## L’accès aux données issues des communications par les services d’État pour la sécurité publique

**418. L‘actuelle menace terroriste nécessite un travail commun entre les principaux acteurs du numérique.** Les services de l’État et les entreprises du web possèdent les indispensables moyens pour limiter la monstruosité du terrorisme issue de la découverte d’internet. L’arsenal législatif contre le terrorisme semble aujourd’hui être complet, néanmoins il paraît manquer un devoir ou une obligation de vigilance et de coopération de la part des grandes entreprises qui permettent les communications avec internet. Une obligation de vigilance et de coopération de la part des grandes entreprises du net et une coopération avec les autorités publiques pourrait participer à la prévention et à un meilleur fonctionnement de la lutte contre la menace terroriste. La morale et le droit ne doivent pas être opposés à l’utilisation de tout type de mise en commun des outils numériques à la disposition. De plus, l’instauration d’un devoir de vigilance permettrait de responsabiliser les entreprises. Il s’agit d’instaurer un engagement en faveur de la moralisation des entreprises afin de permettre d’éviter d’éventuelles nouvelles tragédies humaines liées par exemple au terrorisme. Une loi instaurant une obligation de vigilance et de coopération entre les acteurs du numérique serait notamment justifiée par l’intérêt général et la protection de l’ordre public. L'engagement du secteur privé pour le contrôle des communications numériques (**Section 1**) doit être accompagné par une correcte information transmise par les médias journalistiques qui doivent s’interdire de faire l’éloge du terrorisme (**Section 2**).

### Section I : La justification de l'engagement du secteur privé pour le contrôle des communications numériques

**419. Des collaborations nécessaires entre le secteur public et le secteur privé.** Dans la lutte contre le terrorisme l’utilité qui peut naître de la technologie numérique ne doit pas être écartée ou trop retardée dans le temps à cause d’hésitations. Le rôle que doit lui attribuer l’État est désormais capital. De nombreux États lancent aujourd’hui des appels pour la mise en place de collaborations entre le secteur public et le secteur privé. Ces appels à la collaboration mettent en exergue le besoin des services de renseignement de combattre

l'ennemi par le numérique sous toutes ses formes et laissent ouverte la nécessité d'une refonte structurelle générale des moyens de contrôle. Le sujet est multisectoriel, il englobe individus et structures du monde entier, et les questions liées à la morale sont rapidement raccordées par des questions techniques.

**420. « L'État espion » possède aujourd'hui les moyens techniques pour exister dans les communications sur internet, mais ils ne semblent pas être suffisants.** Les « politiques de surveillance » essayent de faire endosser une part de la responsabilité et du travail aux sociétés commerciales privées du Web. Il faudra attendre pour savoir si les sociétés du Web accepteront cette responsabilité. Une des possibilités pour elles, sera de mettre en place, mais de ne pas dévoiler ces pratiques de surveillance des communications privées. Le risque sera alors d'être surveillés sans une réelle reconnaissance explicite et information préalable. L'objectif étant pour les géants du Web, comme les GAFAM de garder une image de sociétés dédiées uniquement à la communication et non à l'espionnage... À l'ère du numérique il est nécessaire d'augmenter la lutte contre l'utilisation d'internet comme un moyen de communication pour les terroristes (§ **1**) et améliorer l'utilisation et l'encadrement juridique des données issues des communications numériques afin de préserver la sécurité (§ **2**).

## § 1. L'objectif de lutte contre l'utilisation d'internet comme moyen de communication pour les terroristes

**421. Les réseaux sociaux et les applications cryptées[745] sont les nouveaux moyens de communication pour les réseaux terroristes et ils constituent des vecteurs propagandistes.** Internet est aujourd'hui un des premiers lieux de recrutement des réseaux terroristes. Les jeunes sont les utilisateurs principaux de ces médias numériques et ils peuvent être une cible dans les processus de radicalisation. Il faut instaurer une meilleure coopération entre les acteurs du numérique : il s'agit de travailler ensemble dans la lutte contre le terrorisme. La rencontre entre le gouvernement américain et certaines entreprises de la Silicon Valley, telles Facebook, Apple, Twitter, Microsoft, Google en janvier 2016 a été l'étape nécessaire dans cette ébauche de collaboration. Au cours de cette rencontre ont

[745] L'application *Telegram* permet de communiquer sans que personne, ni même les gestionnaires de l'application, puissent lire les communications. *Telegram* utilise un système de cryptage des communications.

été traités des sujets tels l'accès aux *datas* privées par les services de renseignement, les requêtes de dénonciation de comportements « dangereux » identifiés sur les médias sociaux, les questions sur la censure, le cryptage… C'est le nouveau rôle des géants d'internet qui s'esquisse peu à peu, à mi-chemin entre « gendarmes 2.0 » et garants de la liberté d'expression et de communication sur internet.

**422. Le monopole des recherches sur le site internet Google pose des questions sur sa dangerosité.** Aujourd'hui on a tendance à estimer que le moteur de recherche Google pourrait suffire à permettre la liberté d'expression et de communication des opinions. Néanmoins, le moteur de recherche Google peut aussi être dangereux. En effet, on ne devrait pas oublier le passé et l'histoire de nos droits et libertés actuels. On assiste actuellement à une monopolisation concernant les recherches d'informations sur internet par la société américaine Google et sa société « mère » Alphabet. Ces sociétés décident de façon arbitraire ce qui peut faire l'objet de recherches sur internet. Pourtant la libre concurrence existe sur internet mais l'emprise de certains sites est devenue tellement forte qu'il n'est quasiment plus possible pour de nouveaux concurrents de concurrencer le géant Google. Cependant les positions adoptées par des pays tels que la Chine et la Russie sont à bannir, en effet certaines des grandes sociétés américaines sur internet sont censurées. Dans ces États, des web-sites uniquement nationaux souvent copiés de l'étranger dominent le marché, comme en Russie, le réseau social vkontakte.ru

**423. Plusieurs infractions sont à signaler.** Comme le précise Emmanuelle Borner-Kaudel : « il apparaît en réalité que le contentieux résultant de l'utilisation des mots-clés sur internet sans que les propriétaires de ces derniers n'en aient été informés sont fréquents ». Toutefois, il convient de se demander si le prestataire de services, en l'occurrence le moteur de recherche Google, opère par cette technique une communication de type commerciale qui lui est propre. Le juge européen estime que le fait de mettre à disposition des internautes des signes et des identifiants ne signifie pas que le prestataire de service soit rémunéré pour mettre en service les mots-clés[746]. Ainsi que le note l'avocat général, le moteur de recherche doit être neutre au regard des informations qu'il délivre, et les résultats qu'il livre permettent de satisfaire non pas les intérêts de Google mais ceux des internautes. Enfin, le prestataire

[746] CJUE - 23 mars 2010, *Google France et Google Inc c. Louis Vuitton Malletier*, n° C-236/08.

d'un service de référencement sur internet ne peut, selon le juge européen, être tenu responsable des données « qu'il a stocké à la demande d'un annonceur à moins que, ayant pris connaissance du caractère illicite de ces données ou activités de cet annonceur, il n'ait pas promptement retiré ou rendu inaccessibles lesdites données. Ainsi, s'il est bien question en l'espèce de communication électronique, il reste à déterminer si elle présente un caractère sérieux, et éventuellement commercial et quel en est le bénéficiaire »[747]. Les internautes peuvent recevoir des informations de nature commerciale, mais également tout ce qui regarde l'intérêt général[748]. Des motifs légitimes, notamment sécuritaires, justifient l'essor de la coopération entre les acteurs du numérique (**A**). Dans cette perspective de sécurisation publique, les États sollicitent des comportements actifs de la part des entreprises du Web (**B**).

## A – L'incitation à la coopération entre acteurs du numérique

**424. Des mesures visant à inciter à la coopération entre acteurs du numérique.** Dans la lutte contre le terrorisme, les acteurs de la technologie numérique ont un important rôle dans internet et pour la protection de la sécurité publique. Les géants, notamment américains, du web peuvent être sollicités pour accepter de coopérer avec les institutions publiques. Les géants du web sont pour la majorité basés aux États-Unis d'Amérique et le Président Barack Obama avait publiquement manifesté la nécessité de coopérer avec les « géants du Web » à la suite des attentats meurtriers de 2015 à Paris et à San Bernardino[749]. Les protagonistes majeurs du numérique ont multiplié leurs rencontres pour discuter des questions de sécurité publique liées au Web : notamment les gouvernements, les services de renseignement, et les entreprises de la Silicon Valley. L'attentat commis à San Bernardino par un couple djihadiste a mis en lumière le rôle des réseaux sociaux dans les communications et les divers préparatifs précédant les attaques meurtrières. Plusieurs communications numériques douteuses avaient été retrouvées *a posteriori* : ces communications auraient dû permettre la détection de la planification de l'attaque. La découverte de la possible utilisation de l'application cryptée *Telegram* par des personnes radicalisées a également été vivement contestée car cette

[747] *Ibidem*.

[748] BORNER-KAYDEL (E.), *La liberté d'expression commerciale*, Aix en Provence, thèse Université Aix-Marseille, 2014, 482 p.

[749] Los Angeles.

application rend impossible toute surveillance étatique, notamment à cause du fait qu'elle permet de crypter les communications. Ces exemples démontrent le fait que les risques sécuritaires liés aux NTIC engagent désormais de façon décisive les entreprises du web, les rendant éventuellement en partie responsables ou complices en cas de non coopération. Cependant cette situation est en friction avec le droit à la vie privée et le secret des correspondances car elle conduirait le « transporteur de la communication » à surveiller massivement et à fouiller les communications privées.

**425. Le Gouvernement américain en particulier, exige désormais que les *social networks* identifient et signalent les « comportements et communications à risque » en matière de terrorisme**. Néanmoins aucun critère n'a été précisé concernant la définition des « attitudes à tendance terroriste », dès lors des opposants ou militants politiques pourraient être englobés dans cette formule. Selon les entreprises du web ce genre de pratiques conduirait à un recul des droits d'expression sur internet et leur paraît être une obligation de surveillance de masse. Dans cette logique de partage des compétences en matière de contrôle des communications pour des raisons sécuritaires, les autorités attendent également des réseaux sociaux l'effacement des contenus de propagande terroriste. Dès lors la même interrogation de légitimité et de compétence de ces entreprises est alors posée relativement au cadre juridique qui permet la suppression de ces contenus. Il existent plusieurs interrogations des internautes et des sociétés du web face à l'intention de leur faire incomber une sorte « d'obligation de surveillance massive et de jugement » sur les communications des internautes sur un sujet si sensible, par des critères volontairement indiscrets et indéfinis. De plus, pour des apprentis, il n'est pas évident de parvenir à jauger efficacement la radicalisation. Néanmoins on observe qu'il s'agit d'un rapport de force nécessaire pour la prévention et pour obtenir des meilleurs résultats sécuritaires. Dans cette même hypothèse, aujourd'hui la coopération entre les différents États européens est d'autant plus nécessaire car les auteurs des attentats ne connaissent pas de frontières. Ainsi on devrait coordonner nos forces pour essayer de prévenir, de déjouer les attentats, et d'arrêter leurs auteurs.

## B – Des risques liés aux nouveaux vecteurs des communications

**426. Les risques des communications ludiques.** Dans la lutte contre la menace terroriste, les techniques utilisées par les terroristes pour échapper à toute surveillance peuvent parfois être surprenantes. En effet, on sait que les terroristes et les criminels sont prêts à utiliser tous

les moyens possibles pour arriver à leurs fins. Par exemple des communications suspectes ayant comme objectif la préparation d'un attentat avaient même été trouvées dans les chats dédiées aux jeux en ligne utilisées par les joueurs utilisant la plateforme numérique de Play Station. Dans ce contexte généralisé toute mesure innovante peut apporter des avancées dans la protection de la sécurité. La solution adoptée par *Apple* prend alors tout son sens. La société Apple a décidé de supprimer l'*emoji* pistolet de ses icônes de messagerie sur la version iOS 10[750]. *Emoji* est le terme japonais qui désigne les émoticônes utilisés dans les messages électroniques. L'envoi d'*emojis* relatifs aux armes pose des problèmes auprès des autorités qui ont des grandes difficultés à interpréter et à différencier cette nouvelle forme de langage. *Apple* lutte à sa manière contre le terrorisme, et a décidé de procéder au remplacement du dessein du pistolet noir par un pistolet vert à eau. Ce faisant la société *Apple* applique l'engagement pris auprès du *consortium Unicode*. En effet, en 2015 *Apple* avait effectué des communiqués concernant son opposition à l'ajout de nouveaux *emojis* en lien avec la violence et les armes. Conjointement à *Microsoft, Apple* avait même pris position contre la création d'un *emoji* fusil, souhaité par *Unicode* pour l'événement des Jeux olympiques d'été de Rio en 2016 et notamment l'épreuve de tir[751]. Avec la prise de position liée à l'*emoji* fusil, ces entreprises prouvent qu'elles réalisent l'importance de ces nouvelles communications et démontrent leur volonté de participer ou du moins de donner une image positive et active dans cette lutte. Il faut continuer dans cette voie car certains réseaux sociaux et les claviers numériques des smartphones ont encore des *emoji* suggérant la violence, comme une bombe, une épée ou une baïonnette.

**427. Une nouvelle façon d'expression qui permet une large gamme d'interprétations.** Chaque *emoji* a plusieurs significations ou interprétations possibles. Avec sa prise de position, *Apple* prend part au débat sur la dangerosité des armes à feu. Il s'agit d'un débat ravivé après les attentats et dont s'emparent les associations anti-armes. La suppression de l'*emoji* pistolet des appareils est un geste symbolique pour limiter l'accès aux armes à feu qui permet aussi d'interpeler les citoyens et les politiques. Si la majorité des nouveaux *emoji* ont été reçus favorablement, notamment ceux en faveur de la féminisation des sports et du travail ou de l'hétérogénéité dans les familles, la mutation de l'*emoji* pistolet en pistolet à eau peut

[750] Il s'agit du système d'exploitation mobile développé par *Apple* pour ses appareils.

[751] Unicode est le groupement d'entreprises qui a comme mission de standardiser les *emojis* sur les réseaux sociaux, les smartphones et les services Web.

paraître surprenant. Les citoyens-internautes, n'ont pas dans l'ensemble perçu les intérêts sécuritaires de ces actes et ne le perçoivent pas comme un changement forcément positif car ils estiment être privés de certaines innovations.

**428. Le vocabulaire utilisé peut avoir un objectif sociologique.** Des recherches ont mis en évidence l'effet de la langue pour transmettre une idéologie, il suffit de faire référence au livre *Lingua Tertii Imperii* de Victor Klemperer sur la langue du III[ème] Reich[752]. En effet, parfois la simple modification d'un mot ou d'une expression peut avoir comme conséquence des changements radicaux de comportement chez des individus[753]. La lecture de *Lingua Tertii Imperii*, à 70 ans de distance, reste toujours d'actualité car il montre combien le monde actuel a des difficultés pour guérir de cette langue « infectée », et qu'aucune langue n'est immunisée contre de nouvelles manipulations. Ce qui a fonctionné pour l'essor de la soumission, de violence et de haine dans l'Allemagne nazie pourrait fonctionner pour contrer certaines pratiques dans le monde des communications numériques du XXI[ème] siècle.

**429. L'internaute s'expose à de nombreux risques lorsqu'il utilise certains services internet.** Traditionnellement lorsqu'on évoquait la vie privée, on considérait qu'il s'agissait d'une sphère limitée. Aujourd'hui le développement des NTIC et des différents services du secteur numérique, tels les réseaux sociaux et les moteurs de recherche font que le citoyen-internaute peut se retrouver confronté à une absence de maîtrise de cette vie privée et à un déplacement de la sphère de l'intimité de la vie privée vers la vie publique. Les communications et agissements des internautes génèrent des données numériques qui ont une grande valeur pour les sociétés, et on assiste au risque pour les internautes d'assister à une fuite ou à une réutilisation de ces données personnelles sans leur approbation ou à des fins distinctes de ceux pour lesquels ils avaient initialement donné leur accord. Cependant ces données personnelles peuvent avoir un intérêt pour la protection de la sécurité. Les nouveaux moyens de communication par le numérique impliquent, dans de nombreux cas, la transmission des données personnelles à un tiers. Le règlement européen sur la protection

---

[752] Le philosophe Victor Klemperer a étudié la langue et les mots employés par les nazis. En utilisant une multitude de sources (discours radiodiffusés d'Adolf Hitler, livres et brochures, conversations, etc.), il a pu examiner la destruction de l'esprit et de la culture allemands par la *novlangue* nazie. En 1947, il écrit *LTI, Lingua Tertii Imperii.*

[753] CADOT (J.), « Apple remplace l'*emoji* pistolet par un pistolet à eau : victoire ou aveuglement ? », numerama.com, 02 août 2016.

des données personnelles (RGPD) entré en vigueur le 24 mai 2018 permet d'harmoniser les droits nationaux et d'accentuer la protection des données personnelles dans l'Union européenne[754].

## § 2. L'amélioration de l'utilisation et de l'encadrement juridique des Big data pour garantir la sécurité

**430. Pour réussir notre rôle dans l'époque numérique il faut vaincre aujourd'hui le challenge du *big data*.** Il semble nécessaire d'approfondir les apports du *big data* avec l'Administration, les entreprises et les citoyens, spécialement dans la prévention et la résolution des problèmes de sécurité et dans la lutte contre la criminalité et le terrorisme. Au cœur de ces réflexions, de nombreuses questions juridiques semblent à peine posées. Elles sont pourtant au centre des enjeux puisqu'il est difficile d'imaginer le développement des *Big data* sans monétarisation et sans encadrement juridique. La richesse des analyses réside essentiellement dans le rapprochement des données entre elles. Les perspectives de traitement des *Big data* sont énormes et ouvrent des grandes possibilités en termes de traitement de ces données. Il est très important de comprendre le potentiel des analyses notamment prédictives des *Big data*. Le volume des données stockées est en pleine expansion. Twitter générait en janvier 2013 la quantité de 7 téraoctets chaque jour et Facebook 10 téraoctets[755]. Chaque jour les internautes génèrent 3 trillions d'octets de données et 90% des data ont été créées au cours des trois dernières années. Le *Big data* est un concept opaque qui permet d'espérer de régler un grand nombre de problèmes par les données. L'inquiétude n'est pas tant de comment obtenir les *data* mais de comprendre si on a la possibilité de produire du sens à partir d'elles. Ce n'est pas uniquement l'analyse des données qui pose des problèmes, c'est aussi la façon dont elle est appliquée et par qui. Apprendre à manipuler les données n'est pas facile. Les *datas analysts* sont par exemple capables de prédire avec précision si une personne risque d'être hospitalisée en fonction de

[754] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).
[755] DEPRIS (D.) *Big Brother est parmi nous : surveillance électronique et informatique, terrorisme, guerre, Big Data*, Paris, Éd. Tatamis, 2015, 412 p.

ce qu'il recherche en ligne. Un autre exemple est la prédiction concernant les attaques aux personnes ou aux biens. L'important n'est pas tant la qualité des prédictions, mais de savoir comment les rendre utiles pour des intérêts individuels et collectifs.

**431. À l'ère du numérique, les données, les informations, sont le pouvoir.** Les informations issues des *Big data* sont parfois utilisées pour affirmer le pouvoir de certains sur d'autres[756]. Cela ne devrait pas être ainsi. Si on veut que les citoyens les moins privilégiés soient informés et responsabilisés, ils doivent avoir accès à la même qualité et quantité d'informations et de communications que les privilégiés. On est confrontés à un nouveau défi : On entre dans un monde de prédiction, où de plus en plus de personnes vont pouvoir porter des jugements sur les autres sur la base de données. De nombreux militants pour les droits de l'homme « combattent » afin de réguler ce nouvel écosystème de la prédiction. Le plus souvent ces outils sont conçus pour être utiles, pour accroître l'efficacité, ou pour identifier les personnes qui ont besoin d'aide. On est face au déploiement d'une « technologie d'espoirs ». Pour rendre notre société plus sûre on doit prêter une grande attention aux différentes NTIC numériques qui émergent et apprendre à poser et à trouver des réponses aux questions sur la façon dont ils devraient être mis en service pour améliorer la vie des personnes. Comment utiliser de la meilleure façon les *datas* tout en évitant la violation du droit au respect de la vie privée par l'État ? Dans cette perspective, on étudiera les moyens technologiques pour l'optimisation de l'utilisation des *datas* afin de préserver la sécurité nationale (**A**) et successivement la conciliation des droits individuels avec les *data* (**B**).

## A – L'optimisation de l'utilisation des datas afin de préserver la sécurité nationale

**432. Le *software Smarter Data***. Une grande innovation en matière de sécurité nationale avec l'utilisation du numérique, a été le *software Smarter Data*[757], cette base de données de sécurité publique est l'outil de commandement et d'information de la Gendarmerie nationale française pour la conduite des opérations et le traitement du renseignement opérationnel. Le

[756] RAVAZ (B.), RETTERER (S.), *Droit de l'information et de la communication*, Paris, Édition Ellipses, 2006, p. 174.

[757] Le logiciel Smarter Data a été conçu par la société française Thales.

système *Smarter Data* transmet en temps instantané aux gendarmes les informations nécessaires à l'exécution des missions. *Smarter Data* est une *data base* dotée d'un moteur de recherche alimenté par les gendarmes et un outil d'analyse[758]. Le système est conçu pour que les analystes de la gendarmerie traitent les renseignements collectés dans la perspective d'anticiper les troubles à l'ordre public. Le *Big data* permet l'exploitation des données issues de la dématérialisation de nos vies et de notre société, de l'utilisation d'internet, des réseaux sociaux, des applications…

**433. Dans le cadre de la supervision pour des motifs sécuritaires, les *Big data* peuvent être très avantageux.** Les États disposent de riches bases de données, véritables mines d'informations qu'ils doivent réussir à exploiter afin de fournir des services publics plus en phase avec les attentes des citoyens, et de mieux répondre aux interrogations des acteurs politiques. Pour cela, les institutions publiques doivent former leurs propres experts en *data mining.* Le traitement informatique des *datas* personnelles aura pour vocation, dans le futur, de multiplier les potentialités de l'analyse prospective et prédictive. L'un des grands enjeux des *Big data* porte sur la logistique de l'information, et notamment sur comment assurer que l'information adéquate, notamment en matière de sécurité, arrive au bon moment et au bon endroit[759]. On retrouve dans un « cycle de *Big data* », une donnée se transforme en information, cette information permet de prendre une décision et à la suite de cette décision il est possible d'effectuer une action. Une des nouveautés du *Big data* réside dans l'hétérogénéité des sources et des formats des données[760].

**434. Les *Big data* peuvent révéler beaucoup d'informations pertinentes à la société, notamment concernant la santé et la sécurité[761].** Des applications de ces données peuvent par exemple être la lutte contre des problèmes sociétaux comme la pédophilie, ou encore contre le terrorisme. Le programme américain de surveillance gouvernementale *Prism* a

---

[758] CASTETS-RENARD (C.), *Droit d'internet : droit français et européen*, Paris, Lextenso éd., 2014, p. 486.

[759] DEPRIS (D.) *Big Brother est parmi nous : surveillance électronique et informatique, terrorisme, guerre, Big Data*, Paris, Éd. Tatamis, 2015 p. 412.

[760] *Cf.* Les formes structurées et non structurées des données. *in* HAMEL (M-P), MARGUERIT (D.), « Analyse des Big data : Quels usages, quels défis ? », Paris, Commissariat général à la stratégie et à la prospective, 11/2013, n°8.

[761] ROUVROY (A.), *Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives*, Strasbourg, Conseil de l'Europe, janv. 2016, 53 p. https://pure.unamur.be/ws/portalfiles/portal/13278298/T_PD_BUR_2015_09REV_Rapport_Big_Data_COE_final_Fr.pdf

permis, à travers l'analyse des données, d'anticiper plusieurs tentatives d'attentats. Néanmoins ses détracteurs dénoncent une atteinte généralisée à la vie privée. Les défenseurs de la vie privée sont préoccupés de cette intrusion dans les communications[762]. Selon eux cette ingérence n'est pas justifiée, car les informations réellement cruciales dans la lutte anti-terrorisme peuvent être récupérées par d'autres moyens qui n'enfreignent pas la protection des données personnelles. Dans l'analyse comportementale liée à la mise en place des *Big data*, l'individu est en prédiction de comportement. La justice prédictive est un vrai défi pour les démocraties, une vraie interrogation de légitimité pour les promoteurs des *Big data*[763]. Dans le cadre de la sécurité nationale, pour identifier une personne tous les moyens auxquels l'analyste peut avoir accès doivent être pris en compte et analysés. De nombreuses *data* peuvent permettre cette identification comme par exemple l'utilisation d'un numéro de téléphone, des données de géolocalisation ou une adresse IP[764], et surtout lorsqu'elles sont combinées à d'autres données. Cependant lorsqu'on combine les données et notamment lorsqu'on met en place des corrélations, il y a un risque de violation de la vie privée, dès lors ces pratiques nécessitent d'être strictement encadrées. On assiste à l'évolution dans l'utilisation des *Big data* (**1**) notamment à des fins prédictives en matière de sécurité (**2**).

### 1) L'évolution dans l'utilisation des Big data

**435.** Jusqu'à récemment les *Big data* étaient utilisés majoritairement à des fins commerciales avec par exemple les publicités ciblées utilisées par les sites de vente en ligne, tel que *Amazon*, *Cdiscount, etc.*[765]. Cependant, l'utilisation des *Big data* à des fins uniquement commerciales serait une perte en bénéfices qu'ils peuvent apporter à notre société. Il n'existe pas de différence fondamentale entre l'analyse des données dans le monde commercial et dans le domaine de la sécurité publique. Par exemple la criminologie peut

---

[762] DEBET (A.), « Le programme Prism », Paris, *Recueil Dalloz*, 2013, p. 1736.

[763] FOREST (D.), *E-réputation, le droit applicable à la réputation en ligne*, Paris, Gualino éditeur, Paris, 2014, p.60.

[764] CJUE, question préjudicielle, 19 octobre 2016, aff. C-582/14, *Patrick Breyer c/ Bundesrepublik Deutschland.* Appelée pour la première fois à se prononcer sur le statut de l'adresse IP, la Cour de justice de l'Union européenne estime que la qualification des données à caractère personnel n'a pas à être retenue en toutes circonstances, mais qu'elle doit résulter de l'analyse de critères objectifs comme l'existence de moyens légaux pour accéder aux informations supplémentaires permettant l'identification ou encore la difficulté à accéder auxdites informations. METALLINOS (N.), « Statut de l'adresse IP », Paris, *Comm. Com. Électr.*, décembre 2016, pp. 38-40.

[765] GREFFE (P.), GREFFE (F.), *La publicité et la loi*, Paris, LexisNexis, Litec, 10ème édition, 2004, 1230 p.

bénéficier des grands apports des *Big data*. Un crime commis est considéré comme un signal, celui-ci génère une information, tel le taux de criminalité, ce qui va générer une action, comme l'envoi de plus de patrouilles de police sur un lieu géographique donné. Dans beaucoup d'États, notamment aux États-Unis d'Amérique et dans l'Union européenne on se pose la question de savoir si certains attentats terroristes auraient pu être déjoués avec une meilleure surveillance et utilisation prédictive des données des *Big data*. Notamment après les attentats au marathon de Boston et les attentats à Paris.

**436. Augmenter la sécurité intérieure en utilisant tous les moyens possibles pour lutter contre le terrorisme est une des priorités majeures liées à l'ère du numérique.** Autrefois il était nécessaire de connaître par exemple les livres consultés par certaines personnes afin de pouvoir suspecter ou retrouver ceux qui voulaient porter atteinte à l'État ou pour prévenir leur comportement criminel. Aujourd'hui il est possible de faire ceci en analysant les « clicks », par exemple lors de la consultation de vidéos de propagande terroriste djihadiste. Comme tout citoyen-internaute[766], les terroristes laissent des traces numériques avec beaucoup d'informations, notamment lors de l'utilisation des smartphones, des mails, des cartes de crédit, l'achat de billets d'avions, et l'achat de matériels pour communiquer ou pour créer des armes. Selon les experts, avec des logiciels de *data analytics* ces informations peuvent être très utiles pour lutter contre le terrorisme[767]. La transmission des données par les sociétés des télécommunications, tels que les mails ou les appels téléphoniques peut aider les enquêteurs à prédire certains actes criminels ou terroristes. Le développement des *data analytics* pour analyser et filtrer les énormes quantités de données qui inondent les bases de données peuvent être utiles pour prévenir des menaces terroristes et la cyber criminalité. Les institutions étatiques doivent continuer à mettre en pratique et à utiliser ce nouveau concept de sécurité[768]. Le *data analytics* est un moyen révolutionnaire pour traquer les personnes qui pourraient porter atteinte à la sécurité de la société. Le *data*

[766] L'internaute moyen disposerait d'une quinzaine de comptes sur des services en ligne. Nul n'y échappe aujourd'hui et on est conduits à renseigner à chaque fois un formulaire d'inscription contenant des informations personnelles. Outre ces éléments déclarés explicitement, on laisse des traces de façon plus ou moins consciente qui relève des données personnelles, la trace de nos achats, de nos navigations, de notre endroit de localisation lors de l'envoi d'un courriel, des dates et heures auxquelles on a mis à jour un document.

[767] LEROY (J.), *Droit pénal général*, Paris, LGDJ, 2016, pp. 434-436.

[768] ONU, Conférence internationale des points focaux de la lutte antiterroriste sur les situations propices à la propagation du terrorisme et sur la promotion de la coopération régionale, 13 – 14 juin 2013, Genève, Suisse.

*analytics* permet d'effectuer un tri parmi les milliards d'informations anodines échangées à travers les réseaux sociaux sur internet. L'important étant l'optimisation de l'information issue des *Big data*.

### 2) L'approche prédictive à des fins sécuritaires

**437. Le concept de gouvernementalité algorithmique.** Selon Antoinette Rouvroy, on assiste à l'essor d'une « gouvernementalité algorithmique » composée en trois temps : la récolte de quantité massive de données avec la constitution de *datawarehouses*, suivie par le traitement de ces données afin de produire des connaissances et *in fine* l'action sur les comportements, notamment par l'approche prédictive[769]. L'approche prédictive, même si elle n'est pas encore généralisée, peut devenir très utile pour la police ou l'armée dans le domaine de la sécurité. Avec les *Big data* prédictifs, les États-Unis expérimentent de nouvelles méthodes de lutte contre la criminalité, notamment avec l'utilisation de *PredPol*[770]. *PredPol* est un *software* conçu aux États-Unis qui utilise les bases de données des infractions pénales, les données démographiques et d'autres types d'informations afin de prédire la date et le lieu où les prochains crimes et délits ont la plus forte probabilité de se produire[771].

**438. Ainsi, les autorités peuvent anticiper et se préparer à intervenir dans ces zones géographiques, à un instant donné.** Les premières expérimentations du logiciel *PredPol* ont été réalisés en 2011 par la police californienne. Le système recense les données des infractions passées et les utilise grâce à un algorithme pour prédire l'avenir. Avec *PredPol* des améliorations ont été observées dans les services qui l'utilisent. Par exemple lorsque la police de Los Angeles a utilisé le *software* les infractions ont alors baissé dans les cinq mois qui ont suivi le déploiement du software. Dans les autres États américains qui n'ont pas utilisé cette technologie, les infractions en sont restées au même niveau ou ont augmenté[772].

---

[769] ROUVROY (A.), Thomas BERNS (T.), « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », La Découverte | Réseaux 2013/1 - n° 177 pages 163 à 196 ISSN 0751-7971, en ligne sur http://www.cairn.info/revue-reseaux-2013-1-page-163.htm

[770] Pour « Predictive policing ».

[771] En langue française « logiciel ».

[772] BENSOUSSAN (A.), *Informatique et libertés*, Paris, Éd. Francis Lefebvre, 2012, pp. 754-757.

Par conséquent les *Big data* ouvrent une nouvelle ère pour les professionnels de la sécurité et de la défense. Dans ce contexte le *big data* tout comme le *cloud*, sont des techniques qui permettent de rapprocher les données, ce qui permet de comprendre que derrière les *big data* il ne faut pas uniquement voir la collecte massive d'informations. Au-delà de ce constat, les outils permettant de stocker et de manier d'importantes quantités de données sont aussi utiles pour les enquêtes judiciaires. Auparavant, à partir des données d'une enquête, il était possible extraire des informations[773] mais c'était très précis, donc assez limité. Actuellement on peut par exemple imaginer intégrer un témoignage d'une personne à une enquête en cours et s'en servir pour la résolution d'une autre enquête. Les données sont plus exhaustives, l'accès et la combinaison de ces informations est beaucoup plus rapide. Les *Big data* permettent de croiser les informations avec d'autres sources, comme l'*open data*[774]. Il est possible de rouvrir d'anciennes enquêtes criminelles et utiliser ces nouvelles technologies pour les résoudre ou les rapprocher entre elles. Le développement des technologies d'information et de communication, en multipliant les moyens de captation des informations et des *datas*, a accentué la possibilité de contrôle des personnes[775]. Conscients de ces avantages liés au numérique et aux *Big data* il faut aussi parvenir à concilier les droits individuels avec l'utilisation de ces données.

## B – La conciliation du régime des droits individuels et des datas

**439. Les normes constitutionnelles françaises ne contiennent aucune disposition visant la protection des données personnelles ou encadrant la gouvernementalité numérique.** Comme le soulignent Antoinette Rouvroy et Thomas Berns, cette nouvelle gouvernementalité numérique a des risques car elle conduit à des prises de décision automatique ou semi-automatique, anticipant les comportements, les goûts et les choix de chacun, grâce au *data mining* et aux techniques de profilage qui permettent d'individualiser les offres de services sans se préoccuper des intentions ni recueillir les préférences des

[773] Par exemple : le lieu, la personne, la date, l'âge, le type d'événement.

[774] EYNARD (J.), *Les données personnelles*, Paris, Éd. Michalon, 2013, p. 344.

[775] BRASSEUR (C.), *Enjeux et usages du big data. Technologies, méthodes et mises en œuvre,* Paris, Lavoisier, 2013, 202 p.

personnes concernées[776]. Par conséquent si les *Big data* offrent des avantages à la fois sociétaux et économiques, il pose parmi tant d'autres, des questions en termes de protection de la vie privée et des données personnelles des citoyens[777] notamment lorsqu'il est manipulé par les institutions étatiques (1), il est alors nécessaire de maintenir et protéger le principe de finalité de la collecte des données notamment par la création d'un Commissariat aux données personnelles (2).

### 1) La manipulation des données par l'État

**440.** Dans l'évolution de l'utilisation des *Big data* pour la sécurité nationale, les nouveaux spécialistes des masses de données doivent avoir des profils polyvalents et surtout bien connaître les législations et les jurisprudences nationales et internationales. En effet, certaines dispositions législatives peuvent entrer en friction avec l'utilisation de ces nouvelles données. Il s'agit notamment de normes relatives au droit de la vie privée. Il faut en particulier anticiper la création de logiciels et applications illégales, des nullités procédurales et éviter des futurs procès ou condamnations contre l'État. Le principe de légalité doit régir les données à caractère personnel (**a**) et de plus il faut imposer au niveau national et international le respect du droit à l'oubli (**b**).

#### a. Le principe de légalité régissant les données à caractère personnel

**441.** Le cadre normatif applicable en France et en Europe à la collecte et aux usages des données personnelles a été pensé à une époque où les réseaux numériques n'étaient ni utilisés ni appréhendés par les individus de la même manière qu'aujourd'hui. Il est particulièrement frappant de constater que les normes constitutionnelles qui protègent les droits et libertés fondamentaux des individus ne mentionnent nulle part le droit de chacun au respect de sa

[776] Antoinette Rouvroy et Thomas Berns, *« Le nouveau pouvoir statistique »,* Multitudes *n° 40, pp. 88-103, 2010 ; CNIL,* Cahiers Innovation et prospective n° 1, *« La "dictature" des algorithmes : demain, tous calculés ? », pp. 18-20.*

[777] Les données personnelles à protéger sont principalement les données bancaires, les adresses mails, les mots de passe, les dates d'anniversaires, les prénoms, les noms… Ils risquent d'être revendus sur le dark web, afin de réaliser des bénéfices ou de simplement nuire.

vie privée et à la protection de ses données personnelles. Ces droits ne sont inscrits ni dans la Constitution du 4 octobre 1958, ni dans son préambule[778].

**442.** Le principe encadrant les données à caractère personnel est le principe de légalité, alors que pour les données qui ne sont pas des données identifiant les personnes c'est le principe de la liberté. Ce principe de légalité c'est surtout un principe issu du droit de l'Union européenne mais il commence à se généraliser dans les autres pays hors Union européenne. En matière de cyber criminalité internationale on trouve par exemple la Convention de Budapest de 2001[779]. On sait qu'avec internet la notion de limite géographique n'a plus de sens. En conséquence il faut réinventer des règles transnationales car la plupart des réglementations nationales sont limitées et parfois ils n'existent pas de réglementations liées à la gestion des droits relatifs au numérique.

**443. Le transfert des données n'est pas neutre.** Suivant effectivement le pays de l'origine de la donnée il y a des réglementations différentes et parfois il n'est pas possible de procéder à une exportation sans respecter des règles particulières, c'est le cas des flux transfrontaliers de données entre l'Union européenne et les autres pays[780]. Mais c'est aussi le cas de beaucoup de pays qui ont aujourd'hui des réglementations équivalentes à celle de l'Union européenne. C'est le cas par exemple des États-Unis dans le cadre du mécanisme *Safe harbor*, qui est un mécanisme d'adhésion où les sociétés américaines non seulement appliquent la loi locale américaine et s'engagent à respecter la réglementation de l'Union européenne[781]. Par ce biais l'exportation des données personnelles de l'Union européenne vers les États-Unis peut se faire avec un niveau minimum de garanties, c'est le cas notamment de Google, IBM, Yahoo, Amazon[782].

---

[778] Rapport « Numérique et libertés : un nouvel âge démocratique », Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l'âge du numérique, Assemblée Nationale, Paris, publié le 9 octobre 2015, http://www2.assemblee-nationale.fr/documents/notice/14/rapports/r3119/

[779] Convention de Budapest sur la cybercriminalité. Convention adoptée le 23 novembre 2001 par le Conseil de l'Europe, la convention sur la cybercriminalité, dite convention de Budapest, précise en 48 articles les résolutions prises au niveau européen pour un développement harmonieux des nouvelles technologies. Elle contient des dispositions visant à lutter de façon commune et conjuguée contre le crime dans le cyberespace.

[780] SUNIER (P.-A.), *Modèle conceptuel de données*, Paris, Broché, 2016, p. 55-57.

[781] EYNARD (J.), *Les données personnelles*, Paris, Éd. Michalon, 2013, p. 428.

[782] GREFFE (P.), GREFFE (F.), *La publicité et la loi*, Paris, Lexis Nexis, Litec, 10ème édition, 2004, 1230 p.

### b. Nul ne peut détenir des données à l'infini : le droit à l'oubli

**444. Des obligations de péremption.** Depuis l'entrée en vigueur du RGPD, l'entreprises qui constituent ces grandes bases de données ne peuvent plus ne pas prendre en considération le fait que les données à caractère personnel sont soumises à des obligations de péremption. Nul ne peut détenir des données à l'infini ou au-delà d'une certaine période[783]. Le droit à l'effacement, souvent intitulé droit à l'oubli numérique[784], est consacré dans plusieurs hypothèses, notamment : le retrait du consentement, l'opposition au traitement, un traitement illicite (RGDP, art. 17). Ce droit est aussi ouvert aux personnes qui étaient mineures au moment de la collecte des données. Les entreprises privées ou publiques, sauf l'État dans ses activités régaliennes, ne peuvent gérer les données que dans un certain temps qui se trouve par nature limité. La conservation de la donnée est un élément précaire, dont le droit à l'oubli en est le principe. Théoriquement la collecte des données ne doit pas excéder le temps nécessaire à l'atteinte des objectifs pour lesquels elles sont collectées. Passé ce délai, prévaut le « droit à l'oubli » ou l'obligation de destruction des données[785]. Se pose la question du droit à l'oubli des données utilisées pour la sécurité nationale. C'est un droit numérique fondamental que l'on retrouve dans la plupart des pays du monde à travers la notion de prescription ou la notion d'amnistie.

**445. Chaque internaute doit pouvoir gérer son passé[786].** Le droit à l'oubli permet d'éviter d'avoir les informations de sa vie antérieure comme un casier privé pour sa vie dans le futur. C'est un droit fondamental qui n'est pas facile à combiner avec le droit à l'histoire et le droit à la liberté d'expression. Le Tribunal de grande instance de Paris avait été saisi en référé, du refus opposé par Google à une demande de déréférencement d'un lien. L'affaire est intéressante car, peu de juridictions se sont, pour le moment, prononcées sur les critères à prendre en compte pour apprécier les demandes de déréférencement. De plus, en ordonnant

---

[783] SUNIER (P.-A.), *Modèle conceptuel de données*, Paris, Broché, 2016, p. 122.

[784] AUGER (A.), « L'Union européenne et le droit à l'oubli sur Internet », *RDP*, 2016, p. 1841. *in* OBERDORFF (H.), « La République numérique : un nouvel espace pour de nouveaux droits ?», Paris, *RDP*, 2018, p. 665.

[785] Conseil d'État, Le Numérique et les droits fondamentaux, Étude annuelle, Paris, 2014.

[786] Le droit à l'oubli permet de ne pas avoir son passé comme son présent et futur.

le déréférencement au sujet d'un lien dirigeant vers un contenu accusant une personne d'agressions sexuelles à l'égard de mineurs, le TGI rejette les arguments de Google fondés non seulement sur la liberté d'expression, mais aussi sur la qualification de « lanceur d'alerte » de l'éditeur de ce contenu. En effet, le plaignant n'avait pas été condamné dans ladite affaire sexuelle avec mineur, et le tribunal a donc privilégié la sauvegarde de la réputation[787].

**446. Mettre un droit de péremption sur chacune des données, c'est permettre à chacun de retrouver de la liberté par rapport à son passé.** Souvent dans les *Big data* les données ne sont pas soumises à péremption, et elles sont actualisées en temps réel, notamment par des systèmes de ramassage de données dans les réseaux sociaux. La plupart des personnes qui conçoivent des *Big data* cherchent d'abord à augmenter le nombre d'informations, ensuite à les utiliser avec les technologies de rapprochement et occultent la protection des droits fondamentaux. Cette façon de faire est totalement étrangère aux cadres juridiques, et est très souvent motivée par le fait que les entreprises commerciales qui mettent en place des *Big data*, ne savent pas à l'avance ce qu'ils vont pouvoir trouver et donc ne peuvent pas se limiter à l'avance dans la donnée. C'est le fait d'avoir des données non formatées ou très peu formatées qui leur permettra de créer une valeur informationnelle distincte de celle qu'ils pouvaient anticiper[788].

**447. Le droit à l'oubli à la lumière de la décision de la Cour de justice de l'Union Européenne du 13 mai 2014[789].** Cette décision est une décision fondamentale concernant les données personnelles car elle consacre le droit pour chacun d'entre nous d'être l'archiviste de son passé. Le droit à l'oubli c'est le fait de ne pas avoir son passé minant son futur. Le droit à l'oubli est essentiel pour que chaque citoyen puisse vivre normalement. Il est nécessaire de combiner le droit à l'oubli avec le droit à la liberté d'expression et le devoir de mémoire. Il faut préciser ce qu'on veut exprimer ici, en effet lorsqu'on nomme la liberté d'expression, il s'agit plus d'un *right to know,* d'un droit de savoir, d'un droit à l'histoire,

[787] TGI Paris, ord. Réf., 13 mai 2016, *M. X/ Google France et Google Inc. In* « DEBET (A.), Mise en œuvre de l'arrêt *Google Spain* par les tribunaux français », Paris, *Comm. Com. Électr.*, septembre 2016, pp. 36-38.

[788] BENSOUSSAN (A.), *Informatique et libertés*, Paris, Éd. Francis Lefebvre, 2012, 1096 p.

[789] CJUE - 13 mai 2014, *Google Spain c. Agencia Española de Protección de Datos, n° C-131/12.*

du droit de garder cette information pour les générations futures. En rapport avec les dangers de l'oubli, le Prix Nobel de la Paix Elie Weisel a écrit :

> « Le bourreau tue toujours deux fois, la seconde fois par l'oubli »[790].

### 2) Le principe de finalité de la collecte des données

**448. Comment concilier les libertés individuelles et les *Big data* ?** Une des solutions est l'anonymisation. Leur utilisation semble poser moins de problèmes relatifs à la *privacy* avec une anonymisation qui suppose de détruire le lien entre l'information et l'identité[791]. *A contrario* l'anonymisation des données est pour d'évidentes raisons, inutile aux objectifs de sécurité nationale. Étudier le droit applicable aux *Big data*, revient à étudier le droit à la manipulation des données qui permettent de déduire des informations implicites. Ce qu'on cherche à faire avec un *Big data* c'est trouver de la valeur informationnelle qui à la lecture directe de chacune des informations n'est pas apparente mais qui dans la combinaison de ces informations, permettra de faire apparaitre des comportements ou des attitudes qui pourront devenir prédictives. Un des premiers principes que l'on retrouve dans les cadres relatifs aux données personnelles est le principe de finalité de la collecte[792]. Ce principe de finalité de la collecte à l'exploitation asservit l'entreprise à une utilisation conforme à ce qu'a voulu l'individu lorsqu'il a donné son accord. Ce principe de finalité va réduire les possibilités d'utilisation de la donnée. Il y a le risque que le gérant du *Big data*, qui dispose des données, les utilise d'une façon non conforme à la finalité initialement établie.

**449. Le droit est *infra* moral, *infra* éthique et *supra* économique.** Le droit n'a de sens pour exister que par les valeurs qu'il défend. Lorsque ces valeurs ne sont plus partagées par une population en général, le droit est abandonné ou combattu. De la même manière, ce n'est pas parce qu'il existe un marché, qu'il faut tout permettre, le droit intervient pour réguler les

---

[790] WEISEL (E.), *La nuit*, Les éditions de Minuit, Paris, 2007, p. 199.

[791] Avec le numérique les possibilités de croisement des données permettent de rapprocher des faits concernant une personne, qui donne un pouvoir certain à celui qui détient ces informations. Par exemple s'il s'agit d'un acteur économique dont les activités divergent de ceux du citoyen concerné, ce sont de nombreux de ses droits fondamentaux qui peuvent être remis en cause. DENIZEAU (C.) *Droit des libertés fondamentales*, Paris, Vuibert 2de édition, 2012, 324 p.

[792] Article 226-21 du Code pénal.

marchés surtout lorsque ceux-ci peuvent avoir des comportements contraires à l'ordre public ou aux bonnes mœurs. Aujourd'hui on dispose d'un grand nombre d'informations qui permettent de suivre et de tracer une personne en mode instantané. Il doit y avoir un équilibre d'intérêts entre les droits du promoteur du *Big data* d'utiliser ces données et la nécessaire protection de l'individu et de ses libertés fondamentales. Cet équilibre doit être impérativement recherché dans une société démocratique[793].Les droits des personnes sur les *data* sont des droits individuels qui leur permettent de continuer à suivre les données et de comprendre leur utilisation. Le droit de questionnement est un droit par lequel l'individu peut poser une question afin de savoir si un organisme privé ou public, possède ou non des informations nominatives le concernant. L'individu possède un droit d'accès, un droit de modification, un droit de rectification, un droit d'opposition et un droit d'information. Ainsi une entreprise qui crée un *Big data* doit organiser la possibilité pour l'individu de vérifier l'ensemble de ses données. Ces informations constituent des éléments de prédiction de ses comportements. Cette prédiction est aujourd'hui soumise à la loi « Informatique et liberté » susmentionnée. Les frictions seront toujours plus importantes concernant la confrontation États-Unis d'Amérique permettant la libre utilisation des *datas*, y compris nominatifs, et la tradition européenne qui est la limitation de l'utilisation des données personnelles. Il faut développer une stratégie multidisciplinaire pour apporter de nouvelles réponses aux dérives qui risquent de naître avec une large utilisation des *datas*. Selon Pauline Türk il ne faut pas faire preuve de naïveté ou feindre d'ignorer les risques de dérives dans l'utilisation des outils numériques. Ceux-ci peuvent aussi constituer des menaces pour les droits et libertés des citoyens : les conditions de collecte, de tri, de traitement, stockage, revente et exploitation de la masse des données personnelles des utilisateurs[794]. Il est nécessaire de renforcer la sécurité juridique et la coopération avec les géants du Web. *Big data* et droit est une confrontation entre deux régimes juridiques, les États-Unis d'Amérique et l'Europe. Les *datas* aux États-Unis sont laissées dans un cadre de « laisser faire », l'objectif est de développer cette technologie et toutes les utilisations possibles liées aux données et notamment les données personnelles.

[793] MENDEL (T.), *Étude mondiale sur le respect de la vie privée sur l'internet et la liberté d'expression*, Collection Unesco sur la liberté de l'internet, 2013, p. 178.

[794] TÜRK (P.), « La citoyenneté à l'ère du numérique », Paris, *RDP*, 2018, p.623.

**450. La création d'un Commissariat aux données.** Une solution permettant de répondre aux nombreuses questions liées aux données personnelles serait la création d'un « Commissariat aux données ». La France a exporté les droits fondamentaux de l'homme et aujourd'hui elle exporte les droits fondamentaux de l'homme numériques avec la loi Informatique, fichiers et libertés et la loi "pour une République numérique" du 7 octobre 2016. Reste que si chacun d'entre nous dispose d'un droit de questionnement, un droit d'accès, un droit de modification, un droit de rectification, un droit à l'oubli, etc. il faut encore savoir et réussir comment avoir accès à ces droits. Comment savoir que le *data base* situé à l'étranger respecte bien l'ensemble de ces obligations ou si telle entreprise américaine respecte le *Safe Harbor* malgré sa signature et donc sa participation à une convention sur les flux transfrontaliers.

**451. Un Commissariat aux données personnelles pourra rendre effective l'existence et la protection des droits fondamentaux numériques.** La nécessité d'un tiers garant apparaît aujourd'hui (un peu) à l'image du Commissaire aux comptes qui est le garant non pas de l'entreprise, mais pour le public par rapport à l'entreprise[795]. Le Commissaire aux comptes lorsqu'il intercepte des éléments susceptibles d'infractions a une obligation de communication au Ministère public. De la même manière, avec la création d'un Commissariat aux données personnelles, on pourrait savoir si les données à caractère nominatif de chaque individu se trouvant dans un *Big data* le sont en conformité au droit des personnes. Cependant concernant les données utilisées par les forces de l'ordre, elles devraient rester difficilement accessibles.

## Section II : La médiatisation des informations liées au terrorisme

**452. Le terrorisme contemporain est médiatique.** Les journalistes ont une obligation d'information sur tout événement majeur, le côté dramatique et spectaculaire du terrorisme fascine une grande partie du public. Les terroristes actuels utilisent cette dynamique et effectuent des actes pour attirer le plus possible l'attention du monde. Le terrorisme ne doit pas affaiblir l'importance de la liberté d'information dans les médias numériques en tant

[795] Notamment les fournisseurs, les actionnaires, les salariés que cette entreprise utilise.

qu'une des bases absolues des sociétés démocratiques[796]. Cette liberté comprend le droit du public à être informé des questions d'intérêt général, et les réponses données par les autorités publiques. L'opposition au terrorisme ne doit pas être l'excuse ou la « carte blanche » pour l'État afin de limiter la liberté de la presse mais d'une part les journalistes doivent éviter de « servir les intérêts des terroristes » par exemple par des glorifications posthumes (**§ 1**). Et d'autre part dans la poursuite de la protection de la liberté d'information, le Conseil constitutionnel a censuré la disposition, trop ambiguë, instaurant un délit de consultation habituelle des sites terroristes (**§ 2**).

## § 1. Le risque de glorification posthume des terroristes par les médias

**453.** La stratégie d'information concernant la divulgation de certaines informations sensibles pourrait être unique, mais les différents canaux d'information ont des conduites diverses. Une disposition législative obligeant l'anonymisation des terroristes dans les médias serait la meilleure voie pour ne pas glorifier et rendre des martyrs certains terroristes. Ce débat agite ponctuellement les rédactions après les attentats terroristes. Une autre solution, peut-être utopique, serait l'instauration « d'un pacte entre les médias » pour ne plus donner l'identité, ni les choix de vie des terroristes. Les terroristes, notamment à la suite d'attentats suicides, devraient mourir dans l'oubli le plus total et de façon anonyme. Pour eux, l'espoir de mourir en martyr serait alors éloigné et peut-être ceci les ferait réfléchir avant de commettre l'irréparable. Cependant dans un univers journalistique où la liberté est souveraine, un tel « pacte » est inimaginable. Les médias prennent donc des positions individuelles et divergentes. Le traitement médiatique du terrorisme est d'une importance cruciale dans la lutte contre le terrorisme (**A**), et il est nécessaire de parvenir à un juste équilibre des informations transmises (**B**).

### A – Le traitement médiatique du terrorisme

**454. L'attentat de l'été 2016 à Nice a relancé le débat sur leur traitement médiatique.** Un débat qui, pour la première fois, a été porté par les rédactions journalistiques elles-

[796] AGOSTINELLI (X.), DEBBASCH (C.), BOYER (A.), CAPORAL, (S.), DROUT (G.), FERRAND (J.-P.), ISAR (H.), LASSALLE (J.-Y), MONDOU (C.), XAVIER (P.), VERGÉS (J.), *Droit des médias*, Paris, Éd. Dalloz Référence, 2002, pp. 500-501.

mêmes, donnant lieu à des prises de position éditoriales. Certains médias ont décidé de ne plus publier les photos avec les noms des auteurs des attentats[797]. Les rédactions *France Info* et *France Inter* se sont résolus à ne plus publier les images, le journal *Le Monde* a décidé de ne plus publier des photos ou vidéos qui pourraient avoir un effet de glorification posthume. La chaîne de télévision *BFM TV* a déclaré vouloir éviter une mise en avant involontaire et répétitive des attentats. *Europe 1* a décidé de ne plus diffuser les photos des terroristes sur leur site et ne pas citer les noms à l'antenne. *RFI* et *France 24* ont annoncé qu'ils ne diffuseront plus les photos et seront très attentifs à l'utilisation des noms des terroristes. La rédaction de *La Croix* a décidé de se limiter à publier le prénom et l'initial du nom et pas les photos.

**455. D'autres médias ont choisi le cas par cas.** Pour *Le Figaro,* la publication des identités relève du devoir d'information et celle des photos relève du cas par cas. Selon *Libération* : « publier les photos des terroristes et les glorifier, ce n'est pas la même chose ». Pour *France Télévisions* les décisions doivent se prendre au cas par cas et en toute responsabilité, tout en résistant à l'autocensure. *France télévisions* n'a pas été épargnée par les critiques à la suite de la diffusion d'un reportage qui a beaucoup choqué les téléspectateurs. Il s'agissait de l'interview d'un homme au côté du cadavre de sa femme dans l'édition spéciale du 14 juillet sur *France 2*. La direction de l'information a présenté ses excuses reconnaissant la transmission d'images brutales non vérifiées. Pour *TF1* « entre le matraquage d'un nom et d'une photo et un élément d'information, il faut choisir une voie médiane ». Ces positionnements éditoriaux ont suscité des vifs débats et des citoyens se sont emparés de la question, une pétition a été créé sur le site change.org pour demander aux médias la suppression de la divulgation de l'identité des terroristes. Des politiques se sont adressés au Conseil Supérieur de l'Audiovisuel en demandant l'élaboration d'un code de bonne conduite. La couverture des attentats a toujours suscité un débat dans les rédactions mais les journalistes doivent veiller à ne pas trop renoncer à informer le public en s'autocensurant.

[797] AUGRY (M.-L.), Médiatrice des rédactions de France 3, émission « Votre Télé et Vous », Paris, France Télévision.