



FOCUS DÉFENSE - SÉCURITÉ

La Lettre de réflexion de la communauté Défense - Sécurité

Mars 2017

Vers un nouveau dispositif de protection des données à caractère personnel de militaires

Si la protection des données à caractère personnel est une préoccupation ancienne inscrite dans le droit français depuis la loi « Informatique et Libertés » du 6 janvier 1978, l'actualité de ces dernières années a mis en lumière de nouveaux enjeux.

D'une part, la multiplication des menaces, dans un contexte marqué par les récents attentats terroristes, montre combien les militaires, comme d'autres forces de sécurité, mais aussi leur famille, peuvent constituer des cibles de choix pour des organisations terroristes ou criminelles. Plusieurs cas concrets, principalement à l'étranger, de vol de données ou de mise en ligne d'informations personnelles, dévoilant notamment l'identité de militaires engagés sur des théâtres d'opération, ont prouvé l'intérêt que peuvent revêtir de telles données pour ce type d'organisations.

D'autre part, l'évolution rapide des nouvelles technologies, la nécessité de s'ouvrir à la transformation numérique et le besoin de plus en plus de mobilité, exigent de repenser notre stratégie de sécurité et de protection et d'ajuster de manière quasi permanente nos solutions.

La protection des données à caractère personnel appelle donc des réponses multiples et adaptées, techniques, juridiques mais aussi humaines pour gérer des menaces de plus en plus prégnantes.

Les mesures techniques et organisationnelles de sécurité (ex : chiffrement, authentification, analyses d'impacts) permettent de garantir la confidentialité des données et d'en contrôler les accès, ainsi que de s'assurer régulièrement de l'efficacité des dispositifs pour les réadapter autant que de besoin aux risques auxquels le ministère de la Défense peut être confronté. D'ailleurs celui-ci a défini dans une instruction ministérielle ses orientations stratégiques en matière de sécurité des systèmes d'informations, qui déclinent le socle des mesures répondant en ce domaine à l'état de l'art.

En matière juridique, et de façon complémentaire à la loi de 1978, le ministère de la Défense s'est doté récemment d'une protection spécifique des données à caractère personnel de militaires, considérées comme sensibles en raison de leur nature, car associant des données à caractère professionnel (par exemple le grade ou l'affectation dans une unité) et des informations relevant de la sphère privée (par exemple l'adresse personnelle ou la composition familiale).

Ce dispositif innovant est prévu par la loi du 3 juin 2016¹ et son décret d'application du 28 décembre 2016². Il impose aux opérateurs privés (mutuelles, banques, associations...) de satisfaire à certaines exigences lorsqu'ils traitent de données à caractère personnel de militaires, nécessaires à leur activité : autorisation préalable de la CNIL³, criblage de leurs personnels accédant à ces données sensibles, mise en place de mesures de protection dont l'effectivité est contrôlable tant par la CNIL que par le ministère de la Défense. A l'inverse, lorsque ces données ne sont pas nécessaires à l'exercice de l'activité de l'opérateur, la loi permet aux militaires d'exiger du responsable du traitement qu'il supprime toute référence à

leur statut au profit de la mention plus neutre d' « agent public ». Pour renforcer le caractère impératif de ces mesures, la loi a également prévu un ensemble de sanctions pénales pouvant aller jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende à l'encontre des responsables de traitement négligents.

Ce dispositif entre en vigueur à compter du 1er juillet 2017. Il vient ainsi compléter plus largement celui déjà existant en matière de protection de l'anonymat des personnels civils et militaires travaillant dans les services de renseignement, et des personnels militaires œuvrant au sein des forces de sécurité⁴.

Enfin, la politique du ministère de la Défense en matière de protection des données à caractère personnel est complétée par des actions indispensables de formation et de sensibilisation de l'ensemble de ses collaborateurs, en particulier au travers du rappel régulier des règles minimales à respecter en matière d'hygiène informatique. Parce que, via les réseaux sociaux, les personnes elles-mêmes rendent accessibles publiquement et à un niveau mondial des informations les concernant personnellement, le ministère a également publié une nouvelle édition du « Guide du bon usage des réseaux sociaux » qui s'adresse tant aux personnels civils ou militaires qu'à leur famille.

Ainsi, la protection des données à caractère personnel n'est-elle pas qu'une problématique technique, mais s'inscrit bien au contraire dans une stratégie de bout en bout qui mobilise de nombreuses expertises. C'est bien cette logique qui sous-tend également le futur règlement européen sur la protection des données. Il entre en vigueur le 25 mai 2018 et oblige à gérer de manière rigoureuse les données à caractère personnel entre un renforcement des droits reconnus à la personne concernée et des exigences et contraintes plus fortes à l'égard des responsables de traitement de données.

Le ministère de la Défense a d'ores et déjà lancé les travaux de mise en conformité avec ces nouvelles règles qui verront la mise en place d'un nouvel acteur incontournable : le délégué à la protection des données.

ACHC Valérie Porcherot
Chargée de mission auprès du DPID
valerie.porcherot@intradef.gouv.fr

¹ Relative au renforcement de la lutte contre le crime organisé et le terrorisme.

² Articles L4123-9-1 et R4123-45 et suivants du code de la défense.

³ Les associations à but non lucratif continuent de bénéficier d'un régime de simple déclaration mais seront néanmoins soumises au respect des autres exigences.

⁴ Article 39 sexiès de la loi du 29 juillet 1881 ; article 861-1 du code de la sécurité intérieure ; articles 413-13 et 413-14 du code pénal.

