Renforcement des mesures destinées à protéger les données à caractère personnel de militaires

Il est inutile de souligner la grande actualité de la présente étude au vu du contexte actuel de lutte contre le djihadisme et le terrorisme.

Par Florent GASTAUD

Juriste NTIC
Spécialiste des questions Informatique et Libertés

→RDLI 4965

La sécurité des données à caractère personnel des personnels de la Défense, et plus globalement des personnels participant à la défense du territoire national, est une préoccupation majeure de ces derniers mois. Force est de constater que, dans le contexte actuel de lutte contre le djihadisme et le terrorisme, ces personnes sont particulièrement exposées.

Bien que relevant du ministère de l'Intérieur, l'assassinat revendiqué par le groupe État islamique de deux policiers en juin 2016 à leur domicile de Magnanville, Jean-Baptiste Salvaing, commandant de police, et sa compagne, Jessica Schneider, secrétaire administrative, ne peut que rappeler la particulière importance de la sécurisation des données à caractère personnel de ces personnels[1].

La divulgation de données privées relatives à ces individus (adresse du domicile, numéro de téléphone, adresse e-mail, etc.) peut ainsi constituer une atteinte directe à leur sécurité ainsi qu'à celle de leurs proches. Il est donc aisé de comprendre la particulière sensibilité des fuites de données relatives à ces personnels.

Toujours dans le périmètre du ministère de l'Intérieur, la fuite des coordonnées personnelles de 112 000 policiers, adhérents de la Mutuelle générale de la police (MGP)[2], quelques jours seulement avant les assassinats précédemment évoqués, interroge.

Ce type de fuite n'est pas isolé. En décembre 2016, ce sont les données personnelles de militaires américains, et notamment de membres de l'US Special Operations Command (SOCOM)[3], qui furent compromises. L'origine de la fuite provient d'un sous-traitant du Pentagone.

Jean-Marc Todeschini, secrétaire d'État auprès du ministre de la Défense, chargé des Anciens Combattants et de la Mémoire, évoque même de « *nombreuses cyberattaques contre des intérêts français au nom des revendications djihadistes, avec une stratégie de recherche et de publication de données personnelles relatives aux agents du ministère de la Défense* »[4].

Conscient de cette menace, le Gouvernement a souhaité renforcer la sécurisation des données à caractère personnel des militaires.

I. – CRÉATION D'UN RÉGIME SPÉCIFIQUE POUR LES TRAITEMENTS DE DONNÉES DE MILITAIRES

Résultant d'un amendement proposé par le Gouvernement, la loi n° 2016-731 du 3 juin 2016, *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*[5] est venue se doter d'un article 117.

Ce dernier a introduit un nouvel article L. 4123-9-1 au Code de la défense[6].

Complémentaire aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée, « *relative à l'informatique, aux fichiers et aux libertés* »[7], ce nouvel article concerne spécifiquement « *les traitements dont la finalité est fondée sur la qualité de militaires des personnes qui y figurent* ».

L'article R. 4123-45 vient préciser que l'application des dispositions de l'article L. 4123-9-1 du Code de la défense requiert que le traitement contienne *a minima* :

- des données personnelles d'identification (exemple : nom, prénom) ;
- une donnée révélant la qualité de militaire (exemple : statut « militaire »). Il convient à cet effet de souligner que la simple qualité d'« agent public » n'est pas suffisante ;
- une information relative à la vie privée (exemple : adresse ou composition de la famille).

L'objectif est clair : protéger les traitements faisant le lien entre le statut de militaire et une ou plusieurs informations privées concernant ce dernier.

Plusieurs écueils peuvent d'ores et déjà être formulés. D'une part, un certain nombre de personnels, pourtant exposés aux mêmes menaces que les militaires, sont exclus de ce régime. C'est notamment le cas des policiers ou encore des personnels civils de la Défense. Notons à cet effet que plus d'un quart du personnel du ministère de la Défense est civil[8].

D'autre part, en créant des dispositions qui concernent directement la protection des données à caractère personnel au sein du Code de la défense, en lieu et place de procéder à une modification de la loi n° 78-17 du 6 janvier 1978 dite « *Informatique et libertés* », le Gouvernement ne favorise très certainement pas les objectifs de simplification, de compréhension et de qualité du droit[9].

Enfin, la rédaction de l'article L. 4123-9-1 du Code de la défense est ambiguë dès ses premières dispositions. En conditionnant l'application de cet article aux « *traitements dont la finalité est fondée sur la qualité de militaires des personnes qui y figurent* », une certaine confusion semble être réalisée par les rédacteurs de ce texte entre la notion de « *finalité* » et celle de « *donnée traitée* ». Ce nouveau régime, comme l'indique Jean-Marc Todeschini, vise avant tout à renforcer l'encadrement des traitements mis en œuvre par les acteurs privés pour les militaires, tels que les assurances ou les mutuelles[10]. Il a donc pour objectif de sécuriser les traitements dans lesquels sont amenées à figurer des données à caractère personnel de militaires, et non ceux, dont la finalité serait spécifiquement liée au statut de militaire. En guise d'exemple, ce nouveau régime serait ainsi amené, dans son esprit, à viser le traitement d'un assureur dès lors que la finalité de son traitement relève de « *la passation, gestion et exécution des contrats d'assurance* »[11], et qu'il comporte des données personnelles de militaires, qui sont identifiées comme telles. Pourtant, *stricto sensu*, le traitement de l'assureur n'est pas « *fondé sur la qualité de militaires* » mais se contente de traiter de telles données.

II. – LES TRAITEMENTS DE MILITAIRES DÉSORMAIS CONDITIONNÉS À UN RÉGIME D'AUTORISATION

A. – Création d'un régime de double autorisation

Première mesure protectrice pour les traitements de données de militaires : la nécessité qu'ils soient autorisés par la Commission nationale de l'informatique et des libertés (Cnil) préalablement à leur mise en œuvre.

Ainsi, les traitements de données de militaires rejoignent désormais la liste des traitements nécessitant une autorisation préalable de la Cnil, en vertu de l'article 25 de la loi « Informatique et libertés »[12], et au même titre que les interconnexions de fichiers dont les finalités principales sont différentes, les traitements comportant des appréciations sur les difficultés sociales des personnes, les « *blacklists* », etc.

Dans le cadre de son examen de la demande de traitement, la Cnil aura par ailleurs la faculté de recueillir l'avis du ministre de la Défense, qui prononcera un avis à la suite de la réalisation d'une enquête administrative. Notons que cette enquête, qui par définition n'est pas régie par le Code de procédure pénale, peut donner lieu à la consultation des traitements de constatation des infractions à la loi pénale[13] régies par l'article 230-6 du Code de procédure pénale[14].

En pratique, et comme le soulignait très justement la Cnil dans son avis[15] relatif au projet de décret portant application de l'article L. 4123-9-1 du Code de la défense, la Commission devra systématiquement saisir le ministre de la Défense.

En effet, les autorisations de traitements des données de militaires ne peuvent être délivrées si « *le comportement ou les agissements de la personne responsable du traitement sont de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'État* »[16]. Or, la Commission ne pouvant apprécier

(1) Article paru *in Le Monde*, 14 juin 2016, La revendication des meurtres de Magnanville a eu lieu en direct sur Facebook :

(2) Article paru *in Le Figaro*, 27 juin 2016, Les données personnelles de 112 000 policiers ont fuité sur le web :

(3) Article paru *in* ZDNet.com, 31 déc. 2016, *US government subcontractor leaks confidential military personnel data* : <www.zdnet.com/article/us-government-subcontractor-leaks-confidential-military-personnel-data/>.

(4) Article paru sur le site du Sénat, Compte rendu intégral des échanges de la séance du 31 mars 2016 : <www.senat.fr/seances/s201603/s20160331/s20160331018.html>.

(5) Loi n° 2016-731 du 3 juin 2016 « *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* ».

(6) Article L. 4123-9-1 du Code de la défense.

(7) Loi n° 78-17 du 6 janvier 1978 modifiée, « *relative à l'informatique, aux fichiers et aux libertés* » précitée.

(8) Article du secrétariat général pour l'administration du ministère de la Défense, 15 oct. 2016, Politique RH civile et militaire : <www.defense.gouv.fr/sga/le-sga-en-action/ressources-humaines/politique-rh-militaire-et-civile/politique-rh-militaire-et-civile>.

(9) Étude annuelle 2016 du Conseil d'État – Simplification et qualité du droit, sept. 2016 : <www.ladocumentationfrancaise.fr/rapports-publics/164000610-etude-annuelle-2016-du-conseil-d-etat-simplification-et-qualite-du-droit>.

(10) Article paru sur le site du Sénat, Compte rendu intégral des échanges de la séance du 31 mars 2016 : <www.senat.fr/seances/s201603/s20160331/s20160331019.html>.

(11) En référence à la délibération n° 2013-212 du 11 juillet 2013 concernant les traitements automatisés de données à caractère personnel relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurance, d'assistance et par leurs intermédiaires (norme simplifiée n° 16) : <www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000027837527>.

(12) Article 25 de la loi n° 78-17 du 6 janvier 1978 modifiée « *relative à l'informatique, aux fichiers et aux libertés* », précitée.

(13) Article R. 4123-48 du Code de la défense.

(14) Article 230-6 du Code de procédure pénale.

(15) Délibération n° 2016-388 du 8 décembre 2016 portant avis sur un projet de décret portant application de l'article L. 4123-9-1 du Code de la défense.

(16) Article I, alinéa II, de l'article L. 4123-9-1 du Code de la défense.

par elle-même ce risque dans le cadre de sa procédure d'autorisation des traitements, elle devra nécessairement s'en remettre au ministre de la Défense disposant de pouvoirs d'investigations plus étendus lui permettant d'apprécier efficacement les risques suscités.

En réalité, la mise en œuvre de traitements de données de militaires sera donc conditionnée à l'obtention d'une double autorisation :

- du ministre de la Défense, fondée sur le comportement et les agissements du responsable de traitement ;
- de la Cnil, fondée sur l'appréciation des finalités et les conditions de mise en œuvre du traitement.

Notons au passage quelques incohérences dans la conception de ce mécanisme, notamment sur les délais applicables. Le ministre de la Défense dispose d'un délai de deux mois, renouvelable une fois, à compter de sa saisine par la Cnil pour rendre son avis. Or, la Cnil dispose elle-même d'un délai maximal de deux mois, renouvelable une fois, pour se prononcer dans le cadre d'une demande formée au titre de l'article 25 de la loi dite « *Informatique et libertés* » auprès du responsable de traitement. À défaut de s'être prononcée dans les délais, la demande d'autorisation est réputée rejetée. Cette situation se réalisera donc systématiquement si le ministre de la Défense utilise l'intégralité du délai lui étant accordée par décret pour se prononcer…

Cette incohérence théorique trouve cependant ses limites dans la pratique. En effet, la Cnil dépasse quasi systématiquement et bien allègrement les délais de l'article 25 de la loi dite « Informatique et libertés », sans pour autant que les demandes d'autorisation soient en pratique rejetées.

B. – Dérogations au régime d'autorisation

Notons que ce régime d'autorisation comporte deux dérogations :

- pour les associations à but non lucratif ;
- pour les traitements mis en œuvre pour le compte de l'État.

1°/ Publicité de l'autorisation

Par dérogation à l'article 31 de la loi « Informatique et libertés »[17], les délibérations de la Cnil portant autorisation ou refus de traitement de données de militaires ne feront pas l'objet d'une publicité. Conformément à son règlement intérieur, la Cnil réalise habituellement cette publicité sur Légifrance.

En revanche, les autorisations délivrées par la Cnil ainsi que les déclarations de traitements reçues en la matière seront systématiquement communiquées au ministre de la Défense[18].

Ainsi est garantie une plus grande discrétion des responsables de traitements de données de militaires, diminuant de fait leur exposition aux attaques ciblées.

2°/ Un accès restreint aux données de militaires

Seconde mesure protectrice pour les traitements de données de militaires : la restriction des personnes habilitées à accéder aux traitements de données de militaires.

À cet effet, il semblerait, à la lecture du II de l'article L. 4123-9-1 du Code de la défense, que le responsable de traitement ne puisse accorder des accès au traitement de données de militaires qu'aux seules personnes physiques ayant reçu préalablement un avis favorable du ministre de la Défense.

Le ministre de la Défense dispose d'un délai de deux mois pour se prononcer, renouvelable une fois. À défaut, l'avis est réputé favorable[19].

En pratique, les actions suivantes seront donc nécessaires pour les responsables de traitement concernés :

- procéder au fil de l'arrivée de nouveaux salariés à des demandes d'avis auprès du ministre de la Défense afin de disposer de salariés habilités à travailler sur les traitements de données de militaires ;
- mettre en place un mécanisme de gestion des habilitations efficace, avec notamment la réalisation de revues régulières des droits d'accès, fondée notamment sur l'entrée et la sortie des salariés et éventuels prestataires de l'entreprise.

Dans le cadre de ces avis, le ministre de la Défense pourra réaliser des enquêtes administratives pouvant aboutir à des refus d'autorisation d'accès aux données de militaires. L'employeur responsable de traitement devra en conséquence adapter ses processus de recrutement afin d'anticiper, au mieux, les avis du ministre. Ainsi, le responsable de traitement pourrait justifier, compte tenu de la sensibilité des données auxquelles aura accès le futur salarié, de systématiquement demander aux candidats à l'embauche, au cours du processus de recrutement, la communication du B3 du casier judiciaire[20]. Rappelons cependant que le B3 ne comporte que les condamnations les plus graves et les peines privatives de liberté. Or, rien ne préjuge qu'une inscription au B1 ou B2 ne serait pas suffisante, pour le ministre de la Défense, à justifier un refus d'accès aux données de militaires.

3°/ Des prescriptions techniques de sécurité spécifiques

Troisième mesure protectrice pour les traitements de données de militaires : la définition de prescriptions techniques spécifiques ayant pour objectif d'assurer un haut niveau de sécurité pour les traitements de données de militaires[21].

À cet effet, le ministre de la Défense ainsi que le ministre de l'Intérieur devront fixer par arrêtés lesdites prescriptions. À ce jour, ces arrêtés n'ont pas encore été pris. Leur contenu devrait peu ou prou rejoindre les prescriptions actuellement recommandées par l'Anssi (Agence nationale de la sécurité des systèmes d'information), ainsi que celles édictées et contrôlées par la Cnil au titre de l'article 34 de la loi « Informatique et libertés »[22].

La ministre de la Défense vient ainsi s'immiscer dans ce pouvoir de contrôle des mesures de sécurisation traditionnellement réservé à la Cnil, puisqu'il est désormais compétent pour contrôler le respect des prescriptions techniques de sécurité fixées par arrêtés, pour les traitements de données de militaires, en complément de la Cnil.

Les responsables de traitement auront par ailleurs l'obligation de communiquer au ministre de la Défense, en parallèle de leur demande d'autorisation de traitement auprès de la Cnil, les mesures techniques et d'organisation permettant de garantir le respect des prescriptions techniques de sécurité[23]. Aucune précision pratique ne vient pour le moment indiquer comment ces mêmes responsables de traitement pourront communiquer avec le ministre à cet effet. Notons par ailleurs que la constatation de manquements, par le ministre de la Défense, à la lecture du dossier de sécurité ne pourra donner lieu qu'à une simple information de la Cnil.

4°/ Un dispositif spécifique d'alerte en cas de fuites de données de militaires

Quatrième mesure protectrice pour les traitements de données de militaires : la création d'un mécanisme d'alerte en cas de fuites de données concernant des traitements de militaires. Ce mécanisme fait très sensiblement penser à celui d'ores et déjà prévu par l'article 34 *bis* de la loi dite « *Informatique et libertés* »[24] pour les fournisseurs de services de communications électroniques.

À cet effet, les responsables de traitements de données de militaires ont l'obligation d'informer « *sans délai* » la Cnil d'une éventuelle divulgation ou d'un accès non autorisé audit traitement[25]. À charge pour la Cnil de répercuter cette information auprès des ministres de la Défense et de l'Intérieur afin qu'ils puissent prendre toutes mesures adéquates pour garantir la sécurité des personnes impactées par la fuite. Ces ministres pourront notamment ordonner au responsable de traitement d'informer sans délai les personnes concernées de la divulgation ou de l'accès non autorisé aux données[26]. Sans cet accord, le responsable de traitement ne pourra cependant pas prendre l'initiative d'informer les personnes concernées.

Cette dernière disposition interroge, notamment au regard de sa future articulation avec le règlement européen général sur la protection des données (n° 2016/679)[27]. Ce dernier prévoit en effet qu'en cas de violation de données à caractère personnel, le responsable de traitement devra, à compter de sa date d'entrée en vigueur, soit le 25 mai 2018, notifier la violation à l'autorité compétente, mais également, dans les meilleurs délais, aux personnes concernées si ladite violation est « *susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* »[28]. Le règlement prévoit bien une dérogation à cette notification en son article 23, mais celle-ci n'est pas fondée sur un accord préalable de ministre, mais notamment sur la préservation de la sécurité publique, de la défense ou de la sécurité nationale. Ainsi, en cas de contradiction avérée des normes suscitées, le mécanisme d'accord préalable des ministres de la Défense et de l'Intérieur pourrait bien faire l'objet d'un contrôle de conventionalité et être écarté dans sa mise en application, en vertu de la supériorité du droit communautaire sur le droit interne[29].

C. – Un régime applicable à compter du 1er juillet 2017

L'application de l'article L. 4123-9-1 est conditionnée[30] à la publication d'un décret fixant les modalités d'application. Ce décret, créant dans le Code de la défense les articles R. 4123-45 à R. 4123-51, n'entrera en vigueur qu'à compter du 1er juillet 2017[31].

Dès lors, les dispositions de ce nouveau régime relatif aux données de militaires ne seront applicables qu'à compter du 1er juillet 2017.

L'article 117 de la loi n° 2016-731 dispose par ailleurs que les responsables de traitement disposent d'un délai d'une année à compter de l'entrée en vigueur de la loi pour obtenir une autorisation de traitement ou déposer une déclaration de traitement. Dès lors, les responsables de traitement pourront réaliser ces démarches du 1er juillet 2017 jusqu'au 1er juillet 2018. Passé cette date, tout responsable de traitement mis en œuvre en méconnaissance des dispositions de l'article L. 4123-9-1 du Code de la défense sera passible des sanctions prévues à l'article 226-16 du Code pénal[32].

Une fois de plus, l'articulation avec le règlement européen général sur la protection des données (n° 2016/679) interroge. Le règlement entrera en effet en application le 25 mai 2018, soit préalablement au 1er juillet 2018, date à laquelle les responsables de traitements devront, en vertu du droit interne français, avoir obtenu une autorisation ou avoir déclaré leurs traitements de données de militaires.

Or, le règlement européen sonne pour partie le glas des déclarations et procédures d'autorisations préalables formelles au profit d'une logique d'*accountability*. Certes, le règlement prévoit tou-

(17) Article 31 de la loi n° 78-17 du 6 janvier 1978 modifiée « *relative à l'informatique, aux fichiers et aux libertés* », précitée.

(18) Article R. 4123-50 du Code de la défense

(19) Article R. 4123-47 du Code de la défense.

(20) Ducorps-Prouvost É. (Cabinet Soulier), nov. 212, Les antécédents judiciaires des salariés : de quels leviers dispose l'employeur pour contourner le sacro-saint principe du respect de la vie privée ? : <www.soulier-avocats.com/upload/documents/Soulier_Droit_Social_novembre_2012.pdf>.

(21) Alinéa IV de l'article L. 4123-9-1 du Code de la défense.

(22) Article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée « *relative à l'informatique, aux fichiers et aux libertés* ».

(23) Article R. 4123-49 du Code de la défense.

(24) Article 34 *bis* de la loi n° 78-17 du 6 janvier 1978 modifiée « *relative à l'informatique, aux fichiers et aux libertés* »

(25) Alinéa V de l'article L. 4123-9-1 du Code de la défense.

(26) Article R. 4123-51 du Code de la défense.

(27) Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* » (règlement général sur la protection des données) : <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>.

(28) Article 34 du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité.

(29) Concernant spécifiquement les règlements européens : CE, s.-s. réunies, 24 sept. 1990, n° 58.657, *Boisdet*, Rec. p. 251.

(30) Alinéa VII de l'article L. 4123-9-1 du Code de la défense.

(31) Article 3 du décret n° 2016-1946 du 28 décembre 2016 « *relatif à la protection de données à caractère personnel de militaires prévue à l'article L. 4123-9-1 du Code de la défense* ».

(32) Article 226-16 du Code pénal.

jours la possibilité de consulter préalablement une autorité, mais uniquement lorsqu'« *une analyse d'impact relative à la protection des données* [...] *indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* » ou lorsque le droit des États membres le prévoit pour les traitements effectués dans le cadre d'une mission d'intérêt public[33]. Preuve complémentaire, s'il en fallait, des maladresses de conception de ce nouveau régime spécifique dédié aux données de militaires.

Dès lors, et avant même l'entrée en vigueur de ce nouveau régime de protection des données de militaires, sa mise en œuvre peut d'ores et déjà être remise en cause.

(33) Section 3 du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, précité.