

Pourquoi le Conseil d'État autorise une exploitation de données saisies via l'état d'urgence ?



Pourquoi le Conseil d'État autorise une exploitation de données saisies via l'état d'urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.

En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.



Or Nextinact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.

Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « alors même qu'aucune infraction n'est constatée ».

L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.

Selon le PV de perquisition, la police avait procédé à la saisie d'« un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».

Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.

Article original de Guillaume Champeau



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pourquoi le Conseil d'État autorise une exploitation de données saisies via l'état d'urgence – Politique – Numerama