Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
• N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• faire entrer le juge dans la boucle.

Jean-Jacques Urvoas, ministre de la Justice, au Sénat.

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « données contenues dans tout système informatique présent sur les lieux de la perquisition », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « données accessibles à partir du système initial ou disponibles pour le système initial », qui a disparu.

« Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les **données contenues dans tout système informatique ou équipement terminal présent sur les lieux** de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.

La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui **en indique les motifs** et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition. **À compter de la saisie, nul n'y a accès avant l'autorisation du juge**.

L'autorité administrative **demande au juge des référés du tribunal administratif d'autoriser en tout ou partie leur exploitation**. Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il **statue dans un délai de quarante-huit heures** à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative. **Sont exclus de l'autorisation les éléments dépourvus de tout lien avec la menace** que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics. **En cas de refus** du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa, **les données copiées sont détruites** et les supports saisis sont restitués à leur propriétaire.

Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont **restitués à leur propriétaire**, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent, **à l'issue d'un délai maximal de quinze jours** à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent. **À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée**, les **données copiées sont détruites à l'expiration d'un délai maximal de trois mois** à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.

En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. **Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables** en matière de procédure pénale.

Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. **Ses décisions sont susceptibles d'appel** devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article. »

Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.

Article original de Guillaume Champeau

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

- Expertises techniques (virus, spywares, grayware, fraudes, sinistres informatiques) et judiciaires (contrefaçons, 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercrimalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : État d'urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama