CEDH, 13 SEPTEMBRE 2018, BIG BROTHER WATCH AND OTHERS C. ROYAUME-UNI, N°58170/13, N°62322/14, N°24960/15

MOTS CLEFS : FAI - renseignement - CEDH - vie privée - secret des sources - liberté d'expression - liberté de la presse - Snowden

Au lendemain de l'affaire Snowden, les juges européens prennent le cap vers une nouvelle politique de contrôle renforcée des méthodes de renseignement et de surveillance étatique. Dans leur décision « Big Brother Watch and others contre Royaume-Uni », les juges de la Cour Européenne des Droits de l'Homme condamnent le Royaume-Uni pour son régime d'interception et d'obtention massive de données de communication, jugé contraire aux articles 8 et 10 de la Convention.

FAITS : Le gouvernement britannique a mis en place un régime d'interception massive des communications sous deux modes opératoires de surveillance, employés par ses services de renseignement : après l'interception des données par des gouvernements étrangers, ou par complicité avec les fournisseurs d'accès du pays.
Plusieurs organisations et justiciables, tous journalistes ou militants des droits de l'Homme, pointent du doigt ce régime liberticide.

PROCEDURE : Après les révélations d'Edward Snowden, trois requêtes sont déposées à la Cour Européenne des Droits de l'Homme les 4 septembre 2013, 11 septembre 2014 et 20 mai 2015, par seize requérants au total (*Big Brother Watch et autres c. Royaume-Uni* n°58170/13, *Bureau of Investigative Journalism et Alice Ross c. Royaume-Uni* n°62322/14 et *10 Human Rights Organisations et autres c. Royaume-Uni* n° 24960/15). Elles seront finalement réunies sous le même dossier.
Les requérants dénoncent les atteintes au secret des sources des journalistes, à la liberté d'expression (article 10), au droit au respect de la vie privée (article 8), au principe de non-discrimination (article 11) et au droit au procès équitable (article 6). Ils soutiennent que leur ciblage est motivé par la nature de leurs activités, dont les données transitantes pourraient concerner un ou plusieurs gouvernements.

PROBLEME DE DROIT : Quelles garanties pour des professionnels dans un régime de surveillance massive des communications ?

SOLUTION : La Cour condamne partiellement le gouvernement britannique pour la violation des articles 8 et 10 de la Convention. Le Royaume-Uni a méconnu le droit au respect de la vie privée et familiale et des correspondances en ce que sa législation, la loi « RIPA » (*Regulation of Investigatory Powers Act)*, n'insère aucune garantie quant à la sélection des communications examinées et du manque de surveillance sur le choix des « porteurs » internet et des communications interceptées (§ 388). Le gouvernement britannique a également méconnu la liberté d'expression et la liberté de la presse, dès lors que le régime du chapitre 2 de la RIPA ne prévoit des dispositions protectrices uniquement lorsque l'objet de la demande est d'identifier une source (§ 499) et qu'aucune limite n'est strictement posé aux pouvoirs des services de renseignement dans la recherche des éléments normalement protégés par le secret des sources des journalistes (§ 493).

NOTE :

Les révélations d'Edward Snowden sur les programmes de surveillance de masse des pays occidentaux ont bouleversé l'ordre international et suscité la méfiance dans de nombreuses professions. La Cour rappelle dans sa décision les principes déjà édictés permettant d'identifier un régime de surveillance des communications respectueux des libertés fondamentales.

L'état des lieux mitigé du RIPA

Sur le système d'interception de communications, la Cour rappelle les six critères précédemment édictés (*CEDH 4 avr. 1990, Huvig c. France*) devant figurer dans la loi pour pallier tout abus. Ces critères s'appliquant « également pour des interceptions opérées en raison de sécurité nationale » (CEDH, gr. ch., 4 déc. 2015, *Roman Zakharov c. Russie*), les juges ont apprécié les conditions de mise en œuvre, les mécanismes et les recours prévus. Selon les juges, ce type de système entre dans la marge d'appréciation de l'Etat : ils reconnaissent d'ailleurs la prudence des services secrets britanniques depuis les révélations d'Edward Snowden. La Cour sanctionne néanmoins l'absence totale de garanties quant à la sélection des communications examinées et du manque de surveillance sur le choix des « porteurs » internet et des communications interceptées, en considérant que la section 8 (4) ne satisfait pas l'exigence de « qualité de la loi », et ne sait prêter attention à ce qui est « indispensable à une société démocratique ».

Sur l'obtention de données auprès de fournisseurs d'accès, la Cour rappelle sa décision *Ben Faiza contre France* du 8 février 2018, favorable à un régime d'interception de données de géolocalisation par l'opérateur téléphonique lorsque le régime est prévu par la loi et qu'il est assorti de garanties démocratiques.
Même si le Royaume-Uni a reconnu l'incompatibilité de sa législation au droit de l'UE (CJUE 21 déc. 2016, S*ecretary of State for the Home Department v. Watson and Others*), l'accès aux données conservées n'est pas limité à la lutte contre les « infractions graves » et ne fait l'objet d'aucun examen préalable par un tribunal ou un organe administratif indépendant. La Cour retient ainsi la non-conformité des dispositions du chapitre 2 du RIPA au sens de l'article 8 de la Convention.

La Cour retient une troisième violation au regard de l'article 10 de la CESDH. Le régime ne peut être « conforme à la loi » si des dispositions protectrices s'appliquent uniquement lorsque l'objet de la demande est d'identifier une source (§ 499), et qu'aucune limite n'est prévue aux pouvoirs des services de renseignements de rechercher des éléments protégés par le secret des sources des journalistes (§ 493).

Une décision durable ?

Cette décision rappelle une nouvelle fois le Royaume-Uni à revoir sa copie sur le régime d'interception massive de communications au regard de la garantie des droits fondamentaux, qui avait à l'origine jusqu'au 1er novembre pour corriger ses erreurs selon les attentes de la Cour Suprême nationale.
Elle remet au centre des préoccupations les méthodes utilisées par les services de renseignement, et suscite la question quant au mystère des techniques de chaque Etat. Néanmoins, cette décision n'est pas garantie d'une effectivité absolue puisque les Etats pourront souvent justifier d'intérêts nationaux prépondérants face au respect de libertés individuelles.
Comment garantit-on finalement ses droits fondamentaux lorsque les recherches des services s'établissent dans l'ombre et obstruent nos principes les plus chers ?

Kenza CHERIF
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC
2018

ARRET :

§ 387 « *the Court considers that the decision to operate a bulk interception regime was one which fell within the wide margin of appreciation afforded to the Contracting State. Furthermore, in view of the independent oversight provided by the Interception of Communications Commissioner and the IPT, and the extensive independent investigations which followed the Edward Snowden revelations, it is satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers under section 8[4] of RIPA* » .

§ 388 « *In view of these shortcomings and to the extent just outlined, the Court finds that the section 8(4) regime does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention.* »

§ 447 « *In light of the foregoing considerations, the Court considers that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicate with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence agencies. In this regard, it observes that the high threshold recommended by the Venice Commission – namely, that the material transferred should only be able to be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques – is met by the respondent State's regime. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the regime. On the contrary, following an investigation the ISC found no evidence whatsoever of abuse.* »

§ 493 « *In this regard, paragraphs 4.1 – 4.8 of the IC Code require special consideration to be given to the interception of communications that involve confidential journalistic material and confidential personal information (see paragraph 90 above). However, these provisions appear to relate solely to the decision to issue an interception warrant. Therefore, while they might provide adequate safeguards in respect of a targeted warrant under section 8(1) of RIPA, they do not appear to have any meaning in relation to a bulk interception regime. (…) In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications.* »

§ 499 « *Nevertheless, these provisions only apply where the purpose of the application is to determine a source; they do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist's communications data there are no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Court considers that the regime cannot be "in accordance with the law" for the purpose of the Article 10 complaint.* »