Les nouveaux droits fondamentaux reconnus sur le terrain numérique

publié le **22/08/2015**, vu **3995 fois**, Auteur : Vincent Julien

L'émergence des nouveaux outils du numérique suscite un investissement toujours plus important des technologies dans notre vie quotidienne. A ce titre, de nouveaux droits ont logiquement pu être reconnus...

Création de nouveaux droits dans l'espace numérique :

Le développement de l'outil Internet a entraîné la reconnaissance de nouveaux droits fondamentaux : il s'agit du "droit d'accéder à Internet", ou du "droit à la protection des données personnelles" de l'utilisateur, lequel implique notamment le "droit à l'oubli" depuis l'année 2014 : à ce titre, le numérique constitue un vecteur de protection de la sécurité juridique des internautes à part entière.

Section I/ Le droit à la protection des données personnelles

Le droit à la protection des données personnelles a été reconnu pour la première fois en droit français par la loi "Informatique et Liberté" du 6 janvier 1978, laquelle reconnaît deux catégories de droits : la première recouvrant des droits à caractère subjectif (Sous-section I), la seconde renvoyant à des principes objectifs (Sous-section II).

§.1/ Première catégorie de droits :

Il s'agit d'une part du droit d'opposition disponible pour les personnes, et visant à ce que des données personnelles ne fassent pas l'objet d'un traitement, excepté lorsque le ce traitement répond à une obligation légale ou lorsque ce droit a été expressément écarté par l'acte autorisant le traitement.

Ce droit d'opposition s'exerce notamment au moment de la collecte d'information, ou au plus tard en s'adressant au responsable du fichier : c'est un droit personnel qui ne peut être étendu aux informations relatives à des tiers ou des membres de la famille de la personne concernée, excepté les cas de représentation de mineurs ou majeurs protégés. Lorsque ce droit joue pour la personne concernée, l'organisme contacté dispose d'un délai de deux mois pour répondre à la demande d'opposition : la réponse n'emporte pas mécaniquement l'accord de l'organisme, et celui-ci peut refuser d'accepter la demande d'opposition, pour peu que ce refus soit justifié par le responsable du traitement, sauf lorsque la demande est manifestement abusive.

En cas d'absence de réponse, emportant refus tacite, la personne peut saisir la CNIL et les tribunaux. Ce droit d'opposition n'existe cependant pas pour de nombreux fichiers du secteur public comme ceux des services fiscaux, des services de police, de justice ou de la sécurité sociale.

Il s'agit aussi du droit d'accès aux informations, tendant à déterminer si le traitement comporte des

informations personnelles, ce qui implique cas échéant le droit d'en obtenir communication :

La personne souhaitant exercer ce droit doit écrire au responsable de fichier pour lui demander de faire parvenir une copie, en langage clair, de l'ensemble des données concernant l'intéressé qui sont à sa disposition, et joint à cet égard une pièce d'identité avec mention des dates et lieux de naissance dans le but de prouver son identité au responsable du fichier. En l'absence de réponse formulée de manière satisfaisante dans un délai de deux mois suivant cette demande, l'intéressé peut alors porter plainte auprès de la CNIL.

Néanmoins, si un responsable de traitement estime que la demande est manifestement abusive, il peut là encore ne pas y donner suite : l'affaire est alors portée devant un juge et la preuve du caractère abusif de la demande sera à la charge du responsable du système de traitement.

Enfin, le droit de rectification implique que l'individu puisse exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées des informations le concernant, si celles-ci s'avèrent "inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite". L'intéressé devra effectuer les mêmes démarches que pour le droit d'accès aux informations, tandis que le responsable du système de traitement sera soumis aux mêmes obligations précédentes (respect d'un délai de deux mois suivant l'introduction de la demande.

Cependant, là encore ce droit comporte des limites et ne peut s'appliquer aux traitements littéraires, artistiques et journalistique : de plus, si les héritiers d'une personne décédée peuvent exiger du responsable d'un traitement de prendre en considération le décès et, ou de procéder aux mises à jour nécessaires, les fichiers de police, gendarmerie et renseignement excluent tout exercice du droit de rectification.

§.2/ Seconde catégorie de droits :

Les droits de seconde catégorie proclamés par la loi "Informatique et Libertés" revêtent un caractère plus objectif : ils visent moins à garantir la sécurité personnelle, qu'à proclamer le concept de "sécurité humaine" dans le cyberespace.

On retrouve ces droits aux premiers articles de la loi, qui posent et déterminent les lignes conductrices concernant l'utilisation de l'informatique face aux libertés. Ainsi, l'article 1er de la loi dispose que "l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne droit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques". Par la suite, les articles 2 et 3 vont préciser les champs d'application de la loi, notamment en précisant qu'elle s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans ces fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles.

Les définitions des données à caractère personnel, des traitements de ces données, ainsi que des fichiers comportant les données sont posées d'un côté, quand les acteurs du monde numérique, notamment les responsables de traitement de données ou le destinataire dudit traitement sont désignés en parallèle. Ces innovations en matière de ligne directrice, de politique de l'utilisation de l'informatique sont notamment nées du rapport Tricot, qualifiant de démission le fait de "s'en remettre entièrement à l'informatique pour apprécier des situations humaines".

Cependant, tandis que cette logique avait permis de proscrire en 1978 le profilage automatique, les dernières initiatives prises en matière de renseignement tendent à redessiner les contours des

politiques

contemporaines liées à l'usage de l'Internet : la sécurité policière menace alors de prendre progressivement le pas sur la « sécurité humaine ».

Section II/ Le droit d'accès à internet

L'accès à Internet revêt déjà de fondamental, la possibilité qu'il offre de garantir l'exercice de libertés fondamentales classiques comme la liberté d'entreprendre, la liberté d'association, ou de promouvoir un ensemble de droits fondamentaux : en ce sens, il implique non seulement la liberté d'accéder à Internet, mais encore le principe contemporain de" neutralité de l'Internet".

§.1/ La liberté d'accéder à Internet :

Le Conseil constitutionnel s'est prononcé sur le caractère fondamental de ce droit dans le cadre d'un recours formé contre la loi favorisant la diffusion et la protection de la création sur Internet qui confiait à la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (HADOPI) :

Cette autorité disposait du pouvoir de prononcer une sanction administrative de suspension de l'accès Internet à l'encontre d'une personne qui, ayant fait l'objet de deux avertissements préalables, omettait de veiller à ce que l'accès Internet ne soit pas utilisé pour diffuser, recevoir des contenus en méconnaissance des droits d'auteur. Le Conseil constitutionnel releva en l'espèce que cette sanction de suspension de l'accès Internet pouvait "conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile", tandis que seule "(…)l'autorité judiciaire est gardienne de la liberté individuelle" et que "nul ne peut être puni qu'en vertu d'une Loi établie et promulguée antérieurement au délit, et légalement appliquée". La condition formelle de légalité de la loi pénale, impliquant que la loi soit prise par le Parlement pour être considérée comme légalement appliquée, n'étant pas remplie en l'espèce, le Conseil constitutionnel déclarait inconstitutionnelle la mesure de suspension de l'accès Internet prise par HADOPI.

Plus précisément, dans cette décision du 10 juin 2009, le Conseil constitutionnel proclamait le caractère fondamental du droit d'accès à Internet en proclamant "qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et opinions, [la liberté de communication protégée par l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen] implique la liberté d'accéder à ces services".

Internet constitue donc un vecteur essentiel d'exercice de la liberté d'expression, et priver les citoyens de la possibilité d'accéder à ce service, restreignait mécaniquement la plénitude de l'exercice de cette liberté fondamentale : c'est à ce titre que l'accès à l'Internet constitue un droit fondamental, qu'il met à la charge de l'Etat l'obligation de ne pas couper l'accès au réseau.

§.2/ Le principe de neutralité d'Internet :

Le concept de "neutralité du net" est dégagé pour la première fois par le juriste américain Tim Wu :

Il s'agit de garantir que "le réseau public, pour qu'il puisse aspirer à être d'utilité maximale, traite tous les contenus, sites et plateformes de la même manière, ce qui lui permettrait de transporter toute forme d'information et d'accepter toutes les applications." Dans une logique d'optimisation du réseau, l'ensemble des informations doit pouvoir jouir de la garantie du meilleur effort fourni par

l'opérateur, sans garantie de résultat ni de discrimination, dans sa transmission d'un point à un autre. Il s'agit en fait de promouvoir la même liberté de circulation à toutes les informations, ce qui garantit non seulement l'optimisation du réseau Internet, mais encore la plénitude de l'exercice de la liberté d'expression.

Ce principe de "neutralité de l'Internet", progressivement reconnu en France, s'inscrit dans un processus de normalisation de recommandations, d'évolution du droit mou jusqu'au droit dur :

Au premier stade, l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) formule en 2010 dix recommandations, lesquelles visent à respecter la liberté d'envoyer et de recevoir le contenu, à utiliser les services ou faire fonctionner les applications, connecter le matériel et utiliser les programmes de son choix, dès lors qu'ils ne nuisent pas au réseau ou visent encore à respecter des critères de pertinence, proportionnalité, d'efficacité de non-discrimination dans les pratiques de gestion de trafic des opérateurs.

La normalisation de ces recommandations pourrait découler de la transposition de l'ensemble des réformes proposée au Parlement européen, connu sous le nom de "troisième paquet télécom" tandis que l'ordonnance du 24 août 2011, prise sur le fondement des directives européennes en matière de réseaux et services de communications électronique, ajoute à la liste fixée par l'article 32-1 du Code des postes et des communications électroniques, l'objectif de "veille à l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communications au public en ligne pour l'acheminement du trafic et l'accès à ces services".

Enfin, une proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques visant à faire de l'Europe un continent connecté reprenait les recommandations formulées par l'ARCEP en matière de "neutralité de l'Internet".

Cependant, reprenant la logique de la loi LOPPSI II visant à bloquer des sites à caractère pédopornographique, la loi du 13 novembre 2014 relative à la lutte contre le terrorisme prévoit dorénavant la possibilité pour l'autorité administrative de faire retirer les contenus de sites Internet provoquant directement à des actes de terrorisme ou faisant publiquement l'apologie de ces actes : le principe de « neutralité de l'Internet » est donc fortement tempéré, voire exclu par des impératifs sécuritaires qui, s'ils sont conjoncturels, engendrent des conséquences structurelles dans le cyberespace : la nécessité de contrôler la normalité de l'activité numérique prend alors nettement le pas sur l'objectif de protection des libertés personnelles.

Section III/ Le droit à l'oubli

Les dispositions de la directive européenne 95/46/CE impliquent que les internautes puissent demander, sous certaines conditions, la suppression des liens vers des informations portant atteinte à la vie privée : la Cour de Justice de l'Union Européenne reconnaît d'ailleurs le caractère fondamental de ce nouveau "droit à l'oubli".

§.1/ Les dispositions de la directive 95/46/CE :

Dès 1995, les Etats membres de l'Union Européenne prenaient une directive visant à protéger les libertés et droits fondamentaux des personnes physiques, notamment ceux ayant trait à leur privée au regard des traitements de données à caractère personnel. Cependant, ces droits personnels devaient être conciliés avec l'objectif de la libre circulation des données à caractère personnel entre Etats membres, de « meilleur effort » possible dans la circulation des données.

La directive précise surtout des notions importantes : la donnée à caractère personnel constitue

ainsi « toute information concernant une personne physique identifiée ou identifiable », quand le fichier de données à caractère personnel comprend « (..) tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminées » : ce dernier peut alors faire l'objet de toute opération ou ensemble d'opération à l'aide de procédés automatisés, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, ou encore le rapprochement ou l'interconnexion.

Le responsable du traitement s'entend quant à lui comme une personne physique ou morale, une autorité publique, un service ou tout organisme qui seul, ou avec d'autres, détermine les finalités et moyens du traitement de données à caractère personnel : à cet égard, les finalités et moyens sont déterminés par le droit national ou communautaire. L'article 4 prévoit en effet qu'il incombe aux Etats membres d'appliquer les dispositions nationales au regard de la directive lorsque traitement est effectué dans le cadres des activités d'un établissement du responsable du système de traitement, ou lorsque le responsable du traitement n'est pas établi sur le territoire de l'Etat membre ou sur le territoire de la Communauté. Parmi les règles prévues par la directive, les Etats membres sont tenus de garantir ainsi à toute personne concerné le droit d'obtenir dudit responsable de traitement la rectification, l'effacement ou le verrouillage des données en raison du caractère incomplet ou inexact des données.

Il ressort de l'ensemble de ces dispositions que la personne physique identifiée ou identifiable grâce aux données faisant l'objet du traitement, peut demander à l'établissement du responsable de traitement agissant sur le territoire de la Communauté, le retrait de données le concernant. Cependant, ces dernières devront avoir un caractère inexact et, ou incomplet.

§.2/ L'arrêt du 13 mai 2014 de la Cour de Justice de l'Union Européenne :

La Cour était saisie par la juridiction espagnole dans le cadre d'un litige opposant "Google" à l'autorité de protection des données personnelles :

L'autorité avait ordonné à la multinationale californienne de désindexer des données relatives à deux articles de presse évoquant les dettes passées et réglées par le plaignant, dans le but que celles-ci disparaissent des résultats de recherche fait sur le nom du plaignant.

La Cour rappela dans cette affaire que les exploitants de moteurs de recherche sont des responsables au sens de la directive, et qu'une conception large de la notion d'établissement doit être privilégiée : l'entreprise "Google", disposant d'une filiale en Espagne assurant la promotion et la vente des espaces publicitaires sur le moteur de recherche, relevait ainsi de cette catégorie, et constituait un établissement.

Par ailleurs, il s'agissait de rappeler que la personne pouvait s'adresser directement à un moteur de recherche pour obtenir la suppression des liens vers des pages Internet contenant des informations portant atteinte à sa vie privée, sans que ce droit ne soit pourtant absolu : le droit fondamental à la protection de la vie privée, notamment des données personnelles, devait ainsi être concilié avec l'intérêt économique du moteur de recherche. Dans ce souci de conciliation, la nature de l'information, sa sensibilité pour la vie privée de l'intéressé et l'intérêt que représente cette information pour le public à la recevoir, au regard notamment du rôle joué dans la vie publique par cette personne, devaient être interprétés de manière casuistique.

Or, dans le cas d'espèce, la Cour énonce qu' « eu égard à la sensibilité des informations contenues dans les annonces pour la vie privée de ladite personne et au fait que leur publication initiale avait été effectuée 16 ans auparavant, la personne concernée justifie d'un droit à ce que ces informations ne soient plus liées à son nom au moyen d'une telle liste. Dès lors, dans la mesure où il ne semble pas exister, en l'occurrence, de raisons particulières justifiant un intérêt

prépondérant du public à avoir (…) accès à ces informations (…) il appartient à la juridiction de renvoi de vérifier que la personne peut (…) exiger la suppression desdits liens de cette liste de résultats ».

La mutation des droits fondamentaux dans l'espace numérique :

Certains des droits fondamentaux traditionnels, transposés sur le terrain numérique, ont nécessairement connu une mutation importante : les évolutions ayant affecté la "liberté d'expression" ou la "liberté personnelle" en témoignent.

Section I/ La liberté d'expression

L'avènement d'Internet correspond au besoin contemporain de disposer d'une information toujours plus universelle, toujours plus rapide : à cet égard, le développement du numérique modifie substantiellement les régimes traditionnels de liberté d'expression, mais consacre parallèlement un régime commun applicable sur le terrain numérique.

§.1/ Des régimes juridiques traditionnels affectés :

La liberté d'expression était traditionnellement régie par des régimes juridiques distincts, et particulièrement adapté à chacun de ces usages :

La presse, diffusée sous la forme de journaux imprimés, était régie par la loi du 29 juillet 1881 quand la communication téléphonique assurée par les opérateurs de télécommunications était régie par le code des postes et télécommunications. Quant à la communication audiovisuelle assurée par câble ou satellite, le régime juridique applicable était fixé par la loi du 30 septembre 19861.

Ces trois libertés d'expression étaient notamment soumises à différents contrôles : la première était dispensée de "contrôle a priori", la seconde soumise au contrôle du secret des correspondances, quand la troisième était soumise au régime d'autorisation.

Avec l'avènement d'Internet, c'est la convergence de ces trois modèles de libertés d'expression qui est privilégiée : aujourd'hui, le réseau permet, sinon incite à la diffusion de ces trois modes d'expression sur une même plateforme. Face à ce phénomène de convergence, le législateur dût uniformiser les différents régimes jusqu'alors applicables.

La loi pour la confiance dans l'économie numérique du 21 juin 2004 a eu pour objet de transposer la directive « commerce électronique », et catégorise désormais les modes d'exercice de la liberté d'expression : on parle ainsi des « communications électroniques », lesquelles regroupent les « communications au public par voie électronique » et les communications ayant le caractère d'une correspondance privée. Les « communications au public par voie électronique » comprennent notamment la « communication au public en ligne », et la communication audiovisuelle .

Pour ce qui est des acteurs, la loi de transposition fixe encore deux grandes catégories : il s'agit des éditeurs de services sur Internet et des hébergeurs. Les premiers ne sont soumis à aucune obligation de déclaration préalable, ou d'autorisation, quand les limites à leur liberté d'expression sont fixées par la loi du 28 juillet 1881, et que leur droit de réponse est prévu par la loi sur la confiance dans l'économie numérique de 2004. Concernant les seconds, ils sont quant à eux responsables pénalement et civilement au même titre que les opérateurs téléphoniques, s'ils avaient connaissance de l'activité illicite ou, si après avoir été informés, ils n'ont pas agi promptement pour retirer le contenu ou le rendre inaccessible.

Enfin, une nouvelle catégorie juridique intermédiaire de « services de médias audiovisuels à la

demande » est apparue : elle regroupe les services de télévision de rattrapage et de vidéo à la demande, et soumet ces services à des obligations de diffusion d'œuvre européennes, de soutien à la production, de protection des mineurs.

§.2/ Un régime commun encadré :

La démocratisation de l'outil Internet appelle à des initiatives en matière de protection des droits qui trouvent à s'exercer sur le terrain numérique, quand la jouissance de ces droits reste cantonnée à la sphère d'exercice des droits et libertés fondamentaux d'autrui:

La liberté d'expression est ainsi tempérée par les nécessités de lutte contre les actes de provocation à la discrimination ou à la haine envers des personnes en raison de leur origine, de leur religion ou de leur orientation sexuelle, contre les actes de négation de crimes contre l'humanité, de diffamation, d'injure ou encore de révélation de l'identité d'agents des services de renseignement. Dans cette logique, les pouvoirs publics ont notamment pris certaines mesures propres à assurer la régulation de l'usage d'Internet :

la loi LOPPSI II ajoute ainsi à l'article 6 de la loi du 21 juin 2004 pour la Confiance dans l'Economie Numérique (LCEN) les dispositions suivant lesquelles, "lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal194 le justifient, l'autorité administrative notifie (…) les adresses électroniques des services de communication a public en ligne contrevenant aux dispositions de cet article auxquelles (…) doivent être empêcher l'accès sans délai".

Parallèlement, la LCEN prévoit l'obligation pour les fournisseurs d'accès à internet et les hébergeurs de mettre en place un dispositif de signalement des contenus illicites, sinon de retrait des contenus signalés, les service intéressés sont appelés à définir des mesures de police sur les contenus autorisés allant de l'interdiction des appels à la violence, la lutte contre la xénophobie, ou l'objectif de lutte pour la protection des mineurs. Cependant, afin de concilier le objectifs de sécurité en matière d'économie numérique avec le "principe de neutralité de l'Internet", et de circulation libre de l'information, les fournisseurs ne sont pas soumis à une obligation générale de surveillance, ou d'enquête sur les faits ou circonstances révélant ces activités illicites

Enfin, faisant écho à la loi LOPPSI II, mais justifiée cette fois par des nécessités de lutte contre la provocation à des actes terroristes, l'article 12 de la loi du 13 novembre 2014 prévoit désormais la possibilité de retirer les contenus des sites provocant ou faisant l'apologie du terrorisme : néanmoins, l'autorité administrative ne dispose plus de la seule faculté de notifier les adresses électroniques de ces services de communication, mais peut désormais de sa propre initiative, en l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, procéder d'office au retrait de ces contenus.

Section II/ La liberté personnelle

La liberté personnelle recouvre traditionnellement le droit à la vie privée, l'inviolabilité du domicile, la liberté d'aller et de venir... Si certains de ces droits et libertés fondamentaux sont aujourd'hui menacés sur le terrain numérique, de nouveaux moyens numériques à disposition des autorités de poursuite ont nécessairement été développés.

§.1/ L'émergence de nouvelles menaces liées au numérique

La Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité dresse un panorama des différentes menaces numériques pour les droits fondamentaux des internautes :

Cet instrument distingue les menaces numériques selon qu'elles entrent dans la catégorie des "infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes d'informations", dans celle des "infractions numériques", des "infractions se rapportant au contenu" ou dans les "infractions liées aux atteintes la propriété intellectuelle et aux droits connexes". Plus schématiquement, le Conseil d'Etat distingue dans son étude annuelle relative au "numérique et [aux] droits fondamentaux", les atteintes à la sécurité qui ont pour cible le numérique en visant à entraîner le dysfonctionnement d'un système informatique, et celles pour lesquelles le numérique est un moyen de commettre une infraction. Enfin, certaines infractions entrant dans le champ d'application des atteintes ayant pour cibles des atteintes à la sécurité sont spécifiques, car relevant d'atteintes spécifiques contre les intérêts fondamentaux de la Nation.

Cependant, on peut aujourd'hui dresser une autre typologie des menaces sur le terrain numérique : la première catégorie regrouperait l'ensemble des infractions commises sur le cyberespace, selon que le numérique constitue le moyen de commettre l'infraction ou la cible principale de l'infraction. La seconde catégorie regrouperait quant à elle les atteintes à caractère informationnel, selon qu'elles visent à diffuser ou propager des informations d'une part, qu'elles soient à fin publicitaire, personnelle, ou même terroriste ou selon qu'elles visent à recueillir des informations confidentielles cette fois. Là encore il s'agira autant d'informations personnelles, que commerciales, politiques ou même militaires.

Cette dernière typologie nous permettra notamment de confronter deux modèles de sécurité contemporaine par la suite : le premier relèverait du modèle policier hybride, à mi-chemin entre police politique privilégiant le renseignement intérieur, et sécurité militaire mettant l'accent sur les intérêts d'Etats dans un contexte de balance des puissances sur le terrain géopolitique, quand le second aurait trait cette fois au modèle de "sécurité humaine" qui privilégierait la protection des populations face à la défense des intérêts d’Etats, tendant progressivement à mettre l'Etat au service des individus, et non plus à contraindre les individus à être au service des Etats.

Or, si on compte autour de 35millions de victimes directes du fait des guerres interétatiques, pour 165 à 170millions de victimes massacrées par leurs propres Etats au XXème siècle, le phénomène conduirait à repenser la notion de souveraineté traditionnelle. Il s'agirait aujourd'hui de privilégier la souveraineté des individus sur la souveraineté des Etats, d'entendre non plus la souveraineté comme un droit classiquement absolu (droit de guerre, calcul froid des intérêts) mais comme un devoir, une "responsabilité de protéger" les populations à la charge de l'Etat.

§.2/ Le développement de nouveaux dispositifs à disposition des autorités de poursuite.

Le "Big Data" a conduit à renforcer l'efficacité des moyens d'action de la police, que celle-ci ait pour tâche de "constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs", ou qu'elle ait pour tâche de sauvegarder l'ordre public en prévenant les infractions. Le renseignement fera l'objet d'une plus approfondie par la suite.

Le numérique, quand il ne conduit pas à optimiser l'usage de modes traditionnels d'investigation, permet de développer de nouveaux modes opératoires inédits. Il ne sera cependant question que des modes d'investigation traditionnels ici:

Le numérique conduit notamment à optimiser l'usage des fichiers de police en permettant l'interconnexion des différentes informations utilisées et, ou conservées : le "Traitement d'Antécédents Judiciaires" (TAJ) a notamment permis de faire fusionner le "Système de Traitement des Infractions Constatées" (STIC) de la police nationale avec le "Système Judicaire de Documentation et d'Exploitation" (JUDEX) de la gendarmerie nationale, il regroupe aujourd'hui 12,2 millions de fiches sur des mis en cause et permet dorénavant de procéder à des enquêtes

administratives concernant le recrutement à des emplois présentant une sensibilité particulière depuis la loi du 18 mars 2003 sur la sécurité intérieure. Parallèlement, le Fichier des Personnes Recherchées (FPR) rassemble les informations relatives à l'ensemble des personnes recherchées ou disparues, dans le cadre de la police judiciaire ou de législations administratives spécifiques (législation applicable sur le droit des étrangers par exemple) : il regroupait quelques 400 000 fiches au 1er novembre 2010 selon les estimations de la CNIL.

La conservation et l'utilisation des données biométriques à des fins de comparaison a aussi été optimisée par l'utilisation des technologies liées au numériques : si le nombre d'intéressés par le Fichier National Automatisé des Empreintes Digitales (FNAED) regroupait environ 900 000 personnes en 1997, il avoisine en 2008 les 3millions de personnes quand le Fichier National Automatisé des Empreintes Génétiques (FNEG), s'il regroupait un ensemble de 2 635 personnes en 2002, concerne 806 356 personnes en 2008 avant d'atteindre à son tour les 2 millions de personnes en 2012.

Enfin, le procédé de classique de vidéosurveillance est aussi affecté, à tel point que l'on parle dorénavant de "vidéo-protection intelligente" : c'est que le nombre de ces "learning machines", capables de détecter des mouvements atypiques, de reconnaître un visage, ou de lire automatique des plaques d'immatriculation concernait déjà un ensemble de 70 000 caméras sur la voie publique en 2011. Un an plus tard, elles sont au nombre de 935 000 sur l'ensemble du territoire, tandis que la CNIL n'a opéré que 150 contrôles de cette activité, pour une vingtaine de sanctions prononcée.