



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*

GUIDE DU BON USAGE DES RÉSEAUX SOCIAUX



À destination des militaires et civils
du ministère des Armées et de leur entourage



SOMMAIRE



RETENEZ CETTE RÈGLE FONDAMENTALE	5
LES ERREURS À NE PAS COMMETTRE	6
1 - Ce que vous ne devez pas écrire.....	7
2 - Ce que votre entourage ne doit pas écrire	8
3 - Ce qu'une photo révèle	9
BONNES PRATIQUES :	
COMMENT VOUS PROTÉGER SUR LES RÉSEAUX SOCIAUX ?	10
1 - Adoptez les bons réflexes	11
2 - En opération	15
3 - Votre entourage a un rôle essentiel	16
4 - Que faire en cas d'injures ou de menaces ?	17
RISQUES ET DANGERS :	
POURQUOI VOUS PROTÉGER SUR LES RÉSEAUX SOCIAUX ?	18
1 - Vous êtes une cible	19
2 - Vous pouvez mettre en péril la sécurité de vos camarades, de l'Institution et de ses opérations	19
3 - Vous avez un devoir de réserve et de discrétion	20
EN RÉSUMÉ.....	24
LEXIQUE.....	25

INTRODUCTION

Les réseaux sociaux permettent aujourd'hui une grande liberté d'expression sur un espace qui, même lorsqu'il est privé, est de fait accessible à tous. Le ministère des Armées n'en interdit pas l'usage à son personnel militaire et civil.

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, LinkedIn, TikTok...) en toute sécurité.**



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

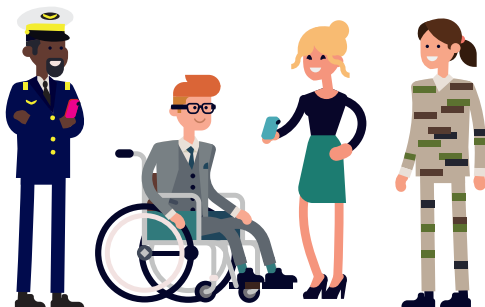


LES ERREURS À NE PAS COMMETTRE

1 - CE QUE VOUS NE DEVEZ PAS ÉCRIRE

2 - CE QUE VOTRE ENTOURAGE NE DOIT PAS ÉCRIRE

3 - CE QU'UNE PHOTO RÉVÈLE

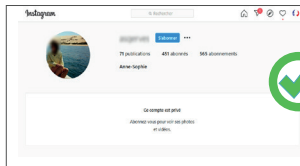
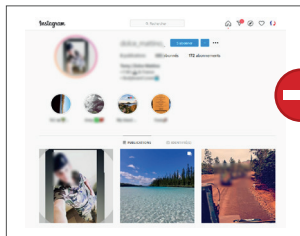


1 - CE QUE VOUS NE DEVEZ PAS ÉCRIRE

Votre nom, votre grade, votre unité d'affectation, votre géolocalisation... en bref, tout renseignement qui peut mettre en péril votre situation ou votre entourage.

Ce compte Instagram (masqué pour des raisons de sécurité) est un compte public. 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, où l'on distingue en plus un tatouage (détail qui permet d'identifier une personne encore plus facilement). Il raconte sa vie quotidienne en *stories* et photos dans son fil d'actualité avec son emploi du temps, des lieux identifiés, des *hashtags* militaires..., ses états d'âme et donne des renseignements sur ses amis (commentaires avec noms d'utilisateurs non protégés).

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 son entourage.



Sur son compte, cette jeune femme a l'intelligence de présenter une biographie discrète sur un compte privé, rendant inaccessibles ses publications sans son accord. Une bonne initiative à prendre en exemple.

2 - 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 indiscretions.

Quelques exemples de ce qu'ils doivent s'astreindre à ne pas publier :



Mon mari me manque, J-10 avant la terre ferme ;)



Une pensée pour ceux qui vivent leur première mission



Bonne mission, bonne mer



Aujourd'hui notre fils fête ses 25 ans sur le *Charles de Gaulle*



Mon copain part dans 5 jours et 3 heures en mer :(



J'ai une pensée pour ma sœur qui est en mission



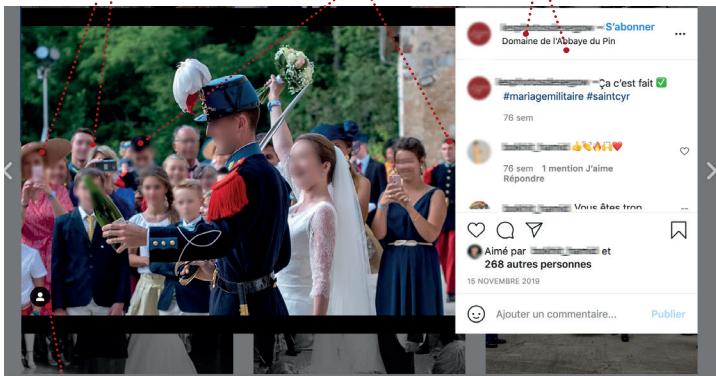
3 - CE QU'UNE PHOTO RÉVÈLE

Présence de personnes facilement identifiables de l'entourage proche des mariés

Présence d'autres militaires

Dans les propriétés de la photo (métadonnées):

- modèle et configuration de l'appareil photo
- auteur
- localisation



Identification des comptes des mariés par l'auteur de la photo

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. En opération, publier un contenu lié à cette opération est tout simplement interdit (p. 13).

BONNES PRATIQUES: COMMENT VOUS PROTÉGER SUR LES RÉSEAUX SOCIAUX?

1 - ADOPTEZ LES BONS RÉFLEXES

2 - EN OPÉRATION

**3 - VOTRE ENTOURAGE
A UN RÔLE ESSENTIEL**

**4 - QUE FAIRE EN CAS D'INJURES
OU DE MENACES?**



1 - ADOPTEZ LES BONS RÉFLEXES

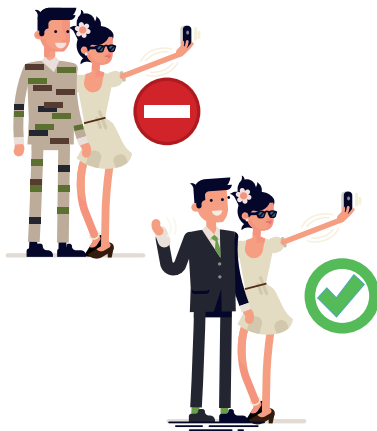
LORS DE LA CRÉATION DE VOS PROFILS

- **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 :**

- Il est interdit de faire état de votre statut d'agent de la défense. **L'appartenance au ministère** (fonction, unité, photo en uniforme, bande patronymique, badge nominatif, 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.



- **Sur votre profil professionnel (LinkedIn, Viadeo...):**

- Les **contenus** que vous divulguez ne doivent **être ni trop détaillés** ni trop précis (affectation, spécialité, etc.). **Pour rappel, LinkedIn est un réseau social public, à vocation professionnelle, mais tout aussi accessible que les autres réseaux. Il ne déroge pas aux réglementations citées précédemment.**
- **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 ? Divulgue-t-elle des informations (badge nominatif, lieux identifiables, bande patronymique, etc.) ?
Rappel : les photos à caractère professionnel et opérationnel sont interdites.

CHOISISSEZ DES MOTS DE PASSE ROBUSTES

Personne ne doit pouvoir deviner vos mots de passe. Créez des mots de passe impersonnels et avec toutes sortes de caractères. Ne les dévoilez à personne. Évitez de les mémoriser automatiquement sur vos sessions. Ne les notez pas dans vos carnets ou sur des *post-it* qui traînent sur votre bureau !

ACTIVEZ L'AUTHENTIFICATION À DEUX FACTEURS

Avec l'authentification à deux facteurs, on fait appel à deux facteurs différents pour s'assurer de l'identité de l'utilisateur de façon plus sûre. Par exemple : vous vous connectez au site internet de votre banque avec votre mot de passe (premier facteur). Un code à quatre chiffres est alors envoyé sur votre téléphone par SMS (deuxième facteur). Une fois le code reçu, vous le saisissez et vous pouvez alors entrer sur le site et poursuivre pour accéder à votre compte. Rappelons qu'utiliser uniquement un système de mot de passe vous expose à de nombreux risques. Les mots de passe peuvent être découverts facilement par des pirates informatiques chevronnés ou encore captés par des tentatives de hameçonnage. Ils sont aussi souvent oubliés, parfois peu sécurisés ou partagés entre utilisateurs. Plus sécurisée que l'authentification simple, l'authentification à deux facteurs rend plus difficile le piratage de vos données.

AU QUOTIDIEN SUR VOS PROFILS

- **N'acceptez** sur les réseaux sociaux personnels **que des personnes connues**.
- **Respectez la réglementation** (cf. p. 13).
- Ne communiquez **pas d'informations confidentielles** susceptibles de mettre en danger les opérations, la vie de ceux qui les mènent et de leurs familles ou de nuire à l'image des forces armées (cf. p. 7).
- **Il est interdit d'évoquer 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.).
- **Il est interdit d'utiliser la géolocalisation (*géotaggage*)** ni l'identification (*taggage* nominatif) sur les photos publiées. Exemples: Strava, Nike Run Club, Adidas Running.

* Dans le prolongement des restrictions sur la mention de la qualité militaire dans certains traitements de données à caractère personnel (cf. notamment art L. 4123-9-1 du code de la défense).

- **Il est interdit d'identifier 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. p. 20) à l'utilisation des réseaux sociaux.

Les applications en flux direct

Très populaires sur les réseaux sociaux, ces fonctionnalités (**Facebook Live, IG direct, TikTok et Twitch**) permettent de faire vivre en direct un événement ou son quotidien au monde entier 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 législation et la réglementation (cf. p. 13) et à réfléchir aux dangers de ces applications pour votre sécurité et celle de vos collègues/compagnons d'armes.

VERROUILLEZ TOUJOURS VOS SESSIONS

Sur votre poste de travail, déconnectez-vous de vos réseaux sociaux ou verrouillez automatiquement votre session ou votre téléphone, même pour deux minutes d'absence.

2 - EN OPÉRATION

Pour votre sécurité, celle des opérations et missions, certaines règles strictes sont à appliquer sous peine de sanctions (cf. p.13 et 14):

MATÉRIEL

- **Désactivez** la géolocalisation de votre *smartphone* et de vos objets connectés (montres, etc.).
- **Vérifiez** les paramètres de sécurité, modifiés sans préavis par Facebook, etc.

CONTENUS

- Il est interdit de filmer ou photographier pendant les combats. Cet acte 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 (EMA) avant d'être diffusés. En dehors de cette chaîne dédiée, il est interdit de diffuser tout contenu lié à l'opération sur vos profils.

Il n'existe aucune exception à la validation des images d'opérations par l'EMA.

3 - VOTRE ENTOURAGE A UN RÔLE ESSENTIEL

1^{er} principe : tout est conservé sur les réseaux sociaux !

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

3^e principe : toute publication est une porte d'entrée pour exercer des pressions, y compris violentes, et/ou **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** (cf. p. 8).

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

- Il est interdit de communiquer sur des informations sensibles, votre statut professionnel, vos missions en France comme à l'étranger ou vos activités. **Demandez à votre entourage** (famille, amis, connaissances) **de ne pas le faire non plus**.
- Précisez-leur qu'ils vous mettent dans l'embarras et en danger lorsqu'ils vous questionnent publiquement sur les réseaux sociaux, **au sujet d'informations que vous ne pouvez pas communiquer**, et qu'ils prennent un risque eux-mêmes.
- **Sur les profils de vos proches**, si ces derniers diffusent une photo où vous apparaissez, demandez-leur de ne pas vous identifier comme agent de la défense.

- Sur tout autre profil (exemples : page officielle du ministère des Armées, 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.**

4 - QUE FAIRE EN CAS D'INJURES OU DE MENACES ?

Vous ou vos proches êtes victimes de propos injurieux :

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, etc.) en cliquant sur « Signaler ».
3. Signalez le contenu également sur les plateformes du Gouvernement : **<https://cybermalveillance.gouv.fr/>** ou **<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.



RISQUES ET DANGERS : POURQUOI VOUS PROTÉGER SUR LES RÉSEAUX SOCIAUX ?

- 1 - VOUS ÊTES UNE CIBLE
- 2 - VOUS POUVEZ METTRE EN PÉRIL
LA SÉCURITÉ DE VOS CAMARADES,
DE L'INSTITUTION
ET DE SES OPÉRATIONS
- 3 - VOUS AVEZ UN DEVOIR
DE RÉSERVE ET DE DISCRÉTION



1 - VOUS ÊTES UNE CIBLE

Depuis plusieurs années, le ministère des Armées 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. **Leur objectif : exercer une pression et/ou proférer des menaces contre 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.

2 - VOUS POUVEZ METTRE EN PÉRIL LA SÉCURITÉ DE VOS CAMARADES, DE L'INSTITUTION ET DE SES OPÉRATIONS

Comprendre les risques, c'est également saisir votre possible impact sur la sécurité du ministère des Armées 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 est interdite car elle 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.

*Pour en savoir plus, consultez les articles 421-1 et suivants du code pénal.

En décembre 2020, le site Mediapart révèle qu'il a trouvé, via différentes applications, plus de 800 profils de soldats français déployés à l'étranger et plus de 200 profils de membres des forces spéciales.

Une enquête à retrouver sur Youtube:

<https://www.youtube.com/watch?v=LbcqJpQSuMg>



3 - VOUS AVEZ UN DEVOIR DE RÉSERVE ET DE DISCRÉTION

QU'EST-CE QUE LE DEVOIR DE RÉSERVE ? 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 avez donc l'obligation de respecter le devoir de réserve, la règle de discrétion et le secret professionnel, sous peine de sanctions (cf. p. 13 et 14).

FAKE NEWS: LES QUESTIONS À SE POSER FACE À UNE INFORMATION POUVANT ALTERER VOTRE DEVOIR DE RÉSERVE ET DE DISCRETION

Qu'est-ce qu'une *fake news* ? En français, *fake news* se traduit par fausses informations (aussi appelées *infox*). Les fausses informations englobent toute allégation ou imputation d'un fait dépourvu d'éléments vérifiables de nature à la rendre vraisemblable.

Comment évaluer la qualité et la pertinence d'une information et discerner le vrai du faux ? Voici quelques questions à se poser automatiquement :

Qui est l'auteur de l'information ? L'auteur est souvent identifié par son nom, par ses initiales ou par l'intitulé d'un site correspondant au compte du réseau social sur lequel se trouve l'information. Parfois, il n'est pas mentionné ou il écrit sous un pseudonyme ou pour un organisme. Il est important de déterminer la légitimité de l'auteur : est-il un expert ou non sur le sujet ? Certains sites proposent même d'accéder, *via* un lien hypertexte, à la biographie d'un auteur d'article et à l'ensemble de ses publications.

Quel est l'objectif de l'auteur ? Relater des faits ou exprimer son opinion sont deux choses différentes.

D'où vient l'information ? Les sources d'une information sont primordiales pour déterminer sa crédibilité. L'origine d'un chiffre ou d'une citation, quand elle est mentionnée, permet au lecteur de s'y référer directement. Certains sites proposent des liens hypertextes renvoyant vers les sites sources.

L'information a-t-elle été publiée sur d'autres réseaux sociaux / sites ? Il est important de comparer et de croiser les sources. Cela permet de voir si l'information est présente sur d'autres plates-formes et de voir comment elle est traitée ailleurs.

De quand date l'information ? Il est important de savoir à quel moment les faits relatés se sont produits. Par exemple, certaines fausses informations s'appuient sur des images prises dans des contextes et à des moments différents pour commenter un sujet d'actualité. Les légendes sous les images, la date de publication d'un *post* ou d'un article, les métadonnées sont susceptibles d'apporter de précieux renseignements.

L'information présente-t-elle des détails incohérents ? Par exemple, lorsque l'image ne correspond pas à la légende qui l'accompagne, cela doit éveiller les soupçons sur la véracité de l'information.

Que disent les commentaires ? Parce qu'ils soulignent parfois l'incohérence d'une information, les commentaires des internautes sont utiles pour jauger la crédibilité des informations avancées.

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

LA LÉGISLATION ET LA RÉGLEMENTATION

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.**

[...]

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

Article 39 sexies de la loi du 29 juillet 1881 modifiée sur la liberté de la presse et l'arrêté modifié du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense.

Articles 413-13 et 413-14 du code pénal pour certains services ou unités spécialisés : services spécialisés de renseignement (cf. l'article R811-1 du code de la sécurité intérieure) et forces spéciales (arrêté modifié du 20 octobre 2016).





EN RÉSUMÉ

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 uniquement en tant que citoyen, mais en tant que membre de cette Institution.

CADRE LÉGAL

- Devoir de **réserve**
- Règle de **discretion**
- 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 (pendant les heures de service, dans une enceinte militaire, en tenue, etc.)

LEXIQUE

Facebook : Facebook est un réseau social en ligne qui permet à ses utilisateurs de publier des images, des photos, des vidéos, des fichiers et documents, d'échanger des messages, de joindre et créer des groupes et d'utiliser une variété d'applications sur une variété d'appareils.

Twitter : Twitter est un réseau social de *microblogage*. Il permet à un utilisateur d'envoyer gratuitement des micromessages, appelés *tweets*, sur Internet, par messagerie instantanée ou par SMS. Ces messages sont limités à 280 caractères.

Instagram : Instagram est une application, un réseau social et un service de partage de photos et de vidéos. L'appellation Instagram est un mot-valise bâti à partir de *Insta*, de l'anglais *Instant camera* (appareil photographique instantané), et de *gram*, du mot anglais *telegram*.

LinkedIn : LinkedIn est un réseau social professionnel en ligne. LinkedIn fonctionne sur le principe de la connexion (pour entrer en contact avec un professionnel, il faut le connaître auparavant ou qu'une de nos connexions intervienne) et du *réseautage* (mise en relation professionnelle).

Youtube : YouTube est un site web d'hébergement de vidéos et un média social sur lequel les utilisateurs peuvent envoyer, regarder, commenter, évaluer et partager des vidéos en *streaming*. Les vidéos sont accessibles par catégories et à l'aide de mots-clés (*tags*) et peuvent être importées sur un *blog* personnel. Tout internaute inscrit peut publier des commentaires et aimer (ou non) les vidéos en ligne.

TikTok : TikTok est une application mobile de partage de vidéos et de *réseautage* social. TikTok permet aux utilisateurs de visionner des clips musicaux, mais également de filmer, monter et partager leurs propres clips. L'utilisateur choisit une chanson, puis se filme par-dessus pendant 60 secondes. L'application comporte de nombreux titres ainsi que de nombreux genres musicaux, dont le hip-hop et la musique électronique. Elle est connue pour être populaire auprès des célébrités.

Twitch : Twitch est un service de *streaming* vidéo en direct et de vidéo à la demande. Le site se concentre principalement sur la diffusion en direct de jeux vidéo y compris des compétitions d'e-sport puis se diversifie sur d'autres contenus — notamment musicaux et discussion — depuis la fin des années 2010.

Viadeo : Viadeo, désormais appelé JDN Viadeo, est un réseau social professionnel français. Viadeo permet de construire et d'agréger son réseau de contacts, en vue de faciliter le dialogue entre professionnels. C'est aussi un outil de gestion de e-réputation (réputation en ligne) ou marketing personnel.

Strava, Nike Run club, Adidas running... : ces applications sont utilisées pour enregistrer des activités sportives *via* GPS. Le cyclisme et la course à pied concentrent la majorité des activités enregistrées sur ces sites. Les athlètes peuvent se suivre (à la manière de Twitter) pour être notifiés des nouvelles activités envoyées sur le réseau par leurs abonnements. Les activités peuvent ensuite être analysées ; un résumé de l'activité montre les données importantes comme la distance parcourue ou la vitesse moyenne.

Pour télécharger le guide:
www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf



Directrice de la publication : Yasmine-Eva Farès Emery
Création DICOd - juillet 2021

 **FACEBOOK**
[@Armees.gouv](https://www.facebook.com/Armees.gouv)

 **TWITTER**
[@Armees_Gouv](https://twitter.com/Armees_Gouv)

 **INSTAGRAM**
[@Armees_Gouv](https://www.instagram.com/Armees_Gouv)

 **YOUTUBE**
Ministère des Armées

 **LINKEDIN**
Ministère des Armées

Retrouvez-nous sur www.defense.gouv.fr