Peter KIMPIÁN
Unité de la protection des données, Droits de l'homme et Etat de droit, Conseil de l'Europe

« LA SURVEILLANCE ET LA PROTECTION DE LA VIE PRIVEE »

Pour mettre en exergue le lien entre surveillance et nécessaire protection de la vie privée, il convient de s'appuyer sur la Convention européenne des droits de l'homme et la juridiction qui veille à son respect, la Cour européenne des droits de l'homme.

Pour ce faire, nous analyserons les articles pertinents de la Convention et les différentes jurisprudences de la Cour.

I. ARTICLE 8 DE LA CEDH

Il énonce que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Ainsi, les traitements de données par les organismes d'application de la loi entravent le droit à la protection de la vie privée et le droit à la protection des données.

S'agissant des actions menées par les forces de l'ordre dans le cadre de la lutte contre le terrorisme sont susceptibles de representer une ingérence dans ces droits. Comme telle, elle ne peut être justifiées si elle est prévue par la loi, nécessaire dans une société démocratique et poursuit un objectif légitime.

II. ARTICLE 11 DE LA CONVENTION 108 MODERNISEE[1]

Il permet trois régimes d'exceptions. Le troisième régime permet d'appliquer des exceptions aux articles 4 paragraphe 3, article 14 paragraphes 5 et 6 et article 15 paragraphe 2, a, b, c et d pour les objectifs legitimes de la sécurité nationale et de la défense tout en respectant les conditions génerales précisées ci-dessus. Il convient de limiter certains pouvoirs du Comité conventionnel ; de l'autorité de contrôle sur les transferts internationaux ; de l'autorité de contrôle sur l'exigence de la démonstrabilité du respect des conditions légales du transfert international ; et sur sa capacité d'intervention ; de l'autorité de contrôle sur ses pouvoirs d'investigation et d'intervention, sur ses fonctions relatives aux transferts internationaux, sur son pouvoir de rendre des décisions réglementaires et d'infliger des sanctions (administratives), sur son droit de se tourner vers le pouvoir judiciaire.

III. « PREVUES PAR LA LOI »

Les ingérences du gouvernement doivent être ancrées dans le droit interne. Ces lois doivent respecter des exigences de qualité. A savoir, elles doivent être prises en respectant les exigences d'un Etat de droit, être accessibles et être prévisibles. Par ses meusures, il s'agit de protéger les personnes concernées contre les ingérences arbitraires des autorités publiques.

1 « La version modernisée de la Convention 108 de 1981 réaffirme les principes d'origine de la Convention, en renforce certains et énoncequelques nouvelles garanties. Il a fallu adapter ces principes aux réalités du monde en ligne tandis que despratiques inédites ont conduit à la reconnaissance de nouveaux principes. Les principes de transparence, de proportionnalité, de responsabilité, de limitationdes données, de respect dela vie privée pris en compte dès la conceptionetc. Sont désormais reconnuscomme des éléments clés du mécanisme de protection et ont été intégrés dans l'instrument modernisé » En ligne https://rm.coe.int

La CrEDH, dans l'arrêt MALONE c. ROYAUME-UNI[2], a jugé, quant à l'exigence de prévisibilité dans le contexte de la surveillance secrète des communications, que : le gouvernement doit s'assurer que « la loi [use] de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit [...] » ; et que la loi doit définir l'étendue et les modalités d'exercice du pouvoir discrétionnaire exercé par les autorités avec « une netteté suffisante – compte tenu du but légitime poursuivi – [...] ».

La Cour, dans son arrêt WEBER & SARAVIA[3], pose des garanties minimales : la nature des infractions susceptibles de donner lieu à un mandat d'interception ; la définition des catégories de personnes susceptibles d'être mises sur écoute ; la fixation d'une limite à la durée de l'exécution de la mesure ; la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; les précautions à prendre pour la communication des données à d'autres parties ; et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

IV. « NECESSAIRES DANS UNE SOCIETE DEMOCRATIQUE »

Pour justifier de telles ingérences, il faut que les meusures répondent a un besoin social impérieux. Les mesures doivent être proportionnelles au but légitime poursuivi. Pour les apprécier, les Etats disposent d'une marge d'appréciation dont les critères sont l'adéquation, la nécessité (au sens strict) et la proportionnalité (au sens strict).

Aujourd'hui, la Cour relève différents critères. Pour le critère du **soupçon raisonnable**, la Cour juge qu'il faut une base factuelle suffisante pour

2 CEDH, 26 avril 1985, Malone c/ Royaume-Uni, Requête n° 8691/79
3 CEDH, 29 juin 2006, Weber et Saravia c/ Allemagne, Requête n° 54934/00

appliquer des mesures de rassemblement de renseignements secrets, afin de permettre une appréciation de la nécessité de ces mesures qui doivent être fondées sur un soupçon individuel concernant un individu donné (ARRET SZABÓ[4]). Elle juge aussi qu'il faut « vérifier s'il existe une base factuelle suffisante pour soupçonner la personne visée par la demande de mesures [de surveillance] » (ARRET ZAKHAROV[5]). Enfin, elle insiste : cela se peut uniquement dans le cadre de l'existence démontrable d'un soupçon raisonnable, qui permettrait à l'autorité de réaliser un test de proportionnalité approprié (ARRET SZABÓ).

Pour le critère de la **stricte nécessité**, il faut prendre en considération générale, l'objectif de la préservation des institutions démocratiques. Puis, en parallèle, il faudra prendre en considération particulière, la nécessité et la proportionnalité des meusures ayant pour but l'obtention de renseignements vitaux dans le cadre d'une opération individuelle donnée.

Enfin, pour le critère de **l'autorisation judiciaire**, la Cour établit qu'il faut une procédure d'autorisation indépendante du pouvoir exécutif (ARRET ZAKHAROV) ; et, dans ce domaine, qu'un contrôle externe par une instance indépendante, de préférence par un juge avec une expertise particulière, devrait être la règle, et que des solutions de substitution à l'exception, afin de préserver des garanties d'indépendance, d'impartialité et le bon déroulement de la procédure, devraient exister (ARRET SZABO).

V. NOUVELLES AFFAIRES

La Cour, dans son arrêt IVASHCHENKO c. RUSSIE[6], a jugé que ne constituait pas une violation de l'article 8 de la CEDH, l'inspection de l'ordinateur d'un photographe journaliste par des douaniers, en raison de suspicion de matériaux extrémistes, avec copie des photos et mots de passe.

4 CEDH, 12 janvier 2016, Szabó et Vissy c/ Hongrie, Requête n° 37138/14
5 CEDH, 4 décembre 2015, Roman Zakharov c/ Russie, Requête n°47143/06
6 CEDH, 13 février 2018, Ivashchenko c/ Russie, Requête n° 61064/10

La Cour, dans son arrêt BENEDIK c. SLOVENIE[7], a jugé que constituait une violation de l'article 8.2 le fait que la Slovénie ait demandé sans autorisation judiciaire préalable à un FAI d'identifier un utilisateur sur base d'une adresse IP dynamique dans le cadre d'une enquête concernant des images/vidéos pédopornographiques, alors que l'ingérence aurait dû doit être « prévue par la loi ».

Enfin, la Cour, dans son arrêt BIG BROTHER WATCH c. ROYAUME-UNI[8], a jugé que :

1. Les procédures de sélection et de recherches manquaient d'une surveillance indépendante et adéquate, en particulier dans le choix de « porteurs » Internet pour l'interception, ainsi que pour la sélection des communications interceptées. Ainsi, les exigences de l'article 8(2) en matière de "qualité de la loi" n'ont pas été rencontrées et les ingérences n'ont pas été reconnues comme étant "nécessaires dans une société démocratique".
2. Le régime, quant au système d'acquisition de données auprès des fournisseurs de services de communication, est dépourvu des garanties qui auraient du être intégrées dans le droit national (accès aux données dans l'unique but de lutter contre les "crimes graves" et accès soumis au contrôle préalable d'un tribunal ou d'une instance administrative indépendante). Ainsi, cela constitue une violation de l'article 8.
3. En matière de sources journalistiques et d'informations journalistiques confidentielles : le régime d'interception massive des communications, et le régime d'acquisition des données auprès des fournisseurs de services de communication ne sont pas encadrés par des garanties suffisantes appliquées à ces domaines journalistiques. Ainsi, cela constitue une violation de l'article 10.
4. Enfin, le système de partage de renseignements par le gouvernement ne constitue pas en soi une violation des articles 8 et 10. Les gouvernements toutefois disposent d'une marge d'appréciation pour décider des mesures nécessaires pour guarantir la sécurité nationale.

7 CEDH, 24 avril 2018, Benedik c/ Slovénie, Requête n° 62357/14
8 CEDH, 13 septembre 2018, Big Brother watch c/ Royaume-Uni, Requêtes n° 58170/13, 62322/14 et. 24960/15