COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CDDH(2023)R99 Addendum 1
28/11/2023

COMITÉ DIRECTEUR POUR LES DROITS DE L'HOMME
(CDDH)

_____

COMMENTAIRES ADOPTÉS PAR LE CDDH SUR DES RECOMMANDATIONS DE L'ASSEMBLÉE PARLEMENTAIRE

Recommandation de l'APCE 2258 (2023)
« Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État »

Recommandation 2258 (2023) - « Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État »

1. L'Assemblée parlementaire se réfère à la Résolution 2513 (2023) « Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État » et recommande au Comité des Ministres :

1.1 d'adopter une recommandation aux États membres du Conseil de l'Europe sur la surveillance secrète et les droits humains, surtout à la lumière des menaces que présentent les nouvelles technologies de surveillance et les logiciels espions, en tenant dûment compte des normes internationales les plus élevées, de la jurisprudence de la Cour européenne des droits de l'homme et du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE no 223, «Convention 108+»). La recommandation devrait mettre l'accent sur les points suivants :

1.1.1 les conditions d'acquisition de logiciels espions par les agences et organes gouvernementaux des États membres ;

1.1.2 les conditions d'utilisation de la technologie des logiciels espions à des fins d'application de la loi et de sécurité nationale ;

1.1.3 les conditions de vente et d'exportation de la technologie des logiciels espions vers des pays tiers ;

1.1.4 les procédures d'autorisation, les mécanismes de supervision et de contrôle juridictionnels, les mécanismes de notification et les voies de recours applicables à l'utilisation de logiciels espions par les autorités nationales ;

1.1.5 les mécanismes garantissant une obligation de rendre des comptes en cas d'utilisation illégale de logiciels espions ;

1.1.6 les normes de diligence raisonnable en matière de droits humains pour les entreprises de logiciels espions ;

1.1.7 l'aspect transnational de la surveillance numérique et de l'utilisation de logiciels espions ;

1.1.8 le rôle des parlements nationaux ;

1.2 d'examiner la faisabilité d'une convention du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions ;

1.3 de coordonner ses initiatives avec d'autres organisations internationales, y compris l'Union européenne et l'Organisation des Nations Unies, dans les domaines de la protection des données, de la surveillance ciblée et des logiciels espions, à des fins d'établissement de normes et de coopération.

COMMENTAIRES DU CDDH

1. Le CDDH prend note de la Recommandation 2258 (2023) de l'Assemblée parlementaire « Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État ». Il partage les inquiétudes de l'Assemblée sur la nature profondément intrusive de ces outils, en raison du rôle joué par les téléphones mobiles dans la collecte, le stockage et le traitement d'un grand nombre de données personnelles hautement sensibles, et du risque qui en découle de violations graves du droit à la vie privée et familiale, tel que protégé par l'article 8 de la Convention européenne des droits de l'homme (la Convention).

2. Le CDDH rappelle la jurisprudence de la Cour européenne des droits de l'homme (la Cour) concernant la surveillance secrète et l'article 8. La Cour a reconnu que même des mesures de surveillance très étendues et/ou intrusives peuvent exceptionnellement être nécessaires dans une société démocratique et donc autorisées en vertu de l'article 8. Ce faisant, la Cour a toutefois souligné les exigences et les garanties énoncées dans la Convention, bien qu'elle n'ait pas encore prononcé d'arrêt concernant Pegasus ou un logiciel espion similaire. De tels arrêts pourraient engendrer de nouveaux développements dans la jurisprudence de la Cour.

3. En ce qui concerne l'exigence de la Convention selon laquelle les mesures de surveillance doivent poursuivre un « but légitime », la Cour a affirmé que, dans le cas de mesures de surveillance ciblées, il doit exister un soupçon objectivement raisonnable, fondé sur des indications factuelles, de soupçonner la personne concernée de préparer, de commettre ou d'avoir commis des actes criminels ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrètes. En outre, les mesures de surveillance doivent être « conformes à la loi », c'est-à-dire qu'elles doivent avoir un fondement dans le droit national et être compatibles avec l'État de droit. Cela implique la prévisibilité, c'est-à-dire que la loi doit être suffisamment claire pour donner aux citoyens une indication adéquate des circonstances et des conditions dans lesquelles les autorités publiques sont habilitées à recourir à de telles mesures.

4. La Cour a indiqué que pour que les mesures de surveillance soient « nécessaires dans une société démocratique », comme l'exige la Convention, elles doivent renfermer des garanties adéquates et effectives contre l'arbitraire et le risque d'abus. La Cour a précisé les garanties minimales qui doivent être inscrites dans la loi pour éviter les abus : (i) définir la nature des infractions susceptibles de donner lieu à un mandat d'interception ; (ii) définir les catégories de personnes susceptibles d'être mises sur écoute ; (iii) fixer une limite à la durée de la mesure d'interception ; (iv) prévoir une procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; (v) définir les précautions à prendre lors de la communication des données à d'autres parties ; et (vi) définir les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.

5. Enfin, la Cour a déclaré que les mesures de surveillance secrète doivent faire l'objet d'un contrôle et d'un examen au moment où elles sont ordonnées pour la première fois, pendant leur exécution et après qu'elles ont cessé.

6. Le CDDH rappelle en outre les normes de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et son Protocole d'amendement (STCE n° 223).

7. Le CDDH note en particulier la proposition de l'Assemblée parlementaire visant à ce que le Comité des Ministres adopte une recommandation aux États membres sur la surveillance secrète et les droits humains. Le CDDH considère que l'élaboration d'un instrument non contraignant serait envisageable et présenterait une réelle valeur ajoutée, compte tenu de la gravité de la menace pour le droit des individus à la vie privée que représente l'abus potentiel de Pegasus et des logiciels espions similaires. Un tel instrument pourrait se présenter sous la forme d'une recommandation, mais également de lignes directrices appliquant les principes de la jurisprudence de la Cour en matière de logiciels espions, accompagnées d'exemples de bonnes pratiques nationales existantes.

8. Rappelant son implication dans la rédaction en 2002 des Lignes directrices du Comité des Ministres sur les droits de l'homme et la lutte contre le terrorisme, qui abordaient la collecte et le traitement des données à caractère personnel et les mesures qui interfèrent avec la vie privée, le CDDH serait disposé à contribuer aux travaux portant sur tout nouvel instrument non juridique, en tenant compte des développements ultérieurs de la jurisprudence de la Cour et de l'adoption du protocole d'amendement à la Convention STE n°108.

9. Concernant la proposition de l'Assemblée parlementaire invitant le Comité des Ministres à examiner la faisabilité d'une convention du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions, le CDDH estime que ces aspects pourraient être examinés dans le cadre du suivi de la Recommandation CM/Rec(2016)3 du Comité des Ministres sur les droits de l'homme et entreprises.