Liberté et sécurité dans un monde anomique de données

Sébastien-Yves LAURENT,
Professeur des universités à la Faculté de droit et de science politique de l'université de Bordeaux, enseignant à Sciences-Po

Les rapports annuels successifs de la CNCIS – qui me fait le grand honneur de me donner la plume – attestent en continu et ce depuis plus de vingt ans, que le rapport entre libertés fondamentales et sécurité est un des enjeux les plus délicats à faire respecter dans l'État de droit. L'« ordre public » est un point de jonction classique entre ces deux paradigmes depuis le XIX^e^ siècle. Bien plus récentes, les « données » nées avec l'informatisation de la société dans les années 1970, se trouvent à la croisée de deux libertés, la liberté de correspondre et la protection de la vie privée, qui entrent quotidiennement en conflit avec l'impératif de sécurité dont l'État est le garant et l'ordonnateur. Depuis la loi de 1991, votée par le Parlement français pour éviter de nouvelles condamnations de son système d'écoutes gouvernementales par la CEDH, c'est la CNCIS qui a la charge de trouver le positionnement dans ce qui est souvent désigné comme étant un « équilibre » entre, d'une part, les motifs inscrits dans la loi et pour lesquels des « interceptions de sécurité » mais aussi des « données techniques » peuvent être demandées à la Commission et, d'autre part, la liberté de correspondre, socle fondamental tant de notre droit des libertés que du droit public. On relèvera que le terme d'« équilibre » entre sécurité et liberté, est employé couramment par abus de langage : il postule d'emblée une position où les deux « plateaux de la balance » seraient à la même hauteur. Or, la situation la plus courante est celle d'un non-équilibre… tendant vers un équilibre qu'il est impossible de définir, de jauger ou de mesurer, tout comme l'est le non-équilibre.... Il s'agit donc en fait d'une tension dialectique qui est au cœur de l'État de droit sur un plan juridique et de la démocratie libérale sur un plan politique. Quoi qu'il en soit, on constate que désormais ce sont les interceptions et les captations de données qui sont aujourd'hui – dans le monde entier – un point de cristallisation quotidien de la tension sécurité-libertés.

La CNCIS : des interceptions de correspondance aux méta-données

« Arbitre », « vigie »[1] ... bien des termes peuvent caractériser la Commission qui a la charge de se prononcer – *a priori* – sur les demandes d'écoutes administratives. De 1180 lignes écoutées en permanence en 1991, la CNCIS est passée à 1540 en 1997, 1670 en 2003, puis en 2008 à 1840 « cibles »[2], enfin à 2 190 en 2014 : d'évidence le nombre est modeste et les rapports détaillés de la CNCIS montrent chaque année que la lutte anti-terroriste en pré-judiciaire mobilise une grande partie de ces quotas. Dès sa fondation, la CNCIS avait eu à connaître des « données » car l'article 22 de la loi de 1991 l'autorisait à exercer un contrôle – *a posteriori* – sur les demandes de données techniques faites dans le cadre d'une demande d'interception de sécurité. Le périmètre de la CNCIS s'est élargi depuis : ainsi à compter de 2006, par l'article 6 de la loi n° 2006-64, elle a la charge de se prononcer (toujours *a posteriori*) – dans le cadre de la lutte antiterroriste – sur les demandes de données techniques de connexion ou de communication faites hors du contexte d'une demande d'interception. Ceci peut concerner les numéros de téléphone, les numéros d'abonnement à des services de communications électroniques, la (géo-) localisation des terminaux, enfin les « fadettes ». Le rôle de la CNCIS aurait pu être renforcé de façon considérable à la fin de l'année 2014 si la loi de programmation militaire[3] (LPM) lui avait attribué le contrôle des données techniques de connexion dans le cadre, élargi, de la loi de 1991. Mais l'article 20 de la LPM a confié cette charge à une « personnalité qualifiée » nommée par le Premier ministre (sur proposition de la CNCIS) pour procéder au contrôle des demandes de données techniques de connexion[4] par les autorités exécutives. Parce qu'elles s'appuient sur les principes de légalité (conformité de la demande aux motifs inscrits dans la loi), de proportionnalité (rapport entre le risque encouru supposé et l'atteinte à la vie privée) et de subsidiarité (possibilité éventuelle d'emploi alternatif d'autres moyens), les décisions de la CNCIS démontrent clairement qu'elle œuvre au quotidien en faveur de « l'équilibre », le Conseil d'État ayant déclaré en septembre 2014 qu'il souhaitait d'ailleurs une extension très ample de sa capacité de contrôle[5]. Demain la « personnalité qualifiée » créée par la LPM de 2013

1) Sébastien-Yves Laurent, *Pour une véritable politique publique du renseignement*, Paris, Institut Montaigne, 2014, p. 54.
2) Ce qui a représenté une croissance notable, car un même individu peut avoir plusieurs lignes.
3) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019.
4) Les données techniques de communication ou de connexion sont en fait ce que l'on appelle aussi des « méta-données », ainsi qu'on le verra plus loin.
5) Conseil d'État, *Le numérique et les droits fondamentaux*, Paris, Documentation française, « Les rapports du Conseil d'État », 2014, p. 30.

aura un rôle tout aussi important que la CNCIS en matière de traitement de la tension sécurité-libertés, mais uniquement en matière de données.

Doutes sur les données

Data / données, ces termes sont partout. Leur ubiquité est totale. Mais ils ne sont jamais définis, nourrissant souvent des contresens. De quoi en effet parle-t-on ? Il est indispensable d'associer l'approche technologique et l'approche juridique. À défaut de sens stabilisé, nous proposons ici une approche toute personnelle : il faut revenir à sa matérialité pour comprendre cette curieuse réalité. La donnée est une information, soit une réalité à l'origine immatérielle, qui est médiatisée et transformée par un traitement informatique/numérique. Ce peut être aussi à l'origine un signal (image, son), porteur d'information et qui est numérisé. Celui-ci le rend matériel en l'inscrivant sur des supports physiques, aujourd'hui de plus en plus variés, aussi bien sédentaires que nomades. Non seulement le support de la donnée est mobile, mais la donnée elle-même est beaucoup plus un flux qu'un stock. La donnée brute (sous sa forme numérique), est donc la transformation de l'information, porteuse de sens, en un langage spécifique (usant de symboles) permettant des calculs, des mises en relation, des instructions. Par ailleurs pour le sens commun, malentendu supplémentaire, la donnée n'est pas la donnée brute de l'informaticien dont nous venons de parler mais la donnée immédiatement signifiante pour l'entendement humain.

On peut distinguer deux grands ensembles de données : les données qui ont un contenu informationnel et les méta-données qui sont en fait des données sur les données, c'est-à-dire pour lesquelles les informations prennent le sens d'informations métriques et statistiques sur des informations. Il s'agit par exemple des données de communication (données sur les communications téléphoniques et sur les échanges utilisant l'Internet), dont nous avons parlé *supra*. Si l'on tente de les définir par leur objet, il existe deux grandes catégories de données, les données personnelles, c'est-à-dire contenant des informations sur un individu et des données relatives aux personnes morales, notamment les entreprises.

En ce qui concerne la première catégorie, la plus médiatisée, celle touchant aux individus, le droit français très innovant qu'était la loi du 6 janvier 1978 (dite « informatique et libertés ») à l'époque de sa réalisation, a consacré les données dans son sens contemporain (articles 5 et 25) et clairement consacré la notion de « données nominatives » (article 31). Celles-ci sont devenues avec la loi du 6 août 2004 les « données à caractère personnel ». Avec cette loi, il s'agissait alors de se conformer au droit européen, en l'occurrence à la directive de l'Union européenne (UE)

de 1995, elle-même fortement inspirée de la convention 108 de 1981[1] qui avait créé l'appellation de « données à caractère personnel ». Malgré ce droit français qui fut à l'origine adapté à la technologie de son temps, le droit paraît aujourd'hui dépassé. En effet, les données de 1978 ne sont pas celles de 2004 qui ne sont pas celles d'aujourd'hui. En outre les données demeurent un angle mort de la réflexion juridique, de la part du législateur autant que de la doctrine. Si la notion de données doit être éclaircie et approfondie, il doit en aller de même des usages non judiciaires de la part des autorités. Ainsi, il demeure des doutes et des imprécisions juridiques fortes sur la captation de données dans un cadre non judiciaire.

On relèvera enfin que la focalisation sur les données personnelles a presque fait des données propres aux personnes morales une catégorie de second ordre. Les accords « Swift » et « Safe Harbour » inconséquemment signés par l'UE avec les États-Unis étaient déjà extrêmement dangereux. Depuis, l'effet Snowden[2] (été 2013) a révélé l'ampleur de l'espionnage économique qui est d'abord un espionnage des données.

Des garanties fondamentales et répétées depuis plus de cinquante ans : l'isolat européen dans le monde (des données)

On connaît bien aujourd'hui les notions fondamentales énoncées très clairement par la Cour de Strasbourg en s'appuyant sur la Convention de sauvegarde des droits de l'homme et dégagées par sa jurisprudence : l'ingérence d'une autorité publique dans la vie privée et dans les correspondances doit se conformer aux principes de légalité et de proportionnalité. Les États signataires se sont lentement adaptés à cet esprit en matière de communication, à commencer par la France qui ne le fit qu'avec la loi de 1991, acte de naissance de la CNCIS. Aux textes internationaux et européens fondateurs sur le secret des correspondances (Déclaration universelle des droits de l'Homme de 1948, Convention précitée de 1950, Pacte international des droits civils et politiques de 1966… etc. jusqu'aux directives de l'UE de 1997 et 2002), se sont ajoutés des textes spécifiques sur les « données », de la convention 108 du Conseil de l'Europe en 1981 à la directive UE de 1995 actuellement en cours de refonte en vue d'élaborer un règlement voté en 2013 et applicable en 2016[3]. L'ensemble de l'édifice, parfois assez composite, a été conforté par l'inscription dans la Charte des droits fondamentaux de l'UE en 2009.

---

1) Celle-ci s'inspirait très largement de la loi française de 1978…
2) *Cf.* Philippe Hayez, « L'effet Snowden. Les politiques du renseignement dans les démocraties », *Le Débat*, n° 181, septembre-octobre 2014, p. 94-102.
3) Un projet a été présenté par la Commission le 25 janvier 2012.

Il faut à ce stade rappeler une évidence : nulle part au monde les données ne sont mieux protégées qu'en Europe. Encore faut-il relever que 46 pays (dont les 28 membres de l'UE) avaient (en 2014) ratifié la convention 108 dont la Russie. C'est un pas important même si la convention ne concerne que le domaine de la cybercriminalité et si les États-Unis ne sont pas soumis à la juridiction de la Cour de Strasbourg…. Il ne faut pas pour autant se laisser emporter par une vue irénique sur la situation européenne : ceci est certes dû à la tradition politique et juridique libérale, mais aussi au fait que c'est une réaction à l'intensité de la surveillance et de la captation de données sur le continent. Il faut rappeler une seconde évidence : ce sont les institutions européennes qui jouent le rôle de vigie et contraignent bien souvent les autorités nationales à respecter des règles d'inspiration libérale. La Cour de Strasbourg, le Conseil de l'Europe, la commission « Libe » du Parlement européen [1], le commissaire européen à la « Justice, aux droits fondamentaux et à la citoyenneté » [2], l'Agence des droits fondamentaux (créée en 2007), enfin le groupe de travail a portée consultative « G29 » rassemblant les autorités de contrôle de chacun des États-membres, exercent un contrôle vigilant à cet égard qui trouve toujours une solide résonance médiatique. Dans le monde réel et dans le monde des données, l'UE est en situation d'exception par son droit très protecteur des données et la multiplicité d'organes juridictionnels et consultatifs qui assurent le contrôle de l'application : ceci ne signifie pas pour autant que les États-Membres assurent un respect strict des textes fondamentaux et des décisions juridictionnelles.

L'intensité des captations de données

Le monde numérique croît, inégalement géographiquement et sociologiquement, mais il croît. Sur plus d'une décennie (2000 à 2014), il a augmenté de plus 670 %. Près de 3 milliards d'individus (et leurs données) seraient aujourd'hui connectés. Peu d'entreprises ne le sont pas. Les marges de progression pour les individus sont importantes : en Asie le taux de pénétration n'est que de plus de 30 %, en Afrique de plus de 20 % et d'à peine 45 % au Moyen-Orient. Cette croissance globale de l'Internet repose sur un océan de données qui s'étend à chaque seconde de connexion.

L'effet Snowden a complètement occulté le travail d'enquête mené par le Parlement européen douze ans plus tôt. Le rapport du député

1) Désignée sous le nom de « commission des libertés civiles, des affaires intérieures et de la justice ».
2) Dans la nouvelle commission (2014-2019), le partage semble être différent avec une commissaire à la « Justice, aux consommateurs et à l'égalité des genres » et un commissaire (par ailleurs vice-président de la commission à la « Meilleure règlementation, aux relations interinstitutionnelles, à l'État de droit et à la Charte des droits fondamentaux »).

Gerhard Schmid[1] avait conclu à l'existence d'un réseau planétaire d'interceptions satellitaires et filaires organisé par les États-Unis en ciblant le continent avec l'aide active d'un État membre de l'Union européenne. À l'époque, le rapport s'alarmait plus des usages de ces interceptions à finalité d'espionnage économique que des enjeux pour les libertés fondamentales. Ce rapport rendu en juillet 2001 avait débouché sur une motion votée par le Parlement le…6 septembre 2001. Néanmoins, il fut le premier rapport public à établir l'existence d'un réseau mondial d'interceptions associant 5 pays, réseau qui était pourtant bien connu des spécialistes[2]. Douze ans après le rapport Schmid, les documents Snowden ont montré la persistance du réseau constitué lors de la Guerre froide, désormais orienté vers la captation de données.

Aujourd'hui comme hier c'est la situation stratégique qui explique, voire justifie ce dispositif d'interception : c'était hier la nécessité de surveiller les capacités nucléaires soviétiques qui était à l'origine du dispositif aérien et satellitaire à vocation électro-magnétique des États-Unis et de l'OTAN. C'est aujourd'hui le terrorisme qui est l'argument principal pour mettre en place un dispositif mondial d'interception des données numériques. Les pratiques de surveillance ont fortement évolué : ponctuelles et ciblées (« targeted surveillance »), elles semblent désormais de plus en plus permanentes et générales (« dragnet surveillance »[3]). L'un des grands dommages collatéraux de la lutte antiterroriste post-2001 est d'avoir brouillé la notion de suspect, cardinale jusque-là dans la totalité des dispositifs pénaux. Les stratégies de contre-surveillance[4] mises en place par les terroristes dans le monde réel et dans le monde cybernétique sont en partie efficaces et amènent les services anti-terroristes à élargir leur surveillance. Ceci a été en quelque sorte théorisé autour de l'idée que le « signal faible » (d'une activité criminelle ou terroriste) peut être débusqué en mettant en place une « surveillance de masse » – pour reprendre les termes employés, dès 1973 (!), par James B. Rule[5] – dans un tout autre contexte, qui s'exerce d'abord et avant tout dans le monde des données. L'idée est que les algorithmes permettent de détecter le « signal faible » dans le « bruit » des données interceptées. Qui plus est l'espionnage économique amène à procéder par la même technique du chalutage pour brasser les données utiles à l'espionnage économique.

---

1) *Cf.* Gerhard Schmid, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON (2001/2098 (INI),* Rapport A5-0264/2001, Parlement européen, 11 juillet 2001, 210 p.
2) *Cf.* Jeffrey T. Richelson and Desmond Ball*, The Ties That Bind : Intelligence Cooperation Between the UK/USA Countries*, Boston, Unwin Hyman, 1990, 426 p.
3) Jacob Appelbaum, Intervention au Conseil de l'Europe, 28 janvier 2014.
4) Sur cette notion, *cf.* Maurice Cusson, « La surveillance et la contre-surveillance », dans : Maurice Cusson, Frédéric Lemieux et Benoît Dupont, *Traité de sécurité intérieure*, Lausanne, Presses polytechniques et universitaires romandes, 2008, p. 429-436.
5) *Cf.* James B. Rule, *Private Lives and Public Surveillance*, New York, Schocken Books, 1974 [1re éd.: 1973], 382 p.

Un « équilibre » illusoire ?

La poussée sécuritaire post-2001 très dénoncée[1] dans les pays occidentaux est patente. Elle a généré des théories sur l'état d'exception[2] alimentant une critique radicale de l'État de droit et des régimes démocratiques : ce n'est pas là le moindre de ses dangers. Le droit européen et au-delà le droit de *common law* mettent en avant le principe de proportionnalité : dans un État de droit la violence et la coercition doivent être exercées avec mesure, dans un esprit de « proportionnalité ». Il reste que si la notion a envahi le vocabulaire publiciste, elle demeure bien faible en pratique dans le droit français par rapport à d'autres pays. Ce principe est aujourd'hui d'un point de vue normatif, cardinal en dehors de nos frontières mais il est sans aucune portée en matière d'interceptions de masse qui ne sont pas régulées.

Outre le fait que le droit international ne prohibe pas l'espionnage[3], il ne connaît pas les données en dehors de la convention 108 ; de portée géographiquement limitée. Dans cette situation que faire ? La question de la régulation ne se pose pas car il n'existe ni juridiction, ni autorité, ni même volonté. Les interceptions de données ne font d'ailleurs l'objet de communiqués et (vraisemblablement) d'échanges sur ces pratiques concurrentes entre les puissances que depuis que les États-Unis ont été contraints de réagir aux indignations après 2013. À défaut, peut-on espérer une forme d'auto-régulation de la part des « five eyes » et principalement des États-Unis, les seuls à ce jour clairement identifiés ? La commission *ad hoc* nommée par le président Obama a remis en décembre 2013 un rapport subordonnant les interceptions de données à des impératifs de sécurité nationale[4] et indiquant clairement que les pratiques : « must not be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries »[5]. Cette (mauvaise) plaisanterie n'était qu'un élément de langage destiné aux chancelleries occidentales « alliées » et « partenaires ».

Les données ignorent la géographie[6]. En mouvement permanent ou stockées (provisoirement) dans des pays garantissant une moindre protection juridique, elles cherchent en permanence à échapper à

---

1) Pour ne s'en tenir qu'à des auteurs français, *cf.* Eric Sadin, *Surveillance globale. Enquête sur les nouvelles formes de contrôle*, Paris, Climats, 2009, 234 p. et Michaël Foessel, *État de vigilance. Critique de la banalité sécuritaire*, Paris, éditions les bords de l'eau, 2010, 155 p.
2) Giorgio Amgaben, *État d'exception. Homo sacer II/1*, Paris, Seuil, « L'ordre philosophique », 2003, 151 p.
3) Fabien Lafouasse, *L'espionnage dans le droit international*, Paris, Nouveau monde éditions, « Le Grand jeu », 2012, 491 p.
4) The President's Review group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 12 December 2013, 304 p.
5) *Ibid.*, p. 19.
6) On lira avec profit l'excellent : "Cyberespace : enjeux géopolitiques", *Hérodote*, 1er-2e trimestre 2014, nº 152-153, 312 p.

quelque contrainte que ce soit. Le droit international ignore le monde des données. Les droits internes sont très différents sur les données mais leur profitent, plus qu'aux citoyens et aux entreprises. Il reste que leur mouvement n'est brownien qu'en apparence : elles sont entre les mains de ceux qui les stockent, les font circuler, parce qu'ils les vendent. Les acteurs économiques du numérique, fournisseurs d'accès, hébergeurs, producteurs de contenus sont les auteurs de cette mobilité planétaire. La commercialisation de grande ampleur des données par temps de globalisation et la dé-territorialisation de la surveillance annihilent la dialectique sécurité-libertés. On peut donc parler d'une situation d'anomie entretenue aussi bien par les grands États acteurs de la surveillance que voulue par les sociétés numériques multinationales. Il est assez peu probable que les structures de gouvernance de l'Internet – IGF et Icann notamment – puissent faire en l'état évoluer la situation des données. Il reste que le fonctionnement de ce « système » repose sur la confiance : si les citoyens d'une part, les usagers de l'autre (qui sont les mêmes, mais peuvent réagir pour des raisons différentes) la remettent en cause, alors, mais seulement alors, la situation anomique pourrait être remise en cause.