GUIDE DU BON USAGE
DES RÉSEAUX SOCIAUX

À destination de tous les militaires et civils du ministère de la Défense et de leur entourage

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

Pour télécharger le guide :

www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf

Sommaire

Intro

Les réseaux sociaux permettent aujourd'hui une grande liberté d'expression sur un espace, qui, même lorsqu'il est privé, peut rester accessible à tous. Le ministère de la Défense n'en interdit pas l'usage à ses agents. Cependant, il est fondamental que vous soyez sensibilisés à ses dangers pour vous protéger. **Ce guide a pour vocation de vous aider, vous et vos proches, à utiliser les réseaux sociaux (Facebook, Twitter, Instagram, YouTube…)** en toute sécurité.

1re partie

Risques et dangers : pourquoi vous protéger sur les réseaux sociaux ?

1 / Vous êtes une cible

2 / Vous pouvez mettre en péril la sécurité de l'Institution et de ses opérations

3 / Vous avez un devoir de réserve et de discrétion

07

1 / Vous êtes une cible

Depuis plusieurs années, le ministère de la Défense fait face à une **menace terroriste*** accrue, à l'étranger comme sur le territoire national. Votre appartenance à l'Institution fait de **vous une cible privilégiée de personnes ou de groupes malveillants,** et en particulier des terroristes.

> ***Exemple :*** *en mars 2012, Mohammed Merah abat trois militaires à Toulouse et Montauban, et en blesse un autre grièvement. Ces quatre personnes ont été ciblées du fait de leur statut de militaire.*

Ces individus maîtrisant Internet et les réseaux sociaux collectent vos données personnelles et les associent avec vos données professionnelles. **L'objectif : exercer une pression et/ou proférer des menaces sur vous**. Ils peuvent aussi cibler un de **vos proches** (famille, amis) afin de vous atteindre.

> ***Exemple :*** *un militaire en opération extérieure a publié sur son profil Facebook un message destiné à son entourage. Sa famille a dû être placée sous protection sur un site militaire après avoir reçu des menaces liées à ce message.*

**Pour en savoir plus, consultez l'article 421-1 du code pénal.*

08

2 / Vous pouvez mettre en péril la sécurité de l'Institution et de ses opérations

Comprendre les risques, c'est également saisir votre possible impact sur la sécurité du ministère de la Défense et de ses agents.

Toute diffusion de contenus (textes, photos ou vidéos) relatifs à votre activité professionnelle et/ou à celle de l'Institution sur les réseaux sociaux peut se révéler être une menace pour la sécurité du personnel de la défense, des opérations et de leur succès, dans la mesure où elle renseigne les personnes mal intentionnées.

3 / Vous avez un devoir de réserve et de discrétion

Dès que vous faites état, directement ou indirectement, à travers les réseaux sociaux, de votre qualité de personnel de la défense (militaire comme civil), vous vous exprimez en tant que membre de l'Institution. Vous êtes garant de son image. Vous devez donc respecter le devoir de réserve et la règle de discrétion (cf. page 10).

Il est indispensable de garder cette réflexion en tête : toute publication sur les réseaux sociaux peut porter atteinte à l'image du ministère et des armées.

3 / Vous avez un devoir de réserve et de discrétion

La réglementation

pour le personnel militaire

Article L4121-2 du code de la défense

« Les opinions ou croyances, notamment philosophiques, religieuses ou politiques, sont libres. **Elles ne peuvent cependant être exprimées qu'en dehors du service et avec la réserve exigée par l'état militaire.** Cette règle s'applique à tous les moyens d'expression. Elle ne fait pas obstacle au libre exercice des cultes dans les enceintes militaires et à bord des bâtiments de la flotte. Indépendamment des dispositions du code pénal relatives à la violation du secret de la défense nationale et du secret professionnel, **les militaires doivent faire preuve de discrétion pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.**

En dehors des cas expressément prévus par la loi, les militaires ne peuvent être déliés de cette obligation que par décision expresse de l'autorité dont ils dépendent.
L'usage de moyens de communication et d'information, quels qu'ils soient, peut être restreint ou interdit pour assurer la protection des militaires en opération, l'exécution de leur mission ou la sécurité des activités militaires. »

pour le personnel civil

Article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires

« Les fonctionnaires sont tenus au secret professionnel dans le cadre institué par le code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations, ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions ».

pour l'ensemble du personnel de la Défense

- **Respect du secret professionnel**

Article 226-13 du code pénal

« La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. »

- **Respect et préservation de l'anonymat de certains agents**

Arrêté du 9 août 2016 modifiant l'arrêté du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense.

Arrêté du 20 octobre 2016 relatif à la préservation de l'anonymat des membres des unités des forces spéciales.

2e partie

Bonnes pratiques : comment vous protéger sur les réseaux sociaux ?

1 / Retenez cette règle fondamentale

2 / Adoptez les bons réflexes

3 / En opération

4 / Votre entourage a un rôle essentiel

5 / Que faire en cas d'injures ou de menaces ?

1 / Retenez cette règle fondamentale

Séparez sur les réseaux sociaux votre vie privée de votre vie professionnelle !

En pratique, cela signifie que, sur un profil personnel, aucune information à caractère professionnel n'est diffusée et vice versa.

2 / Adoptez les bons réflexes

A. Lors de la création de vos profils

- **Avant de les créer :** veillez à **sécuriser vos adresses mail et vos terminaux (ordinateurs, smartphones, tablettes…)** correctement. Pour en savoir plus, consultez les guides sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) **www.ssi.gouv.fr**

- **Avant de publier :** assurez-vous que vos actions (publications, partage, « j'aime ») **ne sont pas configurées par défaut en mode « public »**, mais qu'elles sont au contraire seulement accessibles aux contacts que vous autorisez (« amis/connaissances uniquement/ groupes fermés »).

- **Sur votre profil personnel :**

  - Ne faites pas état de votre statut d'agent de la défense. **L'appartenance au ministère** (fonction, unité, photo en uniforme, bande patronymique, etc.) **ne doit pas être identifiable** en consultant votre profil.

  - Préférez l'utilisation d'un pseudonyme et/ou d'un avatar, afin d'éviter tout risque d'identification.

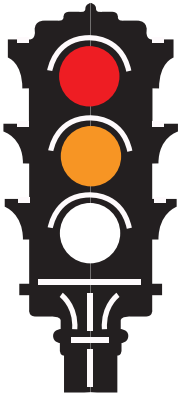
2 / Adoptez les bons réflexes

- **Sur votre profil professionnel (LinkedIn, Viadeo) :**
  - Les **contenus** que vous divulguez ne doivent **être ni trop détaillés** ni trop précis (affectation, spécialité, etc.).
  - **Préférez l'appellation** « agent de la fonction publique » lorsque vous mentionnez votre statut*.
  - Ne donnez **pas d'informations privées** (adresse postale, téléphone, etc.) ou de liens vers vos profils privés.
  - La publication d'une photographie doit également être réfléchie. Est-elle utile ? Adaptée au contexte d'emploi ?

* Conformément à l'article 117 de la loi n° 2016-731 du 3 juin 2016 (qui permet de faire remplacer la qualité de militaire par celle d'agent de la fonction publique dans certains traitements de données à caractère personnel).

2 / Adoptez les bons réflexes

B. Au quotidien sur vos profils

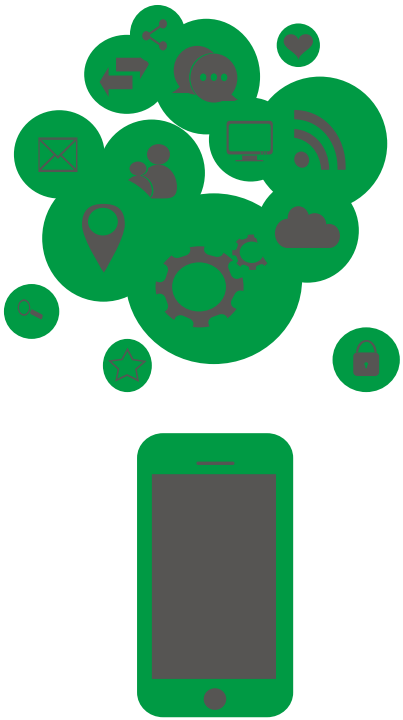


- **N'acceptez** sur les réseaux sociaux personnels **que des personnes connues**.
- **Respectez la réglementation** (cf. p. 10).
- Ne communiquez **pas d'informations confidentielles** susceptibles de mettre en danger les opérations, la vie de ceux qui les mènent ou de nuire à l'image des forces armées (cf. page 8).
- **N'évoquez pas vos missions** (passées, en cours et surtout à venir) ou votre emploi du temps, même partiellement.
- **Vérifiez** systématiquement les **arrière-plans de vos vidéos/photos** avant de les publier (pas de sites militaires, de camarades en tenue, etc.).
- **N'utilisez pas la géolocalisation (*géotaggage*)** ni l'identification (*taggage* nominatif) sur les photos publiées.
- **N'identifiez pas les autres agents** du ministère dans vos commentaires ou en photo/vidéo.
- **Vérifiez les paramètres de confidentialité** (modifiés sans préavis par Facebook, etc.) et changez régulièrement vos mots de passe.
- **Sensibilisez votre entourage** (cf. page 19) à l'utilisation des réseaux sociaux.

2 / Adoptez les bons réflexes

C. Les applications en flux direct

Très populaire sur les réseaux sociaux, ce type d'application (**Facebook Live et Periscope**) permet de faire vivre en direct un événement ou son quotidien à des milliers de personnes non identifiées et non identifiables depuis un simple smartphone.



L'utilisation de ce type de publication est interdite dans les enceintes militaires et, plus largement, lors de vos activités professionnelles, lorsqu'un lien peut être établi de près ou de loin avec la défense.

Nous vous invitons à vous référer à la réglementation (cf. page 10) et à réfléchir aux dangers de ces applications pour votre sécurité et celle de vos collègues/ compagnons d'armes.

3 / En opération

Pour votre sécurité, celle des opérations et missions, certaines règles strictes sont à appliquer :

1. Matériel :

- **Désactivez** la géolocalisation de votre smartphone.
- **Vérifiez** les paramètres de sécurité, modifiés sans préavis par Facebook, etc. (cf. page 13).

2. Contenus :

- **Filmer ou photographier** pendant les combats est un **acte d'indiscipline** qui met en danger votre sécurité et celle de vos compagnons d'armes. C'est aussi un **moyen de renseigner l'ennemi** sur nos procédures et tactiques.
- **Toute diffusion de photos et de vidéos** informant sur le camp (entrée/sortie, agencement, etc.) et les missions (cartes, matériels, écrans, programmation, etc.) est **interdite**.
- Des **équipes images** sont **missionnées** pour réaliser des photos et/ou des vidéos en opération. Ces reportages sont validés par l'État-major des armées avant d'être diffusés. En dehors de cette chaîne dédiée, il est interdit de diffuser tout contenu lié à l'opération sur vos profils.

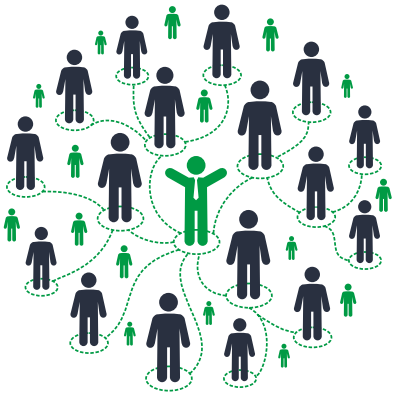
4 / Votre entourage a un rôle essentiel

1er principe : **rien ne disparaît** sur les réseaux sociaux !

2e principe : les données (photos, vidéos, messages…) que vous publiez **ne vous appartiennent plus**.

3e principe : toute publication est une porte d'entrée pour **obtenir des informations** concernant une personne ou une institution. Ainsi, il est possible de réaliser une véritable enquête sur vous, d'identifier vos proches, vos habitudes, vos centres d'intérêt, votre emploi du temps et, par conséquent, tous les éléments **nécessaires à une surveillance, une localisation, des menaces**, etc.

Pour votre sécurité, la leur, mais aussi pour celle de tous les agents du ministère et des opérations, il est donc primordial de leur **expliquer ce qu'ils peuvent et ne peuvent pas faire**.



4 / Votre entourage a un rôle essentiel

4e principe : respecter la discrétion de l'agent de la défense sur les réseaux sociaux :

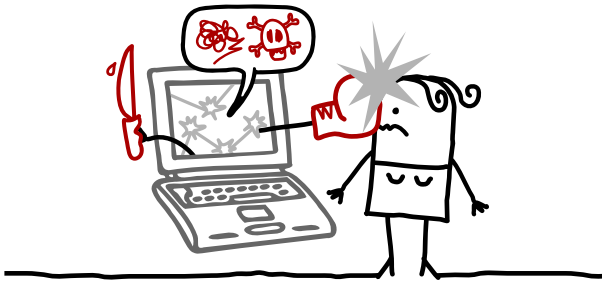
- Vous ne devez pas communiquer sur des informations sensibles, votre statut professionnel, vos missions en France comme à l'étranger ou vos activités. **Informez votre entourage** (famille, amis, connaissances) **de ne pas le faire à votre place.**
- **Précisez-leur qu'ils vous mettent dans l'embarras lorsqu'ils vous questionnent publiquement** sur les réseaux sociaux, **au sujet d'informations que vous ne pouvez pas communiquer**.
- **Sur les profils de vos proches**, si ces derniers diffusent une photo où vous apparaissez, indiquez-leur de **ne pas vous identifier** comme agent de la défense.
- **Sur tout autre profil** (exemples : page officielle du ministère de la Défense ou profil d'une connaissance), si vos proches vous reconnaissent sur une photo ou une vidéo, **demandez-leur de ne pas vous *tagger* et de ne faire allusion ni à votre identité ni à votre métier.**

5 / Que faire en cas d'injures ou de menaces ?

Vous ou vos proches êtes victimes de propos injurieux, diffamatoires, racistes, sexistes, homophobes ou menaçants :

1. Ayez immédiatement le réflexe d'en **garder une preuve**, faisant apparaître la date de celle-ci (capture d'écran, impression…)
2. Dénoncez le compte auprès de la **plate-forme fournisseur** (Facebook, Twitter…) en cliquant sur « Signaler ».
3. Signalez-le également sur la **plate-forme du Gouvernement** : **https://www.internet-signalement.gouv.fr/PortailWeb/**
4. **Rapprochez-vous de votre service juridique** qui vous conseillera et vous aidera à engager les poursuites judiciaires adéquates : dépôt de plainte pénale/assignation devant le tribunal civil.

- En cas de menaces sérieuses : **rendez compte en priorité à votre chef/supérieur** avec les preuves du contenu.



3e partie

Les erreurs à ne pas commettre

1 / Ce que vous ne devez pas écrire

2 / Ce qu'une photo révèle

3 / Ce que votre entourage ne doit pas écrire

1 / Ce que vous ne devez pas écrire

Sur son compte Twitter (masqué pour des raisons de sécurité), un jeune a reproduit, en guise de biographie, la devise d'un régiment de l'armée de terre.

Une rapide vérification du compte permet de confirmer qu'il s'agit bien d'un militaire. Il apparaît en uniforme sur sa photo de profil. Il raconte sa vie quotidienne avec son emploi du temps (horaires de train, lieux et dates de sa prochaine mission Sentinelle), ses états d'âme et donne des renseignements sur sa petite amie (nom, localisation, établissements scolaires fréquentés, famille…).

C'est une mine d'informations pour une personne malveillante. En plus d'enfreindre les règles applicables et de s'exposer à des sanctions, le jeune homme fait, sans même s'en rendre compte, courir des risques inutiles à ses camarades et à sa petite amie.

Il compte dans ses abonnés une jeune femme qui a l'intelligence de présenter une biographie discrète sur un compte privé, rendant inaccessibles ses tweets *sans son accord. Une bonne initiative à prendre en exemple !*

2 / Ce qu'une photo révèle

Voici les éléments obtenus par l'observation (sans logiciel particulier) d'une photo d'apparence anodine diffusée sur le profil d'un réseau social :

Dans les propriétés de la photo (métadonnées) :
- modèle et configuration de l'appareil photo ;
- auteur ;
- localisation.

Sur la photo elle-même :
- absence de personnes circulant sur le parapet (site non sécurisé ?)

Sur la photo elle-même :
- orientation du site en fonction des ombres

Sur la photo elle-même :
- présence de conteneurs près du poste de garde (contenu ? utilisation potentielle pour se dissimuler ?)

En résumé, publier un contenu (photo, vidéo, fichier) sur un réseau social n'est pas sans conséquences : si vous êtes suivi par une personne malveillante ne disposant d'aucun matériel spécifique, vous pouvez néanmoins sans vous en rendre compte la renseigner, et ce, en temps réel.

3 / Ce que votre entourage ne doit pas écrire

Le besoin de vos proches d'exprimer leur ressenti concernant vos missions ou activités peut les conduire à commettre malgré eux des indiscrétions.

4e partie

Résumons

Dès que vous faites état, directement ou indirectement, par le biais d'images ou de propos, de votre qualité de personnel de la défense sur les réseaux sociaux, vous ne vous exprimez plus en tant que citoyen lambda, mais en tant que membre de cette Institution.

Cadre réglementaire	• Devoir de réserve • Règle de discrétion • Respect de la confidentialité • Garant de l'image des armées
Responsabilités	• Séparez votre vie personnelle de votre vie professionnelle • Sécurisez vos comptes et profils • Sensibilisez votre entourage
Conduite à tenir	• Maîtrisez l'utilisation des réseaux sociaux et le contenu de vos publications • Faites attention aux visages, bandes patronymiques et arrière-plans de vos photos/vidéos • Respectez le cadre particulier des opérations • Ne faites pas usage des applications de flux direct

Directrice de la publication : Valérie Lecasble
Chef de projet : Cellule réseaux sociaux de la DICoD
Contributeurs : EMA/COM, DICoD, SIRPA terre, SIRPA marine, SIRPA air
Chef du bureau des éditions : CF Jérôme Baroë
Conception graphique : Christine Pirot
Secrétaire de rédaction : Isabelle Arnold
Chef de fabrication : Jean-François Munier
Création DICoD - décembre 2016

www.defense.gouv.fr