LE LOGICIEL ESPION PEGASUS

et ses répercussions sur les droits de l'homme

Service de la société de l'information
DGI(2022)04

Auteurs :
Tamar Kaldani
Zeev Prokopets

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Edition anglaise :
Pegasus Spyware

Toute demande de reproduction ou de traduction de tout ou d'une partie de ce document doit être adressée à la Direction de la communication (F-67075 Strasbourg cedex ou publishing@coe.int). Toute autre correspondance relative à ce document doit être adressée à la Direction Générale Droits de l'homme et État de droit.

Couverture et mise en page :
Service de la société de l'information
Conseil de l'Europe

Images : Shutterstock

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale du SPDP.

© Conseil de l'Europe, juin 2022

LE LOGICIEL ESPION PEGASUS

et ses répercussions sur les droits de l'homme

Auteurs :

Tamar Kaldani
Introduction et parties consacrées aux répercussions

Zeev Prokopets
La surveillance des téléphones mobiles et le logiciel espion, les règles de base pour une meilleure protection

Conseil de l'Europe

Table des matières

Abréviations

CdE	Conseil de l'Europe
Convention 108	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108)
Convention 108+	Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223)
Cour	Cour européenne des droits de l'Homme
CEDH	Convention européenne des droits de l'homme
UE	Union européenne
APCE	Assemblée parlementaire du Conseil de l'Europe
NU	Nations Unies

Introduction

La transformation numérique et les innovations en matière de technologies de la communication nous ont permis d'être mieux connectés et intégrés et de bénéficier d'un meilleur accès aux services. Parallèlement, elles offrent aussi aux États la possibilité d'accroître leur surveillance et de s'ingérer dans les droits de l'homme et les libertés fondamentales. Les récentes révélations sur le logiciel espion Pegasus qui a ciblé des journalistes, des défenseurs des droits de l'homme et des responsables politiques, notamment dans un certain nombre d'États membres du Conseil de l'Europe (CdE), ont suscité un tollé général. L'utilisation d'une technologie intrusive de ce type porte non seulement atteinte à la réalisation effective du droit au respect de la vie privée et de la liberté d'expression, mais aussi à la notion d'autonomie personnelle, voire à l'intégrité physique des personnes. Les pratiques de surveillance mises au jour jusqu'ici pourraient également nuire au principe même de l'État de droit et à la crédibilité des institutions démocratiques.

La sécurité nationale et les activités criminelles suscitent des inquiétudes qui peuvent justifier l'utilisation exceptionnelle de technologies de surveillance des communications. Les services répressifs et les services de renseignement cherchent à atteindre un but légitime lorsqu'ils recourent aux écoutes téléphoniques, analysent des métadonnées ou surveillent directement des appareils mobiles de façon dissimulée pour obtenir les informations nécessaires en vue de prévenir, d'enquêter et de poursuivre les crimes ou de combattre les menaces qui pèsent sur la sécurité nationale.

Toutefois, la marge d'appréciation de l'État même « dans des affaires liées à la sécurité nationale n'est plus uniformément large » [1].

[1] Conseil de l'Europe / Cour européenne des droits de l'hommes, Sécurité nationale et jurisprudence européenne des droits de l'homme, 2013, page 2.

Les États sont liés par des instruments internationaux[2], régionaux[3] et nationaux relatifs aux droits de l'homme. Corollaire de la Convention européenne des droits de l'homme (CEDH) et de la jurisprudence de la Cour européenne des droits de l'homme (Cour), les États membres ont des obligations négatives, en ce sens qu'ils doivent s'abstenir de toute atteinte aux droits fondamentaux, et des obligations positives, c'est-à-dire qu'ils doivent protéger activement ces droits ; cela comprend également la protection des personnes contre les actes d'acteurs non étatiques[4].

L'utilisation à grande échelle de dispositifs d'écoute des communications et la surveillance secrète ouvrent toujours la voie à d'éventuels agissements arbitraires de la part des autorités de l'État, qui menacent la réalisation effective d'un certain nombre de droits et libertés fondamentales, dont le droit au respect de la vie privée et familiale et de la correspondance (article 8 de la Convention) et la liberté d'expression (article 10). Les conséquences d'outils de surveillance de masse ou de surveillance ciblée tels que Pegasus dans les régimes autoritaires pourraient être catastrophiques. Un certain nombre de régimes autoritaires utilisent déjà des outils de surveillance de haute technologie, qui servent à traquer les opposants et à supprimer la liberté d'information et d'expression[5]. Dès lors, le développement et le déploiement des technologies de surveillance doivent s'accompagner de garanties juridiques appropriées et effectives qui assurent la protection adéquate des personnes et un juste équilibre entre tous les intérêts en présence et les droits et les libertés en jeu.

[2] Tels que la Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques.

[3] Tels que la Charte africaine des droits de l'homme et des peuples ou les instruments et le système interaméricains des droits de l'homme.

[4] Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux (adoptée par le Comité des Ministres le 11 juin 2013 lors de la 1173e réunion des Délégués des Ministres), paragraphe 4.

[5] Résolution 2045 (2015) de l'APCE sur les opérations de surveillance massive, paragraphe 8.

Malheureusement, le scandale du logiciel espion Pegasus n'est pas le premier à révéler une surveillance de masse et le recours à des technologies intrusives en tant qu'armes d'espionnage contre des journalistes, des défenseurs des droits de l'homme et des responsables politiques. Les pratiques d'intrusion, aussi bien à grande échelle que ciblées, minent la confiance des citoyens dans les pouvoirs publics qui utiliseraient des outils de surveillance pour cibler des personnes pour lesquelles il n'y a pas de raison de soupçonner qu'elles aient commis un acte répréhensible ou qu'elles présentent un danger notable pour la démocratie et l'État de droit.

Les allégations de surveillance arbitraire de plus de 50 000 numéros de téléphone figurant sur une liste ayant fait l'objet d'une fuite et à laquelle ont eu accès Forbidden Stories[6] et Amnesty International[7] en 2021, ainsi que les récentes alertes[8] sur le recours généralisé au logiciel espion Pegasus dans le monde entier, ont déclenché l'ouverture d'enquêtes et de procédures judiciaires dans un certain nombre d'États.

En mars 2022, le Parlement européen a créé une Commission chargée d'enquêter sur l'utilisation du logiciel Pegasus et d'autres logiciels espions de surveillance et de déterminer si cette utilisation est conforme à la législation et les droits fondamentaux de l'Union européenne (UE)[9].

---

[6] https://forbiddenstories.org/case/the-pegasus-project/

[7] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[8] Voir par exemple : https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/ https://www.euronews.com/next/2022/05/02/pegasus-spyware-spain-s-prime-minister-and-defence-minister-s-phones-infected-by-spying-so

https://www.frontlinedefenders.org/en/statement-report/report-jordanian-human-rights-defenders-and-journalists-hacked-pegasus-spyware

https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets

https://scroll.in/latest/1022972/pegasus-case-supreme-court-panel-seeks-response-from-dgps-of-all-states-on-spyware-purchase

https://citizenlab.ca/tag/nso-group/

[9] Communiqué de presse sur le lancement des travaux de la commission d'enquête du Parlement européen : https://www.europarl.europa.eu/news/fr/press-room/20220412IPR27112/la-commission-d-enquete-du-pe-sur-pegasus-a-lance-ses-travaux

Cette Commission réclamera les documents voulus et cherchera à obtenir le témoignage de nombreux acteurs, en particulier des services de renseignement des États membres, d'élus et de hauts fonctionnaires. D'ici à un an, elle devrait présenter des recommandations sur les mesures à prendre par la Commission européenne et les gouvernements nationaux[10]. La Haute-Commissaire des Nations Unies (NU) aux droits de l'homme, s'adressant le 14 septembre 2021 aux membres de la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe (APCE), a demandé aux États de mettre en place un moratoire sur la vente de ces technologies et de contenir l'industrie de la surveillance [11].

Le présent rapport a été élaboré par le CdE. Il explique le fonctionnement du logiciel espion Pegasus et analyse ses répercussions sur les droits de l'homme et les libertés fondamentales, en particulier le droit au respect de la vie privée et la liberté d'expression. En outre, il souligne que le logiciel Pegasus a ou pourrait avoir un effet paralysant sur d'autres droits de l'homme et libertés fondamentales, notamment le droit à la dignité, la liberté de réunion, la liberté de religion, et même l'intégrité physique et psychologique de la personne. Le rapport met l'accent sur les instruments juridiques et les normes bien établies dont dispose le CdE pour faire respecter les droits fondamentaux et renforcer la protection contre la surveillance illégale et injustifiée, qu'elle soit massive ou ciblée. Le rapport offre également des règles de base pour une meilleure protection afin de réduire au minimum l'exposition possible non seulement au logiciel Pegasus mais aussi à d'autres attaques malveillantes.

[10] https://www.aldeparty.eu/renew_europe_welcomes_the_inquiry_committee_on_pegasus_spyware_scandal

[11] Discours de la Haute-Commissaire des Nations Unies aux droits de l'homme : https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe

1. La surveillance des téléphones mobiles et le logiciel espion

Ces dernières décennies, les gouvernements et les agences associées ont redoublé d'efforts et investi des fonds considérables pour être en mesure de pénétrer tous les réseaux et appareils de télécommunication. Les agences de sécurité nationale avaient l'habitude d'avoir des accords avec des fournisseurs de technologies en vertu desquels les entreprises accordaient aux agences un accès spécial à leurs produits par le biais de portes dérobées. Certains de ces accords demeurent. Depuis peu, l'opinion publique est de plus en plus sensible aux questions de sécurité numérique et de vie privée (les révélations d'Edward Snowden sur la surveillance de masse opérée par le gouvernement des États-Unis ont été un premier coup de semonce) et les grandes entreprises ont fermé les portes dérobées aux gouvernements.

Des entreprises comme Apple (et bien d'autres) allouent des budgets sans précédent à la sécurité, développent des fonctionnalités telles que le chiffrement de bout en bout et mettent en place des équipes d'ingénieurs spécialisés qui travaillent en permanence à l'identification et à la correction rapide de failles de sécurité. Il existe également des programmes de prime à la faille détectée avec lesquels des entreprises invitent les pirates informatiques à s'introduire dans leurs produits. Ces programmes offrent des primes relativement attrayantes aux personnes qui détectent des failles non corrigées[12] – jusqu'à 100 000 USD – mais le problème est que ces failles valent des millions sur le marché noir.

Ces évolutions font que les gouvernements sont incapables d'espionner et sont désespérément à la recherche d'une solution. Leurs besoins et le budget quasiment illimité dont ils disposent ont créé une « industrie » et un marché, où les pirates informatiques cherchent continuellement des failles exploitables, tandis que les fournisseurs travaillent sans relâche à y remédier. Les pirates informatiques ayant trouvé une faille vendent leurs informations soit aux fournisseurs, soit au plus offrant sur le marché noir. Sur ce dernier, les acheteurs sont les organisations qui créent des logiciels espions et les vendent ensuite aux gouvernements et parfois à d'autres organisations.

[12] Les failles non corrigées sont des failles exploitables dont le fournisseur n'a pas connaissance. Par conséquent, aucun correctif n'est disponible ou en cours de développement.

Ce marché ne diffère en rien d'un autre marché et repose essentiellement sur l'offre et la demande : tant que la demande existe (et en réalité augmente) l'offre suivra, et il y aura toujours quelqu'un pour fournir les produits. L'un des fournisseurs les plus prospères (et donc connu de tous) est le groupe israélien NSO à l'origine de Pegasus, un logiciel espion qui peut être installé discrètement sur un téléphone intelligent et avoir accès à toutes ses fonctionnalités, y compris la caméra et le microphone.

Le logiciel est conçu pour des appareils fonctionnant sous différents systèmes d'exploitation (Android, iOS, Windows, Blackberry et Symbian) et il les transforme en outils de surveillance. D'après le groupe NSO, le logiciel Pegasus n'est vendu qu'à des gouvernements et seulement à des fins de géolocalisation de criminels et terroristes.

Son fonctionnement

Le logiciel espion Pegasus peut infecter les téléphones de cibles à l'aide de différents mécanismes. Il peut s'agir d'un message (SMS, iMessage, WhatsApp, courriel) qui contient un lien vers un site web. Une fois que la cible a cliqué sur le lien en question, il libère un logiciel malveillant qui infecte l'appareil.

Il peut aussi s'agir d'un simple message qui infecte l'appareil et ne requiert aucune interaction de la part de son propriétaire. Ces attaques « zéro clic » ou exploitations « zéro clic » profitent de failles dans les services de messagerie.

Outre les exploitations « zéro clic », le logiciel Pegasus recourt également à des attaques par « injection réseau » : en naviguant sur internet, une cible peut s'exposer à une attaque sans avoir à cliquer sur aucun lien malveillant. Il suffit d'attendre que la cible en question se rende sur un site web qui n'est pas entièrement sécurisé alors qu'elle navigue normalement sur internet. Lorsqu'elle se rend sur un site non protégé, le logiciel intercepte l'opération et infecte l'appareil.

Toutefois, cette technique est plus difficile à mettre en œuvre qu'une attaque d'un téléphone à l'aide d'une URL malveillante ou d'une exploitation « zéro clic », car il est nécessaire de surveiller l'utilisation du téléphone de la cible jusqu'à ce que son trafic internet ne soit plus protégé. Cela passe normalement par l'opérateur mobile de la cible, auquel certains gouvernements peuvent avoir accès ou qu'ils peuvent contrôler.

En raison de cette dépendance, il est difficile voire impossible pour les gouvernements de cibler des personnes en dehors de leur juridiction. Les exploitations « zéro clic » ne présentent pas de telles limitations.

En plus de ces mécanismes, il existe également une option manuelle. Ainsi, si un agent parvient à obtenir le téléphone de la cible, le logiciel espion peut être installé manuellement. Dans tous les cas, l'objectif est de prendre le contrôle total du système d'exploitation de l'appareil mobile, soit par le rootage (pour les appareils Android), soit par le débridage (*jailbreak* en anglais, pour les appareils iOS).

Habituellement, le rootage d'un appareil Android est réalisé par l'utilisateur en vue d'installer des applications et des jeux issus de sources non officielles, ou de permettre l'utilisation de fonctionnalités bloquées par le fabriquant.

De même, un appareil Apple peut être débridé pour permettre l'installation sur le téléphone d'applications non disponibles sur l'App Store, ou pour l'utiliser sur d'autres réseaux cellulaires.

Tant le rootage que le débridage suppriment les contrôles de sécurité intégrés aux systèmes d'exploitation Android ou iOS et permettent aux systèmes d'exploitation d'exécuter du code modifié.

Dans le cas de logiciels espions, une fois l'appareil déverrouillé, l'intrus peut déployer d'autres logiciels pour sécuriser l'accès à distance aux données et aux fonctions de l'appareil. Il est probable que l'utilisateur ne remarque absolument rien, à moins qu'il observe des anomalies manifestes sur son appareil (voir Indices d'infection).

Les versions antérieures de Pegasus étaient installées sur les téléphones intelligents soit au moyen de failles dans des applications couramment utilisées, soit par hameçonnage ciblé, c'est-à-dire que l'utilisateur, trompé, était amené à cliquer sur un lien ou à ouvrir un document qui installait secrètement le logiciel.

À partir de 2019, les utilisateurs de Pegasus ont pu installer le logiciel sur les téléphones intelligents par l'intermédiaire d'un appel manqué sur WhatsApp qu'ils pouvaient même supprimer de l'historique des appels, ce qui faisait que le propriétaire du téléphone ne se rendait compte de rien. Un autre moyen consistait à simplement envoyer un message au téléphone d'un utilisateur sans émettre de notification. Ces deux failles spécifiques ont été corrigées après avoir été découvertes, mais de nouvelles failles encore inconnues maintiennent les exploitations « zéro clic » bien vivantes.

En d'autres termes, la dernière version du logiciel espion Pegasus ne nécessite aucune interaction de la part de l'utilisateur du téléphone intelligent. Pour qu'une attaque réussisse, il suffit qu'une application ou un système d'exploitation présentant une faille particulière soit installé sur l'appareil.

Les conséquences

Une fois installé, le logiciel Pegasus peut théoriquement récolter tout type de données contenues sur l'appareil et les transmettre à l'auteur de l'attaque. Il peut exécuter tout type de code sur l'appareil de la cible, utiliser la caméra et le microphone de celui-ci par des commandes à distance et en temps réel, extraire les contacts, les historiques d'appels, les recherches sur internet, l'historique de navigation, les SMS, les photos, les vidéos, les paramètres, les enregistrements de localisation, ainsi que des informations provenant d'applications telles que iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype et autres.

Le logiciel Pegasus surveille également les données saisies au clavier d'un appareil infecté et toutes les communications écrites, y compris les mots de passe, sont visibles à l'auteur de l'attaque.

Les indices d'infection

Si vous avez des raisons de croire que vous êtes surveillé, voici une liste d'indices qui peuvent démontrer que votre téléphone est infecté :

1. Votre téléphone est soudainement plus lent que d'habitude.
2. Votre téléphone s'éteint parfois tout seul.
3. Vous devez recharger la batterie de votre téléphone plus souvent que d'ordinaire.
4. Vous trouvez des dossiers ou des fichiers inhabituels et inconnus sur votre appareil (principalement Android).
5. Vous êtes souvent redirigé vers des sites inconnus.
6. De très nombreuses fenêtres intruses apparaissent tandis que vous naviguez sur internet.
7. Vous remarquez une augmentation soudaine de l'utilisation des données.
8. Des applications nouvelles ou inconnues sont installées sur votre téléphone.

Si vous remarquez des changements de ce type sur votre téléphone, un moyen relativement facile de savoir s'il est infecté est d'utiliser le Mobile Verification Toolkit (MVT) d'Amnesty International. Fonctionnant sous Linux et MacOS, cet outil examine les fichiers et la configuration de votre téléphone en analysant une sauvegarde effectuée à partir du téléphone.

Bien que l'analyse ne permette pas de confirmer ou d'infirmer si un appareil a été piraté, elle permet de détecter des indicateurs de piratage, ce qui constitue généralement une preuve suffisante d'infection.

L'outil peut notamment détecter la présence de processus logiciels spécifiques exécutés sur l'appareil, ainsi qu'une série de domaines utilisés dans le cadre de l'infrastructure globale soutenant le réseau de logiciels espions.

2. Les répercussions sur le droit au respect de la vie privée

Comme il a été décrit ci-dessus et d'après la description produit du logiciel Pegasus[13], son utilisation ne nécessite pas de coopérer avec les entreprises de télécommunication, et il peut facilement venir à bout du chiffrement, du SSL, des protocoles propriétaires, et de tout obstacle introduit par les communications complexes dans le monde entier. Il permet de surveiller la voix et les appels VoIP en temps réel. Il donne accès, à distance et de façon dissimulée et illimitée, aux appareils mobiles de la cible, et donc à ses relations, identités virtuelles, localisations, appels téléphoniques, messages textuels et vocaux, courriels, photos, vidéos et autres fichiers, contacts, mots de passe, écoutes environnementales, projets et activités révélant des informations particulièrement sensibles (en lien notamment avec la santé, la vie sexuelle, les opinions politiques, les croyances religieuses ou autres) non seulement en ce qui concerne la cible mais aussi ses enfants et les autres membres de sa famille, collègues, amis, clients, et autres contacts.

Le mode opératoire du logiciel Pegasus démontre clairement sa capacité à être utilisé pour une surveillance aussi bien ciblée qu'indifférenciée. Il constitue à première vue une ingérence dans l'exercice des droits protégés par l'article 8 de la CEDH et il va à l'encontre des normes et approches[14] établies par la Cour européenne dans sa vaste jurisprudence relative à la surveillance ciblée des communications et à l'interception indiscriminée ou en masse de données de communication.

Tout d'abord, toute ingérence dans la vie privée ne peut se justifier au regard de l'article 8§2 que si :

a) elle est prévue par la loi, qui doit être accessible, prévisible, précise et suffisamment claire quant aux règles, circonstances et conditions dans lesquelles la surveillance est autorisée et menée. La loi doit également comporter des garanties adéquates et effectives ainsi qu'un contrôle pour prévenir les abus, et

[13] La description produit du logiciel Pegasus est disponible à l'adresse suivante : https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf

[14] Voir également les affaires récentes suivantes : Big Brother Watch et autres c. Royaume-Uni [GC], n° 58170/13, 25 mai 2021, et Centrum för rättvisa c. Suède [GC], n° 35252/08, 25 mai 2021.

offrir des voies de recours effectives aux personnes en cas d'abus[15]. Elle doit également être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8.

b) elle vise un ou plusieurs des buts légitimes énumérés au paragraphe 2 de l'article 8, notamment la sécurité nationale, la sûreté publique et la prévention des infractions pénales. La notion de sécurité nationale doit être clairement interprétée par le droit national et fournir l'éventail des crimes et délits menaçant la sécurité nationale ainsi que les autres crimes graves ou exceptionnellement graves autorisant les autorités à utiliser des mesures de surveillance secrète pour prévenir ces crimes et mener des enquêtes de manière efficace.

c) elle est nécessaire dans une société démocratique pour atteindre ces buts légitimes. Les autorités de l'État ont l'obligation d'assurer des mécanismes efficaces (notamment des tribunaux nationaux, des mécanismes de contrôle et de suivi, ainsi qu'un droit de regard du public) pour éviter l'arbitraire et garantir un juste équilibre entre le droit au respect de la vie privée et le but légitime visé par l'ingérence. Le critère de « stricte nécessité » n'est rempli que si l'action envisagée permet objectivement de protéger ou préserver une institution démocratique et, si elle est susceptible, d'un point de vue subjectif, de fournir des renseignements essentiels dans le cadre d'une enquête en cours.

Dans les affaires Roman Zakharov c. Russie et Szabó et Vissy c. Hongrie, la Cour européenne des droits de l'homme a également noté que le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière de mesures de surveillance secrète apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La Cour a réitéré avec fermeté les normes qu'elle a établies dans sa jurisprudence antérieure en la matière, à savoir que pour

[15] Voir également Roman Zakharov c. Russie [GC], n° 47143/06, 4 décembre 2015 ; Szabó et Vissy c. Hongrie, n° 37138/14, 12 janvier 2016 ; Iordachi et autres c. République de Moldova, n° 25198/02, 10 février 2009 ; Rotaru c. Roumanie [GC], n° 28341/95, 4 mai 2000 ; Kennedy c. Royaume-Uni, n° 26839/05, 18 mai 2010 ; Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, n° 62540/00, 28 juin 2007.

évaluer efficacement la nécessité et le caractère raisonnable de toute intrusion dans la vie privée ou les communications, toute mise sur écoute ou surveillance secrète doit être autorisée par une autorité nationale indépendante et impartiale investie du mandat correspondant. L'autorité délivrant l'autorisation doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale. Elle doit également s'assurer que l'interception requise satisfait au critère de « nécessité dans une société démocratique » prévu à l'article 8§2 de la Convention, notamment qu'elle est proportionnée aux buts légitimes poursuivis, en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs[16].

Pour ce qui est de la mise sur écoute ciblée, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer[17] :

(i) la nature des infractions susceptibles de donner lieu à un mandat d'interception ;

(ii) la définition des catégories de personnes susceptibles d'être mises sur écoute ;

(iii) la fixation d'une limite à la durée de l'exécution de la mesure ;

(iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ;

(v) les précautions à prendre pour la communication des données à d'autres parties ;

(vi) les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des données.

Dans l'affaire Roman Zakharov c. Russie, la Cour a confirmé que ces six garanties minimales s'appliquaient également dans les cas où l'interception était ordonnée pour des raisons de

[16] Voir également Klass et autres c. Allemagne, n° 5029/71, 6 septembre 1978.

[17] Voir aussi les affaires Huvig c. France, n° 11105/84, 24 avril 1990 ; Kruslin c. France, n° 11801/85 24 avril 1990 ; Valenzuela Contreras c. Espagne, n° 27671/95, 30 juillet 1998, Weber et Saravia c. Allemagne, n° 54934/00, 29 juin 2006.

sécurité nationale ; toutefois, pour déterminer si la législation contestée était contraire à l'article 8, la Cour a également pris en compte les modalités suivantes :

a) le contrôle de l'application de mesures de surveillance secrète ;

b) l'existence éventuelle d'un mécanisme de notification ;

c) les recours prévus en droit interne.

En ce qui concerne l'approche de la Cour relative à l'interception en masse de communications[18], la Cour considère dans sa récente jurisprudence que le processus doit être encadré par des « garanties de bout en bout » afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, c'est à dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération – et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré *a posteriori*. À cet égard, la Cour a particulièrement insisté sur le fait que les sélecteurs utilisés par les autorités lors d'interceptions en masse doivent être autorisés et approuvés par les juridictions nationales ou les organes indépendants investis du mandat correspondant. De l'avis de la Cour, ce sont des garanties fondamentales qui constituent la pierre angulaire de tout régime d'interception en masse conforme à l'article 8[19].

Parallèlement à l'article 8 de la CEDH, aux arrêts de la Cour européenne, aux résolutions de l'Assemblée parlementaire, notamment la Résolution 2045 (2015) sur les opérations de surveillance massive[20], et aux déclarations[21] et recommandations[22] du Comité des ministres,

[18] Voir par exemple Big Brother Watch et autres c. Royaume-Uni [GC], n° 58170/13, 25 mai 2021.

[19] Voir aussi le rapport de la Commission de Venise, selon lequel deux des garanties les plus importantes dans un régime d'interception en masse sont l'autorisation et le contrôle du processus : https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-f

[20] https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=21692

[21] Voir par exemple la Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c801b

[22] Voir par exemple la Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804e4a20

la Convention 108[23] – seul instrument international juridiquement contraignant dans le domaine de la protection des données qui ait une portée mondiale[24] –, établit les principes de base pour la protection des données, les garanties pour les personnes et le contrôle des opérations de traitement des données, qui sont particulièrement importants dans le contexte du logiciel Pegasus ou d'autres technologies de surveillance.

Bien que le droit à la protection des données à caractère personnel ne constitue pas un droit autonome parmi les différents droits et libertés de la Convention, la Cour européenne a reconnu que la protection des données à caractère personnel revêt une importance capitale pour la jouissance du droit au respect de la vie privée et familiale, du domicile et de la correspondance. L'article 8 est le principal vecteur de la protection des données à caractère personnel dans le système de la Convention, même si des considérations liées à cette protection peuvent également entrer en jeu sur le terrain d'autres dispositions de la Convention et de ses protocoles additionnels[25].

La Convention 108+, modernisée et ouverte à la signature et à la ratification en octobre 2018, a réaffirmé l'importance des principes fondateurs et en a établi de nouveaux, notamment la transparence, la responsabilité, le « respect de la vie privée dès la conception » et l'analyse d'impact relative à la protection des données qui sont particulièrement pertinents dans le contexte du logiciel espion Pegasus.

La Convention 108+ exige des autorités publiques et des entreprises privés qu'elles améliorent la qualité des données, renforcent la protection des données sensibles, mettent en place un niveau élevé de sécurité des données, et assurent une plus grande équité, transparence et responsabilité, notamment de la part des développeurs et prestataires de services, qui doivent démontrer de manière proactive leur conformité avec les règles en matière de protection des données. Elle établit en outre des exigences plus strictes pour la licéité du traitement, la proportionnalité, la limitation des finalités et la minimisation des

[23] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

[24] La Convention 108 a été ratifiée par 55 États parties, dont 9 pays non-membres du Conseil de l'Europe.

[25] Guide sur la jurisprudence de la Convention européenne des droits de l'homme - Protection des données, Première édition - 31 décembre 2020, page 7.

données, rappelant que les données traitées doivent être adéquates, pertinentes et non excessives. Le principe de proportionnalité s'applique également en ce qui concerne les moyens et méthodes déployés au cours de la surveillance.

La Convention 108+ donne plus de moyens d'action aux individus, en leur offrant un plus grand contrôle sur leurs données et des droits renforcés. Parallèlement à leurs autres obligations, les responsables du traitement des données doivent mettre en œuvre le principe du « respect de la vie privée dès la conception » dans le développement des produits ou services, et examiner au préalable l'impact probable du traitement des données sur les droits de l'homme et les libertés fondamentales.

Il est important de rappeler que les États parties à la Convention 108+ ne pourront plus exclure du champ d'application de la Convention certains types de traitement des données, par exemple à des fins de sécurité nationale et de défense. Les exceptions possibles à un nombre limité de principes, comme la transparence, sont soumises aux conditions fixées par la Convention et, en tout cas, un examen et un contrôle indépendants et effectifs doivent être garantis. La Convention 108+ renforce également les pouvoirs d'enquête et d'adoption de mesures correctrices ainsi que l'indépendance des autorités de protection des données. Elle accroît également leur coopération internationale et les possibilités d'actions et d'enquêtes communes, notamment contre l'utilisation illégale et injustifiée des technologies de surveillance sophistiquées.

Afin de protéger les personnes et la société dans son ensemble contre toute ingérence illégale dans les droits de l'homme et notamment dans le droit au respect de la vie privée, les normes établies par la Convention 108+ pourraient dès à présent être utilisées et mises en œuvre par les autorités publiques menant des activités dans ce domaine.

3. Les répercussions sur la liberté d'expression

Un rapport d'enquête publié par un consortium international[26] de journalistes a révélé que 200 journalistes dans le monde entier avaient été la cible du logiciel espion Pegasus. Le Bureau du Rapporteur spécial pour la liberté d'expression de la Commission interaméricaine

[26] https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

des droits de l'homme de l'Organisation des États Américains (OEA) a également noté le nombre de victimes de tentatives d'espionnage par le logiciel Pegasus, dont des journalistes mexicains, des défenseurs des droits de l'homme et des dirigeants de l'opposition[27]. D'après la Secrétaire générale d'Amnesty International, les chiffres montrent clairement une généralisation des abus, qui mettent en danger la vie des journalistes, de leur famille et de leurs associés, portent atteinte à la liberté de la presse et font taire les médias critiques.

Le droit à la liberté d'expression et d'information, tel que garanti par l'article 10 de la Convention, constitue l'un des fondements essentiels d'une société démocratique et l'une des conditions primordiales de son progrès et de l'épanouissement de chacun. La liberté d'expression vaut non seulement pour les « informations » ou les « idées » accueillies favorablement ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui offensent, choquent ou dérangent l'État ou une fraction quelconque de la population. Toute ingérence dans le droit à la liberté d'expression des journalistes et autres acteurs des médias a donc des répercussions sociétales car c'est aussi une ingérence dans le droit d'autrui de recevoir des informations et des idées et une ingérence dans le débat public[28].

Même si le droit à la liberté d'expression n'est pas absolu, une ingérence dans celui-ci n'est admissible que si elle est prévue par la loi, qu'elle poursuit l'un des buts légitimes énoncés à l'article 10, paragraphe 2, de la Convention, et qu'elle s'avère nécessaire dans une société démocratique, ce qui implique qu'elle correspond à un besoin social impérieux et est proportionnée au(x) but(s) légitime(s) poursuivi(s).

La surveillance des journalistes et autres acteurs des médias et le suivi de leurs activités en ligne peuvent entraver l'exercice légitime du droit à la liberté d'expression s'ils sont menés sans les garanties nécessaires. Ces pratiques peuvent également menacer la sécurité des personnes concernées et nuire à la protection des sources journalistiques. Pour être compatibles avec l'article 8 de la Convention, les mécanismes de surveillance secrète doivent être assortis de garanties suffisantes et efficaces contre les abus, notamment un contrôle

[27] Communiqué de presse R303/21
https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1218&lID=1

[28] Recommandation CM/Rec(2016)4 du Comité des Ministres aux États membres sur la protection du journalisme et la sécurité des journalistes et autres acteurs des médias
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168064147b

indépendant, car de tels systèmes destinés à protéger la sécurité nationale présentent le risque de fragiliser la démocratie, voire de la détruire, au motif de la défendre[29].

La Cour européenne des droits de l'homme, dans les affaires relevant de l'article 10 de la Convention, a toujours soumis les garanties du respect de la liberté d'expression à un examen particulièrement vigilant. Les garanties à accorder à la presse revêtent une importance particulière et la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse. L'absence d'une telle protection pourrait dissuader les sources journalistiques d'aider la presse à informer le public sur des questions d'intérêt général. En conséquence, la presse pourrait être moins à même de jouer son rôle indispensable de « chien de garde » et son aptitude à fournir des informations précises et fiables pourrait s'en trouver amoindrie.

Selon certaines allégations, le logiciel Pegasus était utilisé pour cibler des journalistes et leurs sources confidentielles. Cela a des effets préjudiciables non seulement sur lesdites sources et les lanceurs d'alertes, mais aussi sur les médias, dont la réputation pourrait être entachée aux yeux de futures sources potentielles, et sur le public, qui a tout intérêt à recevoir des informations transmises par des sources anonymes.

Dans un certain nombre de décisions[30], la Cour européenne s'est penchée sur les risques posés par l'interception en masse de communications par l'intermédiaire d'un « sélecteur fort » lié à des journalistes. La Cour a estimé qu'une telle ingérence est comparable à celle qui résulterait d'une perquisition au domicile ou sur le lieu de travail d'un journaliste. Indépendamment de la question de savoir si les services de renseignement cherchent ou non à identifier une source, il est très probable que l'utilisation de sélecteurs forts ou de termes de recherche liés à un journaliste aboutira à la collecte de très nombreux éléments journalistiques confidentiels, mesure plus attentatoire encore à la protection des sources qu'une injonction de divulgation de l'identité d'une source[31]. Par conséquent, dans l'affaire Big Brother Watch et autres c. Royaume-Uni, la Cour a estimé qu'avant que les services de

[29] Ibid.

[30] Voir, entre autres, Goodwin c. Royaume-Uni, n° 17488/90, 27 mars 1996 ; Sanoma Uitgevers B.V. c. Pays-Bas [GC], n° 38224/03, 14 septembre 2010.

[31] Ibid.

renseignement n'utilisent des sélecteurs ou des termes de recherche dont on sait qu'ils sont liés à un journaliste, ou qui aboutiront très probablement à la sélection pour examen d'éléments journalistiques confidentiels, ces sélecteurs ou termes de recherche doivent avoir été autorisés par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure est « justifiée par un impératif prépondérant d'intérêt public » et, en particulier, si une mesure moins intrusive suffirait à satisfaire un tel impératif. La Cour a également considéré que même en l'absence d'intention d'accéder à des éléments journalistiques confidentiels, et même en l'absence de l'utilisation de sélecteurs ou de termes de recherche rendant très probable la sélection pour examen d'éléments journalistiques confidentiels, il existe néanmoins un risque que de tels éléments soient interceptés, voire examinés, en se trouvant accidentellement « pris dans les filets » d'une interception de masse.

4. Les répercussions sur les défenseurs des droits de l'homme

Les révélations au sujet du logiciel Pegasus confirment que les défenseurs des droits de l'homme sont, avec les journalistes, l'une des principales cibles de la surveillance secrète. Diverses organisations internationales[32] et de la société civile ont exprimé leur profonde inquiétude quant à la situation des défenseurs des droits de l'homme qui sont pris pour cible, font l'objet d'intimidations et de mesures de représailles.

Elles ont appelé à créer un environnement sûr et favorable pour les défenseurs des droits de l'homme et à assurer leur protection, et ont notamment recommandé aux États de s'abstenir d'utiliser les technologies de surveillance pour cibler ces personnes[33].

Les technologies de surveillance sont souvent utilisées pour cibler les défenseurs des droits de l'homme en vue de les dissuader de poursuivre leurs actions, d'infiltrer leurs réseaux et de recueillir des informations contre d'autres cibles. L'intrusion dans la vie privée des défenseurs des droits de l'homme porte non seulement atteinte à leur vie privée,

[32] Résolution adoptée par l'Assemblée générale le 16 décembre 2021 à sa soixante-seizième session, sur le rapport de la Troisième Commission (A/76/462/Add.2, par. 114) 76/174.

[33] https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rights-defenders

mais constitue également un danger pour leur entourage proche et éloigné, compromet leur dignité et leur réputation, et les expose, eux-mêmes ainsi que les membres de leur famille et les autres contacts, à un risque plus élevé d'être victimes de menaces, d'agressions et de violences.

Une enquête criminalistique numérique menée par Front Line Defenders et Citizen lab a dévoilé des dangers spécifiques liés au genre. Le logiciel espion Pegasus a infecté les appareils mobiles de quatre défenseurs des droits de l'homme jordaniens, dont une femme, avocate et journaliste travaillant contre la corruption[34]. Access Now et Front Line Defenders ont également indiqué que les appareils mobiles de deux défenseuses des droits de l'homme issues de la région du Moyen-Orient et de l'Afrique du Nord ont été piratés à l'aide du logiciel espion Pegasus[35].

La surveillance ciblant spécifiquement les femmes peut s'avérer désastreuse pour celles-ci, étant donné que les asymétries de pouvoir entre les hommes et les femmes, aussi bien dans la vie politique que sociale, offrent souvent la possibilité aux autorités de transformer les informations obtenues en armes, par la diffamation, le chantage ou la divulgation de données personnelles. Cela peut inclure la publication en ligne de photos et de conversations privées et intimes[36].

En conséquence, les femmes, prises pour cibles de cette surveillance, vivent dans un état perpétuel de peur, sont isolées socialement et limitées dans leur vie sociale, leur travail et leur militantisme. L'une des victimes a ainsi déclaré : « les libertés personnelles sont terminées pour moi, elles n'existent plus. Je ne suis pas en sécurité chez moi, dans la rue ou nulle part ailleurs »[37].

[34] https://www.frontlinedefenders.org/sites/default/files/jordanpegasusreport.pdf

[35] https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/

[36] Ibid.

[37] https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

5. Les répercussions sur les droits de l'homme et les libertés fondamentales

Les droits de l'homme et les libertés fondamentales sont interconnectés et se renforcent mutuellement. C'est pourquoi les technologies de surveillance intrusive ont un effet paralysant sur d'autres droits de l'homme et libertés fondamentales, et pas seulement sur le droit au respect de la vie privée et la liberté d'expression.

Par exemple, les pratiques de surveillance numérique peuvent également porter atteinte au droit à la santé. En effet, des personnes pourraient éviter de communiquer des données sensibles liées à leur santé avec des soignants, de peur que le principe de confidentialité ne soit compromis. La liberté de religion pourrait également en pâtir, notamment si les propos tenus dans le cadre de la confession et les communications privilégiées avec des responsables de culte étaient interceptés. Des personnes pourraient également s'abstenir d'exercer leur droit à la liberté de réunion et d'association, notamment le droit de créer ou de rejoindre une organisation à but non lucratif ayant des objectifs politiques, philosophiques, religieux ou syndicaux.

La surveillance ciblée ou de masse crée également un climat d'autocensure. Craignant que chacun de leurs actes et mouvements ne soit scruté à la loupe, les personnes sont moins enclines à communiquer sur des sujets spécifiques en ligne ou hors ligne. L'effet paralysant de la surveillance peut également conduire à l'isolement social. Les cibles, ainsi que leurs parents et amis, pourraient s'abstenir de toute interaction, de peur d'être surveillés ou qu'on leur fasse du mal.

Plus important encore, l'accès en temps réel aux données de localisation et de communication pourrait également mettre en danger l'intégrité physique et mentale des personnes, voire leur vie.

Les préoccupations croissantes concernant l'utilisation de logiciels espions à des fins politiques, ainsi que les rapports sur la détention arbitraire, la torture, voire les exécutions extrajudiciaires d'opposants politiques, de journalistes et de militants des droits de

l'homme[38], appellent à des enquêtes immédiates, approfondies, efficaces et indépendantes et à des garanties juridiques renforcées, notamment des mécanismes de surveillance indépendants, impartiaux et efficaces. Les organisations de la société civile demandent également un moratoire sur la vente, le transfert et l'utilisation du logiciel Pegasus jusqu'à ce que le respect des normes en matière de droits de l'homme puisse être garanti. Elles exhortent les États à mettre en œuvre une législation imposant des garanties contre les violations des droits de l'homme et les abus liés à la surveillance numérique, et établissant des mécanismes de responsabilité destinés à offrir des voies de recours aux victimes d'abus de surveillance[39].

[38] https://www.amnesty.org/en/documents/doc10/4516/2021/en/

[39] Ibid.

6. Les règles de base pour une meilleure protection

Il n'y a pas de solution absolue, surtout face à des exploitations « zéro clic ». Cependant, vous pouvez prendre quelques mesures pour réduire au minimum votre exposition potentielle, non seulement au logiciel Pegasus mais aussi à d'autres attaques malveillantes.

1. Dans certains cas (et en particulier pour les appareils Apple), il semble que les infections ne survivent pas à la réinitialisation du téléphone, mais demandent à être réintroduites via des exploitations « zéro clic ». Cela signifie que la réinitialisation fréquente de votre téléphone peut supprimer certains logiciels malveillants, du moins temporairement.
2. N'ouvrez que les liens provenant de contacts que vous connaissez et en qui vous avez confiance. Le logiciel Pegasus et d'autres logiciels malveillants recourent à iMessage et aux SMS pour envoyer des liens qui entraînent le téléchargement et l'installation du logiciel espion. Il en va de même pour les liens envoyés par courriel ou d'autres applications de messagerie. Évitez tout particulièrement les liens de « désinscription » provenant de sources suspectes. En effet, l'une des méthodes connues consiste à envoyer des courriels indésirables pour contrarier la cible, puis à lui envoyer un autre message lui proposant de cliquer sur « désinscription » pour ne plus les recevoir. De nombreuses cibles cliquent allègrement sur le lien de désinscription, provoquant ainsi l'infection.
3. Assurez-vous que votre appareil est mis à jour avec les logiciels les plus récents. Ces mises à jour incluent souvent des corrections des bugs et failles de sécurité. Si votre appareil est sous Android, ne vous fiez pas aux notifications de mises à jour disponibles, vérifiez vous-même la dernière version, car il se peut que le fabricant de votre appareil ne fournisse pas de mises à jour.
4. Aussi évident que cela puisse paraître, restreignez l'accès physique à votre téléphone en activant le déverrouillage par code PIN, empreinte digitale ou reconnaissance faciale.

5. Dans la mesure du possible, évitez les services WiFi publics et gratuits (y compris dans les hôtels). Si vous devez utiliser le WiFi public, utilisez un VPN et évitez d'accéder à des informations sensibles.
6. Chiffrez les données de votre appareil et activez les fonctions d'effacement des données à distance, dans le cas où elles sont disponibles. Si vous perdiez votre appareil ou qu'il était volé, vos données resteraient en sécurité.
7. Lorsque vous communiquez à l'aide d'applications de messagerie chiffrée de bout en bout, activez la fonction de disparition des messages.
8. Dans la mesure du possible, n'utilisez pas vos appareils, cartes SIM et comptes de messagerie personnels ou professionnels pour contacter des sources sensibles. Si possible, procurez-vous d'autres appareils et cartes SIM et créez un nouveau compte de messagerie spécialement pour communiquer avec elles.
9. Votre appareil peut être utilisé pour vous localiser et par la même occasion pour localiser vos sources confidentielles. Si vous vous rencontrez en personne, n'emportez pas vos téléphones avec vous et préférez un lieu neutre (sachez que vous pourriez être surveillés par un système de vidéosurveillance) qui ne peut être associé à votre adresse personnelle ou professionnelle ou à celle de votre source.
10. Supprimez les métadonnées des fichiers et photos sensibles avant de les partager avec d'autres personnes. Les métadonnées d'un fichier peuvent fournir des informations sur la personne qui l'a créé ou envoyé et sur l'appareil utilisé.

ANNEXE : informations complémentaires sur le groupe NSO et le logiciel Pegasus

- Le groupe NSO est une entreprise israélienne soumise à la réglementation israélienne. Officiellement, le groupe déclare ne vendre ses produits qu'à des agences gouvernementales et à des pays préapprouvés, et uniquement à des fins de lutte contre le terrorisme et d'application de la loi.
- Les pays qui sont des utilisateurs connus du logiciel Pegasus (liste partielle) sont les suivants : Mexique – premier client du groupe NSO, a utilisé le logiciel Pegasus dès 2011 pour traquer le célèbre baron de la drogue Joaquín Guzmán ou « El Chapo » –, Émirats arabes unis, Arabie saoudite, Espagne, Pologne, Panama, Pays-Bas, Maroc, Inde, Israël, Allemagne, Hongrie, Bahreïn, Azerbaïdjan, Arménie.
- Pegasus est un logiciel couteux : en 2016, on estimait que les frais annuels s'élevaient à 600 000 USD en plus de frais d'installation à hauteur de 500 000 USD pour un système capable de suivre 10 cibles simultanément.
- Le revenu du groupe NSO en 2020 s'élevait à 243 millions USD.

Ce rapport fournit une description technique du logiciel espion Pegasus et analyse ses éventuelles répercussions sur les droits de l'homme et les libertés fondamentales, en particulier le droit au respect de la vie privée et la liberté d'expression. En outre, il souligne que le logiciel Pegasus a ou pourrait avoir un effet paralysant sur l'exercice d'autres droits de l'homme et libertés fondamentales, notamment le droit à la dignité, la liberté de réunion, la liberté de religion, et même l'intégrité physique et psychologique de la personne. Le rapport met l'accent sur les instruments juridiques et les normes bien établies dont dispose le Conseil de l'Europe pour faire respecter les droits fondamentaux et renforcer la protection contre la surveillance illégale et injustifiée, qu'elle soit massive ou ciblée. Par ailleurs, il offre également des règles de base pour une meilleure protection des personnes.

Tamar Kaldani a été inspectrice de la protection des données personnelles et inspectrice d'État de Géorgie. Elle est actuellement première vice-présidente du Comité consultatif de la Convention 108.

Zeev Prokopets, cadre dirigeant israélien, est concepteur de produits, développeur de logiciels et entrepreneur (Link7).

www.coe.int

Le **Conseil de l'Europe** est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres du Conseil de l'Europe.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE