La condamnation relative des mesures de surveillances massives étatiques : une occasion manquée par la Cour européenne des droits de l'Homme

Olivia Tambou

Citation suggérée : Olivia Tambou, **La condamnation relative des mesures de surveillances massives étatiques : une occasion manquée par la Cour européenne des droits de l'Homme,** *Blogdroiteuropeen Working Paper 4/2021*, juin 2021, Accessible à https://wp.me/p6OBGR-4au

La condamnation relative des mesures de surveillances massives étatiques : une occasion manquée par la Cour européenne des droits de l'Homme,

Olivia Tambou, Maître de Conférences, HdR à l'Université Paris-Dauphine, PSL, External Scientific Fellow au Max Planck Institute du Luxembourg,

Sommaire :

Après la CJUE[1], la Grande chambre de la Cour Européenne des Droits de l'Homme vient de rendre deux arrêts importants condamnant des mesures surveillance massives étatiques. Ces affaires ont été introduites à la suite des révélations faites par Edward Snowden en 2013. La première[2] met à jour trois pratiques des services de renseignements britanniques mises en œuvre pour des raisons de sécurité nationale : les interceptions en masse de communications, l'échange de renseignements avec la NSA, et l'accès aux données des fournisseurs de services internet. La seconde affaire[3] concerne uniquement le régime des interceptions de masse suédois. Dans ces arrêts la CEDH élabore pour la première fois une grille d'analyse pour examiner la conformité des interceptions massives secrètes afin d'offrir une protection contre l'arbitraire et les risques d'abus. Dans l'affaire britannique, la Cour dénonce l'absence d'autorisation indépendante de ces interceptions, l'absence de précisions des catégories de données traitées ainsi que l'absence d'autorisation interne préalable des sélecteurs liés à un individu. Ces lacunes fondamentales entraînent une violation de l'article 8 de la CEDH qui garantit à chacun le droit à la vie privée. L'exigence de « la qualité de la loi » condition préalable pour s'assurer que l'ingérence dans la vie privée est « nécessaire dans une société démocratique », n'est pas

[1] CJUE, 6 octobre 2020, *La Quadrature du Net*, aff. Jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791
[2] CEDH 25 mai 2021, *Big Brother Watch et autres c. Royaume Uni*, Requêtes nos 58170/13, 62322/14 et 24960/15
[3] CEDH 25 mai 202, *Centrum för Rättvisa c. Suède*, Requête no 35252/08

remplie. Il en résulte également une violation de la liberté d'expression des journalistes qui ont été victimes de ces programmes de surveillance. La Cour constate aussi que le régime de transmissions des données par les fournisseurs de service de communication est contraire aux articles l'article 8 et 10 CEDH car il n'était pas prévu par la loi. En revanche, la Cour estime que l'encadrement légal des échanges de renseignements avec la NSA est conforme aux articles article 8 et 10 de la CEDH. Dans la seconde affaire concernant le renseignement suédois, la Cour constate également une violation de l'article 8 de la CEDH. Elle invoque trois carences : l'absence de règle claire concernant la destruction des éléments interceptés, l'absence d'obligation de prendre en compte les intérêts liés à la vie privée en cas de partage de renseignements avec des partenaires étrangers, et enfin l'absence de contrôle *a posteriori* effectif.

La lecture de ces deux arrêts fleuve permet de comprendre pourquoi aujourd'hui la surveillance étatique de masse fait débat, comment finalement la Cour européenne au-delà de la condamnation des régimes en l'espèce accepte en réalité le principe même de ces mesures de surveillance tout en exigeant la présence de garanties minimales. La Cour Européenne des droits de l'Homme aura manqué une occasion d'affirmer l'effectivité du droit à la protection de la vie privée face aux pressions des États.

I- La surveillance étatique de masse : un débat ancien d'une actualité renouvelée

Il s'agit d'une déclinaison technologique du débat ancien entre la nécessité d'assurer un équilibre entre les libertés et la sécurité dans une société démocratique. Or, la guerre contre le terrorisme, le développement des menaces considérées comme réelles contre la sécurité nationale des États ont légitimé le développement de régimes nationaux permettant des interceptions de masse. Pour ceux qui ne sont pas au fait de ce débat, ces affaires présentent trois intérêts. Le premier est la volonté biaisée[4] de la Cour de quantifier cette réalité. « Sept États du Conseil de l'Europe (Allemagne, Finlande, France, les Pays-Bas, le Royaume-Uni, la Suède et la Suisse) ont officiellement mis en place des régimes d'interception de communications en masse acheminées par câble et/ou voie aérienne. »[5] La Cour relève également que trente-neuf, États membres au moins ont conclu des accords de partage de renseignements[6].

Le second intérêt est de concrétiser ce que l'on entend par surveillance étatique massive, en particulier les interceptions de masse qui repose selon la Cour sur un processus en quatre étapes:

(a) « interception et rétention initiale des communications et des données de communication associées (c'est-à-dire des données de trafic qui se rapportent aux communications interceptées) ;
(b) application de sélecteurs spécifiques aux communications retenues et aux données de communication associées ;

[4] L'interception de masse non ciblée serait expressément ou implicitement interdite dans vingt-trois états européens selon opinion séparée du juge Pinto de Albuquerque, point 11.
[5] Cf. point 242 et s. aff. Big Brother Watch
[6] Cf. point 245, aff. Big Brother Watch

(c) examen par des analystes des communications sélectionnées et des données de communication associées ; et
(d) rétention subséquente des données et utilisation du « produit final », notamment partage de ces données avec des tiers »[7]

La Cour analyse aussi en quoi l'interception de masse se distingue des interceptions ciblées, abordée dans sa jurisprudence antérieure[8]. D'une part, les interceptions de masse incluent nécessairement des communications internationales c'est-à-dire en provenance ou sortant du territoire national. Autrement dit des transferts de données vers les pays tiers sont en cause. Cela pose nécessairement la question du niveau de garanties applicables aussi dans l'État tiers par rapport à celui existant en Europe. D'autre part, le but des interceptions de masse est d'emblée plus préventif. Les interceptions ciblées interviennent souvent dans le cadre d'une enquête pénale, dans le but de recherche des éléments de preuve auprès d'individus déterminés. Les interceptions de masse ont souvent un but plus préventif de détection précoce de menaces contre la sécurité nationale, de lutte contre le terrorisme. Enfin, la Cour clarifie que l'interception de masse n'exclut pas un certain ciblage. Elle peut servir à filtrer l'ensemble des communications d'individus sur la base de sélecteurs (mots, clefs, localisation, courrier électronique etc.)

Le troisième intérêt est de rappeler les arguments en présence. Pour les uns, c'est le principe même de la surveillance étatique de masse qui devrait être interdit. La collecte et l'analyse des données de personnes sur lesquels ne pèsent aucun soupçon est en soit disproportionnée[9]. L'importance du volume de données collectées, ainsi que la variété de leur nature, constitue une ingérence particulièrement grave dans la vie privée ayant un effet dissuasif sur d'autres droits tels que la liberté d'expression, d'association.[10] Pour les États, la possibilité de recourir à des mesures de surveillance massive est d'une importance cruciale pour la défense de leur sécurité nationale. D'une part, les États remettent en cause le caractère plus intrusif pour la vie privée de la surveillance massive par rapport à la surveillance ciblée qui permet de collecter les données relatives à un individu précis[11]. Ils revendiquent une importante marge d'appréciation en la matière puisqu'il en va de la sauvegarde de leur État et la défense de leur sécurité nationale. D'autre part, ils invoquent l'utilité de ces mesures qui sont susceptibles de leur permettre de répondre promptement et efficacement à des projets d'attentats, de cyberattaques ou de nouvelles menaces[12] et donc de sauver des vies.

II- L'acceptation de principe des mesures de surveillance étatique par la Cour européenne des droits de l'homme

[7] Cf. point 325, aff. Big Brother Watch.
[8] Il s'agit notamment de la décision Weber et Saravia c. Allemagne, n°54934/00, CEDH 2006-XI, ainsi que de l'arrêt Liberty et autres c. Royaume-Uni, no 58243/00, 1er juillet 2008.
[9] cf. point 316 intervention de l'ONG article 19, dans l'affaire Big Brother Watch.
[10] Cf. point 318, intervention de l'ONG Open Society Justice Initiative (OSJI), dans l'affaire Big Brother Watch
[11] Cf. point 288 observation du gouvernement britannique ou encore point 300, relative à l'intervention de la France, dans l'affaire Big Brother Watch.
[12] Cf. point 303 et s. intervention du gouvernement du Pays-Bas, ou encore point 308 : intervention du Royaume de Norvège, dans l'affaire Big Brother Watch.

La Cour européenne des droits de l'homme admet « l'importance vitale »[13] des mesures de surveillance étatique massive pour détecter les menaces contre leur sécurité nationale. Elle souligne que les États membres jouissent d'une ample marge de manœuvre pour apprécier le type de régime d'interception de masse qu'ils souhaitent. Elle considère que les interceptions de masse ne sont pas en principe contraire à l'article 8 de la CEDH pour protéger pour « leur sécurité nationale ou d'autre intérêts essentiels contre des menaces graves… »[14]. Sans chercher à imposer un modèle idéal, la Cour adopte une position de compromis en exigeant que des garanties soient prises par les États membres.

Mais surtout, la Cour ne tranche pas clairement la question de savoir si la surveillance de masse est plus dangereuse que la surveillance ciblée d'un individu. Son approche globale des interceptions de masse est à cet égard révélatrice. Elle affirme que ces mesures reposent sur un processus graduel avec des ingérences susceptibles d'augmenter au fur et à mesure. Il est difficile d'accepter que la première étape du processus que constitue l'interception de paquets de communication indifférenciée incluant les données dites de connexion constitue une ingérence moindre, ou du moins anodine[15]. On pourrait y voir à demi-mot la reprise d'une autre distinction classique entre les données dites de connexion ou métadonnées[16] et les données de contenus. Or, les données connexion peuvent renseigner de manière très précise et intrusive la vie privée d'un individu. D'ailleurs, la Cour dans un autre passage ne se dit pas convaincue sur le caractère moins intrusif de l'acquisition de données de communications par rapport celle des données de contenus[17]. Preuve s'il en était que la position de la Cour manque de cohérence et de précisions[18]. Au final, on ne peut que souscrire à l'appréciation générale des juges Lemmes, Vehabovic et Bosjak qui considèrent que la Cour a manqué une « excellente occasion d'affirmer pleinement l'importance du droit au respect de la vie privée et de la correspondance face aux ingérences découlant de la surveillance de masse. » On mesure ici toute la différence avec la position récente de la CJUE comme nous le verrons plus en détails dans le point IV. Dans son arrêt précité *La Quadrature du Net,* la CJUE affirme clairement une interdiction de principe de la surveillance de masse, pour ne l'accepter qu'à titre exceptionnel avec des conditions strictes[19]. C'est d'ailleurs ce qui explique que la position de la CJUE ait été tant critiquée par la France au point de demander vainement au Conseil d'Etat de ne pas la suivre[20].

[13] Point. 424 dans l'affaire Big Brother Watch et point 365 de l'affaire suédoise.
[14] Cf. point 347 dans l'affaire Big Brother Watch
[15] En ce sens cf. l'opinion communes concordantes des juges les juges Lemmens, Vehabovic et Bosnjak. point 11 et s. dans l'affaire Big Brother Watch
[16] Les données de connexion sont ainsi les numéros de téléphones appelés, appelants, l'heure de l'envoi d'un message, ou d'un email, les adresses IP utilisées, la géolocalisation etc.
[17] Cf. point 363 et s. ddans l'affaire Big Brother Watch
[18] Cf. pour de nombreuses illustrations l'éloquente opinion du juge Pinto d'Albuquerque dans l'affaire Big Brother Watch
[19] Cf. notre commentaire, A la recherche d'un régime cohérent de protection des données personnelles contre les mesures de surveillance étatique, *AFDI* 2021, à paraître.
[20] Cf. Jacques Ziller, Le Conseil d'État se refuse à emboiter le pas au joueur de flûte de Karlsruhe, *blogdroiteuropéen* 23 avril 2021, https://blogdroiteuropeen.com/2021/04/23/le-conseil-detat-se-refuse-demboiter-le-pas-au-joueur-de-flute-de-karlsruhe-par-jacques-ziller/

III- Les garanties « de bout à bout » exigées des régimes de surveillance étatique massive

Selon l'approche globale adoptée par la Cour, le processus d'interception de masse doit être encadré par « des garanties de bout en bout »[21], c'est à dire que la nécessité et la proportionnalité des mesures prises doivent être appréciées à chaque étape à l'échelle nationale. Le contrôle de la Cour vise alors à vérifier que l'État a bien agit dans les limites de sa marge d'appréciation en vérifiant si « le cadre juridique national définit clairement :

1. Les motifs pour lesquels l'interception en masse peut être autorisée ;
2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;
3. La procédure d'octroi d'une autorisation ;
4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;
6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;
7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement;
8. Les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement. »[22]

La Cour applique ensuite cette grille pour aboutir à la conclusion que tant le régime de surveillance britannique que celui de la Suède violent la CEDH, même si les motifs ne sont pas les mêmes.

A- Les garanties violées par le régime de surveillance britannique

Dans son arrêt Big Brother Watch, la Cour examine l'article 8§4 de la RIPA (Regulation of Investigatory Powers Act 2000) qui autorise le Ministère compétent à émettre un mandat aux fins d'interception de communications extérieures au cours de leur transmission par un système de télécommunication au regard de la grille évoquée ci-dessus. Le fait que seul le Ministre soit habilité à délivrer un tel mandat et non un organe indépendant de l'exécutif constitue une violation de la troisième garantie susmentionnée. Autrement dit, la seule présence d'un contrôle interne visant à vérifier que les conditions pour la réalisation des interceptions étaient bien suivies par le Ministre n'est pas suffisante. Ainsi, il manquait au régime britannique une garantie fondamentale : l'autorisation par une organe indépendant de l'exécutif[23]. La Cour a jugé que cela été particulièrement problématique dans la mesure où il n'existait aucune supervision des catégories de sélecteurs au stade de l'autorisation, de manière à vérifier leur nécessité et leur proportionnalité[24]. En outre, le certificat ministériel délivré en même temps que le mandat pour vérifier *a posteriori* que les éléments interceptés restaient bien dans le cadre

[21] Cf. point 350 dans l'affaire Big Brother Watch.
[22] Cf. point 361 dans l'affaire Big Brother Watch.
[23] Cf. point 377 dans l'affaire Big Brother Watch.
[24] Cf. point 381 et s. dans l'affaire Big Brother Watch.

de ce qui était prévu par la loi, était rédigé dans des termes trop généraux[25]. Le régime des données de communication associées (métadonnées) pour partie identique à celui du contenu des communications souffrait des mêmes carences[26]. En outre, la Cour émet une réserve concernant l'absence de précision concernant les durées de conservation de ces données de communication associées. La Cour a jugé à juste titre qu'une telle lacune ne permettait pas de répondre à l'exigence de prévisibilité posée par l'article 8 de la CEDH[27].

Logiquement la Cour considère que la mise en place de ce régime d'interception permettait aux services de renseignement d'accéder à « des éléments journalistiques confidentiels de manière intentionnelle, en utilisant délibérément des sélecteurs ou des termes de recherche liés à un journaliste ou à un organe de presse, ou de manière fortuite, en prenant accidentellement de tels éléments dans les « filets » d'une interception en masse »[28]. Une telle ingérence « est comparable à celle qui résulterait d'une perquisition au domicile ou sur le lieu de travail d'un journaliste »[29]. Elle considère que de telles mesures ne pourraient être possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures sont « justifiées par un impératif prépondérant d'intérêt public ».[30] L'absence de garde-fous permettant de limiter les possibilités de risques que les interceptions contiennent des éléments journalistiques confidentiels entraîne une violation de l'article 10 de la CEDH.

Enfin, la Cour condamne le fait qu'au moment des faits, l'acquisition de données de communication auprès des fournisseurs de services de communication n'était pas prévu par une loi. Ce point a été admis par le gouvernement britannique, une loi étant en cours d'adoption. Cela explique que cette violation de l'article 8 de la CEDH n'a pas fait l'objet de longs développements.

Pour le reste, la Cour valide la présence de garanties suffisantes dans le régime britannique de façon parfois assez généreuse. Ainsi, la Cour admet d'une manière générale que l'article 8§4 RIPA manque de clarté. Elle estime néanmoins que le code de conduite qui le complétait et qui avait été approuvé par le Parlement et rendu public rendait le droit interne suffisamment prévisible et accessible.[31] La Cour semble aussi céder à certains arguments des États. Elle accepte que tous les sélecteurs ne soient pas précisés dans l'autorisation préalable ou encore que le contrôle judiciaire s'arrête à la phase initiale du processus d'interception et ne vise pas l'application de sélecteurs forts à des individus identifiables.[32] Elle considère que le transfert des données aux partenaires du réseau *Five Eyes* était réalisé selon des garanties propres à « prévenir tout abus ou ingérence disproportionnée »[33] en se fondant sur le code de conduite déjà mentionné. Elle valide également l'échange de renseignements avec les services de

[25] Cf. point 386 dans l'affaire Big Brother Watch.
[26] Cf. point 416 dans l'affaire Big Brother Watch.
[27] Cf. point 423 dans l'affaire Big Brother Watch.
[28] Cf. point 447 dans l'affaire Big Brother Watch.
[29] Cf. point 448 dans l'affaire Big Brother Watch.
[30] Cf. point 450 dans l'affaire Big Brother Watch.
[31] Cf. point 366 et s. dans l'affaire Big Brother Watch.
[32] Cf. par exemple point 353 et s. dans l'affaire Big Brother Watch.
[33] Cf. point 395 et s.

renseignement étrangers tels que la NSA[34]. Une telle approche diffère encore une fois des critiques retenues par la CJUE dans les affaires *Schrems*[35]. Il s'agit sans doute d'une illustration des garanties limitées que peut apporter la Cour Européenne des Droit de l'Homme en raison de l'absence d'un droit fondamental à la protection des données à caractère personnel dans la CEDH. Mais on peut aussi considérer que la Cour ne va pas assez loin dans la protection du droit à la vie privée. C'est d'ailleurs le principal reproche fait par les juges ayant fait des opinions séparées y compris concordantes.

B- Les garanties violées dans le régime suédois de surveillance

Le régime suédois offrait un contrôle juridictionnel en amont des demandes d'autorisation d'interception très entendu. Le juge était à même de vérifier de façon précise les missions les canaux de transmission les catégories de sélecteurs et ainsi d'une manière globale la régularité des activités secrètes d'interception[36]. En revanche, la Cour a constaté une violation de l'article 8 de la CEDH en l'absence de précautions suffisantes pour la communication des données à d'autres parties, (autrement dit le point 5 de sa grille d'analyse précitée). En effet, « ni la loi relative au renseignement d'origine électromagnétique ni aucun autre texte n'impose de prendre en compte les intérêts liés à la vie privée de l'individu concerné au moment de décider de partager des renseignements ».[37] La Cour dénonce également l'absence d'« obligation juridiquement contraignante … d'analyser les garanties offertes par le destinataire étranger des renseignements afin de déterminer si elles sont d'un niveau minimum acceptable. »[38] Cette transmission mécanique constitue une carence portant gravement atteinte au droit au respect de la vie privée, au droit de la correspondance, qui n'apparaît pas contrebalancée par l'intérêt que ces données pourrait présenté pour le renseignement.

La Cour a aussi constaté que le régime suédois d'interception de masse ne comportait pas de règles claires concernant la destruction des éléments interceptés qui ne contenaient pas de données à caractère personnel, (violation point 6 de la grille précitée) [39]. En outre, le régime suédois comportait deux lacunes importantes dans son *contrôle a posteriori* (violation du point 8 de la grille précitée). D'une part, l'Inspection compétente pour superviser les activités de renseignement extérieur en Suède était aussi celle qui exerçait un contrôle a posteriori à la demande d'un particulier. Bien qu'indépendante, cette inspection pouvait être soupçonnée d'impartialité lorsqu'elle était invitée à contrôler ses propres activités de supervision à la demande d'un particulier [40]. D'autre part, dans le régime suédois les particuliers se trouvaient dans l'impossibilité d'obtenir des décisions motivées en réponse de leurs plaintes ou questionnements concernant l'interception de masse. La Cour a alors considéré qu'il s'agissait

[34] Cf. point 510.
[35] CJUE 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18 (affaire dite *Schrems 2*), *ECLI:EU:C:2020:559*
[36] Cf. point 302.
[37] Cf. point 330.
[38] Cf. point 371.
[39] Cf. point 342.
[40] Cf. point 359.

là d'une « carence particulièrement significative » [41], n'apportant pas de garanties contre les usages abusifs et constituant une violation de l'article 8 de la CEDH.

Ainsi la Cour a jugé que « le régime suédois d'interception en masse, considéré dans son ensemble, ne contenait pas de « garanties de bout en bout » suffisantes pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus. »[42]

IV- Les mots de la fin… en attendant les prochains épisodes

L'arrêt Big Brother Watch de la Cour européenne des Droits de l'homme laisse le lecteur sur sa faim. D'une part, il ne dit rien sur la conformité actuelle du régime britannique de surveillance fondé sur la sulfureuse « Snoopers' Charter »[43] (charte fouineuse). La Cour a d'ailleurs été saisie à ce sujet. Il reste à espérer que ces nouvelles affaires lui fournissent l'occasion de mieux asseoir sa doctrine. D'autre part, cette affaire révèle que l'encadrement britannique des mesures de surveillance massive étatique devrait aussi être un point sensible pour l'encadrement des transferts de donnée à caractère personnel entre l'UE et le Royaume-Uni[44]. Dans ce cadre la différence d'approche entre la Cour européenne des droits de l'Homme et la CJUE pourrait avoir un impact non négligeable. Dans son arrêt *La Quadrature du Net*, la Cour a confirmé son interdiction de principe des traitements de surveillance généralisée et indifférenciée à des fins sécuritaire tout en acceptant que certains traitements très intrusifs à des fins de sécurité nationale[45]. De son côté la Cour Européenne des droits de l'Homme semble accepter par principe de tels traitements de surveillance généralisée et indifférenciée à des fins de sécurité nationale en exigeant des garanties de bout en bout. Au-delà de l'approche, le degré des garanties exigées dans les deux ordres est différent. Ainsi, la CJUE exige trois garanties pour les mesures de conservation généralisée et indifférenciée des données à des fins de protection de la sécurité nationale[46]. D'une part, de telles mesures ne sont acceptées qu'en cas de menace grave pour la sécurité nationale, notion strictement définie[47]. D'autre part, la menace doit être réelle, actuelle et prévisible. Les États membres doivent donc invoquer des circonstances concrètes qui justifient de telles mesures. Enfin, de telles mesures de surveillance généralisée doivent être temporairement limitées au strict nécessaire pour un laps de temps qui doit être établi préalablement. Ce délai ne peut être renouvelé que si la gravité de la situation persiste. La CJUE a donc établi des garanties particulières pouvant à titre exceptionnel justifier

[41] Cf. point 364.
[42] Cf. point 373.
[43] L'affaire britannique est fondée sur le *Regulation of Investigatory Powers Act 2000*, dont les dispositions ont été modifiées par le *Investigatory Powers Act 2016*, appelé aussi *Snoopers' Charter*.
[44] Cf. European Data protection Board, Opinion 14/2021 regarding the European Commission Draft implementing decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, adopted on 13 April 2021, sp.p. 35 et s., https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en
[45] CJUE Voir notre commentaire A la recherche d'un régime cohérent de protection des données personnelles contre les mesures de surveillance étatique, à paraître à la chronique de droit de l'UE, *AFDI 2021*.
[46] Cf. Points 138 aff. jointes C-511/18, C-512/18, C-520/19.
[47] Selon la CJUE la sécurité nationale « correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme. » Point 135, aff. jointes C-511/18, C-512/18, C-520/19.

des traitements de surveillance massive étatique à des fins de sécurité nationale. Ces garanties s'ajoutent aux garanties essentielles[48] qui sont similaires à celles édictées par la Cour Européenne des Droits de l'Homme.

Enfin, l'actualité atteste jour après jour de l'appétence des États européens pour maintenir des mesures de surveillance étatique généralisée à des fins sécuritaires[49]. En France, l'exigence de garantie de bout en bout consacrée par la Cour Européenne des Droits de l'Homme devrait aboutir à l'adoption d'un cadre plus conforme en matière de coopération avec les services étrangers. Actuellement, les garanties exigées pour le traitement des renseignements recueillis en cas d'échange de données avec un service allié ne sont pas conformes à la règle dite du « tiers service ». Cette règle interdit à une agence ayant reçu des renseignements d'un service allié étranger de les communiquer à un tiers sans l'accord de ce service[50]. Ainsi, l'encadrement juridique des mesures de surveillance étatique est devenu un véritable serpent de mer qui laisse prédire que de nouveaux épisodes sont encore à venir, tant à l'échelle nationale, qu'européenne.

[48] Sur ces garanties essentielles cf. également la position du Comité Européen de la Protection des Données, recommandations 2/220 sur les garanties essentielles pour les mesures de surveillance, adoptées le 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr

[49] En France, avec le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, ce sont quatre lois qui ont été adoptées en la matière depuis le début du quinquennat, et la neuvième depuis 2012.

[50] En ce sens cf. Jacques Follorou, Renseignement : la France priée de se mettre en règle avec le droit européen, *Le Monde*, 12 juin 2021.