

Réseaux sociaux dans la FPH

Naviguer en
toute sécurité et
responsabilité



Sommaire

LA JOURNÉE EN IMAGES	P. 04
REPÈRES	P. 06
Réseaux sociaux : quels changements en 10 ans ?	
REGARD D'EXPERT	P. 07
Cyberattaques : « Les hôpitaux sont une cible de choix »	
DÉCRYPTAGE	P. 08
Le cadre juridique	
ÉCLAIRAGE	P. 10
« Les réseaux sociaux peuvent améliorer notre bien-être »	
RETOURS D'EXPÉRIENCE	P. 12
Cyberattaques : comment les établissements se protègent ?	
Les réseaux sociaux, un indispensable pour les RH	
BONNES PRATIQUES	P. 15
Pour une bonne hygiène numérique	
ENJEUX	P. 16
Fakes news : dangers et bonnes pratiques	
L'OFFRE ANFH	P. 18
Promouvoir une culture numérique éthique et responsable	
POUR ALLER PLUS LOIN	P. 20

ATOME DE SAVOIRS #17

mars 2026

Directeur de la publication :
Corinne Rouby | ANFH Normandie
Conception, rédaction et photos :
Agence Kogito
Réalisation : Supersoniks

***Nos remerciements
à tous les participants,
intervenants,
prestataires et
organisateurs pour
leur contribution au
succès de cette journée.***

Édito

**par Valérie Dubanet,
présidente de l'ANFH Normandie**

Fenêtre sur le monde et sur la connaissance, le développement d'internet a entraîné l'apparition des réseaux sociaux. En 2025, 5,24 milliards d'entre nous étaient des utilisateurs actifs, soit 63,9% de la population mondiale. Depuis la crise du Covid-19, et même si les établissements n'avaient pas attendu de s'en emparer pour leur communication externe, les réseaux sociaux se sont imposés dans notre sphère professionnelle. Les interactions sociales devenant difficiles, des communautés de services se sont formées. Des équipes se sont organisées avec des modes de communication plus fluides que les mails afin de faciliter l'accès aux ressources techniques et cognitives dans nos champs professionnels respectifs. Entre décembre 2019 et décembre 2020, les centres hospitaliers ont ainsi échangé 27 908 tweets, soit 76 par jour. Au-delà de modifier nos organisations de travail, la numérisation entraîne un mouvement d'extension du travail vers toutes les sphères de la vie. Les usagers et les patients sont eux aussi plus connectés et le digital fait partie de leur parcours de soins.

Nous nous sommes donc installés dans de nouveaux modes de communication et de nouveaux usages sans peut-être bien connaître les règles. Existe-t-il un impact pour la sécurité des établissements ? Où se situe notre responsabilité professionnelle ? Comment garder notre esprit critique vis-à-vis de certaines publications et contenus ? Comment passer entre les mailles du filet ?





La journée en images

Organisée à Deauville le 20 novembre 2025, la journée de l'ANFH Normandie « Réseaux sociaux dans la Fonction publique hospitalière : naviguer en toute sécurité et responsabilité » a réuni plus de 300 agents des établissements de santé, sociaux et médico-sociaux normands.



Animée par Michel Jérôme, la journée a été lancée par Valérie Dubanet. La présidente de l'ANFH Normandie s'interroge et alerte : *« Basé sur l'économie de l'attention, le modèle économique des réseaux permet-il réellement d'utiliser notre esprit critique ? »*

Expert des réseaux sociaux et de l'e-réputation, Frédéric Foschiani, fondateur de l'agence QSN-DigiTal, est intervenu tout au long de la journée pour apporter des conseils et des éclairages sur le fonctionnement et l'évolution des réseaux sociaux.



Capitaine de police, Maxime a rappelé que la santé est un secteur hautement critique ciblé par les cyberattaques pour ses données. *« Les données sont l'or noir du 21^e siècle. Il faut essayer de les protéger en les chiffrant, en utilisant des canaux de communication sécurisés, avec des signatures de clause de confidentialité... »*

Droit à l'image, respect du secret professionnel, devoir de réserve, diffamation... Anne-Sophie Moutier, juriste et enseignante spécialisée en droit de la santé et médico-social, a détaillé les enjeux juridiques liés à l'utilisation des réseaux sociaux dans le contexte du soin et de l'accompagnement.

Les réseaux sociaux : une opportunité pour développer sa marque employeur ou un risque pour la sécurité des établissements ? Deux visions ont marqué la table ronde réunissant Cindy Bernard, chargée de communication, et Céline Diascorn, DRH du Centre Hospitalier Public du Cotentin (CHPC) ainsi que Nicolas Bogucki, directeur du numérique au CHU de Caen, et Cédric Hamelin, responsable de la sécurité du système d'information au CHU de Rouen.



Professeur des universités et chercheur à l'Institut méditerranéen des Sciences de l'Information et de la Communication, Didier Courbet a révélé les mécanismes économiques mais aussi psychologiques qui se cachent derrière notre utilisation des plateformes de réseaux sociaux.

5



Face aux *fakes news*, Camille Lakhli, docteure en sciences cognitives, a invité les participants à questionner les contenus, leurs sources et leurs auteurs mais aussi à développer une posture individuelle d'humilité vis-à-vis de l'information : « *Il faut se méfier de l'illusion de la connaissance et de notre sur-confiance dans nos opinions.* »



En conclusion de la journée, Richard Lefèvre a invité les établissements à « *développer un positionnement éthique et à poser un cadre déontologique de l'utilisation des réseaux sociaux* ». Le vice-président de l'ANFH Normandie a également encouragé les agents à « *conserver leur libre arbitre et leur esprit critique.* »





Repères

RÉSEAUX SOCIAUX : QUELS CHANGEMENTS EN 10 ANS ?

Dix ans après une première rencontre consacrée aux réseaux sociaux, l'ANFH Normandie a de nouveau convié les agents de la Fonction publique hospitalière à une journée de sensibilisation sur le sujet. Aujourd'hui, les réseaux sociaux se sont largement démocratisés dans la sphère professionnelle, avec de nouveaux usages et apprentissages.

En 2016, l'ANFH Normandie organisait une journée régionale consacrée aux réseaux sociaux. 170 agents de la FPH avaient répondu présent. Ils étaient près du double, ce 20 novembre 2025 à Deauville pour échanger sur les réseaux sociaux. Que s'est-il passé en 10 ans ? *« Nous sommes passés de 33 millions d'utilisateurs des réseaux sociaux en France à 54 millions en 2025, soit 81 % de la population. Facebook et Twitter (X désormais) dominaient et TikTok n'existait pas. Nous publions des photos accompagnées de 20 hashtags. Aujourd'hui, ce sont des stories, des reels, des shorts, et les hashtags n'ont plus d'utilité »* détaille Frédéric Foschiani, directeur de l'agence QSN-DigiTal.

Un objectif : capter notre attention

Pour Frédéric Foschiani, le changement le plus impactant reste l'arrivée de l'intelligence artificielle qui gère les algorithmes et facilite la création de contenus mais aussi de faux profils. *« Il est extrêmement facile aujourd'hui de créer du faux qui a l'air vrai. Il faut, plus que jamais, être vigilant. »* L'IA permet également aux plateformes de proposer des publicités toujours plus personnalisées et des contenus qui captent notre attention en continu. En 10 ans, les plateformes sont devenues des espaces de divertissement, d'information et de commerce où le lien social initial s'efface au profit de la consommation de contenus. *« Aujourd'hui, les publications*

de nos amis ne représentent plus que 17 % de ce que nous voyons sur Facebook et seulement 7 % sur Instagram » confirme l'expert.

Quels défis ?

Au sein des établissements de santé et médico-sociaux, les enjeux de cyber sécurité et de protection des données, de comportement éthique des agents ou de stratégie de communication des établissements sont toujours d'actualité. En parallèle, de nouveaux défis ont émergé, avec par exemple l'essor des *fakes news*, qui questionne notre capacité à distinguer les fausses informations, ou les troubles psychosociaux induits par l'usage des réseaux sociaux.

LES RÉSEAUX SOCIAUX LES PLUS UTILISÉES EN FRANCE (EN UTILISATEURS PAR MOIS - JUIN 2025)

- YouTube, 46 millions
- Facebook, 40 millions
- TikTok, 27,8 millions
- Instagram, 26,5 millions
- Snapchat, 26 millions
- Pinterest, 19 millions
- LinkedIn, 17 millions
- X, 15 millions



Invité à témoigner, Maxime, un capitaine de police au sein de la section de protection économique du ministère de l'Intérieur, détaille les menaces numériques qui pèsent sur le secteur de la santé.

Pourquoi le secteur de la santé est-il une cible privilégiée des cyberattaques ?



Les établissements de santé et médico-sociaux sont principalement attaqués afin d'exfiltrer des données sensibles - médicales, de recherche, RH ou financières - en vue de faire de l'extorsion, de l'usurpation d'identité ou de la revente sur le *dark web*. Nous constatons également des cyberattaques dont le but est l'espionnage industriel. Enfin, les hôpitaux sont aussi la cible de sabotages afin de nuire à la réputation d'un établissement ou de provoquer le chaos au sein de la cohésion nationale. En cas d'incident, les conséquences peuvent être critiques : désorganisation des services, rupture de la confidentialité mais surtout risques directs pour la vie humaine. De plus, les coûts d'une cyberattaque peuvent atteindre plusieurs millions d'euros et le temps de remédiation prendre plus d'un an.

Les établissements sont-ils vulnérables ?



L'informatique hospitalière a la particularité de nécessiter de nombreux logiciels avec de forts besoins d'accès internet. Or, plus nous sommes connectés à internet, plus le risque de cyberattaques augmente. Une autre fragilité du secteur provient de l'utilisation de nombreux dispositifs médicaux numériques souvent peu sécurisés et avec une maintenance parfois complexe et pas contractualisée. Ces outils reposent par ailleurs sur de nombreux prestataires et nous constatons de plus en plus d'attaques indirectes : les attaquants passent par les



sous-traitants, la plupart du temps par des compromissions de VPN visant à récupérer des identifiants. Un autre problème est la nécessité de garantir des services à de nombreux utilisateurs - le médecin du soir va avoir besoin des analyses de celui du matin qui va avoir besoin de la radio de l'après-midi, etc. Il est donc difficile de segmenter les accès aux réseaux.

Les réseaux sociaux sont-ils un facteur de fragilité ?



Aujourd'hui, les fuites de données sont amplifiées par l'utilisation des réseaux sociaux et plus généralement par de mauvais comportements numériques de la part des personnes. Par exemple, utiliser le même mot de passe pour ses réseaux sociaux et sa boîte mail professionnelle : si votre mot de passe se retrouve dans la nature à cause d'une fuite, comme celle de LinkedIn en 2016, les attaquants vont tenter d'utiliser les mêmes identifiants sur d'autres plateformes pour accéder à des données sensibles. Attention également au clic malheureux qui introduit le fléau du secteur de la santé : le rançongiciel.



Décryptage

LE CADRE JURIDIQUE

Respect de la vie privée, atteinte au droit à l'image ou au devoir de réserve : précisions sur les fautes juridiques fréquentes sur les réseaux sociaux.



« Les réseaux sociaux sont devenus omniprésents dans notre société, créant autant de risques que de défis dans le milieu du soin et de l'accompagnement » lance Anne-Sophie Moutier. La juriste et enseignante spécialisée en droit de la santé et médico-social détaille le cadre juridique entourant l'usage des réseaux sociaux par les professionnels de la FPH. Dans un premier temps, elle rappelle la dimension publique des réseaux sociaux : « Dès lors que nous publions sur un réseau social, même dans une conversation entre amis ou un groupe "privé", le post est public et engage la responsabilité de son auteur. » Anne-Sophie Moutier détaille ensuite deux fautes fréquentes sur les réseaux sociaux : l'atteinte à la vie privée, et le non-respect de l'obligation de loyauté et d'exemplarité.

Vie privée et droit à l'image



La notion de vie privée inclut notamment le droit à l'image : la diffusion sans autorisation de photo ou d'enregistrement d'une personne est interdite. Cela comprend toute représentation physique permettant la reconnaissance de la personne : le visage mais aussi la voix, un tatouage... La juriste souligne que ce droit se maintient, même dans l'optique d'assurer la continuité des soins : « Ce n'est pas interdit mais il est absolument nécessaire de demander le consentement écrit du patient et de ne pas utiliser son propre appareil. » À noter que le droit à l'image existe également pour l'établissement - il est interdit de se filmer ou de prendre une photo dans l'établissement sans



Cette image générée par IA résume toutes les fautes qu'il est possible de faire en publiant sur les réseaux sociaux : non-respect du droit à l'image des usagers, de professionnels et de l'établissement, violation du secret professionnel par le biais du dossier, dénigrement de l'employeur et diffamation.

9

autorisation – et pour les professionnels de santé. Il est par ailleurs interdit pour un usager de filmer ou de photographier un professionnel sans son accord.

L'obligation de loyauté et d'exemplarité

 S'il participe à une mission de service public - même s'il est employé du privé, un professionnel doit faire preuve de retenue et de modération dans l'expression de ses opinions. « *C'est l'obligation de loyauté et d'exemplarité qui est appelée plus communément le devoir de réserve. Cela signifie que les agents n'ont pas le droit de dénigrer ouvertement leur employeur ou le service public, d'utiliser leur fonction pour faire de la propagande notamment politique, de manquer de respect ou d'être injurieux publiquement envers leur administration* » rappelle la juriste.

QUELQUES RECOMMANDATIONS POUR LES ÉTABLISSEMENTS

- Avoir une politique claire de diffusion de l'information et promouvoir les plateformes sécurisées pour communiquer
- Prévoir du matériel photographique propre à l'établissement
- Créer un guide de bonnes pratiques
- Inscrire la notion de discrétion et de confidentialité dans le règlement intérieur, le livret d'accueil ou le contrat de travail des professionnels
- Rappeler aux usagers dans le livret d'accueil, le contrat de séjour ou le document individuel de prise en charge, qu'il n'est pas autorisé de capter des images des locaux ou des professionnels



Éclairages

« LES RÉSEAUX SOCIAUX PEUVENT AMÉLIORER NOTRE BIEN-ÊTRE »

Professeur des universités et chercheur à l'Institut Méditerranéen des Sciences de l'Information et de la Communication (Université d'Aix-Marseille), Didier Courbet détaille les effets sur la santé de l'usage des réseaux sociaux et plus généralement des écrans et des technologies numériques.



Quels sont les impacts des réseaux sociaux sur notre santé ?



Physiquement, l'usage des réseaux sociaux - et plus largement le temps passé sur les écrans - peut provoquer ou être lié à différents problèmes : surpoids et obésité, troubles du sommeil, myopie, troubles musculo-squelettiques, accidents de la circulation... Sur le plan psychologique, l'augmentation du temps d'écran est liée à une augmentation des risques de troubles affectifs, du bien-être et de la

régulation des émotions : anxiété, dépression, stress, comportements excessifs et problématiques (dépendance à la pornographie, *binge-watching*, jeux d'argent)... Ces troubles peuvent se manifester à travers des phénomènes comme la FOMO (*Fear of missing out*), la peur de manquer « quelque chose d'important » ; la nomophobie, la peur d'être sans son smartphone ; la *Snapchat dysmorphia*, faire de la chirurgie esthétique pour ressembler aux filtres ; ou la cybercondrie, l'hypocondrie développée sur internet.

Les réseaux sociaux ont-ils uniquement des effets délétères ?

 Non, ils ont également des bienfaits. Sur les réseaux sociaux, nous apprenons, nous nous informons, nous jouons... Si vous regardez une vidéo drôle ou jouez à un jeu non-compétitif cela génère du bien-être hédonique, lié au plaisir. Mais les réseaux sociaux permettent aussi d'agir sur le bien-être eudémonique, lié à la réalisation de soi. En se construisant un « beau profil » nous développons une bonne estime de soi : nous sommes contents de l'image positive que nous renvoyons à nos amis et à notre famille. Développer des relations positives avec ses proches est également au cœur du bien-être et les réseaux sociaux permettent cela. L'idée n'est pas d'avoir un maximum d'amis sur les réseaux sociaux mais de communiquer – une blague, une pensée – avec ceux que nous aimons dans la vie quotidienne.

“ *Même à la périphérie de notre champ de vision, les publicités rentrent dans le cerveau à notre insu, vont s'agréger à nos émotions et nous influencer jusqu'à trois mois.*

”

*Didier Courbet,
professeur des universités
et chercheur à l'Institut méditerranéen
des Sciences de l'Information
et de la Communication*

LES REVERS DE LA GRATUITÉ

Les réseaux sociaux reposent sur un système où les utilisateurs accèdent gratuitement aux services tandis que les annonceurs financent les plateformes. Comme le souligne l'adage, « si c'est gratuit, c'est que vous êtes le produit » : cette gratuité n'est pas sans contrepartie. En utilisant les réseaux sociaux, nous sommes observés par des petits programmes informatiques, les cookies, qui permettent aux plateformes de réaliser un profil numérique : données socio-démographiques (âge, sexe...), géolocalisation, ce que nous aimons regarder et faire, nos « likes », etc. Elles vendent ensuite aux annonceurs la possibilité de montrer des publicités ciblées grâce à ces profils. Plus vous restez sur les réseaux sociaux, plus vous regardez de publicités, plus les plateformes gagnent de l'argent.





Retours d'expérience

CYBERATTQUES : COMMENT LES ÉTABLISSEMENTS SE PROTÈGENT ?

Entretien croisé avec Nicolas Bogucki, directeur du numérique au CHU de Caen, et Cédric Hamelin, responsable de la sécurité du système d'information au CHU de Rouen.

Quels risques représentent les réseaux sociaux pour un établissement de santé ou médico-social ?



Cédric Hamelin : Souvent, les agents n'ont pas connaissance que les réseaux sociaux sont très ciblés et scrutés par les attaquants. Il faut faire attention aux informations - sur un service ou l'établissement - que nous publions sur les réseaux sociaux car elles peuvent être utilisées contre nous. Par exemple, nous avons changé de direction générale en septembre 2024. Seulement un mois après nous observions une première tentative d'usurpation d'identité de notre nouvelle directrice générale : un attaquant s'est fait passer pour elle et a contacté une personne du service achats en demandant de passer une commande urgente. Cet exemple est valable pour n'importe quel professionnel : nous avons eu des attaquants qui ont contacté le service RH en se faisant passer pour un agent et en demandant de changer son RIB.



Nicolas Bogucki : Les attaquants se servent de la matière à leur disposition sur les réseaux sociaux pour essayer de comprendre le mode de fonctionnement d'un établissement et connaître la fonction de telle ou telle personne afin de s'immiscer dans nos process.



Les attaquants se servent de la matière à leur disposition sur les réseaux



Nicolas Bogucki,
directeur du numérique au CHU de Caen

Les réseaux sociaux peuvent-ils être utilisés comme porte d'entrée par des personnes malveillantes ?

← **Cédric Hamelin** : C'est rare mais nous avons observé des médecins ou des experts de l'établissement contactés via la messagerie instantanée de LinkedIn. Tout commence par une demande anodine puis, au fur et à mesure, les questions sont plus précises sur le métier afin de recueillir des informations sensibles.

← **Nicolas Bogucki** : Cela passe souvent par une fausse sollicitation de l'expertise d'un professeur, ce qui est une pratique courante : les médecins généralistes demandent régulièrement l'avis de nos médecins professeurs. Pour éviter toute prise de contact illicite, nous avons développé une plateforme de communication sécurisée dédiée aux échanges entre médecins.

Quelles autres mesures avez-vous prises pour limiter ces risques ?

← **Nicolas Bogucki** : Nous essayons de régulièrement sensibiliser nos agents avec des messages internes pour expliquer les risques comme le *phishing*. Nous conseillons également d'éviter au maximum d'utiliser WhatsApp pour communiquer entre professionnels, en particulier s'il y a des échanges de données médicales, et d'utiliser les solutions labélisées Hébergeur de Données de Santé (HDS) ainsi que les messageries cryptées telles que Tchap.

← **Cédric Hamelin** : À Rouen, nous avons fait le choix de bloquer l'accès à l'ensemble des réseaux sociaux - à l'exception des personnes habilitées comme les services RH ou de la Communication - sur le réseau wifi principal. Mais nous avons ouvert un accès à un wifi invité où les agents

” Les attaquants
cherchent à comprendre
nos process

”



Cédric Hamelin, responsable de la sécurité du système d'information au CHU de Rouen.

peuvent se connecter à un réseau internet bénéficiant de nos outils de cybersécurité comme le filtrage ou le blocage de sites malveillants.



Retours d'expérience

DES RÉSEAUX AU SERVICE DE L'ATTRACTIVITÉ ET DE LA COMMUNICATION DES ÉTABLISSEMENTS

Témoignages de Cindy Bernard, chargée de communication, et de Céline Diascorn, directrice des Ressources Humaines du Centre Hospitalier Public du Cotentin (CHPC).



Développer sa marque employeur

« Une des orientations de notre projet stratégique consiste à renforcer notre attractivité auprès des professionnels de santé et des usagers. Les réseaux sociaux sont l'un des outils que nous mobilisons pour atteindre cet objectif, développer notre marque employeur et notre communication. Nous sommes sur une presqu'île avec peu de brassage des professionnels et une forte concurrence du tissu industriel sur certains métiers. Les réseaux sociaux nous permettent d'avoir une visibilité plus importante et une lisibilité accrue.

Nous développons notre image de marque essentiellement sur LinkedIn, en montrant notamment l'image d'un employeur sérieux et avec des moyens. Nous mettons par exemple en avant notre plateau technique, notre richesse

pluriprofessionnelle, les savoir-faire de nos secteurs de soins... Une manière de communiquer qui s'avère efficace : aujourd'hui nous n'avons plus aucun poste vacant, y compris sur les métiers en tension. Les réseaux sociaux sont devenus indispensables pour une DRH d'un établissement de santé. »

Maîtriser sa communication

« Avant, l'établissement peinait à se faire entendre. Nous étions tributaires de la presse, des organisations syndicales et des usagers. Avoir une stratégie réseaux sociaux, c'est reprendre la main sur notre communication et apporter notre point de vue avant qu'il ne soit déformé. C'est aussi un moyen de lutter contre les *fakes news* en transmettant de l'information vérifiée et vérifiable et de valoriser la vie scientifique qui anime notre établissement. »



Face aux cyberattaquants et aux algorithmes conçus pour capter notre attention, nos comportements en ligne déterminent non seulement ce que nous laissons voir aux plateformes et aux publicitaires mais aussi notre sécurité. Le point sur les bons réflexes à adopter pour une utilisation mieux maîtrisée.

Reprendre la main sur ses données personnelles

 Quelles sont les informations que les réseaux connaissent de moi ? Est-il nécessaire de laisser autant de données accessibles ? Frédéric Foschiani invite à s'interroger sur ce que connaissent les réseaux sociaux de nous. *« Ils incitent en permanence à compléter son profil à 100%. Ce n'est pas une obligation, renseignez uniquement les informations strictement nécessaires au fonctionnement du service. »* L'expert conseille également d'aller *« une à deux fois par an dans les paramètres de confidentialité de chacun de ses profils sociaux pour mieux gérer sa visibilité et l'exploitation de ses données personnelles »*.

S'interroger sur les données que nous fournissons est un réflexe à avoir pour l'ensemble de sa vie numérique. *« Regardez ce à quoi ont accès les applications de votre smartphone, alerte Maxime, le capitaine de police. Caméra, microphone, photos, appels téléphoniques, localisation, contacts : est-ce nécessaire pour un simple jeu vidéo ou pour créer un avatar virtuel ? »* Il recommande, a minima, d'autoriser les accès uniquement quand vous utilisez l'application.

Sécuriser ses comptes et ses appareils

Pour protéger ses données, il faut également protéger son appareil et ses comptes. En plus d'avoir des mots de passes robustes, Maxime conseille d'utiliser l'authentification multifacteur (MFA). Il recommande aussi de désactiver

le plus possible son wifi et Bluetooth, d'utiliser un VPN (surtout si vous utilisez des wifis publics) et de redémarrer une fois par semaine son téléphone. *« Dans environ 80% des cas, cela enlèvera les logiciels espions publicitaires. »*

Maîtriser ses messages et son image

 Au-delà de ces aspects sécuritaires ou de paramétrage, les experts insistent sur la maîtrise de ses publications. *« La principale précaution est de faire attention aux informations que nous diffusons nous-mêmes »* insiste Frédéric Foschiani qui conseille de toujours s'interroger sur l'utilité réelle de publier ou de réagir. Il alerte enfin sur les doubles significations - sexuelles, politiques ou criminelles - des émojis.





Conçues pour nous tromper, les fakes news ont, avec les réseaux sociaux, un environnement propice à leur propagation. Dans le domaine de la santé, quels sont les risques et comment s'en prémunir ?



« Jeûner permet de lutter contre le cancer », « La vaccination contre le papillomavirus nuit à la fertilité », « La prise de paracétamol pendant la grossesse augmente le risque d'autisme chez l'enfant »... Voilà quelques exemples de *fakes news* (trad. fausses informations) dans le domaine de la santé que nous pouvons croiser sur internet. Mais qu'est-ce qu'une *fake news* ? « *Le terme est apparu en 2016 lors de la campagne de Donald Trump. Les fakes news sont des informations saillantes, souvent simples et intuitives, qui ont été créées de manière intentionnelle pour tromper et nuire, et se propager le plus efficacement possible*, explique Camille Lakhli, docteure en sciences cognitives. Ces fausses informations sont attrayantes car elles donnent la sensation de comprendre de façon intuitive et simple un problème qui est complexe. »



S'il est facile de créer une fausse information en quelques minutes, il faudra probablement plusieurs heures pour démonter chaque point et montrer la fausseté de l'ensemble.

Loi de Brandolini



PRÉVALENCE EN 2025 DES MESSAGES PORTANT SUR DES SUJETS D'INTÉRÊT PUBLIC QUI CONTIENNENT DES INFORMATIONS FAUSSES OU TROMPEUSES SUR LES RÉSEAUX SOCIAUX :

- TikTok 20%
- Facebook 13%
- X/Twitter 11%
- YouTube et Instagram 8%
- LinkedIn 2%

Source : Science Feedback

Les dangers pour la santé



Diffuser sur des supports variés (photos, vidéos, articles numériques ou papiers, commentaires dans les réseaux sociaux, publicités...), les *fakes news* peuvent avoir des conséquences très néfastes, notamment dans le domaine de la santé. « Elles peuvent entraîner des absences ou des retards de prise en charge de la maladie ou encore favoriser l'adhésion à des pseudosciences et des pratiques non validées scientifiquement. Cela peut aussi provoquer des risques sanitaires collectifs : comme la campagne de dissimulation massive des dangers de la cigarette organisée par l'industrie du tabac au 20^e siècle ou les fausses informations sur le vaccin contre la Covid-19. »



Bonnes pratiques face aux fakes news

 Face aux *fakes news* Camille Lakhlifi appelle à la prudence et à l'esprit critique. Elle insiste d'abord sur le fait de bien lire l'ensemble d'un article et pas uniquement le titre ou la photo, de vérifier si les sources sont bien citées et si la mention d'utilisation d'IA est présente. Elle souligne ensuite l'importance d'interroger et d'évaluer l'auteur : est-il expert du sujet abordé ? A-t-il un intérêt (financier, politique, idéologique) à faire croire à une information ? Enfin, la chercheuse invite chacun à adopter une posture qui accepte le doute et la complexité du monde : se méfier des

propos sans nuance, distinguer l'assurance des orateurs de leur fiabilité, reconnaître les limites de nos propres connaissances, formuler des requêtes neutres lors des recherches sur Internet (chercher « vaccin bénéfiques/risques » plutôt que « vaccin danger »)...



L'offre ANFH

PROMOUVOIR UNE CULTURE NUMÉRIQUE ÉTHIQUE ET RESPONSABLE

Face aux usages spontanés des réseaux sociaux et des risques croissants dans les pratiques professionnelles, l'ANFH Normandie a développé une offre de formation destinée à favoriser un usage éthique des outils numériques. Accessible aux directions d'établissements, aux encadrants ou aux agents, cette offre s'articule notamment autour d'un parcours de formation à la carte. Précisions.



Parcours « Usages numérique et éthique professionnelle »



Conçu pour répondre aux enjeux actuels des professionnels de la fonction publique hospitalière, ce parcours est structuré en trois actions de formation modulables (en présentiel et/ou en distanciel).

Destinée aux directions, encadrants et professionnels impliqués dans la définition d'une politique numérique, la première action « **Empreinte web et réseaux sociaux – Stratégie d'établissement et plan d'action** » a pour objectif de permettre aux établissements de « construire un plan d'action personnalisé pour améliorer la

visibilité numérique de l'établissement ». D'une durée d'une journée, la formation s'articule notamment autour de la réalisation d'un diagnostic des besoins de l'établissement.

La deuxième action « **Encadrer et manager à l'ère des nouvelles technologies: quelles opportunités, quels risques?** » vise à dresser un panorama des usages et mésusages des nouvelles technologies d'information et de communication qui bouleversent les codes du management traditionnel. Adressé aux encadrants et managers, ce module permet d'explorer les bonnes pratiques organisationnelles et les situations problématiques liées au numérique.

CAPSULES VIDÉO : DES FORMATS COURTS POUR DES MESSAGES ESSENTIELS

Pour promouvoir une culture numérique éthique et responsable au sein des établissements, l'ANFH propose également cinq courtes vidéos abordant des thématiques transversales liées aux réseaux sociaux :

- La pratique responsable et maîtrisée des réseaux sociaux chez les professionnels hospitaliers
- Secret professionnel et discrétion professionnelle dans la FPH
- Le devoir de réserve
- L'esprit critique
- L'intelligence artificielle dans les établissements sanitaires, médico-sociaux et sociaux..

Plus de détails sur Anfh.fr :

www.anfh.fr/delegations-regionales/normandie/usages-numeriques-formations-et-outils-disposition-des-etablissements-pour-promouvoir-une-culture

« Les bons usages numériques pour les professionnels hospitaliers » :

le troisième et dernier module est ouvert à tous les agents de la FPH. D'une durée d'une journée, il invite les professionnels à développer des compétences numériques en matière de sécurité des comptes et de protection de l'identité numérique, de vérification de l'information et de communication responsable avec les usagers.

« Éthique 2.0 » : un parcours en ligne pour adopter les bons réflexes numériques



En complément des modules « Usages numérique et éthique professionnelle », l'ANFH propose un par-

cours en *e-learning* pour sensibiliser les agents de la FPH aux risques liés aux usages numériques dans leur environnement professionnel. Accessible sur la plateforme e-formations.anfh.fr, ce parcours s'articule autour de huit séquences avec des contenus courts, concrets et illustrés par des mises en situation sur : les impacts des outils numériques au quotidien, les effets sur la concentration et le bien-être au travail, la cybercitoyenneté, la protection de la vie privée sur Internet, la relation aux usagers, la sensibilisation des patients et visiteurs aux bonnes pratiques ainsi que la sécurité numérique de l'établissement.



OUTIL : KIT DE SURVIE NUMÉRIQUE

Conçu par Frédéric Foschiani pour l'ANFH Normandie, ce guide de bonnes pratiques a pour objectif d'aider à reprendre le contrôle de ses réseaux sociaux. Paramètres de contrôle, de sécurité et de confidentialité du compte, le document propose une *checklist* rapide et accessible des paramètres essentiels pour chacune des principales plateformes : Facebook, Instagram, WhatsApp, Messenger et LinkedIn.

POUR ALLER PLUS LOIN

RESSOURCES

ÉTUDES, ARTICLES, PODCASTS...

- Plongée dans l'algorithme de TikTok France : nos révélations
<https://www.amnesty.fr/actualites/plongee-dans-l-algorithme-de-tiktok-france-rapport>
- *Measuring the State of Online Disinformation in Europe on Very Large Online Platforms First report of the SIMODS project (Structural Indicators to Monitor Online Disinformation Scientifically)*
<https://science.feedback.org/wp-content/uploads/2025/09/SIMODS-Report-1.pdf>

ARTICLES SCIENTIFIQUES

- G.Darcy, H.Mercier, A. Mari, R. Casati, G. Origgi, L.Yahia - Lutter contre la désinformation : Penser autrement l'action publique à l'aune des sciences cognitives
https://osf.io/preprints/osf/fu9cz_v1
- Fourquet-Courbet, M.-P. & Courbet, D. (2020). *Connectés et heureux ! Du stress digital au bien-être numérique*. Paris : Dunod
- Didier Courbet, Marie-Pierre Fourquet-Courbet, Julien Intartaglia. Publicité sur Internet : que reste-t-il des mots, que reste-t-il des images, trois mois après en mémoire implicite ?
- Gritti, Bornstein & Barbot (2023). *The smartphone as a "significant other": interpersonal dependency and attachment in maladaptive smartphone and social networks use*.

TEXTES LEGISLATIFS

- LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- LOI n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux

- LOI n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires
- The AI Act - Règlement (UE) 2024/1689 du 13 juin 2024
artificialintelligenceact.eu

Retrouvez les actualités et ressources de l'ANFH Normandie sur :
www.anfh.fr/delegations-regionales/normandie



ATOME DE SAVOIRS #17

ANFH NORMANDIE

DÉLÉGATION DE CAEN

Parc Athéna - 1, rue Andreï Sakharov
14280 SAINT-CONTEST
Tél : 02 31 46 71 60
mail : bassenormandie@anfh.fr
www.anfh.fr/basse-normandie

DÉLÉGATION DE ROUEN

85 A, rue Jean Lecanuet
76107 ROUEN CEDEX 1
Tél. : 02 32 08 10 40
mail : hautenormandie@anfh.fr
www.anfh.fr/haute-normandie

www.linkedin.com/company/anfh-normandie/