MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER,
DES COLLECTIVITÉS TERRITORIALES
ET DE L'IMMIGRATION

Direction générale
de la gendarmerie nationale

Cabinet

Circulaire nº 94855 du 15 septembre 2011 relative aux règles générales d'emploi des moyens informatiques et des traitements automatisés de données à caractère personnel dans la gendarmerie nationale

NOR : *IOCJ1130110C*

Références :

- Code de la défense ;
- Code pénal ;
- Code de procédure pénale ;
- Loi du 29 juillet 1881 (*Bulletin des lois* nº 637, p. 125 – CLASS. : 59.01) ;
- Loi nº 78-17 du 6 janvier 1978 (*JO* du 7-1-1978, p. 227) ;
- Loi nº 2004-575 du 21 juin 2004 (*JO* du 22-6-2004, p. 11168) ;
- Arrêté du 5 septembre 2011 relatif aux règles générales d'emploi des moyens informatiques et des traitements automatisés de données à caractère personnel dans la gendarmerie nationale (NOR : IOCJ1129972A) ;
- Circulaire nº 31400/DEF/GEND/OE/TI du 7 novembre 1991 (n.i. BO – CLASS. : 44.20) ;
- Circulaire nº 15120/DEF/GEND/2SF/SDTI du 17 avril 2009 (n.i. BO – CLASS. : 98.02).

Pièce jointe : une annexe.

Texte abrogé : circulaire nº 900/DEF/GEND/PM/TI/2C/SSIC du 21 janvier 2004 (n.i. BO – CLASS. : 98.02).

1. **Préambule**

Pour l'exercice de ses missions, la gendarmerie nationale met à disposition des moyens technologiques d'information et de communication ainsi que des traitements automatisés de bases de données à caractère personnel (1).

L'utilisation de ces moyens est encadrée par des dispositions légales et réglementaires. L'accès aux informations, qui résulte de l'utilisation de ces moyens et qui constitue une prérogative exorbitante du droit commun, est de nature à justifier un contrôle strict du respect de la déontologie.

La présente circulaire, prise en application de l'arrêté de septième référence, a pour objet d'en préciser les termes et d'exposer le cadre juridique et les principes déontologiques qui conditionnent les règles d'emploi des moyens informatiques et des traitements automatisés de données à caractère personnel.

2. **Terminologie**

2.1. *Utilisateur*

Au sens de l'arrêté de septième référence, l'utilisateur s'entend comme celui ou celle qui se connecte au système d'information de la gendarmerie ou qui dispose de droits d'accès aux fichiers automatisés.

Il s'agit, notamment, des militaires de la gendarmerie d'active ou de réserve, des personnels civils de la gendarmerie, mais aussi de militaires des armées, de fonctionnaires du ministère de l'intérieur ou d'un autre ministère servant au sein de la gendarmerie (formations mixtes police-gendarmerie, GIR, etc.). Il peut également s'agir de toute autre personne qui, à titre habituel ou non, est autorisée à accéder au système d'information de la gendarmerie ou aux fichiers automatisés de la gendarmerie (ex : les entreprises œuvrant au profit de la STSI²).

2.2. *Système d'information de la gendarmerie (SIG)*

Un système d'information est un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) qui permettent de regrouper, de classifier, de traiter et de diffuser de l'information. Cet ensemble organisé de ressources, parmi lesquelles les moyens informatiques, constitue donc le système d'information de la gendarmerie.

(1) Par souci de clarté, ces traitements sont dénommés « fichiers automatisés » dans le reste du présent texte.

2.3. *Moyens informatiques*

Les moyens informatiques désignent les moyens technologiques d'information et de communication que sont les serveurs, les stations de travail, les postes de consultation, les réseaux internes et externes de la gendarmerie, les terminaux téléphoniques, fixes ou mobiles, ainsi que l'ensemble du parc logiciel, des bases de données automatisées et des périphériques permettant le stockage d'information ou affectés au fonctionnement de ces éléments.

Sont également considérées comme moyens informatiques de la gendarmerie les ressources extérieures accessibles par l'intermédiaire du réseau de la gendarmerie ou par le réseau ADER (ADministration En Réseau).

2.4. *Donnée à caractère personnel*

Constitue une donnée à caractère personnel, au sens de la loi du 6 janvier 1978 modifiée, « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

2.5. *Traitement de données à caractère personnel*

Constitue un traitement de données à caractère personnel, au sens de la loi susvisée, « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

2.6. *Fichier de données à caractère personnel*

Constitue un fichier de données à caractère personnel, au sens de la loi susvisée, « tout ensemble structuré et stable de données à caractère personnel accessible selon des critères déterminés, automatisé ou non. »

3. **Les principes généraux d'emploi des moyens informatiques et des traitements automatisés de données à caractère personnel**

3.1. *Le respect de la légalité*

Le principe de légalité encadrant l'emploi de ces moyens et de ces fichiers automatisés est général et absolu. Il ne peut en aucun cas être contrevenu à la légalité de l'emploi des moyens informatiques ou des fichiers automatisés. En particulier, la recherche de l'efficacité ne saurait justifier un emploi non conforme à la loi et aux règlements.

L'intérêt de la nation, de l'État et la sauvegarde de la paix publique doivent gouverner l'ensemble des actes des utilisateurs du système d'information de la gendarmerie. Toute action ayant pour objet ou pour effet de méconnaître les intérêts fondamentaux de la nation, les intérêts de l'État ou de porter atteinte à la confiance publique est susceptible, au sens du livre quatrième de la première partie du code pénal, de constituer un crime ou délit et peut être puni comme tel.

L'emploi des moyens informatiques et des fichiers automatisés, notamment des fichiers opérationnels de nature judiciaire ou administrative (JUDEX, fichier des personnes recherchées, fichier des permis de conduire...), se fait dans le respect des droits des personnes et des mineurs. Le Conseil constitutionnel a reconnu la valeur constitutionnelle de la protection des données personnelles. Le respect de la dignité des personnes, la renonciation à toute forme de discrimination et le respect de la vie privée ne sauraient être méconnus, sous peine de poursuites pénales conformément aux dispositions des articles 225-1 et suivants et 226-1 et suivants du code pénal. La vigilance sur l'usage des fichiers doit également être absolue. Il est précisé à cet égard que les articles 225-16 à 225-24 du code pénal répriment les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques. En particulier, l'attention est appelée sur les dispositions de l'article 226-22 du code pénal :

« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »

Les règles énoncées ci-dessus ne sont pas exhaustives.

3.2. *Le respect des règles de sécurité*

Une politique de sécurité de ses systèmes d'information est mise en œuvre (*cf.* annexe). Les utilisateurs sont tenus de la respecter. En particulier, ils ne modifient pas sans autorisation la configuration de leur poste de travail et n'y installent pas à leur convenance leurs propres logiciels.

3.3. *Le respect des principes déontologiques*

Les utilisateurs du système d'information de la gendarmerie et des fichiers automatisés sont tenus de faire un usage des moyens mis à leur disposition dans les limites qu'impose la conscience professionnelle. Les exigences de déontologie guident leurs usages des ressources informatiques, notamment lorsqu'ils prennent des mesures intrusives. Par respect d'autrui, ils s'interdisent toute attitude, parole ou geste déplacés, quelles que soient les situations et les personnes auxquelles ils se trouvent confrontés. Ils observent une attitude polie envers les autres utilisateurs de ces ressources et s'imposent de ne pas tenir, au moyen de ces ressources, de propos discourtois au sujet de tiers.

4. **Utilisation du système d'information de la gendarmerie**

4.1. *L'utilisation du SIG est limitée au besoin des missions ou attributions de chacun*

4.1.1. Un usage inapproprié des systèmes d'information peut conduire à la restriction de cet usage et à la sanction du responsable

L'usage à des fins non professionnelles, s'il peut être toléré (messagerie interpersonnelle, internet), ne doit être ni abusif ni excessif. Il ne saurait en tout état de cause avoir d'incidence sur le service.

4.1.2. Le droit d'accéder au système d'information est un moyen de remplir les missions

* Mesures d'urgence

Les responsables informatiques peuvent en cas d'urgence :

– déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;

– isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la présente circulaire ou qui mettrait en péril la sécurité des moyens informatiques.

* Mesures donnant lieu à information

Sous réserve que soit informé le sous-directeur compétent du STSI² ou de l'officier de sécurité des systèmes d'information nationale, et le référent national informatique et libertés pour les fichiers opérationnels dans le cadre de la gestion du référentiel des droits d'accès aux bases opérationnelles – GREFIC, les responsables informatiques peuvent :

– limiter provisoirement les accès d'un utilisateur ;

– à titre provisoire, retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;

– effacer ou isoler toute donnée ou fichier manifestement en contradiction avec la présente circulaire ou qui mettrait en péril la sécurité des moyens informatiques.

* Mesures soumises à autorisation ou responsable du service

Sous condition d'autorisation préalable du sous-directeur compétent du STSI² ou de l'officier de sécurité des systèmes d'information nationale, et du référent national informatique et libertés pour les fichiers opérationnels dans le cadre de la gestion du référentiel des droits d'accès aux bases opérationnelles – GREFIC, les responsables informatiques peuvent :

– retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;

– interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable ;

– proposer d'autres sanctions internes.

Sans préjudice du pouvoir de sanction des autorités militaires de premier et de deuxième niveau, les chefs hiérarchiques de tous niveaux peuvent prendre toutes mesures internes qui permettraient d'assurer le respect des règles générales d'emploi et le bon fonctionnement du système d'information de la gendarmerie nationale.

En outre, des sanctions disciplinaires peuvent être prises, dans le cadre réglementaire fixé par le code de la défense. Les sanctions ne sont pas exclusives de poursuites civiles ou pénales. Le directeur général de la gendarmerie nationale peut, le cas échéant, engager des poursuites civiles à l'encontre des utilisateurs.

4.2. *L'usage d'internet et de la messagerie interpersonnelle doit répondre à des règles d'emploi claires, dont la violation peut donner lieu à des sanctions*

Le personnel de la gendarmerie peut accéder à internet au moyen d'une passerelle sécurisée. Cet accès est principalement réservé à un usage professionnel. À ce titre, il est contrôlé et les traces de connexions sont enregistrées pendant douze mois.

L'internaute fait preuve de vigilance vis-à-vis des informations recueillies et des messages reçus et envoyés.

L'usage de la messagerie interpersonnelle doit également obéir aux règles usuelles de savoir-vivre et de courtoisie. À ce titre, tout message pouvant être assimilé à du harcèlement, à de la diffamation, à des atteintes à la vie privée, à l'image ou à la sensibilité d'autrui est proscrit. L'utilisateur connaît la législation, notamment en matière de fraude informatique, d'atteintes à la personnalité et aux mineurs et d'infractions à la propriété intellectuelle.

Il est rappelé que la messagerie interpersonnelle, mise à disposition par la gendarmerie nationale dans le cadre du service, doit respecter un usage professionnel.

5. **L'emploi des fichiers automatisés dans la gendarmerie**

Il est rappelé que la création d'un fichier au niveau local doit être autorisé par l'échelon central.

5.1. *L'usage des fichiers est limité au droit et au besoin d'en connaître*

5.1.1. Le droit d'en connaître

L'accès aux fichiers fait l'objet d'une habilitation personnelle. Non cessible, elle est liée aux missions.

5.1.2. Le besoin d'en connaître

Tout utilisateur habilité à accéder aux fichiers doit s'assurer que cette consultation est justifiée par la mission du moment. Dans le cas contraire, le droit d'accès ne permet pas, en lui-même, de justifier la consultation des fichiers.

5.1.3. La méconnaissance de ces obligations peut conduire à un retrait des droits d'accès, voire à des sanctions

* Une mesure suspensive des droits d'accès peut être adoptée à titre conservatoire dans l'attente d'une sanction disciplinaire ou d'une sanction pénale. Elle doit impérativement accompagner une procédure de sanction et non s'y substituer.

* Une sanction disciplinaire, pour exploitation non conforme des fichiers automatisés, peut par ailleurs être engagée si l'utilisateur n'a pas respecté les règles d'emploi définies par l'arrêté de référence.

* Le processus de sanction disciplinaire peut également justifier, si les circonstances l'exigent, un signalement au parquet pour retrait d'habilitation d'un officier de police judiciaire.

* Une sanction pénale peut enfin s'envisager, notamment dans les cas où l'usage des fichiers contreviendrait à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans cette hypothèse, il appartient à la hiérarchie de signaler les faits par le biais de l'article 40 du code de procédure pénale.

5.2. *Le contrôle par la hiérarchie*

Les chefs hiérarchiques de la gendarmerie s'assurent du respect, par leurs subordonnés, des règles encadrant l'emploi des fichiers automatisés mis à leur disposition. Ils prennent toutes les mesures utiles pour procéder à la mise en conformité juridique des outils de travail susceptibles d'être créés pour les besoins du service.

6. **Attestation de prise de connaissance**

Chaque utilisateur signe une attestation de prise de connaissance de l'arrêté de septième référence dont l'original est conservé au dossier personnel de l'intéressé. Cette attestation permet de s'assurer que l'utilisateur connaît ses obligations, telles qu'elles sont rappelées dans l'arrêté et précisées dans la présente circulaire. Cette attestation permet également de s'assurer que l'intéressé a conscience des conséquences qui pourraient résulter des manquements à ces obligations.

La présente circulaire ainsi que l'arrêté de septième référence font l'objet d'un module de formation lors des stages de formation initiale et des stages de préparation aux différentes fonctions de commandement.

Pour le ministre et par délégation :
Le général d'armée,
directeur général de la gendarmerie nationale,
J. MIGNAUX

ANNEXE

La sécurité du système d'information de la gendarmerie

1. **L'utilisation du SIG est personnel et confidentiel**

La gendarmerie met à la disposition de son personnel des réseaux et équipements informatiques dans le cadre du service. L'autorisation d'y accéder est personnelle, temporaire et réservée à l'activité professionnelle. À ce titre, la carte professionnelle électronique et le code attribués à chacun pour accéder à son environnement de travail sont strictement personnels et ne peuvent être prêtés. Le titulaire est directement responsable de l'usage qui en est fait.

2. **Les accès aux moyens informatiques sont protégés par la gendarmerie, et cette protection doit être préservée par l'utilisateur**

Aux fins de protection, l'utilisation des équipements informatiques mis à la disposition du personnel de la gendarmerie fait l'objet de contrôles. La gendarmerie peut accéder aux fichiers présents dans les postes de travail et met en œuvre pour ce faire des outils de contrôle ou de sauvegarde d'informations. Les traces de connexion à toutes les applications sont conservées pendant douze mois.

L'utilisation des comptes et des dispositions de contrôle d'accès doivent être protégés par les utilisateurs.

Les utilisateurs doivent prendre toutes mesures pour limiter les accès frauduleux aux moyens informatiques, notamment les comptes et dispositifs de contrôle d'accès et à ce titre ils doivent notamment :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel ;
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel ;
- ne pas prêter ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers ;
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent ;
- informer immédiatement le responsable informatique et l'officier de la sécurité des systèmes d'information (OSSI) de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect ;
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers ;
- s'assurer que l'ordinateur auquel ils ont accès est équipé d'un antivirus à jour ;
- informer l'OSSI lors de leur départ définitif de la gendarmerie.

3. **L'intégrité des systèmes informatiques doit être garantie**

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au système informatique, soit par des manipulations anormales du matériel, soit par l'introduction de logiciels parasites connus sous le nom générique de virus, vers, chevaux de Troie ou bombes logiques.

Modification des environnements

En dehors des modifications ne portant pas atteinte au bon fonctionnement des moyens informatiques, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du responsable informatique.

Par modification d'environnement, on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.

Raccordement de matériels au système d'information de la gendarmerie

Aucun matériel actif ne pourra être raccordé au réseau de la gendarmerie sans l'accord du STSI[2] ou de l'OSSIN.

Traçabilité

En vertu de la loi sur la confiance en l'économie numérique et du décret n° 2006-358 du 24 mars 2006, les données de connexion permettant d'identifier le poste ou l'utilisateur sont conservées et sauvegardées pendant un délai de douze mois pour les connexions internet et fixées par décret pour les applications métiers.

Ces données sont conservées principalement pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales dans le but de mettre ces informations à la disposition de l'autorité judiciaire. Elles peuvent être aussi utilisées à des fins statistiques et de détection de problèmes de réseaux.