La Quadrature du Net

TRANSFORMER LES OBJETS CONNECTÉS EN MOUCHARDS : LA SURENCHÈRE SÉCURITAIRE DU GOUVERNEMENT

31 mai 2023

Communiqué de l'Observatoire des Libertés et du Numérique, 31 mai 2023

Le projet de loi « Orientation et programmation du ministère de la Justice 2023-2027 » a commencé à être discuté au Sénat, et son article 3 fait déjà polémique. À raison.

Au milieu de dispositions qui visent à entériner pêle-mêle les interventions à distance des médecins en cas de prolongation de la garde à vue et des interprètes dès le début de la garde à vue, ou l'extension des possibilités des perquisitions de nuit à des crimes de droit commun, est créé un nouvel outil d'enquête permettant d'**activer, à distance, les appareils électroniques d'une personne à son insu** pour obtenir sa géolocalisation en temps réel ou capter des images et des sons. Art. 3 points 12° et 13° et 17° à 19°.

En clair, il s'agira par exemple pour les enquêteurs judiciaires de **géolocaliser** une voiture en temps réel à partir de son système informatique, d'**écouter** et **enregistrer** tout ce qui se dit autour du micro d'un téléphone même sans appel en cours, ou encore d'activer la caméra d'un ordinateur pour **filmer** ce qui est dans le champ de l'objectif, même si elle n'est pas allumée par son propriétaire. Techniquement, les policiers exploiteront les failles de sécurité de ces appareils (notamment, s'ils ne sont pas mis à jour en y accédant, ou à distance) pour installer un logiciel qui permet d'en prendre le contrôle et transformer vos outils, ceux de vos proches ou de différents lieux en mouchards.

Pour justifier ces atteintes graves à l'intimité, le Ministère de la Justice invoque la « crainte d'attirer l'attention des délinquants faisant l'objet d'enquête pour des faits de criminalité organisée, de révéler la stratégie établie ou tout simplement parce qu'elle exposerait la vie des agents chargés de cette mission » en installant les outils d'enquête. En somme, il serait trop risqué ou compliqué pour les agents d'installer des micros et des balises « physiques » donc autant se servir de tous les objets connectés puisqu'ils existent. Pourtant, **ce prétendu risque n'est appuyé par aucune information sérieuse** ou exemple précis. Surtout, il faut avoir en tête que le piratage d'appareils continuera de passer beaucoup par un accès physique à ceux-ci (plus simple techniquement) et donc les agents encourront toujours ce prétendu risque lié au terrain. De plus, les limites matérielles contingentes à l'installation d'un dispositif

constituent un garde-fou nécessaire contre des dérives d'atteintes massives à la vie privée.

La mesure prévue par l'article 3 est particulièrement problématique pour les téléphones portables et les ordinateurs tant leur place dans nos vies est conséquente. Mais le danger ne s'arrête pas là puisque son **périmètre concerne en réalité tous les « appareils électroniques** », c'est-à-dire tous les objets numériques disposant d'un micro, d'une caméra ou de capteurs de localisations. Cette mesure d'enquête pourrait ainsi permettre de :

- « sonoriser » donc écouter des espaces à partir d'une télévision connectée, d'un babyphone, d'un assistant vocal (type Google Home), ou d'un micro intégré à une voiture ;
- de retransmettre des images et des vidéos à partir de la caméra d'un ordinateur portable, d'un smartphone ou d'une caméra de sécurité à détection de mouvement ;
- de récupérer la localisation d'une personne grâce au positionnement GPS d'une voiture, d'une trottinette connectée ou d'une montre connectée. De nombreux autres périphériques disposant de ces capteurs pourraient aussi être piratés.

Si ce texte était définitivement adopté, cela **démultiplierait dangereusement les possibilités d'intrusion policière**, en transformant tous nos outils informatiques en potentiels espions.

Il est, à cet égard, particulièrement inquiétant de voir consacrer le droit pour l'Etat d'utiliser les failles de sécurité des logiciels ou matériels utilisés plutôt que de s'attacher à les protéger en informant de l'existence de ces failles pour y apporter des remèdes.

Les services de police et de renseignement disposent pourtant déjà d'outils extrêmement intrusifs : installation de mouchards dans les domiciles ou les voitures (balise GPS, caméras de vidéosurveillance, micro de sonorisation), extraction des informations d'un ordinateur ou d'un téléphone par exemple et mise en oeuvre d'enregistreurs d'écran ou de frappes de clavier (*keylogger*). Ces possibilités très larges, particulièrement attentatoires à la vie privée, sont déjà détournées et utilisées pour surveiller des militant·es comme (dans la lutte du Carnet, dans l'opposition aux mégabassines, dans les lieux militants de Dijon, ou dans les photocopieuses de lieu anarchistes, etc.)

Alors que les révélations sur l'espionnage des téléphones par Pegasus continuent de faire scandale et que les possibilités des logiciels espions ont été condamnées par le Haut-Commissariat des Nations Unies aux droits de l'homme, le ministère de la Justice y voit **a contrario un exemple à suivre**. Il tente de légitimer ces dispositifs en assurant que seuls le crime organisé et le terrorisme seront visés via ces « techniques spéciales d'enquête ».

Si le projet de loi renvoie effectivement à des infractions considérées comme graves, cela n'est pas de nature à apaiser les inquiétudes légitimes. En effet, ces mêmes infractions graves ont déjà été utilisées pour poursuivre des actions militantes, que ce soit à l'encontre de personnes solidaires avec les migrants accusées d'aide à l'entrée de personnes en bande organisée, de militants écologistes, encore qualifiés récemment d' « écoterroristes » ou encore de militants contre l'enfouissement de déchets nucléaires à Bure. Plus généralement, le spectre des infractions visées peut aussi dépasser l'imaginaire de la « grande criminalité », y sont inclus notamment : la production et la vente de stupéfiant quelque soit l'échelle, le proxénétisme dont la définition très large peut inclure la seule aide à une personne travailleuse du sexe, les vols en bande organisée…

Concernant la technique de géolocalisation des objets connectés, le spectre est encore plus large puisque l'activation à distance pourra concerner toutes les personnes suspectées d'avoir commis un délit puni de cinq années de prison, ce qui – en raison de l'inflation pénale des lois successives – peut aller par exemple du simple recel, à la

transmission d'un faux document à une administration publique, ou le téléchargement sans droit de documents d'un système informatique.

Surtout, l'histoire nous a démontré qu'il existait en la matière un « effet cliquet » : une fois qu'un texte ou une expérimentation sécuritaire est adopté, **il n'y a jamais de retour en arrière**. À l'inverse, la création d'une mesure intrusive sert généralement de base aux extensions sécuritaires futures, en les légitimant par sa seule existence. Un exemple fréquent est d'étendre progressivement des dispositions initialement votées pour la répression d'un crime choquant à d'autres délits. Le fichage génétique (FNAEG) a ainsi été adopté à l'encontre des seuls auteurs d'infractions sexuelles, pour s'étendre à quasiment l'ensemble des délits : aujourd'hui, 10% de la population française de plus de 20 ans est directement fichée et plus d'un tiers indirectement.

Permettre de prendre le contrôle de tous les outils numériques à des fins d'espionnage policier **ouvre la voie à des risques d'abus ou d'usages massifs extrêmement graves.**

Au regard de la place croissante des outils numériques dans nos vies, accepter le principe même qu'ils soient transformés en auxiliaires de police sans que l'on ne soit au courant pose un problème grave dans nos sociétés. Il s'agit d'un pas de plus vers une dérive totalitaire qui s'accompagne au demeurant d'un risque élevé d'autocensure pour toutes les personnes qui auront – de plus en plus légitimement – peur d'être enregistrées par un assistant vocal, que leurs trajets soient pistés, et même que la police puisse accéder aux enregistrements de leurs vies – par exemple si elles ont le malheur de passer nues devant la caméra de leur téléphone ou de leur ordinateur.

Pour toutes ces raisons, l'article 3 de la LOPJ suscite de graves inquiétudes quant à l'atteinte aux droits et libertés fondamentales (droit à la sûreté, droit à la vie privée, au secret des correspondances, droit d'aller et venir librement). C'est pourquoi nous appelons l'ensemble des parlementaires à oeuvrer pour la suppression de ces dispositions de ce projet de loi et à faire rempart contre cette dérive sécuritaire.

Organisations membres de l'OLN signataires : Le CECIL, Creis-Terminal, Globenet, La Ligue des Droits de l'Homme, La Quadrature du Net, Le Syndicat des Avocats de France, Le Syndicat de la Magistrature.
