La Cour Européenne des Droits de l'Homme procède à une condamnation en demi-teinte de la surveillance “de masse”.

Jean-Philippe Foegle

Édition électronique

URL : <http://journals.openedition.org/revdh/4865>

DOI : 10.4000/revdh.4865

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Jean-Philippe Foegle, « La Cour Européenne des Droits de l'Homme procède à une condamnation en demi-teinte de la surveillance “de masse”. », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 26 octobre 2018, consulté le 06 mai 2019. URL : <http://journals.openedition.org/revdh/4865> ; DOI : 10.4000/revdh.4865

Ce document a été généré automatiquement le 6 mai 2019.

Tous droits réservés

La Cour Européenne des Droits de l'Homme procède à une condamnation en demi-teinte de la surveillance “de masse”.

Jean-Philippe Foegle

- 1 A l'instar de la chanteuse Gala, la Cour Européenne des Droits de l'Homme s'est, dans son arrêt *Big Brother Watch*, libérée de tout désir... De procéder à un renforcement de la prohibition de la surveillance de masse qui semblait partiellement esquissée par la saga des arrêts *Zakharov et Szabo*¹ de 2015 et 2016.
- 2 L'affaire concernait des recours intentés par des journalistes et des organisations de défense des droits de l'homme contre trois régimes de surveillance existant au Royaume-Uni - et dont les abus ont été mis en lumière par les révélations d'Edward Snowden, prévoyant respectivement une interception massive des communications ; le partage de renseignements avec des gouvernements étrangers; et, enfin, l'obtention de données de communication auprès de fournisseurs de services de communication.
- 3 Par un jugement de 212 pages, particulièrement aride et technique, la Cour procède à une condamnation du système anglais de surveillance digitale sur le fondement du droit à la vie privée consacré par l'article 8 de la Convention .
- 4 . Toutefois, loin de condamner *in abstracto* la surveillance de masse, il apparaît que la Cour a essentiellement procédé à une normalisation de son usage dans nombre d'hypothèses, se satisfaisant de l'existence de garanties procédurales adéquates contre les abus, et de l'existence d'un contrôle présentant des garanties suffisantes d'indépendance.
- 5 La décision finale - qui ne semble avoir d'autre fonction que d'offrir aux états un ensemble de “bonnes pratiques” en matière de surveillance puisque le système en cause a été remplacé en 2016 par un système supposément moins intrusif - offre ainsi un tableau en clair-obscur de la position de la Cour sur la question de la surveillance digitale dite “de masse”.

- 6 D'une part, la Cour énonce que les programmes de surveillance institués par le défunt *Regulation of Investigatory Powers Act* Britanniques étaient contraires au droit à la vie privée consacré par l'article 8 de la Convention en raison – notamment – de l'absence de délimitation claire des catégories de données pouvant être collectées et de l'absence de contrôle indépendant des critères permettant de justifier cette collecte. D'autre part toutefois, celle-ci énonce également que les programmes de surveillance *de masse* ne constituent pas nécessairement en eux-mêmes une atteinte disproportionnée au droit à la vie privée, tout en neutralisant l'exigence d'un contrôle judiciaire préalable des mesures de surveillance digitale.
- 7 En **premier lieu**, réaffirmant dans la lignée des arrêts Zakharov et Szabo l'exigence de mise en place de garanties contre l'arbitraire lorsque des mesures de surveillance digitale sont mises en oeuvre, la Cour normalise par la même occasion le recours à la surveillance de masse en jugeant que le choix de recourir à celle-ci relève de la marge d'appréciation des états parties à la Convention.
- 8 Dans l'arrêt *Zakharov*, la Cour avait fait grief à une législation nationale de ne pas avoir énoncé avec suffisamment de précision les circonstances dans lesquelles les pouvoirs publics sont habilités à recourir aux mesures de surveillance digitale. Celle-ci avait notamment souligné que la législation russe de ne donnait aucune indication sur « les circonstances dans lesquelles les communications d'une personne peuvent être interceptées en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique [...] », ce qui conférait aux autorités une « latitude quasi illimitée » en la matière². Si l'arrêt *Zakharov* ne concernait *stricto-sensu* que des mesures de surveillance ciblées et ne portait pas sur le cas spécifique de l'interception de toutes les données à tout moment, celui-ci condamnait *a fortiori* ce type de surveillance, comme en témoigne l'affaire *Szabo*. Dans ce dernier arrêt, la Cour avait noté que la législation hongroise pouvait « potentiellement affecter tout le monde et, qu'à ce titre, elle peut être interprétée comme ouvrant la voie à la surveillance illimitée d'un grand nombre de citoyens »³.
- 9 Faisant application de ces principes, la Cour note en l'espèce (§340-347) que les critères de sélection des données à intercepter et les critères de filtrage ultérieur de celles-ci ne faisaient pas l'objet d'un contrôle adéquat, et ce en dépit de la circonstance que la nature des données collectées – données de connexion et métadonnées – pouvait conduire à révéler nombre d'aspects de la vie privée des personnes visées. En d'autres termes, les services de renseignement avaient la possibilité de déterminer eux-même, sans contrôle externe autre qu'un vague audit *a posteriori*, les critères permettant de sélectionner les catégories de données à collecter et ceux permettant de filtrer les données collectées. En conséquence, la Cour conclut à la violation par le Royaume-Uni de l'article 8 de la Convention en ce que la loi, qui ne prévoyait pas de délimitation claire de la nature des données pouvant faire l'objet d'une collecte et d'un traitement par les services de renseignement, n'atteignait pas un degré de précision suffisant pour remplir le critère - exigeant - de « qualité de la loi » consacré par la Convention.
- 10 Ayant ainsi réaffirmé la nécessité de mettre en place des garanties contre l'arbitraire - et notamment des garanties visant à limiter la quantité de données collectées au strict nécessaire - la Cour normalise toutefois le recours à surveillance dite “de masse” jugeant que celle-ci n'est pas nécessairement contraire à la Convention Européenne des Droits de l'Homme.

- 11 Rappelant la marge d'appréciation dont bénéficient les états en matière de choix des modalités de surveillance des personnes susceptibles de commettre des actes de nature terroriste ou criminelle, la Cour note que la difficulté d'identifier aisément les suspects sur internet offre aux Etats la possibilité, dans le cadre de leur marge d'appréciation, de mettre en place des régimes de surveillance "en masse" des communications sur internet pour remédier à ces difficultés. Dans ce cadre, la Cour juge déraisonnable d'exiger qu'une telle surveillance ait à être limitée aux personnes pouvant être « raisonnablement suspectées » de s'apprêter à commettre un acte de nature terroriste ou un crime, car une telle exigence ôterait au recours à cette mesure de surveillance tout intérêt opérationnel, dans la mesure où il s'agit précisément de procéder à une collecte indifférenciée de données en vue d'un traitement ultérieur de celles-ci. De manière similaire et surprenante au regard de l'arrêt Zakharov pré-cité⁴, la Cour juge que, dans le cadre des mesures de surveillance « de masse », les individus n'ont pas à recevoir notification a posteriori de l'existence d'une interception de leurs données personnelles. (§317)
- 12 Or, une telle position apparaît en contrariété avec le standard édicté par la Cour de Justice de l'Union Européenne dans son arrêt *Tele2*, dans lequel les juges avaient fait grief à la réglementation Suédoise de ne requérir aucune relation entre les données dont la conservation était prévue et l'existence menace pour la sécurité publique, et n'est pas limitée à une période temporelle et / ou une zone géographique ou à un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave (CJUE, Grande Chambre, 21 décembre 2016, *Tele2 Sverige AB et Secretary of State for the Home Department*, Aff. C-203/15 et C-698/15, §106). Voilà qui, comme le souligne Théodore Christakis, contribue à une fragmentation du droit européen encadrant la surveillance digitale.
- 13 D'une manière similaire, la Cour normalise l'échange international de données en masse, jugeant que celui-ci peut être compatible avec la Convention dès lors que la loi encadre de manière suffisamment précise et prévisible les hypothèses dans lesquelles ces données peuvent être partagées et consultées par les autorités nationales (§446-447).
- 14 **En second lieu**, la Cour réaffirme, dans la lignée de ses arrêts Zakharov et Szabo, la nécessité d'instaurer un contrôle indépendant des mesures de surveillance digitale.
- 15 Dans l'arrêt Zakharov précité, les juges du palais des droits de l'homme avaient précisé qu'il importe que l'organisme de contrôle soit suffisamment indépendant à l'égard de l'exécutif et dispose de tous les pouvoirs nécessaires s'assurer que l'interception des données présente un caractère de nécessité et de proportionnalité au regard des buts poursuivis « en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs »⁵. En outre, les pouvoirs de l'organe de contrôle relativement aux infractions qu'il peut déceler, constituent « un aspect important pour l'appréciation de l'effectivité du contrôle qu'il exerce »⁶
- 16 Faisant application de ces principes, la Cour juge que l' *Independent Reviewer of Terrorism Legislation* Britannique, chargé du contrôle de la mise en oeuvre des mesures de surveillance digitale, avait, dans les hypothèses où des mesures de surveillance "en bloc" des communications sur internet avaient été ordonnées, examiné une quantité importante d'informations détenues par les services de renseignement et conclu, à l'issue d'un examen attentif de celles-ci, qu'aucune alternative à la mise en place de surveillance massive des télécommunications n'était satisfaisante pour faire face à la menace

terroriste prévalant à l'époque des faits (§384). Ici également, la marge d'appréciation est mobilisée à l'appui du techno-pouvoir.

- 17 Surtout, la Cour neutralise l'exigence d'un contrôle juridictionnel a priori des mesures de surveillance (§318). Reconnaisant que l'autorisation judiciaire préalable est une "garantie importante contre l'arbitraire" (V en ce sens Arrêt Zakharov, précité, § 249) celle-ci rappelle qu'elle n'a jamais, jusqu'à présent, considéré qu'il s'agissait là d'une "exigence nécessaire" ni que l'exclusion d'un tel contrôle dépasse les limites de ce qui peut être jugé nécessaire dans une société démocratique (V. en ce sens Arrêt Zakharov, précité, § 258).

*

- 18 Particulièrement riche bien que décevant, l'arrêt *Big Brother Watch* n'est guère surprenant au regard du précédent *Centrum För Rättvisa contre Suède* du 19 juin 2018, qui avait d'ores et déjà procédé au même usage – douteux – de la marge d'appréciation des états pour légitimer le recours ponctuel à des mesures de surveillance « de masse », et ce en dépit du fait que la législation Suédoise comme la législation Britannique avaient été sèchement invalidées par la Cour de Justice de l'Union Européenne au motif que celles-ci ne limitaient pas les mesures en cause à une période temporelle et / ou une zone géographique ou à un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave.

- 19 Pris dans leur ensemble, les deux jugements poussent à leur paroxysme la logique de *procéduralisation* de la vie privée à l'oeuvre dans le cadre du droit de l'Union Européenne et du droit de la Convention Européenne des Droits de l'Homme : plutôt que de condamner le principe d'une intrusion toujours plus forte des états dans la vie privée des individus, les Cours semblent se satisfaire de l'existence de garanties procédurales (contrôle indépendant, minimisation supposée des collectes de données) supposées protéger les individus de l'arbitraire. Une telle mutation de la notion de vie privée conduit paradoxalement à affaiblir la notion même de vie privée au sens de l'article 8 de la Convention Européenne des droits de l'Homme. L'arrêt *Big Brother Watch* est topique à cet égard : condamnant un système de surveillance désormais défunt pour édicter les garanties procédurales devant être respectées dans la mise en oeuvre d'une surveillance numérique, la Cour se montre d'autant plus souple sur l'admission du principe de la violation de la vie privée des individus pour lutter contre la menace terroriste, en soulignant qu'une collecte de grandes quantités de données peut être justifiée dans un nombre croissant d'hypothèses.

*

- 20 Cour EDH, 13 septembre 2018, *Big Brother Watch and Others v. the United Kingdom*, Req. n°58170/13, 62322/14 et 24960/15

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Cour. EDH, Gr. ChGC., 4 décembre 2015, *Zakharov c. Russie*, Req. n°47143/06 ; Cour.EDH, 12 janvier 2016, *Szabó and Vissy c. Hongrie*, Req., no. 37138/14
 2. Cour. EDH, Gr. ChGC., 4 décembre 2015, *Zakharov c. Russie*, Req. n°47143/06, §248.
 3. V. en ce sens : Sarah St. Vincent, “Did the European Court of Human Rights Just Outlaw “Massive Monitoring of Communications” in Europe “?, *CDT Blog*, 13 janvier 2016.
 4. Celui-ci a édicté une exigence pour les états de notifier a posteriori aux individus concernés l'existence d'une mesure de surveillance à leur égard, une fois que celle-ci a été menée à son terme.
 5. Cour. EDH, Gr. Ch., 4 décembre 2015, *Zakharov c. Russie*, Req. n°47143/06 préc., §260.
 6. *Idem* , §282.
-

RÉSUMÉS

Particulièrement riche mais également particulièrement décevant, l'arrêt Big Brother Watch pousse à son paroxysme la logique de procéduralisation de la vie privée à l'oeuvre dans le cadre du droit de l'Union Européenne et du droit de la Convention Européenne des Droits de l'Homme. Tout en condamnant un système de surveillance particulièrement intrusif, la Cour Européenne des Droits de l'Homme procède à une légitimation de facto du recours à des systèmes de surveillance digitale « de masse ». De manière similaire, les juges de Strasbourg réaffirment la nécessité d'instaurer un contrôle indépendant des activités de surveillance digitale tout en neutralisant l'exigence d'un contrôle judiciaire préalable de celles-ci

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre)