L'art du trompe-l'œil

À propos des arrêts du 25 mai 2021, Big brother watch et autres c.
Royaume-Uni et Centrum för Rättvisa c. Suède de la Cour européenne
des droits de l'homme

Vincent Sizaire

Electronic version

URL: <https://journals.openedition.org/revdh/12968>

DOI: 10.4000/revdh.12968

ISSN: 2264-119X

Publisher

Centre de recherches et d'études sur les droits fondamentaux

Electronic reference

Vincent Sizaire, "L'art du trompe-l'œil", *La Revue des droits de l'homme* [Online], Actualités Droits-Libertés, Online since 20 September 2021, connection on 08 December 2021. URL: <http://journals.openedition.org/revdh/12968> ; DOI: <https://doi.org/10.4000/revdh.12968>

This text was automatically generated on 8 December 2021.

Tous droits réservés

L'art du trompe-l'œil

À propos des arrêts du 25 mai 2021, *Big brother watch* et autres c. Royaume-Uni et *Centrum för Rättvisa* c. Suède de la Cour européenne des droits de l'homme¹

Vincent Sizaire

- 1 C'est comme la fin d'un cycle. Après la Cour de justice de l'Union européenne – qui, en octobre 2020, a confirmé sa jurisprudence soumettant la surveillance de masse des réseaux informatiques à un cadre juridique rigoureux² – et le Conseil d'État – qui, en avril dernier, a au contraire sensiblement érodé les exigences du juge de Luxembourg en la matière³ – la Cour européenne des droits de l'homme était appelée à son tour à rendre sa copie définitive sur cette épineuse question. L'attente suscitée par son arrêt rendu en grande chambre était à la mesure de la circonspection soulevée par les décisions aux termes desquelles la première chambre avait, en juin 2018, très largement validé cette pratique des services de renseignement – et, plus précisément, celle des services britanniques et suédois⁴.
- 2 La Cour aura-t-elle été sensible aux critiques de la doctrine ou, plus vraisemblablement, à la concurrence jurisprudentielle qui, sur cette question comme sur bien d'autres, s'est installée entre les juridictions suprêmes du continent ? Toujours est-il qu'elle semble avoir pris la mesure de la grande attention avec laquelle sa décision allait être reçue. Au terme de deux arrêts particulièrement volumineux (110 pages pour le premier, près de 180 pages pour le second), elle indique ainsi vouloir construire un cadre jurisprudentiel cohérent et adapté aux spécificités de la surveillance informatique de masse, jugeant que si les règles applicables aux « *interceptions ciblées* [...] *fournissent un cadre utile* [...] *il y a lieu de les adapter pour prendre en compte les caractéristiques particulières de l'interception en masse et, en particulier, l'intensité croissante de l'ingérence dans l'exercice par l'individu de ses droits protégés par l'article 8* [de la convention] »⁵.
- 3 Le nouveau cadre que le juge européen propose permet-il réellement de préserver les citoyens européens des atteintes illégitimes à leur vie privée et familiale ? Présentés par la presse généraliste comme une condamnation de la pratique de certains services de renseignement⁶, les arrêts de la grande chambre sont effectivement de nature à réduire le degré d'immixtion de ces derniers dans le cours de nos échanges

numériques. Pourtant, si l'on analyse les décisions un peu plus avant que ce constat de violation essentiellement platonique – les législations britanniques et suédoises ayant largement évolué depuis l'introduction des requêtes – on ne peut que constater que l'économie générale des décisions de la première chambre est entièrement préservée. Certes, cette nouvelle décision traduit un renforcement des exigences du juge européen s'agissant des garanties contre le risque d'abus de pouvoir que doit offrir le droit national. Mais cela n'enlève rien au fait que le principe même du recours à la surveillance généralisée et indifférenciée de nos échanges numériques, réputé relever de la « *marge d'appréciation* » des États, ne fait l'objet que d'un contrôle particulièrement restreint. En d'autres termes, au resserrement du contrôle de proportionnalité (I) correspond un singulier évincement du contrôle de nécessité (II).

I – Le resserrement du contrôle de proportionnalité

- 4 Alors que les arrêts rendus par la première chambre donnaient parfois l'image peu enviable d'un examen quelque peu approximatif – la Cour évoquant alors ses « *préoccupations* » quant aux insuffisances du cadre réglementaire sans en tirer la moindre conséquence⁷ – les décisions adoptées par la grande chambre témoignent au contraire d'une volonté de clarification et de rationalisation de son contrôle. Présentant de façon didactique les différentes étapes techniques de la surveillance informatique des données informatiques, depuis leur captation brute jusqu'à leur utilisation par les services de renseignement⁸, elle considère que « *le processus doit être encadré par des garanties de bout en bout* », c'est-à-dire à chacune de ces étapes⁹. En conséquence, la Cour est conduite à énoncer très précisément les éléments devant être définis par la législation nationale : celle-ci doit indiquer de façon claire et accessible non seulement « *les motifs pour lesquels l'interception en masse peut être autorisée* » et « *les circonstances dans lesquelles les communications d'un individu peuvent être interceptées* », mais également les procédures gouvernant « *l'octroi d'une autorisation* », « *la sélection, l'examen et l'utilisation des éléments interceptés* » et la conservation des données, ainsi que les procédures organisant le contrôle de la surveillance par une autorité indépendante, tant lors de son déroulement qu'*a posteriori*¹⁰. Précision appréciable, la Cour considère que ces exigences s'appliquent tant aux données de contenu qu'aux données de communication (c'est-à-dire, les données d'identification des personnes utilisant les réseaux numériques), soulignant que ces dernières « *peuvent révéler un grand nombre d'informations personnelles telles que l'identité et la localisation de l'expéditeur et du destinataire, ou encore l'équipement par lequel la communication a été acheminée* » et « *faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée* »¹¹.
- 5 La Cour impose en outre des garanties supplémentaires lorsque la surveillance de masse risque de porter atteinte au secret des sources d'un journaliste. Infirmant sur ce point la position de la première chambre, elle juge que lorsque « *l'examen de communications journalistiques ou de données de communication associées par un analyste [peut] conduire à l'identification d'une source, [...] le droit interne doit impérativement comporter des garanties solides en ce qui concerne la conservation, l'examen, l'utilisation, la transmission à des tiers et la destruction de ces éléments confidentiels* ». En outre, lorsqu'il apparaît que des données qui n'ont pas été recueillies à cet effet « *contiennent malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la*

poursuite de leur examen par un analyste ne devraient être possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial »¹². Ces garanties n'étant pas offertes par le régime britannique de l'époque, le juge en conclut logiquement à la violation de l'article 10 de la convention.

- 6 Enfin, se démarquant là encore de l'arrêt de la première chambre, le juge de Strasbourg considère désormais que des garanties spécifiques doivent être prévues en cas de transfert des données issues de la surveillance de masse aux autorités d'un État étranger ou d'une organisation internationale, rejoignant sur ce point son homologue de Luxembourg¹³. Ainsi, « *les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne* », tandis que « *l'État qui transfère les informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées* », lesquelles doivent être renforcées « *lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière* ». Si la Cour n'exige pas que le niveau de garanties soit identique, elle considère « *que le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant* »¹⁴. Constatant que de telles garanties faisaient défaut s'agissant du transfert de données par les services secrets britanniques, mais également suédois à leurs homologues états-uniens – et comment aurait-il pu en être autrement, s'agissant du programme de surveillance secret révélé par Edward Snowden – elle ne peut que conclure à la violation de l'article 8 de la Convention¹⁵.
- 7 L'arsenal ainsi constitué pour pallier les risques d'abus peut paraître particulièrement exigeant. En concentrant ses exigences sur l'accessibilité et la précision du droit national, la Cour offre en réalité une grande marge de manœuvre aux gouvernements nationaux. Si elle se montre relativement pointilleuse s'agissant des conditions et des modalités de la surveillance qui doivent être définies par la loi, elle laisse une immense latitude aux États membres pour en déterminer le contenu, qu'il s'agisse de la durée de conservation des données collectées ou du choix des critères utilisés par les analystes des services de renseignement pour tenter d'y détecter des comportements suspects. Surtout, elle renonce à tout contrôle de nécessité de cette surveillance de masse, élevant d'autant le risque d'arbitraire.

II – L'éviction du contrôle de nécessité

- 8 Comme nous l'avons indiqué, la Cour a choisi de suivre la position de la première chambre en considérant que « *les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder au mieux la sécurité nationale* », cette marge d'appréciation s'appliquant en l'occurrence au choix de recourir ou non à un système de surveillance généralisée et indifférenciée de nos échanges numériques¹⁶. Ce faisant, elle s'éloigne sensiblement de la position de la Cour de justice de l'Union européenne, qui juge au contraire qu'une telle surveillance ne peut être mise en œuvre que pour faire face à des « *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* » et qui « *se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique* »¹⁷.

- 9 Pour justifier sa solution, la Cour européenne des droits de l'homme relève que « la question connexe de savoir s'il existe des garde-fous suffisants pour garantir que l'interception est nécessaire et justifiée est [...] aussi importante que le degré de précision de la définition des motifs pour lesquels une interception peut être autorisée. En conséquence, la Cour estime qu'un régime qui autorise la mise en œuvre d'une interception pour des motifs relativement étendus peut néanmoins satisfaire aux exigences de l'article 8 de la Convention à condition que le système adopté comporte des garanties contre les abus qui, prises dans leur ensemble, soient suffisantes pour compenser cette déficience »¹⁸. Une justification qui relève du parfait sophisme : les règles permettant d'assurer la proportionnalité de l'atteinte n'ont ni pour objet, ni pour effet de pallier l'insuffisance des règles visant à garantir sa nécessité. Elles ont au contraire vocation à se combiner afin que la restriction de liberté demeure la plus mesurée possible. Une mesure restrictive de liberté ordonnée sans être nécessaire dans une société démocratique restera toujours abusive, quand bien même elle serait par ailleurs strictement réglementée : si l'imprécision des critères de surveillance conduit à méconnaître la vie privée d'une personne en dehors de toute nécessité – par exemple, à raison de ses engagements politiques ou de ses écrits scientifiques – le fait que cette surveillance soit d'une durée limitée ou placée sous la supervision d'une autorité indépendante ne suffira jamais à corriger l'abus.
- 10 Par ailleurs, la proportion de l'atteinte à une liberté ne peut se mesurer qu'en fonction d'un objectif suffisamment précis et tangible pour pouvoir vérifier que l'intensité ou la durée de la mesure ne sont pas excessives. En ce sens, l'abandon du contrôle de nécessité auquel procède la Cour de Strasbourg est d'autant plus préoccupant que les finalités pour lesquelles elle juge légitime de mettre en œuvre la surveillance de masse sont particulièrement extensives, comprenant « la protection de la sécurité nationale, le maintien de l'ordre, la prévention des infractions et la protection des droits et libertés d'autrui »¹⁹. Pour peu que le cadre juridique national soit suffisamment précis et accessible, elle autorise ainsi les services de renseignement à surveiller le plus largement possible leurs concitoyens. Lorsque l'on peut être espionné à tout moment, savoir par le menu de quelle façon on le sera nous autorise-t-il vraiment à nous sentir en sûreté ? La position de la Cour illustre ainsi toutes les limites de la logique de « procéduralisation » du contrôle des atteintes aux droits garantis par la Convention qu'elle adopte depuis de nombreuses années²⁰. Si, demain, un État membre prétendait incarcérer préventivement des individus supposément dangereux afin de sauvegarder sa « sécurité nationale », se bornerait-elle à exiger que ce nouveau régime soit précisément réglementé par la loi ? On n'ose risquer une réponse.

*

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. CEDH 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, req. n° 58170/13, 62322/14 et 24960/15
- CEDH 25 mai 2021, *Centrum för Rättvisa c. Suède*, req. n° 35252/08.
2. Vincent Sizaire, « Savoir resserrer les mailles du filet », *La Revue des droits de l'homme* [En ligne], *Actualités Droits-Libertés*, mis en ligne le 28 novembre 2020.
3. Vincent Sizaire et Jean-Philippe Foegle, « Les fausses notes du souverainisme juridique », *La Revue des droits de l'homme* [En ligne], *Actualités Droits-Libertés*, mis en ligne le 21 juin 2021.
4. 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.
5. Cour EDH (grande chambre), 25 mai 2021, *Big brother watch et autres c. Royaume-Uni c. Royaume-Uni*,
op.cit.
6. « Surveillance de masse : la Cour européenne des droits de l'homme condamne Londres et Stockholm », *le Monde*, 28 mai 2021.
7. Cour EDH, 19 juin 2018, *Centrum för Rättvisa c. Suède*, n° 35252/08, n°150.
8. La Cour distingue ainsi « (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 ; (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 » ; Cour EDH (grande chambre), 25 mai 2021, *Big brother watch et autres c. Royaume-Uni*, n°325.
9. Ibid., n°350.
10. Ibid., n°361.
11. Ibid., n°342 et 363.
12. Ibid., n°450.
13. CJUE, Gr. Ch., 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, aff. C362/14.
14. Cour EDH (grande chambre), 25 mai 2021, *Big brother watch et autres c. Royaume-Uni*, n°362.
15. Ibid, n°427 et Cour EDH (grande chambre), 25 mai 2021, *Centrum för Rättvisa c. Suède*, 35252/08, n°373 et 374.
16. Cour EDH (grande chambre), 25 mai 2021, *Big brother watch et autres c. Royaume-Uni*, n°338.
17. CJUE (grande chambre), 6 octobre 2020, *Quadrature du Net et autres*, C-511/18, C-512/18 et C-520/18, n°135 et 136.
18. Ibid., n°370.
19. Ibid., n° 365.
20. Nina Le Bonniec, *La procéduralisation des droits substantiels par la Cour européenne des droits de l'homme*, Bruylant, Paris, 2017.

ABSTRACTS

Dans ses arrêts du 25 mai 2021, la Cour renforce ses exigences s'agissant des garanties contre le risque d'abus de pouvoir que doit offrir le droit national lorsqu'un Etat recourt à la surveillance de masse de nos échanges informatiques. Mais cette surveillance demeure validée en son principe au nom de la « marge d'appréciation » des États, au prix d'un singulier évincement du contrôle de nécessité de l'atteinte à notre vie privée.

AUTHOR

VINCENT SIZAIRE

Maître de conférences associé à l'Université Paris Nanterre