

Paris, le 23 novembre 2023,

## Communiqué de l'Observatoire des libertés et du numérique

**Le 16 novembre 2023, le Conseil constitutionnel a rendu sa décision sur la loi de programmation de la justice en censurant une disposition relative à l'activation à distance des objets électroniques. Pour les organisations de l'Observatoire des libertés et du numérique (OLN) qui s'étaient fortement [opposées](#) à cette mesure, cette [décision](#) est plus que bienvenue. Pour autant, elle ne saurait constituer une victoire criante.**

Il faut se souvenir des récentes décisions de ce même Conseil constitutionnel faisant peu cas du respect des libertés : [validation](#) de la vidéosurveillance algorithmique dans [la loi JOP 2024](#), légalisation des [drones](#), blanc-seing à l'assouplissement de la procédure pénale dans la [LOPMI](#) au nom d'une « efficacité opérationnelle »... **Si l'on peut saluer le sursaut de la décision de la semaine dernière, il est difficile d'y déceler une volonté de mettre fin à la fuite en avant sécuritaire**, tant cette institution l'a accompagnée ces dernières années. Pour caractériser une atteinte au droit à la vie privée, le Conseil retient qu'il existe un risque pour les tierces personnes étant dans le champ d'une éventuelle captation déclenchée par cette activation à distance du micro ou de la caméra. Si nous saluons l'établissement d'une telle limite, qui pourra servir d'argument pour d'autres types de surveillance, nous regrettons que le Conseil ne prenne jamais en compte le changement de paradigme philosophique et politique qu'implique la possibilité de transformation de tout objet numérique en mouchard de la police.

Cette absence dans le raisonnement s'illustre par **la validation pure et simple de l'activation à distance des fonctions de géolocalisation de téléphone et autres objets connectés (voiture, balises airtag, montre etc) qui repose exactement sur le même procédé technique** que le dispositif censuré : la compromission d'un périphérique, en y accédant directement ou par l'intermédiaire d'un logiciel espion pour en prendre le contrôle à distance. Or, une telle possibilité soulève de graves problèmes en termes de vie privée, de sécurité et d'intégrité des preuves. On le comprend, le caractère intrusif de cette technique, pourtant au cœur des scandales [Pegasus](#) et [Predator Files](#), n'intéresse pas le Conseil.

Pour justifier cette nouvelle forme de surveillance, le gouvernement et ses soutiens [ont répété](#) que les services de renseignement seraient déjà autorisés à activer à distance les micros ou caméras de terminaux. Pourtant, la lecture de [l'article L. 853-2](#) du code de la sécurité intérieure montre précisément l'inverse : ne peuvent être mis en œuvre par les services de renseignement que des dispositifs qui permettent d'accéder à des données qui « s'affichent sur un écran », telles qu'une personne les « introduit par saisie de caractère » ou « telles qu'elles sont reçues et émises par des périphériques. » Autrement dit, le droit actuel ne permet aux services de renseignement que d'enregistrer l'activité d'une personne sur un téléphone ou un ordinateur, mais en aucun cas d'activer à son insu une fonctionnalité supplémentaire comme un micro ou une caméra. Cette pratique, pourtant avancée pour justifier le bien-fondé de la mesure, **semble donc illégale et doit être sérieusement questionnée.**

De façon générale, on assiste à un essor toujours plus important des technologies de surveillance et à une banalisation de leurs usages par les services de police et de renseignement alors que, souvent, elles ne répondent à aucun cadre. Ces pratiques illégales se généralisent aussi bien dans les ministères que sur le terrain, et la licéité de ces outils n'est jamais une préoccupation de ceux qui les utilisent. Qu'il s'agisse de [logiciels illégaux](#) de surveillance algorithmique et reconnaissance faciale, de [fichage sauvage](#) ou encore [d'exploitation de téléphone](#) en garde à vue, l'impunité se répand, l'illégalité se banalise. **Dans ce contexte et avec ces tendances lourdes, la décision du Conseil constitutionnel est salutaire mais nous apparaît malheureusement trop peu engageante pour y voir un avertissement fort contre la surveillance.**

**Organisations signataires membres de l'OLN : Globenet, [Creis-Terminal](#), la Ligue des droits de l'Homme ([LDH](#)), Le Syndicat des Avocats de France ([SAF](#)), le Syndicat de la Magistrature ([SM](#)), La Quadrature du Net ([LQDN](#)).**