017 (1,1 m. de Franciliens concernés 2017)

Cambriolage subi : 8,1% en 2011 ; 10% en 2017 (510 000 ménages franciliens concernés 2017).

Peur d'une agression dans un lieu public, oui (H.+F.), 34%

Peur d'être seul dans son quartier : oui, F. 31%, H., 7%

Peur chez soi, oui, F. 9%.

Victimations personnelles des habitants du parc social (HLM, cités, etc.)

2011, 12% des habitants ; 2017, 18,3% des hab.

Parc social, agressions de tout type : 2011, 5,4 % des habitants ; 2017, 6,2% des hab.

Parc social, vols sans violence : 2011, 5 % des habitants ; 2017, 11 % des hab.

Parc social, cambriolages : 2011, 5,2 % des habitants ; 2017, 7,9% des hab.

Parc social, perception du trafic de stupéfiants dans le quartier : 2011, 39,8 % des habitants ; 2017, 43,9% des hab.

IAU (voir notes de bas de page) sondage de 10 500 Franciliens, H. et F. de 15 ans et +, sécurité des transports en commun.

- Insécurité ressentie à Paris : oui, F. 58%
- Agressions dans les transports en commun : oui F., 40% ; H., 20%. Par moyen de transport : RER, 39% ; métro, 29% ; train, 19% ; bus, 14% ; tramway, 9%.

Sentiment d'insécurité niveau national : "je me sens en insécurité dans mon quartier / mon village : oui, 21% des sondés, soit 10,8% de la population de 14 ans et + - au plus haut depuis 2007. Par sexe : 26% de femmes et 16% d'hommes. Sur 100 personnes se sentant en insécurité 43% ont déjà renoncé à sortir seuls, par peur.

Plus les sondés sont jeunes, et plus ils ressentent l'insécurité dans leur quartier : 23% des 14-17 ans ; 19% des 50 ans et +.

Insécurité à domicile : 16% des sondés la ressentent (au plus haut depuis 2014) ; 15% en 2016. Cela concerne 8,2 m. de Français, 1 Français sur 5, 1 homme sur 10.

Enquête ONDRP sur la sécurité dans les transports (métro, bus, RER, TER) : en moyenne, 45% des usagers ressentent de l'insécurité, F. 51% ; H. 38%.

Sondage auprès de 4 000 étudiants lillois sur la sécurité dans le quartier festif de Masséna-Solférino : souvent en insécurité, 45% de ces étudiants ; déjà victimes d'agression, 15% ; déjà témoins d'agressions, 21% ; déjà victimes de harcèlement de rue : 35%. Sur 889 étudiants victimes d'agression, 78% n'ont pas porté plainte, jugeant cela inutile.

Sondages montrant l'insatisfaction des Français dans les domaines de la sécurité :

- *Avril 2018, Odoxa-Dentsu* : êtes vous satisfait de la sécurité en France ? Non, 53%.

- *Mars 2018, Odoxa-Dentsu* : détention des fichés S les plus dangereux, oui, 87% ; expulsion des fichés S étrangers les plus dangereux, oui 83%.

- *Mars 2018, Ifop-Fondation Jean-Jaurès* - Les Français, les prisons et la détention : pour 50% des Français, les prisonniers sont trop bien traités - + 32% sur la même question en 2000 (21%, comme il faut ; 17%, mal traités). La prison doit d'abord priver les détenus de liberté : d'accord, 49% ; la

prison doit d'abord préparer la réinsertion des détenus, d'accord, 45%. Faut-il emprisonner moins de gens (politique pénale) ? Oui, 47% en 2018 (oui, 64% en 2000) ; faut-il dépenser plus d'argent pour améliorer les conditions de détention des détenus ? Oui, 40% en 2018 (oui, 68% en 2000) ; faut-il augmenter les droits de visites aux détenus ? Oui, 37% en 2018 (oui, 77% en 2000) ; faut-il améliorer les conditions de détention des détenus ? Oui, 40% en 2018 (oui, 68% en 2000).

Faut-il refuser aux prisonniers l'accès à l'ordinateur ? Oui, 68% en 2018

Faut-il refuser aux prisonniers l'accès à l'Internet ? Oui, 79% en 2018

Faut-il refuser aux prisonniers l'accès aux portables ? Oui, 87% en 2018

Tel est l'avis massif et clair de l'opinion française. Cependant, la gauche-laxiste-syndicale exige tout l'inverse. CFDT-directeurs de prison : "Des événements graves sont survenus depuis plusieurs mois dans plusieurs maisons centrales ou quartiers-maisons-centrales" [Décodeur : *Pitié, ils sont méchants ! Laissez les faire ce qu'ils veulent dans les prisons !*] Proposition de prisons 5-étoiles - bienvenue au Hilton-CFDT - l'exact inverse de ce qu'exige l'opinion "l'importance d'espaces extérieurs larges et aérés, la présence d'installations sportives, salles de convivialité (!!) Présence d'unités de vie familiale... Régime plus souple que les portes fermées... Réajuster les conditions de vie... Zones socio-culturelles... Assouplissements nécessaires". Incroyable.

- *Mars 2018, Fiducial-Odoxa* : confiance dans le gouvernement en matière de lutte contre le terrorisme ? oui, 41% (au plus bas depuis mai 2016). pas de problème de sécurité en France : 33% des sondés. Vous sentez-vous parfois en insécurité ? Oui, 61%

- *Mars 2018* : mauvaise opinion de la mondialisation : 60% des Français ; la mondialisation aura des effets négatifs pour l'Europe : oui, 55% ; en France, la mondialisation a un effet négatif sur les salaires, oui, 65%, sur l'emploi, oui, 64%. Besoin de normes plus strictes sur les produits entrants et sortants, oui, 66%. Faut-il plus de mondialisation encore ? Oui, 13%.

Février 2018, BVA-Obs' : 63% des Français trouvent qu'il y a trop d'immigrés en France ; 57% des Français sont mécontents de l'action de Macron en matière d'immigration. 1/3 des Français sont contre toute forme d'asile et d'immigration.

• Migrants, Europe et domaine de l'illicite

Crise de la migration et crime, éléments contextuels[24]

Migrations et crimes - selon l'étude d'un professeur de criminologie (lui-même immigré d'un pays Balte) de l'Université bri-

tannique de Huddersfield, dans les territoires où (outre les populations de souche) s'affrontent deux ou plus cultures allogènes (brassages de populations que la pensée bienséante appelle "mixité sociale" ou "diversité"), la criminalité violente est de 70% supérieure à celle de la moyenne nationale du pays en cause ; vols de voitures, 19% supérieurs ; atteintes à la propriété, 92% supérieurs en moyenne.

Les sans-domicile fixe (SDF) en Europe et en France - Il y a dans l'UE environ 11 m. de gens à la rue, vivant souvent mais pas toujours en centre d'hébergement, en foyer ou en hôtel social. Explosion du nombre des SDF en Europe :

Allemagne (2014-2016) + 150%
Irlande (2014-2017) + 145%
Royaume-Uni (2000-2017) + 169% (mars 2017 : 77 240 ménages hébergés, dont 12 000 enfants
Belgique (2008-2016) + 96%
Espagne (2014-2016) + 20%
France - Ile-de-France 2018, ± 100 000 individus logés chaque soir par l'Etat (+ 50% en trois ans). Pour toute la France (2016-2017) + 17% de SDF sur le territoire.

EUROSTAT : en 2017, les Etats-membres de l'Union européenne ont accordé l'asile à 538 000 réfugiés (60% en Allemagne). Dans ce total : Syriens, 33% ; Afghans, 19% ; Irakiens, 12% ; en Allemagne, 325 400 demandes d'asile ont abouti, 40 600 en France, 35 100 en Italie.

MINEURS NON ACCOMPAGNES (MNA) entrés dans l'UE : de 2008 à 2013, ± 12 000/an ; 2015, 95 200 ; 2016, 63 245 ; 2017, 31 395. En 2017, ces MNA représentent 15% de tous les demandeurs d'asile de moins de 18 ans. Pour 2017, 89% de ces MNA sont des garçons, 77% de 16 à 17 ans ; 16% de 14 à 15 ans ; 14% moins de 14 ans. Nationalités : 1, Afghans ; 2, Erythréens ; 3, Gambiens ; 4, Guinéens, 5, Pakistanais ; 6, Syriens (le SEUL pays en guerre !). Pays d'enregistrement de la demande : Italie (32% des demandes) ; Allemagne (29%) ; Grèce (8%) ; Autriche (4%) ; Suède (4%).

Allemagne[25]

Février 2018 : dans un entretien sur RTL-Deutschland, Mme Merkel est interrogée sur la forte poussée des crimes violents commis par des hommes migrants de 14 à 30 ans ; elle reconnaît l'existence de zones hors-contrôle dans son pays : "Il y a des lieux en Allemagne où les gens ne sont pas en sécurité. Ces lieux existent, il faut le dire clairement et il faut y remédier".

Agressions xénophobes, etc. visant des musulmans : l'Allemagne a 82 m. d'habitants dont environ 4,8 m. de musulmans (d'usage, Turcs), la 2e population musulmane d'Europe après la France. En 2017, 60 lieux de culte islamique ont été dégradés et 33 musulmans blessés, dont plusieurs femmes.

Crimes, etc., commis par des migrants (rapport trimestriel du BKA "Kriminalität im

kontext von Zuwanderung" ; ce dernier terme recouvre les clandestins, demandeurs d'asile en attente (non obtenu) réfugiés, et hors-statut, etc. Voici le détail par année des crimes sexuels dont ces Zuwanderer ont été convaincus[26] :

- 2017 (jan-sept) : 3 466 infractions sexuelles, 13 par jour
- 2016 : 3 404 infractions sex., 9/jour
- 2015 : 1 683 infractions sex., 5/jour
- 2014 : 949 infractions sex., 3/jour
- 2013: 599 infractions sex., 2/jour

Pays-Bas[27]

(Statistics Netherland) pour l'année 2015 : néerlandais suspectés d'un crime, 1,2% de la population (en âge, bien sûr, de le commettre) ; migrants suspectés d'un crime, 2,5 à 3,7 d'entre eux.

Suède[28]

Attaques commises avec de mortellement dangereuses grenades militaires défensives : 4 en 2014, 20 en 2017 (et 39 de ces grenades saisies par la police). Chez les bandits, ces grenades sont vendues 30 € pièce - elles abondent tant au marché noir qu'on vous en donne deux gratis pour tout achat de kalachnikov.

Usage criminel d'arme à feu (homicides, échanges de tirs, etc.) 2017, 306 tirs, 41 morts ; 17 morts en 2011.

Zones hors-contrôle (dites "vulnérables" par la politiquement correcte police suédoise) : elles existent bel et bien dit le syndicat des infirmiers et personnels paramédicaux, qui en compte une soixantaine autour de Malmö, Gothenburg, Stockholm.

Elections de l'automne 2018 en Suède, sondage du quotidien *Expressen*, 19/04/2018 :

Problèmes pour la Suède :
1 - l'immigration, 20% de la pop.,
2 - la santé publique, 19%,
3 - la loi et l'ordre, 12%,
4 - l'intégration des minorités, 10%.

France - migrants et migrations[29]

Eléments contextuels

Qu'est-ce qu'un immigré ? un individu né à l'étranger, de parents étrangers. selon l'Insee (2014) la population française est de 65,8 m. (hors Mayotte). 58,2 m. sont nés en France et 7,6 m. nés à l'étranger dont 1,7 m. de nationalité française (au moins un parent français) - donc ± 6 m. d'immigrés, 8,9% de la pop. française, dont 2,3 m. ont acquis la nationalité française depuis leur arrivée.

Insee 2017 : 7,3 m. de gens nés en France ont au moins un parent immigré, soit 11% de la pop. ; 3,3 m. (45% du total) ont deux parents immigrés. 1,1 m. ont deux parents maghrébins ; 1,1 m. deux parents européens. 50% de ces immigrés sont issus de couples mixtes, avec un seul parent immigré. Père immigré, mère locale, 2,1 m. ; père local, mère immigrée, 1,5 m.

Sur ces 7,3 m. de de gens nés en France avec au moins un parent immigré : 45%, origine européenne ; 31%, maghrébine ; 11% Afrique subsaharienne ; 9%, Asie. Descendants d'immigrés de moins de 25 ans : origine Maghreb, 42% ; Afrique subsaharienne, 19%.

Les SDF en France : L'Insee en compte (2017) 143 000 en France, + 50% de 2001 à 2012 ; 10% en Centre d'hébergement et de réinsertion sociale (CHRS), le reste foyers, hôtels, squatts, rue. Marseille, + de 12 500 SDF.

Faits & données[30]

Les mineurs étrangers isolés (MEI) en France - Obscur disciple d'Emmanuel Kant, Georg Christoph Lichtenberg est passé à la postérité pour son joli aphorisme sur "le couteau sans lame auquel ne manque que le manche". Tel est la cas de ces MEI qui, s'ils sont indéniablement étrangers, ne sont souvent pas mineurs du tout et chassent en meute - donc pas isolés. Dans la France de 2017 les diverses instances officielles françaises, sociales ou autre, "mettent à l'abri" (formule curieusement vague) de 30 à 40 de ces MEI chaque semaine, lesquels s'empressent ensuite de disparaître dans le pays. En 2017, 14 908 de ces supposés MEI ont été déférés à l'aide sociale à l'enfance, + 85% de placements sur 2016.

Les gangs criminels de passeurs - de juillet 2017 à janvier 2018, les guerrers de gangs de passeurs, pour le contrôle des voies de passage vers la Grande-Bretagne, des "parkings stratégiques", ont fait 22 blessés (5 par balles, très graves) ces gangs tribaux sont formés d'Afghans, d'Erythréens, d'Ethiopiens, de Soudanais, de Kurdes, etc. et relèvent du crime organisé. 15 de ces gangs de passeurs ont été démantelés en 2015 ; 20 en 2016, 24 en 2017.

Les trafics criminels de migrantes africaines - pendant que d'aveugles bonnes âmes bêlent sur des malheureuses venues en Europe "chercher une vie meilleure", les proxénètes africains s'enrichissent : 14 d'entre eux sont arrêtés à Marseille début 2018. Au sud de l'Italie, ils achetaient 500 euros pièce des esclaves de 18-25 ans, nigérianes le plus souvent, débarquant de Libye sur des barques de fortune. Ces quelques 30 esclaves étaient alors prostituées à Marseille et alentours, après soumission à un rite Juju-animiste pour renforcer l'emprise. 20 à 30 € la passe, chaque proxénète gagnait ainsi ± 180 000 €/an. Ces esclavagistes africains ont été mis en examen pour "proxénétisme aggravé, trafic d'êtres humains, aide au séjour irrégulier en bande organisée". Bonjour "la vie meilleure".

• Terrorisme, guérillas, etc.

France, les attentats terroristes récents (aboutis)[31]

Ces actes ont d'usage fait l'objet de revendications de l'entité Etat islamique, plus ou moins sérieuses.

Mars 2018 - Trèbes, Aude, et Carcassonne - l'hybride crime-terrorisme Redouane Lakdim (26 ans) prend des otages dans un supermarché et est abattu peu après. 3 morts dont le L-C. Beltrame et le terroriste, et 3 blessés.

Octobre 2017 - Marseille, l'hybride tunisien clandestin Ahmed Hanachi (29 ans) poignarde à mort deux jeunes femmes françaises devant la gare Saint-Charles. Trois morts dont le terroriste.

Avril 2017 - Paris, Champs-Elysées, l'hybride Karim Cheurfi (39 ans) tire au fusil d'assaut sur un fourgon de police et tue un capitaine de police. Deux morts dont le terroriste et deux blessés.

Juillet 2016 - Saint-Etienne du Rouvray (Seine-Maritime), l'hybride Adel Kermiche (19 ans) et un complice attaquent l'église pendant une messe et égorgent le père Jacques Hamel (86 ans). Trois morts dont les deux terroristes.

Juillet 2016 - Nice, le fort perturbé tunisien Mohamed Lahouaiej Bouhlel, 31 ans, lance un poids-lourd sur la promenade des Anglais le soir du 14 juillet. 86 morts dont le terroriste et plus de 450 blessés.

Juin 2016, Magnanville (Yvelines) - l'hybride marocain Larossi Abballa (25 ans) poignarde à mort un couple de policiers à leur domicile et est abattu par le RAID.

Novembre 2015 - Neuf djihadistes "belges", "français", etc., hybrides pour la plupart, rentrés de la zone Syrie-Irak par la route des migrants, massacrent au hasard des passants au stade de France (Saint-Denis), au Bataclan et sur des terrasses de cafés. 130 morts (dont les terroristes, sauf un) et plus de 400 blessés.

Juin 2015 - Saint-Quentin-Fallavier (Isère) le fort perturbé Yassine Salhi (35 ans) décapite son patron puis précipite sa voiture sur un stock de bonbonnes de gaz. Un mort (Salhi se suicide en prison six mois plus tard).

Avril 2015 - Villejuif (94) Sid Ahmed Glam (Algérien, 30 ans, *exception* : nul passé criminel connu) tue une jeune femme, prélude avorté à un attentat visant une église de la ville. Arrêté peu après avec diverses armes de guerre, dont des fusils d'assaut.

Janvier 2015 - Montrouge (92) Puis Paris, porte de Vincennes, l'hybride Amedy Coulibaly (33 ans) tue une policière municipale puis attaque la supérette Hyper Cacher ; 6 morts au total, dont le terroriste.

Janvier 2015 - les hybrides Saïd (35 ans) et Chérif (33 ans) Kouachi, attaquent au fusil d'assaut les bureaux de *Charlie Hebdo*, à Paris : 12 morts (8 membres de la rédaction, un invité, deux policiers et un agent d'entretien). Les deux frères sont abattus deux jours plus tard dans une imprimerie de la Seine-et-Marne.

• Stupéfiants : production, trafics, etc.

Afrique

Usage accru du Tramadol, opioïde de synthèse très populaire en Afrique occidentale.

Amérique du Nord

Canada[32]

(Données 2015, Statistiques Canada) - Ont fumé du cannabis au moins une fois en 2015 : 1 canadien sur 8 (12,3%) ; en 1985, 5,6% des Canadiens. Baisse de l'usage chez les ados, augmentation dans l'âge mûr. (Usage au moins une fois, 2017) : 15-17 ans, 17,5% ; 18-24 ans, 28,4% ; 25-44 ans, 17,7% ; 45-64 ans, 7% ; 65 et +, 1,6%.

États-Unis[33]

La tragique, l'immense, explosion de toxicomanie aux opioïdes :

- Depuis la décennie 1990, les opioïdes de tout type ont tué environ 1 million d'Américains. (NIDA, *National Institute on Drug Abuse*) chaque jour, 115 toxicomanes meurent de surdoses mortelles des divers opioïdes.

Surdoses fatales d'opioïdes chez les Américains blancs : 21,7/100 000,

Surdoses fatales d'opioïdes chez les Américains noirs : 16,4/100 000,

- De 2001 à 2017, la crise des opioïdes a coûté 1 000 Md$ aux Etats-Unis et coûtera encore 500 md$ pour les années 2019-2021. Dans ces sommes : pertes de salaires, pertes de productivité, coûts de santé ; niveaux de l'Etat fédéral, Etats, échelons locaux : pertes d'impôts, services sociaux, éducation, prévention et répression.

Coût de la crise en 2001 : ± 30 md$, en 2017, 115 md$. Seuls coûts médicaux de la crise opioïde, 2001-2017, 215 md$.

- Jusqu'à 2015, la première cause de surdoses fatales aux Etats Unis sont les analgésiques, médicaments type Oxycontin. Depuis, la 1re cause sont les héroïnes de synthèse type Fentanyl.

- Fentanyl : 1 kg en poudre se vend (prix de gros) 80 000 $. Après coupage, il rapporte à la vente au détail 1,6 m$ - 20 fois plus rentable que l'héroïne. Rappelons que le Fentanyl est de 50 fois plus puissant que l'héroïne, 100 fois plus que la morphine. Plus puissant encore : le Carfentanyl (somnifère pour pachydermes) 100 fois plus concentré que le Fentanyl.

- Toxicomanes aux urgences hospitalières : 91 m. d'admissions de juillet 2016 à septembre 2017. Durant toute l'année 2017, ces admissions augmentent de + 30%. Cas spectaculaires : Wisconsin, + 109% d'admissions, Delaware, + 105%, Pennsylvanie,

+ 81%. Le nombre de toxicomanes n'augmente pas en 2017-2018 MAIS les stupéfiants qu'ils prennent sont bien plus dangereux.

- Qui se tue aux opioïdes ? 515 000 morts par surdose aux Etats-Unis, de 2006 à 2017. La plupart de ces victimes proviennent de quartiers deshérités, de cités délaissées - parfois des taux de surdose fatale de 100/100 000 dans les comtés les plus pauvres (qu'ils soient urbains ou ruraux, sans différence notable). Ces comtés recensent aussi les plus hauts taux de divorces, de couples éclatés, de familles monoparentales : l'Amérique misérable et suicidaire (Appalaches, Oklahoma, Sud-Ouest profond, Californie centrale) si loin du rêve promis et vanté...

Europe (sauf France)

Grande-Bretagne[34]

(England+Wales) 2017, 3 744 surdoses mortelles, la plupart du fait d'opioides (stupéfiants, analgésiques détournés, héroïnes de synthèse type Fentanyl, etc.) ; en 2016, 2 593 surdoses mortelles, + 60% sur 2006.

En Grande Bretagne, il s'est délivré en 2015 88,7 m. d'ordonnances pour médicaments opioides et antidépresseurs, plus de 10 pour chaque heure de l'année.

(*University College London Hospital*) décompte pour l'année 2001 500 morts par surdose d'opioides, 900 morts en 2011. L'opioide Tramadol, lui, a provoqué 132 surdoses fatales en 2010, 240 en 2014.

Surdoses fatales par Fentanyl :
- 2015 : 2,7 décès par mois
- Fin 2016 : 8 " "
- Fin 2017 : 10 " "

Chaque mois sur le Dark Web accédé depuis la Grande-Bretagne, il s'opère 300 achats de Fentanyl.

France[35]

Héroïne (données de 2014) : 1,5% des 18-64 ans a essayé l'héroïne au moins une fois dans sa vie ; usage dans l'année : 0,2% des 18-64 ans ; tranche d'âge des 17 ans, une fois dans la vie : stabilité de 2011 à 2014.

Toxicomanie, tranche d'âge des 17 ans (9e étude Escapad, mars 2017, sur 46 054 ados de 17 ans). (De 2014 à 2017) ont déjà fumé du cannabis au moins une fois : 39,1%, moins de 4 sur 10 (au plus bas depuis 2000 - 2014, 47,8%). Déja fumé dans le mois : ± 21% (2014 : 25,5%). Fumeurs fréquents (10 fois+/mois) 2017, 7,2% ; 2010, 9,2%. Baisse aussi de l'usage d'autres stupéfiants : MDMA-Ecstasy, amphétamines, cocaïne, crack, hallucinogènes, etc. au total, 8,8% d'usagers en 2014, 6,8% en 2017.

• Prisons et pénitentiaire

Prisons, prisonniers, Etats-Unis[36]

Fin 2017 détenus (d.) dans les prisons des Etas-Unis :

- *Prisons des Etats* : 1 316 000 d.- ordre public, 152 000 ; stupéfiants, 200 000 ; infractions visant des biens, 237 000 ; infractions violentes, 718 000. Sur ces 718 000 infractions de violence : Coups & blessures volontaires, 138 000 ; braquages + vols avec violences ("robberies"), 174 000 ; infractions sexuelles, 164 000 ; homicides involontaires + blessures graves, 18 000 ; homicide volontaire, 180 000.
- *Prisons fédérales* : 225 000 d. (préventive, 51 000 ; condamnés, 174 000). Sur les condamnés en prison fédérale : troubles à l'ordre public, 66 000 ; violences, 13 000 ; Stupéfiants, 82 000, infractions visant des biens, 110 000.
- *Prisons locales* (county jails) 615 000 d. (préventive, 465 000 ; condamnés, 150 000).
- Juvéniles : 48 000 d.

Détenus pour simple possession de cannabis : prisons fédérales, 1% des d. (92 sur 200 000) ; prisons des Etats, - de 4% des d. ; les prisons des Etats forment 87% des prisonniers des Etats-Unis. 3,4% des prisonniers y sont pour possession de stupéfiants et 11,7% pour toutes infractions liées au stupéfiants (autre que possession simple) ; total des détenus pour infraction liée aux stupéfiants, moins de 15%.

Les Noirs des ghettos et la prison - Noirs (hommes) nés et élevés dans les quartiers deshérités : chaque jour de l'année 2010, 21% du total de ces hommes sont en prison.

Prisons, prisonniers, Europe[37]

[Statistiques pénales de 47 des 52 administrations pénitentiaires du Conseil de l'Europe, manquent : Russie, Ukraine, Lietchenstein & Bosnie-Herzégovine] Population carcérale, Europe, septembre 2016, 859 102 détenus + 1,4% (18 454 détenus de plus qu'en 2015), moyenne, 92 prisonniers pour 100 places ; mesures alternatives (liberté conditionnelle) + 12,3% ; bracelet électronique, ± 1,6 m. d'individus. Médiane européenne détenus/habitants (2016) ± 117/100 000 ; France, ± 103/100 000 ; Allemagne, ± 79/100 000.

France

En 2016, taux de récidive connu : 59%.

Les promesses du président Macron en matière pénitentiaire [38] - Sans exagérer, parlons ici de peau de chagrin : 15 000 places promises dans la campagne présidentielle, 10 000 ensuite ; enfin 7 000 (dont rénovation de l'existant).

Combien de détenus en France, quelle densité pénitentiaire ? [39] - (Ministère de la justice, 1/04/2018) 82 026 écroués, 70 367 détenus, + 1% sur le 1er mars (81 377). Là-dessus, 20 852 en détention provisoire, au plus haut depuis 2006. France (2016) individus sous mesure probatoire 174 500 ; hausse de la population carcérale de 2007 à 2016 : + 12%.

Densité des prisons françaises (fin 2017) 117% (114% fin 2016, Belgique, 120/

100 000) ; densité pour les maisons d'arrêt, de 136 à 141% (M. A. de Fresnes, 200%).

Capacité totale des prisons françaises en février 2018 : 59 765 places. 39% des détenus sont en cellule individuelle.

± 70 000 détenus et ± 28 000 gardiens : la France est au niveau de la Roumanie (comparaisons européennes).

La France pratique-t-elle la "tout-carcéral" ? - non fin 2017, la france compte ± 99 détenus/100 000 habitants ; moyenne de l'Union européenne, 115,5/100 000 ; du Conseil de l'Europe, 133,8/100 000.

Combien d'étrangers dans les prisons françaises ? [40] - [Ministère de la justice] Prévenus et condamnés étrangers détenus dans les prisons françaises au 1/10/2017 : 16 234, 15 239 incarcérés et 995 aménagements de peine.

(Chiffres au 1/02/2018, Garde des Sceaux, Assemblée nationale, mars 2018) ce mois-là, 14 964 détenus étrangers en France (22% du total). 4 pays font 42% des étrangers détenus : Algérie, 1 954 détenus ; Maroc, 1 895 ; Roumanie, 1 496 ; Tunisie, 1 102. Plus bien sûr, tous les détenus de nationalité françaises mais issus de l'immigration maghrébine.

Fin 2007, il y avait en France 11 040 étrangers prisonniers en France (19,02% du total).

Notes

[1] *The Conversation* - 27/04/2018 "Pirates with black magic attack shipping in Indonesian waters".

[2] Global brands counterfeiting report, 2018 - *The Conversation* - 24/04/2018 "Fake drugs are one reason malaria still kills so many".

[3] *Daily Mail* - 9/03/2018 "Revealed : the 50 most dangerous cities in the world" - Business Insider - 6/03/2018 "These were the 50 most violent cities in the world in 2017" Rappelons que toute l'Union eusopéenne a des taux d'homicides sous les 2/100 000.

[4] *New York Times International* - 29/05/2018 "Millions at the top, and a pittance below" - *New York Review of Books* - 10/05/2018 "Taxing the poor" - *RT* - 9/04/2018 "Richest 1% will own two-third of global wealth by 2030" - *The Observer* - 7/04/2018 "Richest 1% on target to own two thirds of all wealth by 2030" - *Le Point* - 22/02/2018 "Comment les riches ont fait sécession" - *Libération* - 19/02/2018 "Combien les 1% les plus riches en France possèdent-ils de la part du PIB ?" - *Reuters* - 16/02/2018 "Homeownership among young britons plunges compared with 20 years ago" - *RT* - 9/02/2018 "Now, when even the Financial Times admits America's superrich have more money than they can spend" - *AP* - 7/02/2018 "Rabobank's California unit pleads guilty in money laundering case".

[5] *Les Echos* - 20/02/2018 "Le crime coûte 50 milliards de dollars annuels à l'Afrique de l'Ouest" - *Quartz* - 24/10/2017 "South Africa's notoriously high crime rate is down, but it doesn't feel that way".

[6] *Weekly Voice* (Bangladesh) - 25/04/2018 "Yaba drug smuggling, addiction rate, record alarming rise in Bangladesh" - *Burma News International* - 5/04/2018 "Thai police seized drugs worth Bt 1,7 Billion, believed to be from Myanmar" - *AP* - 3/04/18 "Thai authorities say thy have seized drugs worth about US$ 29 million and arrested 11 people in recent days, as narcotics cases surge in the country" - *Jane's intelligence weekly* - 2/03/2018 "Organised crime groups in South Korea increasingly operating hybrid licit-illicit businesses, hampering law enforcement efforts".

[7] *Asharq al-Awsat* - 23/04/2018 "Crime rates drop in Saudi Arabia".

[8] *Reuters* - 20/03/2018 "Spike in crime prompts Canada to unveil tougher gun control steps".

[9] *The Trace* - 26/04/2018 "What's the homicide capital of America ? Murder rates in US cities ranked" - *The Trace* - 23/04/2018 "More shooting victims are dying before they reach the hospital, researchers think an increasing intensity of gun violence may be to blame - *The Week* - 22/03/2018 "The plight of black men" - *La Croix* - 23/02/2018 "La violence des armes à feu aux Etats-Unis" - *City Journal* - 14/02/2018 "Looking away from urban crime".

[10] *BFMTV* - 20/04/2018 "Etats-Unis : les fusillades dans les écoles en angmentation constante" - *Fox News* - 3/03/2018 "How prevalent is mental illness in mass shootings" - *Business Insider* - 22/02/2018 "An NRA spokeswoman blamed an insane monster for the mass shooting in Florida - here's the truth about menal illness and guns" - *NBC News* - 17/02/2018 "Connecting mental illness and mass shooting misses the point, experts say - *AP* - 16/02/2018 "*How many US school shooting in 2018 ? Florida high school latest hit by gun violence"* - *NBC News* - 16/02/2018 "Recent school shooting" - *NY Times* - 16/02/2018 - Fact-checking : claims about gun violence and mental illness" - *Paris-Match* - 15/02/2018 "Etats-Unis, la tragique banalité des fusillades à l'école" - *RT* - 15/02/2018 "How many Americans must die before shooting sprees finally end ?" - *Libération* - 15/02/2018 "Les armes à feu aux Etats-Unis : cinq chiffres pour un fléau" - *Le Monde* - 15/02/2018 "Etats-Unis : depuis le début de l'année, pas plus de deux jours sans victimes dans des fusillades de masse" - *CNN* - 15/02/2018 "How US gun culture compares with the worls in five charts" - *NBC News* - 14/02/2018 "Las vegas shooting is deadliest in modern US history".

[11] *Business Insider* - 23/04/2018 "Violence in Mexico is still setting records - and the embattled president just reached a grisly milestone" - *AFP* - 22/04/2018 "Mexique : 7 667 assassinats au Ie trimestre" - *Borderland Beat-Reforma* - 6/04/2018 "There are 35 000 dead in Mexico not identified".

[12] *The Economist* - 5/04/2018 "Shining light on Latin America's homicide epidemic" & "Violent crime -how to cut the murder rate" - *Espaces Latinos* - 22/03/2018 "En Amérique latine, chronique de morts

annoncées - cohabiter avec les homicies" - *Insight Crime* - 12/03/2018 "Why Latin America dominates global homicide rankings".

[13] *Colombia Report* - 27/04/2018 "Is Medellin on the brink of another war ?" - *The Conversation* - 6/04/2018 "Colombia's murder rate is at an all time low, but its activists keep getting killed".

[14] *BILD* - 23/04/2018 "Plus de 500 attaques au couteau ces six derniers mois en Rhénanie-Nord Westphalie" - *The Local De* - 23 /04/2018 "Crime in Germany drops by biggest margin in a quarter century" - *DPA-The Local* - 11/04/18 "Burglaries drop by over 20% in a year, signalling major police success".

[15] *Dernière Heure* - 5/02/2018 "Dix fois moins de hold-up en dix ans : comment expliquer cette tendance ?" - *L'Avenir* - 5/02/2018 "Seulement 11 braquages de banques l'an dernier, un nombre en diminution de 90% en dix ans".

[16] *The Guardian* - 27/04/2018 "Why is violent crime on the rise and who is most at risk?" - *Daily Mail* - 19/03/2018 "Will your house be the next target?" & "Suspects are children under 18, in one in six burglaries".

[17] *Le Parisien* - 17/04/2018 "Londres : au moins 35 meurtres au couteau depuis le début de l'année" - *The Sun* - 15/04/2018 "London stabbings 2018 - London Knife crime statistics" - *AFP* - 8/04/2018 "Le gouvernement britannique annonce des mesures pour enrayer la criminalité" - *Mail on Sunday* - 8/04/2018 "How does London's spate of killings compare with other cities?" - *The Sun* - 1/04/2018 "How many London stabbings have there been and are offences on the rise? Knife crime statistics in the UK" - *Evening Standard* - 21/03/2018 "London stabbing epidemic will get worse before it gets better" - *The Mirror* - 21/02/2018 "Inside UK's evil masked moped crime gangs who use acid and knives to steal phones ans brag they can't be caught".

[18] *The Guardian* - 21/04/2018 "City gangs behind burgeoning crop of countryside crime" - *Professional Security Magazine* - 8/03/2018 "Crime survey shows spike of violence".

[19] *The Guardian* - 27/04/2018 "Being a young black man..." - *Daily Mail* - 12/04/2018 "Knife crime farce: 2 000 offenders a year are dodging jail" - *The Sun* - 10/04/2018 "London cops scared to stop and search as city's murder rate passes New York, says MET chief" - *The Mail on Sunday* - 8/04/2018 "Ex-race chief makes controversial call for tougher policing in Black communities hit by knife crime" - *Daily Mail* - 4/04/2018 "How violent crime rose after Theresa May watered down stop and search powers" - *BBC News* - 4/04/2018 "Stop and search, how successful is the police tactic?" - *The Guardian* - 13/02/2018 "Police numbers drop by 1 200 in six months as wage bill frozen" - *BBC News* - 7/02/2018 "Reality check : what has happened to police numbers?".

[20] *The Local* - 1/02/2018 "Italy's illegal work force is booming, new report warns".

[21] *NL Times* - 28/03/2018 "Over 9 000 incidents of violence against Dutch cops last year" - *NL Times* - 7/03/2018 "Amsterdam wastewater contains most ecstasy in Europe" - *NL Times* - 7/03/2018 "Dutch crime figures much higher than reported: trade-unions" - *NL Times* - 1/03/2018 "Crime down 5% in Amsterdam ; drop seen in most Netherlands" - *NL Times* - 20/02/2018 "Netherlands turning into a narco state, Police union says" - *The Guardian* - 20/02/2018 - Netherlands becoming a narco state" - *NL Times* - 12/02/2018 "More invisible crime in Amsterdam".

[22] *Le Figaro* - 30 mai 2018 "Le nombre de suicides ches les gendarmes, en hausse" - *Aujourd'hui en France* - 9/03/2018 "Gare aux voleurs" - *Le Parisien* - 8/03/2018 "Vols par ruse : les méthodes toujours plus astucieuses des malfrats".

[23] Syndicat national des directeurs pénitentiaires (CFDT) - 16/05/2018 3Revoir la doctrine des maisons centrales" - *Libération* - 28/04/2018 "Selon un sondage, une moitié de Français jugent que les détenus sont trop bien traités" - *France-Info* - 26/04/2018 "Six Français sur dix sont mécontents de l'action du gouvernement depuis un an, d'après un sondage" - *BFMTV* - 12/04/2018 "Le sentiment d'insécurité des Franciliens a reculé" - *BFMTV* - 9/04/2018 "Prisons : les Français favorables à des conditions de détention plus sévères" - *BFMTV* - *Le Figaro* - 6/04/2018 "Terrorisme : la cote de l'exécutif s'effrite" - *Le Figaro* - 30/03/2018 "83% des Français favorables au renvoi des fichés S étrangers" - *L'Obs* - 30/03/2018 "83% des Français favorables à l'expulsion des étrangers fichés S" - *20 Minutes* - 18/03/2018 "Lille : les étudiants ont peur de sortir le soir dans certains quartiers" - *20 Minutes* -

16/03/2018 et *Le Parisien* - 15-03-2018 -"58% des femmes ne se sentent pas en sécurité dans la capitale" - *Afp* - 15/03/2018 "Sondage : 60% des Français ont une mauvaise opinion de la mondialisation" - IAU (Institut d'architecture et d'urbanisme d'ile-de-France) - Mars 2018 "Victimation et sentiment d'insécurité en Ile-de-France" - *Reuters* - 7/02/2018 "Les Français pour le droit d'asile, pas l'immigration, dit un sondage BVA" - *France-Info* - 30/01/2018 "Une femme sur deux ressent de l'insécurité dans les transports en commun" - Enquête cadre de vie et sécurité - 2017 "Victimation en 2016 et perceptions de la sécurité".

[24] Eurostat- communiqué - 16/05/2018 "Plus de 31 000 mineurs non accompagnés parmi les demandeurs d'asile dans l'UE en 2017" - *The Conversation* - 10/04/2018 "Immigration and crime: is there a link ?" - *Le Monde* - 21/03/2018 "De plus en plus de sans-abri partout en Europe" - Eurostat - avril 2018 - réfugiés et asile.

[25] Gatestone Institute - 20/03/2018 "Migrant rape crisis still sowing terror and destruction" - *Anadolu* - 3/03/2018 "Anti-Muslim hate crime surges in Germany" - *RT* - 27/02/2018 "You have to call it by name - Merckel publicly admits no-go areas in Germany".

[26] Attention : les statistiques du BKA ne comportent QUE les crimes élucidés (*aufgeklärten Straftaten*) et seuls quelque 50% des crimes comme le viol sont élucidés. Les données du BKA sont donc très partielles. Le directeur de l'association de la police criminelle (*BDK, Bund Deutscher Kriminalbeamter*) estime, lui, que 90% des agressions sexuelles commises en Allemagne échappent aux statistiques officielles.

[27] *NL Times* - 1/02/2018 "No measurable increase in crime near asylum centers, Dutch justice department".

[28] *RT* - 19/04/2018 "End of multiculturalism ? Swedes say immigration is top issue ahead of election" - *BBC News* - 18/04/2018 "Sweden's deadly problem with hand grenades".

[29] *20 Minutes* - 9/04/2018 "Cinq à six fois plus de mineurs étrangers isolés mis à l'abri depuis trois mois" - *Libération* - 6/04/2018 "Connaît-on le nombre de personnes issues de l'immigration qui vivent en France" ? - *La Croix* - 6/04/2018 "Les personnes sans domicile fixe en France" - *Le Monde* - 8/03/2018 "Le gouvernement face au défi de la prise en charge des mineurs étrangers non-accompagnés".

[30] *Le Parisien* - 17/06/2018 "Marseille : le réseau de proxénètes faisait venir des femmes parmi les migrants" - *Le Point* - 16/02/2018 "Marseille, les prostituées nigérianes étaient achetées 500 € en Libye" - *20 Minutes* - 16/02/2018 "Marseille : des proxénètes prostituaient se jeunes nigérianes après un rite vaudou" - *Le Monde* - 2/02/2018 "Calais : les rixes sont liées à des logiques de passeurs et de territoires" - *Europe 1* - 2/02/2018 "A Calais, une guerre de territoires entre mafias et passeurs" - *Le Parisien* - 2/02/2018 "Pic de violences entre migrants : à Calais, la tension est terrible" - *20 Minutes* - 2/02/2018 "Calais est en proie aux violences attisées par les passeurs".

[31] *Le Monde* - 23/03/2018 "Les attaques terroristes en France depuis trois ans"

[32] Journal de Montréal - 21/02/2018 "Les consommateurs de cannabis ont doublé en 30 ans au pays

[33] *New York Times International* - 1/06/2018 "Fighting an elusive opioid" - *Global Research* - 29/03/2018 "Opioids and the narcotic-fueled genocide of American workers" - *UPI* - 26/03/2018 "US opioid ODs cluster in centers of poverty" - *VOA News* - 6/03/2018 "CDC: rate of opioid overdoses increasing, especially in Midwest" - *CNN* - 6/03/2018 "Emergency room visits for opioid overdose up 30% CDC study finds" - *Washington Times* - 14/02/2018 "Opioids crisis costs estimated $ 1 Trillion from 2001-2017" - *Vox* - 6/02/2018 "Why the opioid epidemic may have fueled America's murder spike"

[34] *New York Times* - 4/02/2018 "Fentanyl add deadly kick to opioid woes in Britain" - *The Sun* - 12/02/2018 "Deaths from addictive opioid painkillers like Tramadol almost double in a decade" - *Daily Express* - 11/02/2018 "Black market painkiller Fentanyl claims almost ten lives every month" - *The Telegraph* - 12/02/2018 "Deaths from painkillers double in a decade as Britain follows US".

[35] *Libération* - 16/02/2018 "La France toxicomane : médicaments psychotropes, héroïne et opiacés" - *Le Figaro* - 6/02/2018 "Les jeunes de 17 ans fument moins de cannabis" - *Le Monde* - 6/02/2018 "Les jeunes consomment moins de cannabis, de tabac et d'alcool".

[36] *Vox* - 17/04/2018 "A Republlcan and a Democrat pointed to marijuana prohibition to explain mass incarceration: they are both wrong" - *The Week* - 22/03/2018 "The plight of black men" - Prison policy initiative (fin 2017) - Fin 2017 aux Etats-Unis, combien de détenus ?

[37] *20 Minutes+Afp* - 20/03/2018 "Le nombre de détenus continue d'augmenter en Europe, les prisons sont presque pleines" - *Reuters* - 20/03/2018 "Le nombre de détenus repart à la hausse en Europe".

[38] *Le Figaro* - 22/04/2018 "Places de prisons : des ouvertures au compte-gouttes".

[39] *Le Figaro* - 22/04/2018 "La surpopulation carcérale atteint des records dans les maisons d'arrêt" - *Le Parisien+Afp* - 19/04/2018 "70 367 prisonniers en France, nouveau record" - *Le Parisien* - 28/03/2018 "Surpopulation, sécurité, droits fondamentaux : situation critique dans les prisons" - *Le Monde* - 7/03/2018 "Prisons : la France est bien l'un des mauvais élèves de l'Europe".

[40] *Libération* - 26/02/2018 "Morano a-t-elle raison quand elle annonce que 15 000 détenus en France sont étrangers ?" - Le Figaro - 16/02/2018 "Plus d'un détenu sur cinq en France est de nationalité étrangère".