Commission nationale de l'informatique et des libertés

Délibération n° 2022-110 du 10 novembre 2022 portant avis sur un projet d'arrêté portant autorisation de mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication du ministère de la défense (demande d'avis n° 21011213)

NOR : *CNIX2303383X*

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère des armées d'une demande d'avis concernant un projet d'arrêté portant autorisation de mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication du ministère de la défense,

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, et notamment son titre IV ;

Après avoir entendu le rapport de Mme Isabelle LATOURNARIE-WILLEMS, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Etant rappelés les éléments suivants :

La Commission a été saisie d'un arrêté qui vise à encadrer la mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication dans les états-majors, directions et services du ministère des armées. Ce texte constitue un acte réglementaire unique au sens du IV de l'article 31 de la loi du 6 janvier 1978 susvisée. Il a donc vocation à encadrer des traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Les traitements projetés ont pour objectif principal d'assurer la sécurité et la défense des systèmes d'information et de communication du ministère de la défense visés à l'article 1er du décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication. Au regard de leurs finalités, ces traitements ont vocation à être régis par le titre IV de la loi du 6 janvier 1978.

La mise en œuvre de traitements de gestion des traces s'inscrit, selon le ministère, dans un contexte d'intensification de la menace d'origine « cyber » et repose sur la nécessité de pouvoir identifier les irrégularités d'accès ou d'utilisation des systèmes d'information. A cet égard, la Commission rappelle que la traçabilité des actions est une mesure élémentaire de la sécurité des traitements et que l'analyse proactive des traces est une mesure essentielle à l'exploitation efficace de la traçabilité. Le projet de déployer des traitements de gestion des traces au sein du ministère des armées s'inscrit dans cette perspective, et répond ainsi aux préconisations de la Commission quant à la nécessité de développer des outils de journalisation.

Par ailleurs, la Commission relève que les dispositifs projetés seront des systèmes de journalisation périmétrique, qui n'ont donc pas vocation à assurer la traçabilité opérationnelle de traitements métier, mais à contribuer à la mise en œuvre globale de la sécurité. Elle rappelle à cet égard que, pour les traitements métier qui seront amenés à contenir des données à caractère personnel, des systèmes de journalisation devront être intégrés afin d'assurer la traçabilité des opérations portant sur des données à caractère personnel, comme elle a pu le rappeler dans sa recommandation relative aux mesures de journalisation (délibération n° 2021 du 14 octobre 2021).

S'agissant du périmètre des traitements concernés, le ministère indique que le projet d'arrêté a, en premier lieu, vocation à couvrir un traitement mis en œuvre par la direction des réseaux d'infrastructure et des systèmes d'information (DIRISI), dont la finalité exclusive est la gestion des traces issues de certains systèmes d'information des services relevant du chef d'état-major des armées, de la direction générale de l'armement et du secrétariat général pour l'administration du ministère. La mise en œuvre de ce traitement est autorisée par un arrêté du 26 juillet 2013 qui n'a été publié qu'au *Bulletin officiel* des armées, et qui a vocation à être encadré par le présent arrêté.

De manière générale, la Commission note que l'intention du ministère est que le projet d'arrêté qu'il lui soumet pour avis, s'il a vocation à couvrir le traitement de la DIRISI, permette également de fixer un cadre juridique à d'autres traitements de données qui répondent à des caractéristiques similaires. Elle relève que le ministère entend limiter les vulnérabilités liées à l'exploitation d'un outil unique de gestion des traces en incitant les différents états-majors, directions et services à mettre en œuvre leur propre traitement de gestion des traces. Dans cette perspective, le projet d'arrêté vise à encadrer les traitements de gestion des traces que les différentes entités du ministère ainsi que les organismes qui lui sont rattachés pourraient mettre en œuvre pour assurer la sécurité et la défense de leurs systèmes d'information respectifs.

Ces éléments rappelés, le projet d'arrêté appelle les observations suivantes.

Emet l'avis suivant sur le projet d'arrêté :

Sur les finalités des traitements

Les traitements projetés ont pour finalités « *d'assurer la sécurité et la défense* » des systèmes d'information précités « *et des informations qu'ils comportent* », « *d'assurer leur gestion et leur exploitation* » et « *d'identifier les irrégularités d'accès ou d'utilisation de ces systèmes et des informations qu'ils comportent contraires aux dispositions législatives ou réglementaires en vigueur* » (par exemple, les usages non conformes aux règles et principes d'utilisation de ces systèmes).

D'après les précisions apportées par le ministère, ces traitements permettront aussi de procéder à des analyses des données collectées, pouvant notamment conduire à prononcer des sanctions à l'égard des agents responsables des irrégularités qui auront été constatées ou, plus généralement, apporter une réponse à un incident survenu sur un système d'information.

La Commission observe que, quand bien même les traitements de gestion des traces projetés permettront de procéder à de telles analyses, les décisions relatives aux agents qui seront prises sur le fondement des données qui en sont issues, le seront dans le cadre de traitements distincts, conformément aux finalités de ces derniers.

Sur la délimitation des catégories de données pouvant être enregistrées dans les traitements

Selon les termes du projet d'arrêté, les traitements de gestion des traces ont vocation à encadrer la collecte et l'exploitation *de « données techniques relatives à la traçabilité de l'utilisation des systèmes d'information* » du ministère des armées.

A titre liminaire, la Commission rappelle que les données de traçabilité correspondent, au sens de l'article 101 de la loi du 6 janvier 1978, aux données relatives aux opérations de collecte, de modification, de consultation, de communication (y compris les transferts), d'interconnexion et d'effacement portant sur des données à caractère personnel. Ces données doivent permettre d'établir le motif, la date et l'heure des opérations de consultation et de communication des données et, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et les destinataires de celles-ci.

L'article 2 du projet d'arrêté prévoit que les traitements de gestion des traces pourront comporter, outre des données de traçabilité (« *notamment adresse IP, adresse URL, date et heure de connexion au système d'information* »), des « *données d'identification* » (« *notamment nom, prénom, numéro de matricule* […] »), « *d'authentification* » (« *notamment identifiant de certificat électronique, jeton d'accès* ») ainsi que des « *données permettant la communication et les échanges* » (« *notamment objet des courriels, éléments de nommage des fichiers, volume des fichiers* »).

L'énumération des données susceptibles d'être traitées au titre de chacune de ces quatre catégories n'est pas limitative. Le ministère justifie ce choix par la nécessité de pouvoir faire face aux évolutions technologiques à venir, dans un contexte de transformation numérique constante.

Sans remettre en cause cet impératif, la Commission rappelle que le traitement de ces données ne devra pas porter une atteinte disproportionnée à la vie privée des personnes concernées. A cet égard, elle invite le ministère à prévoir des garanties sur les points suivants.

En premier lieu, la notion de « *données d'identification* » est susceptible de faire l'objet d'une interprétation large et, ainsi, de couvrir de nombreuses catégories de données. La Commission observe que la nécessité d'anticiper les évolutions technologiques à venir ne saurait justifier l'absence de délimitation des « *données d'identification* » susceptibles d'être collectées. Dès lors, le projet d'arrêté devrait soit fixer une liste limitative des données susceptibles d'être traitées au titre de cette catégorie, soit, à tout le moins, exclure certaines d'entre elles. A cet égard, la Commission prend acte de l'engagement du ministère d'exclure explicitement la photographie des données collectées au titre des « *données d'identification* ».

En tout état de cause, elle invite le ministère à limiter le traitement de données relevant de cette catégorie aux seules données strictement nécessaires à l'identification de l'utilisateur dont la trace est enregistrée.

En deuxième lieu, s'agissant des « *données permettant la communication et les échanges* » mentionnées au 4° de l'article 2 du projet d'arrêté, la Commission prend acte de l'engagement du ministère de modifier ce projet pour exclure expressément le traitement du contenu des correspondances au titre de cette catégorie de données.

Par ailleurs, les données relatives aux échanges et correspondances sont susceptibles de concerner un nombre important de personnes comprenant, outre les agents habilités à accéder aux systèmes d'information du ministère, les personnes avec lesquelles ces agents échangent des courriers électroniques. La Commission invite le ministère à prendre les mesures nécessaires pour garantir que ne seront conservées que les données relatives aux échanges et correspondances pertinents au regard des finalités des traitements.

En dernier lieu, au-delà du périmètre et du volume des données pouvant être traitées, la Commission considère que l'information délivrée aux personnes concernées par le traitement de leurs données devra être régulièrement mise à jour afin d'énumérer précisément les données susceptibles d'être collectées.

Sur les mesures mises en place pour exclure le traitement de données sensibles

L'arrêté encadrant les traitements de gestion des traces ne peut pas fonder le traitement de données sensibles au sens du I de l'article 6 de la loi du 6 janvier 1978, dès lors qu'un tel traitement doit être autorisé par décret en Conseil d'Etat pris après avis motivé et publié de la Commission.

En l'espèce, le ministère a mis en place des mesures organisationnelles pour exclure la collecte de telles données, en faisant en sorte que les traitements projetés ne collectent pas l'objet des messages ni le nom de fichiers comportant une mention du caractère privé de la correspondance. Cependant, il n'est pas exclu que ces

informations contiennent des données sensibles, sans que l'émetteur ait mentionné le caractère privé du message. Dans cette hypothèse, la Commission invite le ministère à assurer une information directe, régulière et renforcée de ses agents quant à la nécessité de mentionner le caractère privé de leurs correspondances et d'exclure absolument l'inscription de données sensibles dans leurs correspondances et leur navigation sur le web.

Sur les durées de conservation

L'article 3 du projet d'arrêté fixe une durée maximale de conservation des données d'un an, « *avant, le cas échant, archivage intermédiaire pour une durée ne pouvant excéder cinq ans à compter de leur enregistrement* ».

En premier lieu, la Commission rappelle que la notion d'archivage intermédiaire implique une nécessaire restriction des accès aux données. A cet égard, elle prend acte de l'engagement du ministère de modifier l'article 3 en ce sens et de préciser les finalités concernées par l'archivage.

En second lieu, le projet d'arrêté prévoit que « *le service de santé des armées conserve les informations et données à caractère personnel qu'il traite conformément à l'article R. 6113-9-2 du code de la santé publique* ». D'après les précisions apportées par le ministère des armées, cette disposition visait à répondre au besoin initial de créer un traitement de gestion des traces spécifique à ce service. Dès lors que ce projet a été écarté et que la DIRISI exploitera les traces produites par les systèmes d'information du service de santé des armées, le ministère s'est engagé à supprimer cette disposition, ce dont la Commission prend acte.

Sur les accédants et destinataires des données des traitements

L'article 4 du projet d'arrêté énumère les accédants et destinataires des données du traitement. La Commission relève que seuls des agents publics dûment habilités pourront accéder au traitement ou être destinataires des données qui en sont issues. Elle observe donc qu'aucune transmission ou accès ne sera possible vis-à-vis d'autres personnes, notamment les éventuels fournisseurs de solutions auxquels le ministère aurait recours (par exemple pour des opérations de support de « niveau 3 » sur des équipements ou systèmes).

Sur l'information des personnes concernées

Le projet d'arrêté prévoit que les responsables de traitement informent les personnes concernées selon les modalités définies à l'article 116 de la loi du 6 janvier 1978.

Le ministère précise qu'un document rappelant les règles en matière de sécurité informatique, signé par chaque agent lors de son arrivée, pourra être mis à jour pour intégrer une mention d'information propre à l'application de l'arrêté encadrant les traitements de gestion des traces. En outre, cet arrêté pourra être mis en ligne sur l'espace intranet du ministère.

D'une part, la Commission observe que certains agents auront, avant la mise en œuvre des traitements, signé un document rappelant les règles de sécurité. Ce document ne contient donc pas de mentions d'information sur les traitements qui auront vocation à être mis en œuvre. Elle invite dès lors le ministère à informer individuellement ces agents.

D'autre part, la Commission considère que les mentions d'information devront être adaptées aux spécificités du traitement mis en œuvre conformément à l'acte réglementaire.

Enfin, des personnes autres que les agents habilités à accéder aux systèmes d'information du ministère pourraient être concernées par les traitements de gestion des traces. Il n'est en effet pas exclu, au regard du traitement d'informations relatives aux échanges et correspondances, que des données à caractère personnel concernant les destinataires ou les auteurs de telles communications (qu'il s'agisse d'autres agents ou de personnes extérieures au ministère) fassent l'objet d'un traitement. La Commission estime que des mesures qui permettent d'assurer l'information de ces personnes devront être mises en œuvre et observe que, dans cette perspective, le ministère entend insérer une mention d'information sur son site web.

Sur les mesures de sécurité

A titre liminaire, si les dispositions encadrant les traitements intéressant la sûreté de l'Etat et la défense n'imposent pas la réalisation d'une étude d'impact sur la vie privée, la Commission considère qu'au regard de la nature des traitements envisagés et du nombre de personnes potentiellement concernées, il est souhaitable que le ministère en réalise une afin de s'assurer que les conditions de mise en œuvre du traitement limitent effectivement les risques sur la vie privée des personnes concernées.

En premier lieu, le ministère indique que le système proposé ne permettra pas de modifier les données brutes. Cet élément, combiné à la ségrégation matérielle et logique du traitement de gestion des traces et à la mise en œuvre d'une prise d'empreinte conservée tout au long du cycle de vie de la donnée, permettra d'assurer l'intégrité des données.

En deuxième lieu, la Commission accueille favorablement le fait que le ministère ait mis en œuvre une authentification conforme à sa délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, en rendant obligatoire une authentification à double facteur avec carte à puce et mot de passe.

En troisième lieu, les données stockées et les communications seront chiffrées avec des algorithmes et des procédures de gestion de clés conformes à l'annexe B1 du référentiel général de sécurité.

En quatrième lieu, la Commission relève que les opérations réalisées sur les traitements de gestion des traces mis en œuvre dans le cadre du présent acte réglementaire unique feront elles-mêmes l'objet d'une journalisation spécifique, et que le texte prévoit que les données associées seront conservées pendant une durée de cinq ans, ce qui n'apparaît pas conforme aux préconisations de la Commission. Sauf à ce que des éléments justifient cette durée et qu'il soit démontré qu'elle permet de faire diminuer un risque résiduel important, la Commission considère cette

durée comme disproportionnée. A cet égard, elle prend acte de l'engagement du ministère de réduire cette durée à trois ans.

Par ailleurs, elle recommande que des mesures soient mises en œuvre pour assurer l'intégrité des données de journalisation, notamment en mettant en œuvre une politique d'accès restreint à cette journalisation, différente de celle du traitement principal.

En dernier lieu, la Commission rappelle que l'ensemble des traitements mis en œuvre sur le fondement de cet arrêté devront respecter les mêmes critères en termes de sécurisation des données que ceux présentés à la Commission dans le cadre de sa saisine.

La présidente,
M.-L. Denis