Introduction

Régulièrement depuis plusieurs décennies, les pratiques entourant les interceptions de communication ont occupé une place importante dans l'actualité, suscitant des débats de société, politiques, juridiques, sociologiques. Les risques de dérives des États démocratiques vers des pratiques qui rappellent celles des régimes totalitaires ont été à maintes reprises pointés du doigt par les défenseurs des libertés en Occident. Plus les technologies de communication évoluent, plus les espaces de communication se déploient, plus les tentations de contrôler ce qui s'y dit et s'y écrit semblent fortes. Ainsi, à côté des interceptions ciblées, qui visent un ou quelques individus en particulier se sont multipliées les possibilités d'interceptions massives des communications. Ces deux pratiques ont à ce jour déjà une assez longue histoire. Mais l'avènement de la société d'Internet (le « cyberespace ») a sans nul doute marqué un tournant dans les pratiques et les ambitions de ceux qui recourent aux interceptions. Car l'architecture même du cyberespace, réseau planétaire de flux continus, facilite – bien que techniquement l'opération soit des plus complexes – l'exploitation de ces masses de données qui parlent à la fois des individus, observables un à un, et des groupes humains. Les technologies de communication se sont multipliées, étendues, mais dans le même temps aussi celles d'interception, que ce soit à des fins de sécurité, de surveillance, de contrôle, d'espionnage économique, politique, militaire ou autre. La pratique semble décomplexée : tous les États pratiquent les interceptions légales, nombreux sont ceux qui pratiquent des interceptions qui sortent de ce cadre légal, ou n'en ont pas défini. Les interceptions semblent souvent être pratiquées tous azimuts, nombreux étant les motifs légitimant leur recours, mais bénéficiant aussi d'une panoplie de technologies qui, selon les présentations des produits commerciaux, n'auraient guère de limites, capables de tout intercepter ou presque, qu'il s'agisse de communications filaires ou non, quels que soient les protocoles ou les milieux par lesquels passent les infrastructures de communication (terre, air, mer). Les débats de la dernière décennie ont insisté sur l'érosion de la confiance entre pays alliés qui n'ont cessé de s'espionner, d'intercepter les communications de leurs dirigeants politiques ou industriels ; ils

ont aussi insisté sur l'affaiblissement des droits et libertés des citoyens partout dans le monde. Si la responsabilité des acteurs qui décident de la mise en œuvre des interceptions est essentielle, le rôle de la technologie ne l'est pas moins. Car elle détermine, au-delà du droit lui-même, les limites de ce qu'il est possible de faire. Le rôle des inventeurs, chercheurs, ingénieurs, développeurs, industriels, marchands, est tout aussi crucial que celui des clients qui tirent profit de ces technologies, même si ces derniers n'ont sans doute pas toujours pleine conscience de la manière dont la technologie fonctionne, ni des effets qu'elle peut produire. Les utilisateurs finaux des résultats de l'interception dépendent à la fois des technologies qu'ils ne maîtrisent pas, et leurs concepteurs, techniciens et ingénieurs qui en maîtrisent certes le versant technique, mais qui restent parfois éloignés des implications sociales et politiques de leur travail. Nombreux sont les acteurs qui naviguent ainsi dans un univers de méconnaissance, d'ignorance, de croyances, voire d'impensé.

Définitions de l'interception (et de quelques notions associées)

Commençons par clarifier les termes de notre étude.

Si l'on s'en réfère à la définition proposée par le Centre national de ressources textuelles et lexicales (CNRTL)[1], il faut voir dans l'interception au moins deux grandes catégories d'actions. La première consiste à arrêter l'objet ou le message, afin qu'il ne parvienne pas à son point final, la seconde à prendre connaissance d'un message destiné à un tiers. L'arrêt de la progression du message peut également se traduire par sa destruction. Ces deux facettes de l'interception sont déclinées de la façon suivante par le CNRTL :

> « L'action de prendre quelque chose au passage, de le détourner de sa destination ; l'action de prendre connaissance d'une conversation, d'un message destiné à autrui ; l'action d'arrêter la diffusion de quelque chose, la progression de quelqu'un ; dans le domaine militaire l'opération consistant à arrêter, à détruire un objectif ennemi (navire, avion, missile) en mouvement. »

L'interception est également définie dans des documents à portée juridique, technique ou politique. Ainsi l'UIT (Union internationale des télécommunications) formule-t-elle une définition qui insiste davantage sur la dimension technologique des interceptions. Elle regroupe plusieurs pratiques telles que :

> « L'acquisition, la visualisation, la capture ou la copie de tout ou partie de la teneur de toute communication, y compris les données relatives

1. https://www.cnrtl.fr/definition/interception.

> au contenu, les données informatiques, les données relatives au trafic et/ou leurs émissions électroniques, que ce soit par des moyens filaires, sans fil, électroniques, optiques, magnétiques, oraux ou autres, pendant la transmission, par l'utilisation de tout dispositif électronique, mécanique, optique, à ondes, électromécanique ou autre. » [ITE 12]

L'interception désigne un ensemble de pratiques, qui sont réservées à des acteurs spécifiques, principalement étatiques, à des fins de renseignement et/ou de lutte contre la criminalité, le terrorisme, et de défense de la sécurité nationale : « L'interception comprend tous les actes de surveillance, de copie, de détournement, de duplication et de stockage des communications au cours de leur transmission par ou pour les services de police ou de renseignement » [PRI 21].

Les interceptions peuvent être effectuées sur tous les vecteurs de communication, s'appliquer à tous types de contenus (voix, image, texte), impliquant le recours à des moyens d'interception aussi diversifiés que le sont les supports et contenus visés : « Le terme "interception" est défini dans l'article 2510(4) du titre 18 du Code des États-Unis comme l'acquisition audio ou autre de la teneur de toute communication filaire, électronique ou orale par l'utilisation de tout dispositif électronique, mécanique ou autre » [DEP 20].

> « Une "interception" (*intercept*) est le terme utilisé pour décrire l'interception (*interception*) secrète d'une communication privée par les services de renseignement ou les forces de l'ordre. L'interception d'appels téléphoniques – par exemple au moyen d'écoutes téléphoniques, etc. – est peut-être l'exemple le plus connu. Toutefois, en vertu de la loi de 2000 sur la réglementation des pouvoirs d'investigation (Regulation of Investigatory Powers Act) (RIPA), les "communications interceptées" couvrent également d'autres types de communications, notamment les téléphones portables, les courriers électroniques, les télécopies et le courrier ordinaire. » [JUS 06]

Il convient également de distinguer l'interception de la surveillance, même si les deux pratiques sont étroitement liées.

Pour le CNRTL[2], la surveillance est :

> « L'action ou fait de surveiller une personne dont on a la responsabilité ou à laquelle on s'intéresse ; une activité policière consistant à surveiller

2. www.cnrtl.fr/definition/surveillance.

> des personnes suspectes ou des milieux à risques, pour prévenir des actions délictueuses ou criminelles, pour garantir la sécurité publique. »

« Surveiller » c'est, toujours selon le dictionnaire du CNRTL[3] :

> « Observer quelqu'un avec une certaine attention pour comprendre son comportement ; veiller sur une personne dont on a la responsabilité morale ou à laquelle on s'intéresse ; observer les agissements d'adversaires potentiels, les lieux d'où peut survenir le danger. Une sentinelle surveille le pont ; se tenir informé, par des moyens policiers, des activités de personnes jugées suspectes, du comportement de collectivités, de groupes, de lieux à risques. »

Ainsi l'interception n'est-elle généralement qu'une composante de la surveillance. Il est possible de surveiller des individus sans recourir nécessairement aux interceptions de leurs communications. Mais lorsque la surveillance s'exerce sur leurs communications, à côté de l'interception prend place tout un ensemble de pratiques, de techniques, telles que l'observation, la collecte, etc. créant ainsi une longue chaîne de processus dans laquelle l'interception vient s'insérer :

> « La surveillance des communications est le contrôle, l'interception, la collecte, la conservation et la rétention d'informations qui ont été communiquées, relayées ou générées par des réseaux de communication à un groupe de destinataires par un tiers […] À son tour, la surveillance des communications ne se limite plus à l'interception d'un messager ou à la fixation d'une "pince crocodile" sur une ligne téléphonique. Il existe désormais quatre méthodes principales de surveillance des communications : la surveillance de l'Internet, l'interception des téléphones mobiles, l'interception des lignes fixes et les technologies d'intrusion (qui sont expliquées en détail ci-dessous). La surveillance sur les réseaux internet, mobiles et fixes peut se faire avec ou sans la coopération de l'opérateur du réseau… » [PRI 18]

> « L'interception des communications n'est qu'un type de surveillance secrète parmi les nombreux autres utilisés par les forces de l'ordre et les services de renseignement afin de prévenir et de détecter les crimes graves (y compris les activités terroristes). Toutefois, pour des raisons qui sont examinées en détail ci-dessous, le droit britannique traite depuis

3. www.cnrtl.fr/definition/surveiller.

longtemps l'utilisation des informations obtenues à partir de communications interceptées différemment des autres formes de surveillance. » [JUS 06]

On ne saurait donc réduire la surveillance à la seule pratique des interceptions.

L'interception consiste en la réalisation d'une action sur le système de télécommunications (modifier ou interférer avec le système ou ses opérations, monitorer les transmissions), de laquelle doit en résulter la mise à disposition des contenus de la communication à une personne qui n'est pas son destinataire. L'interception peut avoir lieu pendant la transmission de l'information, mais également de manière différée lors de son stockage par exemple qu'il soit antérieur ou postérieur à la transmission : « L'interception consiste à obtenir la teneur d'une communication – comme un appel téléphonique, un courriel ou un message sur les réseaux sociaux – au cours de sa transmission ou pendant qu'elle est stockée sur un système de télécommunications » [HOM 17].

On peut résumer le principe de l'interception en un schéma simple. Si nous considérons deux interlocuteurs A et B (deux individus, groupes, « acteurs ») qui échangent un ou plusieurs messages, l'interception est l'intervention d'une tierce partie (C), non invitée à l'échange, qui souhaite pouvoir entendre, lire, savoir ce qui se dit ou s'écrit dans cet espace intime constitué entre A et B.

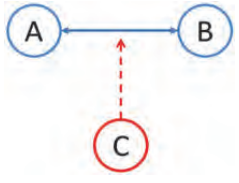

Figure 1. *Schéma élémentaire du principe d'interception*

Cela implique que pour C, l'échange entre A et B présente une valeur, un intérêt (réel ou potentiel). Il espère en tirer un bénéfice, un avantage sur A, sur B, ou sur d'autres parties non directement impliquées dans l'échange entre A et B. Du point de vue de A et B, l'entité C est un intrus qui porte atteinte à cet espace d'intimité qu'est celui de la communication.

Nous reviendrons ultérieurement sur ce schéma de base, qui pourra être complété et complexifié afin d'intégrer d'autres acteurs et d'y intégrer en particulier ceux de la technologie.

Rappelons quelques-uns des traits caractérisant l'interception de communications :

– l'accès aux contenus mêmes des échanges est la spécificité de l'interception. L'accès aux métadonnées et non aux contenus relève-t-il alors toujours des interceptions, et notamment du cadre juridique qui les régit ?

– l'interception ne paraît pas être strictement limitée aux données en transit, mais peut également s'appliquer aux données stockées de manière statique dans un espace de mémorisation (mais alors quelle différence y a-t-il entre interception, accès, intrusion ?) ;

– l'interception est l'une des modalités de la surveillance, qu'elle peut donc compléter et accompagner ;

– l'interception n'a d'intérêt que dans la mesure où émetteur et récepteur du message ignorent son existence, ignorent la présence d'une oreille ou d'un regard indiscret sur leurs communications. Mais nous verrons qu'émetteur et récepteur ont appris à évoluer quand bien même leurs communications sont interceptées ou menacées de l'être. Des tactiques ou stratégies de résistance se sont développées.

La notion d'interception se décline ainsi en interceptions légales, stratégiques, tactiques, massives (*bulk*), passives, actives (énumération non exhaustive). La distinction entre interceptions ciblées (*targeted*) et non ciblées ou massives (*bulk*) est essentielle.

Les interceptions ciblées sont celles qui visent un ou plusieurs individus en particulier, de manière précise. L'interception ciblée peut être « utilisée contre des citoyens britanniques soupçonnés d'activité illégale ; elle peut être menée contre une personne ou dans un lieu spécifique par la police, les agences de renseignement ou les forces armées ; la demande doit préciser spécifiquement qui ou quoi sera espionné et où ; le terme "ciblé" peut également être entendu de manière thématique. Par thématique, on entend des groupes de personnes, une zone particulière, un certain nombre d'organisations »[4].

> « Les États ont accès à un certain nombre de techniques et de technologies différentes pour effectuer la surveillance des communications privées d'un individu ciblé. Les capacités d'interception en temps réel permettent aux États d'écouter et d'enregistrer les appels téléphoniques de toute personne utilisant un téléphone fixe ou mobile, grâce à l'utilisation des capacités d'interception obligatoirement intégrées dans tous les réseaux de communication au nom des besoins de surveillance des États. Il est possible de déterminer l'emplacement d'une personne,

4. www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf.

> de lire et d'enregistrer ses messages. En plaçant une écoute sur un câble internet relatif à un certain lieu ou à une certaine personne, les autorités de l'État peuvent également surveiller l'activité en ligne d'un individu, y compris les sites web qu'il ou elle visite. » [RUE 13]

Les interceptions massives (*bulk*) se distingueraient des précédentes à la fois par leur objectif et leur dimension technologique : captant des données en plus grands volumes, par exemple en exploitant les flux de données circulant sur Internet, elles ne seraient pas utilisées dans le cadre des enquêtes, mais plutôt pour la collecte du renseignement : « L'interception massive est un outil vital conçu pour obtenir des renseignements axés sur l'étranger et identifier les personnes, les groupes et les organisations à l'étranger qui représentent une menace pour le Royaume-Uni » [FAC 15].

> « [L'interception massive] se fait en se branchant sur les câbles internet qui transportent le trafic internet mondial ; les agences de renseignement ont maintenant le pouvoir légal de mettre ces câbles sous écoute et de s'emparer d'une partie de l'activité internet ; l'interception massive est vaste, repose rarement sur une enquête précise et est utilisée pour rechercher des complots, des comportements ou des activités qui pourraient être de nature criminelle ou terroriste. »[5]

> « L'interception est la capacité d'écouter ce que quelqu'un dit ou écrit. L'Investigatory Powers Act (la loi sur les pouvoirs d'investigation) prévoit deux types d'interceptions : l'interception ciblée et l'interception massive. L'interception ciblée est utilisée lorsque l'objet de l'enquête est connu. L'interception massive est utilisée lorsque l'objectif est inconnu. L'interception massive consiste à recueillir de grandes quantités de trafic internet dans le monde entier. Comme l'interception massive est utilisée pour découvrir plutôt que pour enquêter, elle peut être vue comme une forme d'enquête précriminelle. »[6]

Les interceptions « massives » ont débuté bien avant les récents programmes tant décriés des agences de renseignement américaines :

> « L'interception en masse des télégrammes, connue sous le nom de "censure des câbles", a commencé en même temps que la censure postale le 2 août 1914, quelques jours avant le déclenchement officiel de

5. www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf.

6 . www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf [Consulté le 1er mars 2017].

> la Première Guerre mondiale. Au début, l'objectif principal était d'interdire complètement le trafic diplomatique ennemi plutôt que de l'intercepter de manière sélective. Des censeurs ont été installés dans les bureaux de câblodistribution de Londres et à Porthcurno, en Cornouailles, qui était alors devenu un centre de relais pour les câbles sous-marins internationaux du monde entier. » [KEE 17]

La seconde notion essentielle est celle de « données », qui se déclinent en plusieurs catégories. Ainsi sera-t-il question des données relatives aux contenus (le contenu étant l'information communiquée), des données relatives au trafic (c'est-à-dire en rapport avec la communication), des métadonnées (une catégorie de données que l'on distingue des données de contenus)[7], des données informatiques, données de localisation, données de communication stockées (« at rest », « in the cloud », « in storage »), données en mouvement (ou dynamiques, en anglais « data in transit », « data in motion »), données à caractère personnel, privées, sensibles, confidentielles, secrètes, etc.

Les données dynamiques, ou en mouvement, sont la cible première des interceptions.

Notre définition de l'interception des communications : rééquilibrer une asymétrie informationnelle

L'interception crée ou révèle des rapports de force dont le postulat de base est qu'elle vise à rééquilibrer une asymétrie informationnelle qui se crée entre les parties impliquées dans une communication.

Les parties créent ainsi un espace de confidentialité, et ceux qui en sont exclus estiment que cette situation leur est préjudiciable ou que l'accès à la connaissance leur est indispensable.

Les variables en jeu sont :

– l'espace de communication, domaine cible des attaques d'interception, constitué des technologies de communication ;

7. « Données techniques nécessaires à l'acheminement d'une communication » [En ligne]. Disponible à l'adresse : www.signal.eu.org/blog/2015/04/20/eu-org-les-metadonnees-et-la-loi-renseignement. « Les métadonnées désignent un ensemble d'informations standardisées relatives à un fichier, telles que le nom de l'auteur, la résolution, l'espace colorimétrique, les informations de copyright et autres mots-clés qui lui sont appliqués » [En ligne]. Disponible à l'adresse : www.helpx.adobe.com/fr/bridge/using/metadata-adobe-bridge.html.

– la dimension défensive : les techniques de protection (contre les menaces d'interception) ;

– la dimension offensive : les technologies d'interception.

La dimension technologique est centrale. Le droit lui-même peut sembler contraint par la technologie dont il s'efforce d'intégrer les évolutions :

> « La section 702 elle-même est un amendement relativement nouveau à la loi Fisa […] Elle a été rédigée pour tenir compte des développements technologiques antérieurs, mais aussi pour s'adapter aux changements futurs tout en restant neutre sur le plan technologique. »[8]

> « Même la Cour suprême a commencé à reconnaître les limites de sa capacité à établir un cadre juridique qui marie convenablement la doctrine du quatrième amendement et les technologies émergentes. »[9]

État de l'art des recherches récentes sur les interceptions

Les CIT (Communication Interception Technologies)[10] et plus largement les technologies de surveillance électronique ont suscité des débats dans les années 1980 [OFF 85 ; OFF 87], puis surtout à la fin des années 1990 avec les rapports concernant le réseau Echelon [WRI 98 ; BEC 99 ; CAM 99 ; SCH 01]. Ces débats ont été renouvelés dès le début des années 2010 et ce, avant même les révélations d'Edward Snowden [HOF 05 ; DEA 10 ; BUT 12 ; CON 13 ; BEL 14]. Les CIT y sont dépeintes comme des « armes » indispensables à la lutte contre le crime, comme des outils incontournables du renseignement policier. Mais au-delà de ces quelques références académiques et rapports produits sur la période, nous constatons que le volume de travaux en sciences humaines et sociales traitant spécifiquement des technologies d'interception reste faible. Les débats juridiques et éthiques se taillent la part du lion (les interceptions, puis plus largement la surveillance, motivent des débats sur le

8. « Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act, Presented to The Robert S. Strauss Center for International Security and Law and The University of Texas School of Law, Austin, Texas » [En ligne]. Disponible à l'adresse : www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=70&ModuleId=9757&Article=1619167, 14 septembre 2014.

9. « Failing to Keep Pace: The Cyber Threat and Its Implications for Our Privacy Laws, Washington » [En ligne]. Disponible à l'adresse : www.nsa.gov/news-features/speeches-testimonies/Article/1608850/, 23 mai 2018.

10. Nous retiendrons cet acronyme anglais afin de ne pas le confondre avec celui de TIC, qui renvoie aux Technologies de l'information et de la communication.

droit à la vie privée ou *privacy*), et le thème de la société de surveillance ou société panoptique est décliné dans des travaux de nature sociologique et politique. Ce sont surtout les pratiques d'interception et de surveillance, les effets produits, les organisations qui les déploient, les conséquences sur les sociétés, la scène internationale ou les individus qui suscitent l'intérêt au cours de ces débats.

Au cours de la dernière décennie, les travaux qui se sont attachés en sciences humaines et sociales à l'analyse du phénomène des interceptions ont essentiellement adopté trois types d'approches : juridique, historique, politique/sociologique/géopolitique.

Ces travaux sont significatifs de l'onde de choc provoquée par les révélations Snowden et qui s'est manifestée au travers de débats à l'échelle planétaire sur les questions de surveillance, de libertés (de parole, d'opinion, etc.), de vie privée (*privacy*), mais aussi de géopolitique d'Internet [CLE 14] ou de gouvernance, de souveraineté numérique, de protection des données, de sécurité et de défense nationale, de configuration des rapports de force au sein de la scène internationale, des rapports entre économie/industrie, citoyens et État.

Approche juridique

Les études juridiques traitent des interceptions sous plusieurs aspects en proposant :

– de comparer les régimes juridiques applicables aux interceptions dans plusieurs pays [GAL 16a], au travers de leurs particularités ou convergences en matière de répartition des pouvoirs d'interception, des niveaux et modalités de protection du secret des communications, des conditions d'interception des contenus, d'accès aux données de trafic et d'utilisateurs, d'accès aux données stockées [POL 16] ;

– de débattre de la question des droits fondamentaux (liberté d'expression, respect du secret des correspondances, etc.) confrontés à l'évolution des droits nationaux en matière d'interception [MAK 11 ; NGW 17] ;

– d'analyser la place, du point de vue du droit, de chaque acteur impliqué dans les procédures d'interception [GAL 16a] ;

– de discuter les limites de la valeur probante des données collectées lors des interceptions [GAL 16b] ;

– d'envisager les conditions du respect des droits des individus face aux interceptions menées illégalement ou aux abus des interceptions légales [EIJ 18] ;

– de confronter le droit existant aux évolutions technologiques et à l'adaptation du crime à son environnement (par exemple lorsque les interceptions criminelles exploitent les communications Wi-Fi [THO 15].

Approche historique

À l'image de l'étude réalisée par David Sherman [SHE 16] publiée par la NSA en 2016, qui porte sur les briseurs de code de Bletchley Park dès le début de la Seconde Guerre mondiale, de nombreux travaux s'intéressent à des moments particuliers de l'histoire (les interceptions durant la Première Guerre mondiale, durant la Seconde Guerre mondiale, durant la guerre froide, etc.).

Le travail de Bernard Keenan [KEE 16 ; KEE 17] sur les interceptions couvre au contraire plusieurs siècles d'histoire. Il propose une chronologie des interceptions en Angleterre construite autour de trois périodes : une phase dite de « prérogatives » royales, de 1590 (ou 1634) à 1984 ; une phase « d'obscurcissement » (obfuscation) de 1985 à 2015 ; une période dite de « transparence », à compter de 2016.

La première période (1634-1984) s'ouvre avec l'ouverture au public du service postal en Angleterre, présenté comme le moyen de dissémination des savoirs, de l'information et du commerce. Le contrôle centralisé sur l'information ouvre une nouvelle voie dans les méthodes du renseignement, dans des domaines aussi divers que la lutte contre le crime, contre toute forme de conspiration politique, qu'elle soit nationale ou étrangère. Sur le plan juridique, dès cette époque, le secret des correspondances est un principe inscrit dans la loi (1657)[11] et les courriers ne peuvent être interceptés et ouverts que sur autorisation d'un juge. La loi permet de sanctionner quiconque interfère avec la Poste. Mais les autorisations ne sont cependant pas destinées à assurer un contrôle des pratiques du pouvoir étatique qui demeurent couvertes par le secret jusqu'au XXI^{e} siècle.

La seconde période (1985-2015) dite d'obfuscation s'ouvre sur l'affaire Malone, du nom d'un trafiquant poursuivi par la justice et qui a saisi en 1979 la Haute Cour après avoir appris que la police avait intercepté ses appels téléphoniques. La Haute Cour débouta Malone, rappelant qu'il n'y a rien d'illégal dans les écoutes, le principe de protection de la vie privée n'existant pas dans le droit de Common Law. Malone porte alors l'affaire devant la Cour européenne des droits de l'homme de Strasbourg.

11. « June 1657: An Act for setling the Postage of England, Scotland and Ireland ». Dans *Acts and Ordinances of the Interregnum*, 1642-1660, Firth, C.H. et Rait R.S. (dir.) (Londres, 1911), p. 1110-1113, British History [En ligne]. Disponible à l'adresse : www.british-history.ac.uk/no-series/acts-ordinances-interregnum/pp1110-1113.

Cette dernière estime que l'article 8 de la Convention européenne des droits de l'homme accorde aux Britanniques un droit à la vie privée et par conséquent que les interceptions de communications ont interféré avec ce droit. Pour rendre de telles interceptions légales, il faut réunir plusieurs conditions, aux termes de l'article 8 : le pays doit préciser les limites de l'interception dans la loi, et la légalité de l'interférence est conditionnée au respect de deux principes : la nécessité et la proportionnalité. Le Royaume-Uni se dote d'une loi en 1985 (*Interception of Communication Act* 1985), votée par le gouvernement Thatcher, qui privatise les entreprises de télécommunication et permet à l'État de conserver ses prérogatives en maintenant son pouvoir d'interception. Cette loi de 1985 sera remplacée par le Ripa en 2000 (*Regulation of Investigatory Powers Act* 2000). Ce texte est suffisamment imprécis ou général pour accorder aux autorités des pouvoirs larges, s'appliquant à tous types de technologies. Le texte se veut technologiquement neutre : « Son haut degré d'abstraction a permis de garantir sa "neutralité technologique", dans la mesure où il a établi des règles générales applicables aux différentes formes de médias numériques » [KEE 17].

C'est cette méthode que Keenan qualifie d'obfuscation[12]. Les révélations de Duncan Campbell (sur la nature du réseau Echelon) et d'E. Snowden viendront confirmer l'existence des pratiques étatiques qui s'embarrassent peu des droits des citoyens, en captant de manière massive des données d'individus ordinaires. L'étendue des pouvoirs liés aux interceptions est large, laissant aux autorités le champ libre pour mener des programmes d'interceptions massives, partager des données avec des pays tiers, pirater des systèmes, imposer des contraintes aux opérateurs, etc. L'opacité entourant ces pratiques fut telle qu'aucune des organisations (*Investigatory Powers Tribunal*, *Interception of Communications Commissiosnner*) supposées contrôler les pratiques d'interception et formuler des avis ou recevoir des plaintes de citoyens ne semblait être informée de leur ampleur.

Les débats ouverts par Snowden et certaines organisations de défense de la vie privée ont coïncidé avec une prise de conscience des conséquences de la vie en ligne : les individus sont plus exposés aux regards des entreprises privées et des acteurs étatiques. Cette période est la troisième que propose de considérer Keenan, qu'il nomme période de transparence. Elle s'ouvre en 2016.

12. L'obfuscation peut être définie comme une « stratégie de protection de la vie privée sur Internet » en publiant des informations fausses ou suffisamment imprécises de sorte que les informations vraies ou pertinentes soient masquées (l'obfuscation est donc une stratégie d'anonymisation, de masquage) ; ou comme une technique consistant à « rendre illisible pour un humain un programme, tout en le gardant pleinement fonctionnel » : fr.wiktionary.org/wiki/obfuscation. On pourra préférer le terme « obscurcissement » à « obfuscation », considéré comme un anglicisme.

Selon Keenan, ce qui a changé au cours des dernières décennies, c'est la place désormais moins centrale de l'individu. Il n'est plus le « point de référence » essentiel, les puissances fondées sur la surveillance n'ayant pas seulement la capacité de toucher les individus mais des groupes entiers ; ces individus et groupes peuvent être définis selon des caractéristiques suggérées par leurs données. Le fait que les États puissent collecter ou intercepter massivement les données crée les conditions de la surveillance de masse. Cela n'implique pas que tous les individus de la société fassent l'objet d'une observation spécifique, mais signifie que les données de chacun d'entre nous peuvent être présentes dans un processus d'analyse.

Approche politique, sociologique, géopolitique

Le projet UTIC

Le projet de recherche UTIC (projet de recherche mené en France, coordonné par D. Bigo – Science Po Paris – et financé par l'Agence nationale de la recherche – ANR) portait sur « les usages des technologies liées à l'interception des communications téléphoniques et internet par les services de police et de renseignement et par leurs prestataires privés », s'intéressant plus spécifiquement au cas de la France dans son environnement européen. Le projet mené sur la période 2014-2019 s'inscrivait dans le contexte post-Snowden, période de controverses ou polémiques autour des pratiques des États en matière d'interceptions des communications et de leurs conséquences sur les sociétés modernes, les démocraties, les individus. Le projet focalisait son attention sur quatre axes : les logiques de surveillance, les discours de justification, la redéfinition des limites des démocraties et la souveraineté des États.

Le projet a analysé plusieurs aspects de l'interception :

– avec Internet, les États peuvent exercer une surveillance sur les sociétés par le biais de la surveillance de leurs communications. Les nouvelles capacités techniques ont contribué à en asseoir le caractère massif. Le fait qu'elles soient réalisées en vrac, sans mandats individualisés a-t-il changé la nature de l'interception ? Comment définir cette massivité ? Porte-t-elle atteinte à la vie privée de tous les individus dont les données sont collectées de la sorte ?

– les interceptions massives sont justifiées par diverses finalités : lutte contre le crime, terrorisme, renseignement économique ou politique, etc. La justification du caractère massif des interceptions diffère selon les services de renseignement, au sein d'un même pays, puis entre pays. Le projet a tenté d'analyser ces rapports ;

– l'internationalisation des enjeux de sécurité, couplée à la dimension mondiale d'Internet, confère une dimension nouvelle aux pratiques d'interception et de surveillance. La collecte des données sort du cadre national, les données sont échangées

entre services de renseignement, des opérateurs privés agissant internationalement sont impliqués dans les processus de collecte, rétention et traitement des données. Le projet s'est intéressé à ces hybridations (public-privé, alliances, coopération internationale, etc.) et leurs effets sur la définition des objectifs de sécurité, sur les pratiques d'interception, sur l'appréciation des risques et des effets produits notamment sur les droits fondamentaux.

Le projet a donné lieu à la production d'un ensemble de rapports dont nous synthétisons ici les principales conclusions :

– le rapport réalisé par Philippe Guillot et Daniel Ventre, « Capacités d'interception et de surveillance. L'évolution des systèmes techniques », explore le large éventail de technologies ou techniques d'interceptions disponibles à l'ère des communications électroniques, ainsi qu'aux moyens permettant de se protéger de ces pratiques et de les contrer. « La compréhension des techniques, des technologies, des capacités, ressources, moyens utilisés, déployés, développés, demeure essentielle […] Car il ne saurait y avoir de mesure saine des enjeux sans évaluation ou compréhension, ne serait-ce qu'*a minima*, des possibilités » [GUI 19] ;

– la première partie du rapport « Techniques et contre-mesures techniques » [SIL 18] s'intéresse spécifiquement à l'utilisation du *Deep Packet Inspection* (DPI) dans la surveillance en France et en Europe. Pour ses auteurs, en matière d'interceptions massives, le droit évolue afin de s'adapter aux évolutions technologiques. Ce n'est donc pas tant le droit qui contraint les capacités technologiques et leurs usages, que ces dernières qui s'imposent au droit. C'est la réunion des intérêts économiques des entreprises et des objectifs sécuritaires des États qui paraît dicter les règles du jeu. Les technologies DPI ont été utilisées de manière abusive dans plusieurs États. « La limite tacitement admise entre l'usage légitime ou illégitime de ces technologies, selon que l'État soit "démocratique" ou non, et celles des finalités, est ténue » [SIL18, p. 77]. La seconde partie du rapport analyse le phénomène de résistance à la surveillance ;

– Laurent Bonelli et Francesco Ragazzi [BON 14] rappellent que dans un contexte hypertechnicisé, le renseignement recourt encore à des techniques traditionnelles de collecte et de traitement des informations, les pratiques des professionnels de la sécurité étant enracinées dans des habitudes institutionnelles ;

– la contribution de Didier Bigo et Laurent Bonelli [BIG 19] s'intéresse également aux acteurs du renseignement et à leurs pratiques, soulignant l'hétérogénéité du monde du renseignement, notamment dans ses techniques de surveillance :

> « Il semble que les techniques numériques soient mises à profit de deux manières. Premièrement, elles peuvent être utilisées en appui au cadre plus traditionnel du raisonnement conjectural afin d'établir les preuves

> nécessaires au pouvoir judiciaire. Deuxièmement, elles peuvent également être utilisées pour imposer un raisonnement préventif et prédictif. Les logiques et les mécanismes de raisonnement propres à chaque univers et à ses acteurs – qu'il s'agisse de la police, de l'armée ou des communications – sont donc à considérer comme plus importants que les technologies elles-mêmes. En d'autres termes, ce ne sont pas les technologies informatiques qui jouent un rôle en elles-mêmes, mais plutôt l'entrée des informaticiens dans les milieux du renseignement et la manière dont ils formulent les problèmes par rapport à la technologie. »

– Félix Tréguer, dans « Seeing like big tech: Security assemblages, technology, and the future of state bureaucracy » [TRÉ 19] dépeint le pouvoir croissant des entreprises privées en raison de leur maîtrise sur les données. Pour exercer un pouvoir sur un monde numérisé, l'État doit penser comme l'industrie des Big Data, et s'adapter à ses logiques, se les approprier, au-delà d'un simple partenariat public-privé et des traditionnelles compositions visant à réguler les réseaux de télécommunications ;

– le rapport rédigé par Sébastien-Yves Laurent et Maxime Kheloufi [LAU 18] propose une analyse juridique qui s'intéresse à deux catégories de normes s'appliquant aux échanges de communications individuelles, que sont le « secret des correspondances » (SC) et la « protection des données personnelles » (PDP). La première a été selon les auteurs remplacée par la seconde dans notre univers cybernétisé. Ils concluent qu'en dépit de l'adaptation des législations pour une meilleure protection des données personnelles, « les États n'ont pas atténué leur droit à exercer de la surveillance numérique » ;

– dans « Les gouvernances mondiales fragmentées de l'Internet » [LAU 19], il est question de l'enjeu plus global de gouvernance d'Internet. Ce pouvoir sur Internet, ses infrastructures réseau, ses applications, l'organisation de son architecture, la place des États et le partage des responsabilités avec le secteur privé, la possibilité d'imposer ses règles du jeu, décide notamment du pouvoir sur les données, leur flux, et des possibilités en matière d'interception et de mainmise sur les communications planétaires.

L'ouvrage de Joseph Fitsanakis

Depuis le XIX^e^ siècle, les gouvernements ont toujours fait en sorte de s'assurer un accès aux communications des usagers, légitimé par la lutte contre le crime et des impératifs de sécurité nationale. Ce qu'ils firent sans rencontrer de véritable résistance de la part des opérateurs de télécommunications. Dans les années 1930, l'arrivée du téléphone ne changea guère cette situation, nombreux étant les États ayant nationalisé leurs systèmes de téléphonie, considérés comme sensibles, au même titre que

l'armée ou la police. Les États-Unis faisaient exception, le téléphone étant privatisé, mais l'État exerçait sur lui un contrôle strict. De ces périodes de l'histoire date la relation de coopération étroite entre les entreprises de télécommunication et l'État (ses polices, ses agences de renseignement). Mais dans les années 1980, deux facteurs viennent perturber cet équilibre. La numérisation tout d'abord révolutionne le secteur des télécommunications, en autorisant techniquement la création d'un ensemble large de nouveaux services, pouvant être vus comme autant d'obstacles aux capacités d'interception étatiques. Puis un facteur de nature politique menace ces capacités, à savoir la dérégulation du marché et la privatisation des entreprises du secteur des télécommunications (durant le mandat de D. Reagan aux États-Unis, et de M. Thatcher au Royaume-Uni), ce qui se traduit par la fin du monopole d'AT&T en 1984 (États-Unis) et la privatisation d'une partie de British Telecom en 1984 (Royaume-Uni), une fragmentation du marché et une augmentation du nombre potentiel d'interlocuteurs pour l'État. Les interactions entre agences de sécurité étatiques et secteur privé deviennent plus complexes.

La transition technologique impose donc une évolution rapide des moyens d'interception et pour les gouvernements, il s'agit de garantir la possibilité de les réaliser. Ils ont poursuivi cet objectif par les régulations afin de limiter les moyens techniques des réseaux qui favorisaient la sécurité de l'information. C'est à cette fin que les gouvernements votent la Calea (1994, États-Unis) et la Ripa (2000, Royaume-Uni). Dans les deux cas, la principale mesure consiste à imposer aux opérateurs de téléphonie l'adaptation de leurs systèmes et technologies aux besoins d'interception de l'État. Ces lois ne définissent pas des normes techniques ni des critères spécifiques, mais posent simplement le principe de l'obligation.

L'ouvrage propose également un état de la littérature en remontant aux années 1960, aux États-Unis et au Royaume-Uni. Des travaux qu'il recense, on retiendra quelques idées fortes : on y relève que les opérateurs de télécommunication répondent sans résistance aux demandes de la police en matière d'interceptions [DAS 59] ; on y dénonce les pratiques d'un gouvernement américain intrusif, exerçant une surveillance sur les citoyens en recourant à des moyens illicites (on est alors dans les années 1970) ; s'installe alors une défiance vis-à-vis des gouvernements et des autorités de sécurité, les données officielles sur les interceptions sont mises en doute, les renseignements sont suspectés de cacher la réalité de leurs pratiques pour échapper à leurs responsabilités. À partir du scandale du Watergate, la critique de l'État se fait plus appuyée. Les interceptions sont l'une des pratiques les plus importantes pour les appareils de sécurité occidentaux, au point de les voir assumer les utilisations hors-la-loi, les excès étant facilités par la relation étroite, intime, entre agences de sécurité ou de renseignement et opérateurs.

L'auteur rappelle utilement la taxonomie des interceptions qui avait été proposée au Royaume-Uni dans le rapport du groupe d'expert « Smith Group 2000 » [SMI 00] et qui distingue trois types d'interception :

– active : désigne une interception logicielle, configurée par du personnel du fournisseur internet (ISP) et qui est applicable par exemple à la surveillance des courriers électroniques. Les courriels ciblés sont copiés et envoyés à un serveur des autorités ;

– semi-active : une unité de collecte est placée dans les locaux de l'agence de renseignement (le GCHQ), connectée au réseau. Les communications des personnes sous surveillance sont routées *via* l'unité de collecte ; des adresses IP présélectionnées sont attribuées aux personnes placées sous surveillance ;

– passive : une unité de collecte des données est connectée au réseau. Mais dans cette configuration, l'unité surveille le trafic en permanence. Les agences de l'État doivent ici fournir, installer, maintenir les matériels et logiciels, et l'unité peut intercepter sans informer le fournisseur.

Dans les modèles semi-passif et actif, les systèmes font partie intégrante des réseaux de télécommunications.

L'évolution importante en termes de pratiques d'interception réside dans le transfert de la charge de l'interception vers l'industriel. Désormais, contrairement aux pratiques qui prévalaient jusqu'alors, les opérations d'interception sont mises en œuvre par les opérateurs.

L'essentiel des publications sur les interceptions se concentre sur les pratiques et leurs dimensions juridiques et politiques. Peu de travaux, si ce n'est une littérature technique spécialisée (informatique, télécommunications), s'attardent sur les technologies d'interception elles-mêmes, ce qu'elles permettent concrètement de réaliser, la manière dont elles fonctionnent, mais aussi la manière dont elles sont conçues et par qui (chercheurs, ingénieurs, industriels, hackers, etc.), comment et par qui elles sont diffusées (entreprises, marchés, clients), et les effets qu'elles produisent sur les plans tactiques, stratégiques, politiques, et plus généralement en termes de pouvoirs.

Dans un article publié en 2018, Akin Unver [UNV 18] explore les enjeux que soulève la surveillance numérique dans les démocraties et les autocraties, ainsi que les mécanismes qui caractérisent le complexe industriel de surveillance (en anglais SIC, *surveillance-industrial complex*). La place de la technologie, et plus précisément de la course technologique, est au centre de son analyse politique du dilemme surveillance-protection de la vie privée. Il estime que ce ne sont pas tant les intentions qui rendent la surveillance problématique que son modèle économique. Si les débats centrés sur les enjeux de l'opposition entre sécurité et protection de la vie

privée ne sont pas tout à fait nouveaux, les termes ont radicalement changé du fait de l'évolution de l'environnement technologique, mais aussi politique puisqu'il place cette transition au 11 septembre 2001 :

> « L'évolution rapide des technologies de connexion crée un système où les informations personnelles numérisées et les données officielles ont désormais de multiples points d'accès, ne peuvent pas être supprimées de manière fiable, n'expirent pas et peuvent être diffusées sur des plates-formes numériques à un rythme infini et à une vitesse vertigineuse. » [UNV 18]

Akin Unver distingue deux catégories de techniques ou pratiques : celles qui sont organisées sur la base des technologies de surveillance d'une part, et celles de contournement de la surveillance. Ces technologies évoluent de concert et équilibrent le rapport de force : « La technologie elle-même est neutre et prend en charge de façon comparable tout l'éventail » [UNV 18].

Si le complexe SIC renvoie par analogie à la notion de « complexe militaro-industriel », sa nature en est cependant différente. Car dans le SIC, la relation n'est plus fondée sur un bénéfice mutuel, mais plutôt sur une logique de contrainte dont le type de « complexe » n'est d'ailleurs plus spécifique à la seule politique américaine. L'État serait la partie dominante : ses agences de renseignement collectent les données qui sont sur des bases de données ou des systèmes de communication appartenant au secteur privé ; les agences tirent avantage des technologies qui évoluent sans cesse offrant ainsi les moyens de dépasser les cadres juridiques contraignants ; elles font supporter aux entreprises privées le coût politique et économique de la surveillance.

Le prisme historique aide à comprendre la nature des évolutions technologiques et de leurs applications. Nous serons plus particulièrement attentifs aux formes de pouvoirs que permettent de construire, entretenir, renforcer ou affaiblir les technologies d'interception utilisées dans leurs multiples contextes.

Les questions traitées dans cet ouvrage

Cet ouvrage est organisé comme suit :

– un premier chapitre décline les multiples contextes dans lesquels ont pris et continuent de prendre place les interceptions de communications. Mises en œuvre par les belligérants au cours des guerres d'hier à aujourd'hui, leur utilité ne s'est jamais démentie, essentielle au renseignement, fournissant des informations-clés aux niveaux tactiques, opérationnels et stratégiques, orientant des décisions politiques et

militaires. Mais les interceptions sont aussi au service du pouvoir politique, au service du prince, qui espionne les diplomates mais aussi ses proches ou ses adversaires politiques, pour mieux asseoir son pouvoir par la maîtrise du secret. Les interceptions sont aussi l'un des instruments de la lutte policière contre le crime. Les services de renseignement en usent bien sûr. Et les États n'hésitent pas à s'en servir pour surveiller et contrôler. Les cadres d'utilisation sont multiples. Les évolutions technologiques dans le domaine des communications ont introduit de nouvelles modalités auxquelles les techniques d'interception ont dû s'adapter ;

– le deuxième chapitre se focalise sur les enjeux du chiffrement. De multiples techniques, méthodes et technologies d'interception existent aujourd'hui, qui permettent de (pratiquement) tout intercepter. Les catalogues des entreprises commercialisant des technologies d'interception le laissent du moins penser. Le chiffrement des communications apparaît donc comme l'un des moyens – si ce n'est le seul ? – de protection des contenus des communications. Mais ceux qui s'efforcent d'intercepter, quelles que soient leurs motivations, entendent bien contourner l'obstacle du chiffrement. Si la cryptographie n'est pas infaillible (les systèmes de chiffrement peuvent simplement être mal implémentés), des méthodes permettent de le fragiliser (les *backdoors* en particulier), d'autres de le contourner. Le chiffrement est un enjeu politique, autour duquel se cristallisent les débats sur la souveraineté des États. La libéralisation de la cryptographie entamée dans les années 1990 est venue mettre à mal ce pouvoir de contrôle absolu des États sur ce qui était alors une « arme » de guerre, avant de devenir un outil accessible à tous, bien plus difficilement contrôlable. Les États, bien sûr, n'ont pas rendu les armes et si les interceptions des communications planétaires telles que les réalise la NSA par exemple semblent ne viser que les métadonnées et non les contenus directement, ces derniers conservent toute leur valeur stratégique. La manière d'y accéder en dépit des obstacles cryptographiques est un défi permanent ;

– le dernier chapitre fait du « pouvoir » son objet et analyse les relations qui ont pris forme entre les divers acteurs intervenant sur la technologie de l'interception, de sa création, conception, commercialisation, à son utilisation. Les relations entre citoyens, chercheurs, concepteurs des technologies, entreprises, États sont analysées. Nous traiterons ainsi de la relation particulière qui s'est nouée entre l'État et l'entreprise, oscillant entre contrainte et coopération ; des limites du contrôle des technologies (et donc du contrôle par les technologies) voulu par les États ; mais aussi de la fragilité des bases sur lesquelles s'appuie le pouvoir construit sur la confiance dans le chiffrement.