Données personnelles et cybersurveillance

Me Cécile Doutriaux
Avocate et membre de la Chaire Cyberdéfense & Cybersécurité des écoles de Saint-Cyr Coëtquidan.

Décembre 2014 - Article III.17

Cet article a fait l'objet d'une première publication dans la RDN Décembre 2014 - n° 775.

Les nouvelles technologies décuplent les capacités de surveillance et les possibilités d'intrusion dans la vie des citoyens.[1] M. Edward Snowden, ancien employé de la CIA,[2] a rendu publiques en 2013[3] des informations secrètes de l'Agence Nationale de la Sécurité américaine[4] et révélé les programmes de surveillance Prism, XKeyscore, Boundless Informant et Bullrun du gouvernement américain ainsi que Tempora, Muscular et Optic Nerve du gouvernement britannique. Cet espionnage massif des données personnelles des citoyens, au niveau mondial, aurait été justifié par la lutte contre le terrorisme, notamment par le Patriot Act aux États-Unis. De nombreux pays, tels que l'Allemagne, la France, l'Espagne, le Brésil, se sont ouvertement indignés[5] des pratiques de la NSA au motif que ses agissements susciteraient un état de suspicion, préjudiciable aux bonnes relations de confiance entre les nations. Pourtant, la cybersurveillance des citoyens n'est pas une pratique nouvelle, dont les États-

[1] Éric Denécé « le contrôle et la coordination des activités de renseignement », janvier 2013.
[2] L'Agence Centrale du Renseignement américaine créée en 1947 a pour mission d'acquérir des renseignements clandestins pour assurer la sécurité du territoire national, selon les directives du Président des Etats-Unis ou du Directeur du Renseignement National.
[3] Notamment par l'intermédiaire du Washington Post le 9 Juin 2013 publié par Barton Gellman, Aaron Blake et Greg Miller et par le Guardian du 17 Juin 2013.
[4] La National Security Agency (NSA) est un organisme gouvernemental du département de la Défense des États-Unis, responsable du renseignement d'origine électromagnétique, de la sécurité des systèmes d'information et du traitement des données du gouvernement américain.
[5] L'Express 18 décembre 2013.

Unis auraient l'exclusivité car si les moyens de surveillance des « Five Eyes »[6] sont de grande ampleur, l'Union européenne n'est pas inactive et intercepte aussi les données personnelles.[7]

Cette réalité du cyberespionnage remet en question la confiance des citoyens accordée aux autorités gouvernementales, tenues de garantir le secret des correspondances électroniques et la protection des données personnelles, étant rappelé que selon la loi « l'informatique doit être au service de chaque citoyen et ne doit porter atteinte ni à la vie privée, ni aux libertés individuelles ou publiques ».[8]

I. La protection nationale et internationale des données personnelles et du secret des correspondances électroniques

Les sources de données se sont considérablement diversifiées et les données ne sont plus seulement collectées et stockées par les administrations et les entreprises mais sont également mises en ligne par les individus eux-mêmes. Cette réalité implique de protéger ces données personnelles et la protection instaurée par la loi varie selon le type de données (personnelles,[9] sensibles [10]et de connexion[11]).

Les données de connexion sont particulièrement visées par le cyberespionnage et à l'instar de l'adresse IP, elles sont assimilées à des données à caractère personnel et sont protégées au titre du respect à la vie privée[12] reconnu par l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'homme et des Libertés fondamentales.[13]

Plusieurs États,[14] ont élaboré des législations nationales protectrices des données personnelles, comme c'est le cas en France avec la loi informatique, fichiers et libertés du 6 janvier 1978. Ces lois nationales posent les principes fondamentaux de la protection des données, tels que la confidentialité et l'effacement des données à l'issue du délai fixé pour leur conservation. Les données personnelles sont également protégées au niveau européen. Ainsi, la Convention n°108 du Conseil de l'Europe de 1981[15] a pour objet de garantir, sur le territoire de chaque État, à toute personne physique, le respect à sa vie privée à l'égard du traitement automatisé des données à caractère personnel. L'article 5 de la directive 2002/58/CE dispose que l'internaute doit être informé de l'existence de toute collecte

[6] Alliance entre le Royaume-Uni, les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande en matière d'échange de renseignements.

[7] Voir Journal « Le monde » du 20 mars 2013 http://www.lemonde.fr/international/article/2014/03/20/les-services-secrets-britanniques-ont-acces-aux-donnees-des-clients-francais-d-orange_4386266_3210.html.

[8] Article 1er de la loi Informatique, fichiers et libertés de 1978.

[9] Sont les informations relatives à une personne physique, identifiée ou qui peut être identifiée, directement ou indirectement, par référence aux éléments qui lui sont propres, tels que les noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, empreinte digitale, ADN etc…elles peuvent être collectées et stockées, avec la possibilité d'un droit d'accès et de rectification par leurs titulaires.

[10] Les données personnelles sensibles font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses, relatives à la santé ou à la vie sexuelle et ne peuvent être collectées, sauf si la personne concernée a donné son consentement exprès.

[11] Les données de connexion, permettent l'identification du titulaire d'un abonnement, depuis un numéro de téléphone ou une adresse IP et peuvent être collectées dans des conditions strictement déterminées par la loi.

[12] En France, le respect du droit à la vie privée est garanti par l'article 9 du Code Civil.

[13] Article 8 « Toute personne a droit eu respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

[14] Notamment la Belgique, l'Islande, les Pays-Bas, l'Espagne et la Suisse avec par exemple, la loi fédérale suisse sur la protection des données du 19 juin 1992 http://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf consulté le 05/09/2014.

[15] Convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, élaborée sur la base de travaux réalisés par l'OCDE et quatre Etats membres non européens (Australie, Canada, Japon et Etats-Unis).

d'informations, qu'il a le droit d'en connaître la finalité et de s'y opposer.[16] Plus ancienne, la directive 95/46/CE[17] adopte quant à elle une approche réglementaire globale pour protéger les données personnelles des citoyens européens et assurer la libre circulation des données au sein de l'Union Européenne. Elle considère que toute collecte de données à caractère personnel doit être licite, loyale et non excessive au regard des finalités poursuivies.

Cette protection des données personnelles est complétée par le secret des correspondances électroniques, reconnu par de nombreux textes nationaux et internationaux tels que les articles 12 de la Déclaration universelle des droits de l'homme de 1948,[18] 8 de la Convention Européenne des Droits de l'Homme de 1950,[19] 17 du Pacte international relatif aux droits civils et politiques de 1966,[20] par l'article 37 de la Constitution de l'Union Internationale des télécommunications de 1992[21] mais également par la directive de l'Union Européenne sur le secteur des télécommunications de 2002 à l'article 5.[22] En France, le secret des correspondances est assuré par l'article L.241-1 du code la sécurité intérieure[23] et l'article 226-1 du Code Pénal protège la vie privée des citoyens.[24]

Malgré toutes ces dispositions, des quantités importantes de données personnelles de citoyens américains et européens sont collectées par les services de renseignements des États.

II. La cyber surveillance des données des citoyens par les États est-elle légale ?

La nécessité d'assurer la sécurité nationale permet aux États d'user de pouvoirs exceptionnels, pouvant limiter la protection dont bénéficient les citoyens. Ces mesures, dérogeant au principe de la protection des données personnelles et au secret des correspondances, sont-elles légales ?

[16] « Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données ».

[17] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L 281 du 23/11/1995 p. 0031 - 0050

[18]Article 12 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

[19] Article 8 de la CEDH : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

[20] Article 17 du Pacte international relatif aux droits civils et politique : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance…toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

[21] Article 37 de la Constitution de l'Union Internationale des télécommunications : « Les Etats Membres s'engagent à prendre toutes les mesures possibles, compatibles avec le système de télécommunication employé, en vue d'assurer le secret des correspondances internationales ».

[22] Article 5 : « Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée».

[23] Article L241-1 : « Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci ».

[24] Article 226-1 du Code pénal : « Est puni d'un an d'emprisonnement et de 45.000 € d'amende le fait, au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui ».

Il convient de distinguer les renseignements obtenus par des moyens ouverts et autorisés, c'est-à-dire par des inspections de sécurité et ceux obtenus par des moyens clandestins, c'est-à-dire par l'espionnage.

A. La collecte clandestine des données opérée par les États est-elle licite ?

Si l'espionnage en temps de guerre est autorisé et défini par l'article 29 du Règlement de La Haye de 1907,[25] il n'existe aucune définition de l'espionnage en temps de paix, et à ce jour, aucune convention internationale n'est venue règlementer les activités d'espionnage électronique entre les États, en dépit de leur augmentation massive.

Pour autant, un acte d'espionnage constitue-t-il une violation du droit international, pouvant engager la responsabilité des États ? En réalité, la responsabilité des États, à raison de l'activité de leurs services secrets, ne donne pas lieu à des développements juridiques abondants dans la mesure où ces affaires appellent un règlement discret, par voie de négociations directes ou diplomatiques et la sanction est d'autant plus inconcevable qu'il s'agit d'une pratique réciproque et habituelle entre les États. Ainsi, dans les affaires d'espionnage, les États poursuivent l'agent de renseignement devant les juridictions nationales, sans entreprendre d'actions répressives contre l'État commanditaire. Ainsi, en France, l'agent de renseignement peut être jugé devant les juridictions nationales, sur la base de l'article 702 du Code de Procédure Pénale[26]dès qu'il entretient des intelligences avec une puissance étrangère[27] et livre des données informatisées[28]dont la divulgation est de nature à porter atteinte aux intérêts fondamentaux de la nation.[29] Bien évidemment, les agents coupables de cyberespionnage peuvent être poursuivis pour intrusion dans les systèmes informatiques sur le fondement de l'article 323-1 du Code Pénal,[30] la peine étant aggravée lorsque l'atteinte est portée à l'encontre d'un système de traitement automatisé mis en œuvre par l'Etat.[31] Juger l'agent, c'est l'option choisie par les États-Unis le 19 mai

[25] Article 29 : « Ne peut être considéré comme espion que l'individu qui, agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la partie adverse.
Ainsi les militaires non déguisés qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, ne sont pas considérés comme espions ».

[26] En temps de paix, les crimes et délits contre les intérêts fondamentaux de la nation sont instruits et jugés par les juridictions de droit commun (Cour d'Assise, Tribunal Correctionnel) et selon les règles du code pénal, lorsque les faits poursuivis constituent un crime ou un délit prévu et réprimé par les articles 411-1 à 411-11 du code pénal.

[27]Article 411-5 Code Pénal : « Le fait d'entretenir des intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents, lorsqu'il est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de dix ans d'emprisonnement et de 150.000 euros d'amende ».

[28] Article 411-6 Code Pénal : « Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225.000 euros d'amende ».

[29] Article 410-1 Code Pénal : « Les intérêts fondamentaux de la nation s'entendent de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel ».

[30] Article 323-1 du Code Pénal : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende et les intrusions contre les systèmes informatiques de l'État sont punies plus sévèrement de cinq ans d'emprisonnement et à 75.000 € d'amende ».

[31] Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45.000 euros d'amende. Lorsque les infractions ont été commises à l'encontre d'un système de traitement automatisé de

2014 en décidant de poursuivre cinq militaires chinois accusés de cyberespionnage pour accès illicite aux ordinateurs et diffusion de virus informatique.[32]

Cela signifie-t-il qu'aucune sanction ne peut être prise contre l'État lui-même pour ses actes de cyberespionnage ? Un État est souverain sur son territoire ce qui l'autorise à préserver ses frontières de toute influence extérieure, mais ce qui le contraint aussi à respecter la souveraineté des autres États. Ainsi, l'espionnage engagerait la responsabilité des États, en cas de violation simultanée de l'intégrité territoriale, qui constitue un casus belli en vertu de l'article 2 de la Charte des Nations Unies.[33] Toutefois, en termes de territorialité, il est difficile de fixer avec précision les frontières du cyberespace et l'accès aux données ou aux systèmes informatiques se fait « à distance » par l'agent de renseignement, au moyen de logiciels espions par exemple, de sorte qu'il n'y a pas véritablement de violation de l'intégrité territoriale de l'État. Cette réalité rend en définitive purement hypothétique la répression du cyberespionnage pratiqué par les États en temps de paix et les déclarations publiques outragées des chefs d'État sur ce sujet visent d'avantage à circonscrire l'indignation des citoyens qu'à susciter une rupture des relations internationales.

B. La cybersurveillance autorisée par les interceptions de sécurité et la collecte des données de connexion

Si l'ingérence des États dans la vie privée des citoyens est possible, elle doit être fondée en fait [34] et prévue des lois accessibles, prévisibles et relativement détaillées, pour offrir des garanties aux personnes visées par le cybersurveillance dans les sociétés démocratiques. [35]

Pour se justifier, envers les citoyens, des accusations d'espionnage massif, les États-Unis ont déclaré avoir agi sur la base du Patriot Act, un ensemble de lois sécuritaires votées en réaction aux attentats du 11 Septembre 2001 et élaborées pour permettre aux services de renseignement américains d'accéder aux données stockées dans les serveurs des sociétés américaines, y compris en dehors des États-Unis. Pour faire face à la menace terroriste, des dispositions ont également été prises en Europe pour déroger au secret des correspondances électroniques en cas de menace grave, en réaction aux attentats terroristes de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005. En effet, l'Union européenne[36]autorise la collecte des données de connexion et la directive 2006/24/CE[37] impose aux opérateurs de téléphonie et aux fournisseurs d'accès à internet de conserver, pendant un délai compris entre six et vingt quatre mois, variable selon les législations nationales des pays,[38] toutes les données permettant d'identifier les internautes, de les localiser et de connaître la date et la durée de leurs communications.

---

données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75.000 € d'amende ».

[32] Daniel Ventre, Des militaires chinois recherchés par le FBI pour cyberespionnage économique, blog econflicts, http://econflicts.blogspot.fr/2014/05/des-militaires-chinois-recherches-par.html, 21 mai 2014.

[33] Article 2 de la Charte des Nations Unies : « Tous les États doivent s'abstenir de recourir à la menace ou à l'emploi de la force contre
l'intégrité territoriale ou l'indépendance politique de tout État.

[34] Cour Européenne des Droits de l'Homme, Janowiec et autres c. Russie [GC], nos 55508/07 et 29520/09, §§ 213-214, 21 octobre 2013.

[35] Rapport de la Division de la recherche de la Cour européenne des droits de l'homme, sécurité nationale et jurisprudence européenne 2013.

[36] L'Union européenne est une organisation régionale, fondée sur un traité qui gère la coopération économique et politique entre ses 28 États membres que sont l'Autriche, la Belgique, la Bulgarie, Chypre, la République tchèque, l'Estonie, le Danemark, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne, la Suède, le Royaume-Uni et la Croatie.

[37] Directive européenne 2006/24/CE relative à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

[38] La durée de conservation des données de connexion est d'une année pour la France et la Belgique, et d'un mois pour l'Allemagne.

En France, deux dispositifs distincts et complémentaires permettent d'exercer une surveillance sur les communications électroniques des citoyens. L'un fondé sur l'article L.241-2 du code de la sécurité intérieure,[39] l'autre fondé sur l'article L.34-1-1 du Code des Postes et des communications électroniques.[40]Les motifs avancés pour justifier cette surveillance des réseaux et des communications électroniques sont la sauvegarde de la sécurité nationale,[41] des intérêts fondamentaux de la nation et la lutte contre le terrorisme. A ce titre, les opérateurs de téléphonie et les fournisseurs d'accès à Internet sont tenus de conserver les données de connexion de leurs usagers pendant une année en France et de les mettre à la disposition des autorités, conformément à l'article 34-1 du Code des Postes et des Communications électroniques.[42] De plus, depuis la loi de programmation militaire n°2013-1168 du 18 décembre 2013 (LPM), l'article L. 246-1 du code de la sécurité intérieure[43] autorise le recueil des informations traitées ou conservées par les réseaux et des données de connexion relatives à l'identification des numéros d'abonnement, à la localisation des équipements utilisés, ainsi qu'aux communications d'un abonné. De fait, la loi de programmation militaire unirait en un seul et même régime les dispositions de la loi de 1991 relative aux interceptions de sécurité et celles de la loi antiterroriste de 2006 relative au recueil des données de connexion.

Ces mesures, qui apportent des restrictions au respect de la vie privée et à la protection des données personnelles, ont été prévues par l'article 8 alinéa 2 de la Convention Européenne de Sauvegarde des Droits de l'homme et des Libertés fondamentales qui mentionne la possible ingérence d'une autorité publique dans l'exercice du droit à la vie privée, si cette ingérence constitue une mesure nécessaire à la sécurité nationale. Il existe donc une limite au respect de la vie privée, anticipée par les textes, dans la mesure où l'intérêt collectif doit primer sur l'intérêt individuel, puisqu'il s'agit avant tout de préserver la cohésion de la société dans son ensemble. Par conséquent, la cybersurveillance des données des

[39] Article L.241-2 du Code de la sécurité intérieure : peuvent être autorisées, à titre exceptionnel, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme.
Article L.244-2 du code de la sécurité : le ministre de la défense ou le ministre de l'intérieur peuvent recueillir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires, pour la réalisation et l'exploitation des interceptions autorisées par la loi.

[40] Article L.34-1-1 du Code des Postes et des communications électroniques : Afin de prévenir les actes de terrorisme, les agents dûment habilités des services de police et de gendarmerie nationales peuvent exiger des opérateurs la communication des données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. L'application de cet article a été prorogée jusqu'au 31 décembre 2015.

[41] Article L1111-1 du Code de la Défense : « La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République.

[42] Article L34-1 (modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24) Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre la mise à disposition de l'autorité judiciaire ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense (OIP – 1er ministre) différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques.

[43]Article L. 246-1 du code de la sécurité intérieure : Pour les finalités énumérées à l'article L. 241-2, peut être autorisé le recueil des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. Cet article entra en vigueur le 1er janvier 2015.

citoyens, expressément prévue par les textes, aussi bien au niveau national, européen et international est parfaitement légale.

Si des règles exceptionnelles sont admises, ces dispositions accordent-elles pour autant tout pouvoir aux États ?

Si des considérations de sécurité nationale peuvent affecter les garanties offertes aux citoyens par les lois nationales et internationales, la nécessité de combattre la criminalité terroriste ne saurait justifier que l'on étende indéfiniment les interceptions de sécurité et des limites sont posées pour éviter les abus. En effet, il ne peut être porté atteinte au secret des correspondances électroniques que par l'autorité publique, à titre exceptionnel, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.[44]Le pouvoir de surveiller en secret les citoyens n'est tolérable si les moyens prévus par la législation restent acceptables dans une société démocratique. La Cour Européenne des Droits de l'Homme est venue préciser les limites posées à ces mesures exceptionnelles dans plusieurs arrêts. Ainsi, dans l'affaire Klass et autres c. Allemagne,[45] la CEDH précise que les États ne disposent pas d'une latitude illimitée pour assujettir les citoyens à des mesures de surveillance secrète, au nom de la lutte contre le terrorisme. Dans l'affaire Leander contre Suède,[46] la Cour a rappelé que l'ingérence de l'État dans la vie privée de ses citoyens doit être fondée sur un besoin social impérieux et proportionnée au but légitime recherché. Enfin, le pouvoir d'ordonner des mesures de surveillance secrète des citoyens n'est admissible que s'il est strictement nécessaire à la préservation des institutions démocratiques, ce qui signifie concrètement qu'il doit y avoir des garanties suffisantes et effectives contre les abus. Ainsi, il ne suffit pas de se prévaloir des lois pour justifier la surveillance massive des données des citoyens, il faut également pouvoir sanctionner tout usage abusif et un contrôle doit être assuré par des autorités administratives indépendantes ou judiciaires. En France, il existe deux autorités administratives indépendantes, la Commission Nationale de l'Informatique et des Libertés (CNIL) chargée de veiller au respect de la vie privée et des libertés dans le monde numérique et la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) chargée de vérifier la légalité des interceptions de sécurité et des données techniques de communications. Alors que la CNIL dispose d'un pouvoir de contrôle et de sanctions (notamment pécuniaires), la CNCIS est principalement tenue d'effectuer un contrôle a posteriori et d'adresser des recommandations aux ministres, sans bénéficier d'un véritable pouvoir de contrainte.

III. Les mesures de cybersurveillance sont-elles proportionnées et légitimes ou remettent-elles en question l'État de droit ?

Si la protection de la sécurité nationale est un but légitime pouvant entraîner des restrictions au respect de la vie privée, les mesures de cybersurveillance doivent être proportionnées par rapport aux finalités poursuivies. Or selon E. Snowden, « La majorité des gens dans les pays développés utilisent internet et les États en profitent secrètement pour étendre leurs pouvoirs, au-delà de ce qui est nécessaire et approprié ». En France, la Ligue de défense des droits de l'Homme et la Fédération internationale de défense des droits de l'Homme ont déposé plainte contre X le 11 juillet 2013, pour contester la légalité, au regard du droit français, du programme de cybersurveillance américain Prism. Selon ces associations, « cette intrusion sans contrôle dans la vie de chacun constitue un danger considérable pour les libertés individuelles, qui doit être enrayé sous peine de voir disparaître l'État de droit ».

[44] Selon l'article L.241-1 du Code sécurité intérieure.
[45] Affaire Klass et autres c. Allemagne (Requête n o 5029/71) arrêt du 6 septembre 1978.
[46] Affaire Leander c. Suède (Requête n o 9248/81) arrêt du 26 mars 1987.

Dans son arrêt « Digital Rights Ireland » rendu le 8 avril 2014,[47] la Cour de Justice de l'Union Européenne a invalidé la directive n° 2006/24/CE du 15 mars 2006, au motif que l'obligation générale de conservation des données de connexion constitue une ingérence grave et de vaste ampleur dans les droits fondamentaux au respect de la vie privée, en permettant de fournir des indications très précises sur les habitudes de la vie quotidienne, les activités exercées et les relations sociales des individus. De plus, selon la Cour, dès lors que la directive couvre les données de toute personne sans distinction et fixe la durée de conservation sans tenir compte de son utilité par rapport aux objectifs poursuivis, cette ingérence n'est pas proportionnée. Le G29 [48] a adopté le 10 avril 2014 un avis qui a souligné l'illégalité de la surveillance massive, systématique et sans distinction des citoyens européens.
Le 16 juillet 2014, le Haut-commissariat des Nations Unies aux droits de l'homme a publié un rapport sur la surveillance des citoyens par les moyens de communications numériques qui indique que la surveillance de masse des gouvernements instaure « une dangereuse habitude » qui remplace les mesures d'exception dans de nombreux pays, de sorte qu'il incombe aux États de démontrer que cette ingérence n'est ni arbitraire, ni illégale.

Dans la mesure où les organismes internationaux chargés de la protection des libertés des citoyens ont estimé à l'unanimité que l'exigence de proportionnalité n'avait pas été respectée par les États, peut-on parler d'une dérive sécuritaire ? Pour la principale association française des acteurs de l'Internet, qui rassemble notamment AOL, Dailymotion, Google, Deezer, PriceMinister, Facebook ou encore Yahoo, la collecte des données de connexion, autorisée par l'article 246-1 du Code de la sécurité intérieure, pose de « graves questions en termes de protection des droits et libertés individuelles ».

Certes, en France, l'article 226-1 du Code Pénal protège la vie privée des citoyens et il est vrai que tout citoyen dispose d'un recours auprès de la CNCIS au titre de l'article 243-9[49] du code de la sécurité intérieure. Effectivement, les réclamations écrites des citoyens réceptionnées par la CNCIS ont donné lieu à un contrôle systématique de la légalité des interceptions de sécurité[50] et « si la commission estime qu'une interception de sécurité est abusive, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue » qui est, dans la pratique, est le plus souvent suivie.[51]Cela étant, si certaines garanties sont concrètement données aux citoyens, les chiffres semblent corroborer la position des organisations internationales qui ont jugé disproportionnées ces mesures massives de surveillance. En effet, selon le rapport de la CNCIS 2012-2013, les interceptions de sécurité relative à la lutte contre le terrorisme n'ont représenté que 19% des demandes en 2012.[52]

La possibilité pour un État d'invoquer des considérations de sécurité nationale pour amoindrir les droits des citoyens est forcément préoccupante et on ne peut totalement écarter les risques d'abus.

[47] Arrêt Cour de Justice de l'Union Européenne du 8 avril 2014 Digital Rights Ireland Ltd Contre Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform,Commissioner of the Garda Síochána, Irlande.

[48] L'article 29 de la directive du 24 octobre 1995 sur la protection des données personnelles a institué un groupe de travail qui rassemble les représentants de chaque autorité indépendante de protection des données nationales et qui a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays hors UE. A ce jour, les 27 États membres ainsi que les pays de l'Espace Économique Européen (Islande, Liechtenstein, Norvège), disposent d'une loi « informatique et libertés » et d'une autorité de contrôle indépendante.

[49] Article L.243-9 du code de la sécurité intérieure : « De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du présent titre. Si la commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue ».

[50] En 2012, cinquante-deux particuliers ont saisi la CNCIS par écrit et la majorité de leur demande a été traitée, étant précisé que les simples appels téléphoniques ne donnent généralement pas lieu à des vérifications.

[51] Les recommandations adressées au Premier ministre en 2012 visant l'interruption de quatorze interceptions de sécurité ont toutes été suivies et les trente huit préconisations de la commission ont également toutes été suivies par les services titulaires de l'autorisation d'interception.

[52] 21ème Rapport d'activité de la CNCIS 2012-2013.

Toute personne qui fait l'objet d'une mesure de surveillance, basée sur des motifs de sécurité nationale, doit bénéficier de garanties contre l'arbitraire. Cela étant, le système de cybersurveillance pourrait trouver en lui-même sa propre limite puisque la captation des données en masse, qui consiste à tout intercepter au motif que cela pourrait toujours servir un jour, n'est pas véritablement efficace puisque seule l'analyse fine des données interceptées est utile.