Délibération n° 2017-206 du 20 décembre 2017

de la Commission de Contrôle des Informations Nominatives portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité

« *Gestion des Habilitations et des Accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* »

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Arrêté Ministériel n° 2016-501 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion administrative des salariés ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives.

La Commission de Contrôle des Informations Nominatives,

Conformément à l'article 1er alinéa 1 de la Loi n° 1.165 du 23 décembre 1993, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, Autorité Administrative Indépendante, a pour mission de veiller au respect de ces dispositions. A ce titre, elle est notamment habilitée à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la loi.

C'est ainsi que dans le cadre de ses fonctions, la Commission insiste sur l'importance de sécuriser les systèmes d'information (SI) et de garantir la confidentialité des données que celui-ci contient. A cet effet, elle recommande de mettre en place un véritable système d'habilitation afin que chaque utilisateur du SI ne puisse accéder qu'aux données dont il a besoin pour l'exercice de sa mission, ce qui se traduit au niveau interne par la mise en place d'un mécanisme de définition des niveaux d'habilitation d'un utilisateur dans le système, et d'un moyen de contrôle des permissions d'accès aux données.

La mise en place d'un tel système étant aujourd'hui de plus en plus répandue, la Commission souhaite, par la présente recommandation, préciser les grands principes de protection des informations nominatives applicables aux traitements automatisés d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* ».

Les principes ainsi consacrés par la présente délibération s'appliquent aux traitements soumis à autorisation :

- mis en œuvre par des personnes physiques ou morales de droit privé, visées à l'article 6 de la Loi n° 1.165 du 23 décembre 1993 ;

- mis en œuvre par des responsables de traitements, organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public portés sur une liste établie par Arrêté Ministériel**,** tels que mentionnés à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

Ils s'appliquent également aux personnes morales de droit public ou aux Autorités publiques qui demeurent quant à elles soumises au régime de demande d'avis.

I. Champ d'application et qualification du traitement

L'habilitation est fonction d'un profil préalablement défini, généralement lié à une position hiérarchique ou à une fonction au sein de la structure, et non à une personne déterminée.

Cela permet de faciliter la gestion des accès en cas de mouvement de personnel. Au contraire, lorsque les accès sont attribués par personne, il convient d'être extrêmement réactif et de supprimer sans délai tout accès en cas de départ d'un membre du personnel du service ou de la structure.

L'habilitation doit conférer ainsi à chaque utilisateur les droits qui sont strictement nécessaires à l'accomplissement de ses attributions. A ce titre, elle doit déterminer, notamment :

- les données et applications auxquelles celui-ci peut avoir accès, de manière dédiée ou partagée (réseau local ou partagé, dossiers de travail, imprimantes, téléphones, etc.) ;
- l'étendue des droits ainsi conférés : accès en simple consultation, en inscription, en suppression.

Cette habilitation impliquant la collecte d'informations nominatives, le traitement automatisé y afférant est soumis aux formalités prévues par la Loi n° 1.165 du 23 décembre 1993. En effet, un responsable de traitement peut décider de procéder au contrôle ou à la surveillance des habilitations informatiques mises en place au sein de son entité.

A cet égard, la Commission indique que cette notion de contrôle ou de surveillance du système de gestion des habilitations se conçoit comme « *toute activité qui consiste en la collecte, la détection et/ou l'enregistrement, dans le cadre de rapports établis à intervalles réguliers, des données à caractère personnel d'une ou de plusieurs personnes, relatives à l'utilisation des habilitations informatiques* ».

A titre d'exemple, elle considère ainsi que cette définition peut inclure la supervision par le biais d'un système de remontée d'alerte et/ou d'alarme.

Il résulte de ce postulat que dès lors que le système de gestion des habilitations informatiques est utilisé par le responsable de traitement soit à des fins de contrôle ou de surveillance, soit dans le cadre de « *soupçons d'activités illicites* », le traitement est alors soumis à l'autorisation préalable de la Commission, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

A contrario, dès lors que le système de gestion des habilitations informatiques n'est pas utilisé à des fins de contrôle ou de surveillance, le traitement est alors régi par l'Arrêté Ministériel n° 2016-501 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion administrative des salariés.

Au vu de ces éléments, la Commission estime nécessaire de retenir les principes fondamentaux ci-après exposés.

II. Grands principes en matière d'habilitations informatiques

➢ *Des profils d'habilitation définis, formalisés et auditables*

En premier lieu, la Commission rappelle qu'il est nécessaire pour toutes les catégories de comptes (nominatifs ou collectifs), d'identifier et d'authentifier tout utilisateur en fonction notamment du niveau de risque associé à la ressource, du type d'utilisateur ou encore du type d'accès. Cette séparation des tâches et des domaines de responsabilité permet ainsi de limiter l'accès à des données à caractère personnel aux seuls utilisateurs dûment habilités.

A cet égard, elle demande de respecter d'une part le principe du « *besoin d'en connaître* » qui correspond à la définition, par le métier, des habilitations nécessaires pour l'activité d'un utilisateur donné, et d'autre part le principe « *du moindre privilège* » qui consiste à mettre en place les habilitations strictement nécessaires aux activités liées à chaque compte.

Elle demande également que les modalités d'octroi des habilitations soient documentées.

La Commission rappelle, par ailleurs, que les permissions d'accès des utilisateurs doivent être supprimées ou modifiés dès lors que ces derniers ne sont plus habilités à accéder à une ressource car ils ont quitté l'entité ou bien changé de fonctions.

Elle relève enfin qu'il est impératif de s'assurer du respect des règles de gestion des habilitations. Les propriétaires du système d'information doivent ainsi contrôler régulièrement la pertinence des profils et des accès accordés.

- ***Une politique de validation des habilitations et de gestion des mobilités***

La Commission insiste sur le fait que toute demande d'habilitation doit être validée au moins par le responsable hiérarchique de la personne habilitée. Par ailleurs, si ledit responsable délègue cette tâche, il doit toutefois nécessairement conserver la responsabilité des habilitations de son équipe et de celles attribuées aux personnes effectuant des prestations de service pour son compte.

La Commission demande également au responsable de traitement de veiller à la gestion efficace de tout changement de poste ou de départ afin d'éviter l'accumulation des habilitations. Ainsi lorsqu'une personne est mutée ou quitte l'entité, les habilitations dont elle disposait doivent être modifiées ou retirées immédiatement.

III. <u>Personnes concernées et fonctionnalités du traitement</u>

- ***Personnes concernées***

Les personnes concernées par ce type de traitements sont l'ensemble des utilisateurs du système d'information, quelle que soit la nature de leur activité au sein de l'entité (salarié, consultant en mission, prestataire, stagiaire, etc.).

- ***Fonctionnalités***

La Commission considère qu'un traitement automatisé ayant pour finalité « *Gestion des habilitations et des accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » est susceptible d'avoir, notamment, les fonctionnalités suivantes :

Dans le cadre de la gestion des habilitations *:*

- octroyer / délivrer aux utilisateurs du SI les moyens techniques et fonctionnels permettant de s'authentifier au système d'information afin de pouvoir exercer la fonction et les missions pour lesquelles ils ont été recrutés ;
- gérer les évolutions de droits, les mobilités internes et les départs ;
- mettre à jour les comptes systèmes dans le cadre de changement d'informations administratives (ex : changement de patronyme) ;
- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;
- procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- établir des alertes et/ou des rapports qui permettent de détecter tout risque de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- établir des preuves en cas de litige avec tout utilisateur (employé, prestataire…).

Dans le cadre de la sécurité anti-virus :

- mettre en place des remontées d'alertes sur les risques d'intrusion ;
- établir des rapports (ex : audit de sécurité, détection de risques…).

IV. Licéité du traitement

Aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, « *les informations nominatives doivent être collectées et traitées loyalement et licitement [...] pour une finalité déterminée, explicite et légitime, et ne pas être traitées ultérieurement de manière incompatible avec cette finalité* ».

A ce titre, la Commission rappelle les dispositions de l'article 14.1 de la recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 aux termes desquelles *« les employeurs devraient éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée des employés* » et « *les personnes concernées devraient être convenablement et périodiquement informées en application d'une politique claire en matière de respect de la vie privée* ».

En conséquence, la Commission appelle l'attention des responsables de traitement sur le fait que les informations nominatives des utilisateurs du système d'information, exploitées dans le cadre des traitements qui font appel aux dispositifs concernés par la présente délibération, ne sauraient être détournées de la finalité pour laquelle elles ont initialement été collectées.

En outre, ces dispositifs ne sauraient donner lieu à des pratiques abusives portant atteinte aux libertés et droits fondamentaux des personnes concernées mais également aux droits conférés par la Loi aux Délégués du Personnel et aux Délégués syndicaux.

C'est pourquoi, conformément aux dispositions de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, le demandeur devra apporter les éléments permettant à la Commission de s'assurer que le traitement est « *nécessaire à la poursuite d'un objectif légitime essentiel* », et que les droits et libertés des personnes seront protégés.

V. Justification du traitement

En application de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993, la Commission considère qu'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » peut être justifié par :

- ***Le respect des obligations légales du responsable de traitement***

La Commission prend acte des obligations particulières de vigilance ainsi que de traçabilité des opérations effectuées imposées à certains établissements. Ainsi, pour les établissements bancaires ou assimilés, de telles obligations sont prévues, entre autres, par les textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers.

La Commission estime donc qu'afin de respecter leurs obligations, ces responsables de traitement ou leurs représentants peuvent mettre en place des procédures de surveillance ou de contrôle des habilitations informatiques, dans le strict respect toutefois des principes définis par la présente délibération.

- ***La réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant***

La Commission considère qu'une procédure de surveillance ou de contrôle des habilitations informatiques peut également être justifiée par un intérêt légitime du responsable de traitement ou de son représentant, tel que :

- l'optimisation de l'accomplissement des missions de travail de ses employés ;
- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;
- la prévention et la détection a priori et a posteriori de toute activité non-conforme ou illicite, par des utilisateurs.

Enfin, la Commission rappelle qu'en cas de lien de subordination ou de lien contractuel, le consentement de la personne concernée doit être libre, spécifique et éclairé. En conséquence, la justification fondée sur le consentement de ladite personne ne pourra être retenue.

VI. Catégories d'informations traitées

Conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission considère que les catégories d'informations suivantes peuvent être collectées et traitées :

- identité : nom, prénom et service de l'employé, nom, prénom et signature du supérieur pour la gestion des habilitations ;
- données d'identification électronique : identifiants de la personne habilitée (login et mot de passe) ;
- compte utilisateur : nom du compte, domaine du compte, groupe d'utilisateurs, type de droits ;
- données de connexion : logs, traces d'exécution, horodatage, fichiers journaux.

VII. Durée de conservation

La Commission rappelle que conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, les informations nominatives objets du traitement ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont exploitées.

Ainsi, au regard des fonctionnalités énumérées au point III de la présente délibération, la Commission demande au responsable de traitement de prévoir les durées de conservation de données suivantes :

- s'agissant de l'identité et du compte utilisateur : 3 mois maximum après le départ de l'employé ;

- s'agissant des données d'identification électronique : la durée d'utilisation du S.I. par la personne concernée ;

- s'agissant des données de connexion : 1 an maximum à compter de leur collecte, en fonction de l'activité exercée.

En tout état de cause, elle recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées, conformément à l'article 10-1 susvisé.

Enfin, la Commission rappelle que dans le cadre de l'ouverture d'une procédure contentieuse, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de ladite procédure.

VIII. Information de la personne concernée

- ***Mentions obligatoires***

La Commission rappelle que conformément aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, les personnes concernées par l'exploitation de leurs informations nominatives doivent être informées des mentions suivantes :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'accès et de rectification aux informations les concernant.

- ***Modalités d'information des personnes concernées***

La Commission appelle l'attention du responsable de traitement sur la nécessité de responsabiliser les utilisateurs du S.I. à la protection de leurs informations nominatives.

D'autre part, dans un souci de transparence envers les employés, ainsi que de loyauté dans la relation de travail, elle demande à ce que le responsable de traitement ou son représentant mette en place une charte informatique, venant préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre, suivant les règles posées au point IV de la présente délibération ;
- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;

- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

Enfin, la Commission insiste sur la nécessité de mettre en œuvre une sensibilisation de l'ensemble des utilisateurs du SI non seulement sur les habilitations qui leurs sont accordées et des responsabilités qui en découlent, mais également sur le fait que toutes leurs actions sont tracées.

IX. Personnes ayant accès aux informations et les destinataires

➢ *Personnes ayant accès aux informations*

La Commission considère que l'accès aux informations objets du traitement doit être limité aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement ou du but recherché. Ces accès devront être définis dans la charte mentionnée au point VIII de la présente délibération.

En ce qui concerne les traitements visés aux article 11 et 11-1 de la Loi n° 1.165 du 23 décembre 1993, elle rappelle que conformément aux dispositions de l'article 17-1 de ladite Loi, le responsable de traitement ou son représentant doit « *déterminer nominativement la liste de personnes autorisées qui ont seules accès, pour les strictes besoins de l'accomplissement de leurs missions, aux locaux et aux installations utilisés pour les traitements, de même qu'aux informations traitées* ».

La Commission rappelle enfin que cette liste, tenue à jour, doit lui être communiquée à première réquisition.

➢ *Destinataires*

La Commission rappelle que les Autorités judiciaires et administratives peuvent, dans le cadre exclusif des missions qui leur sont légalement conférées, être rendues destinataires de données objets du traitement, notamment pour la recherche de preuves ou la constatation d'infractions.

Dans ce cas, des mesures de sécurité particulières devront être prises, concernant notamment le support sur lequel ces informations sont transmises, ainsi que la procédure de transfert, conformément aux dispositions du point X de la présente délibération.

X. Confidentialité et mesures de sécurité

La Commission rappelle qu'en application des articles 17 et 17-1 de la Loi n° 1.165 du 23 décembre 1993, le responsable de traitement ou son représentant doit prendre toutes mesures utiles pour préserver la sécurité des informations objets du traitement.

A cet égard, elle préconise que l'authentification soit effectuée par un identifiant et un mot de passe individuel réputé fort régulièrement changé.

Par ailleurs, les accès des personnes mentionnées au point IX devront faire l'objet d'une journalisation.

La Commission demande en outre à ce que les personnes habilitées à avoir accès au traitement soient astreintes à une obligation de confidentialité particulièrement stricte, précisée par écrit (par exemple dans une charte informatique, une charte administrateur ou le contrat de travail).

Enfin, elle admet que des données puissent être extraites et/ou copiées sur un support distinct en vue d'une communication aux Autorités administratives ou judiciaires légalement habilitées. Elle rappelle que dans ce cas, toute copie ou extraction de ces données devra être chiffrée sur son support de réception.

Après en avoir délibéré, la Commission :

Rappelle que :

- la gestion des habilitations informatiques implique la mise en œuvre d'un traitement automatisé d'informations nominatives, au sens de l'article 1er de la Loi n° 1.165 du 23 décembre 1993 ;

- tous les traitements ainsi exploités devront remplir les conditions fixées par la Loi n° 1.165 du 23 décembre 1993, telles que précisées dans le cadre de la présente délibération.

Le Président

Guy MAGNAN