Organisation du numérique, qui fait quoi ?

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante dont une des missions est de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions législatives. Elle dispose d'un pouvoir de sanction (3 millions € puis jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial à partir du 25 mai 2018).

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de sécurité des systèmes d'information. Elle apporte des conseils aux entreprises et aux particuliers dans le domaine de la cyberdéfense et de la cybercriminalité.

L'Autorité de régulation des communications électroniques et des postes (ARCEP) est une autorité administrative indépendante chargée de réguler les communications électroniques et les postes en France. Elle vient de mettre en œuvre le site internet « monreseaumobile.fr » qui est un outil cartographique qui vous permet de comparer les opérateurs mobiles à partir d'une carte géographique interactive.

L'Agence du numérique est chargée de l'impulsion, de l'animation et de l'accompagnement des projets et des initiatives numériques dans les territoires par les collectivités publiques, les réseaux d'entreprises, les associations et les particuliers. Son portail net-public.fr a pour mission d'accompagner l'accès de tous à l'internet.

Le Conseil national du numérique a pour mission de formuler de manière indépendante et de rendre publics des avis et des recommandations sur toute question relative à l'impact du numérique sur la société et sur l'économie.

La Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) produit des fiches pratiques informatives et opérationnelles dans le domaine du numérique. Elles sont régulièrement actualisées en fonction des évolutions de la réglementation.

Le portail service-public.fr propose des dossiers, fiches pratiques et des "questions réponses" sur le thème de l'internet.

Le ministère de l'Intérieur a mis en oeuvre le portail "Internet-signalement.gouv.fr" qui se définit comme étant le portail officiel de signalement des contenus illicites de l'internet. Vous y trouverez également des pages d'informations relatives à l'utilisation d'internet.

Sur internet, vous bénéficiez d'un cadre protecteur mis en place par le législateur qui y a transposé trois grandes catégories de mesures :

- Protection du droit de propriété (identité numérique, droit à l'image, droit d'auteur, liberté de panorama...).
- Protection de la personne (droit au déréférencement, diffamation, désinformation, usage de la collecte des données...).
- Protection du consommateur (commerce en ligne et paiement en ligne).

Deux dispositions majeures législatives s'appliquent dans le domaine du numérique :

Article 226-4-1 - Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

Article 227-22 - Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100000 euros d'amende lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communications électroniques ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux.

--

La jurisprudence complète le cadre législatif et réglementaire. Elle est très souvent réactive, quelquefois elle entraîne des corrections législatives (Porn Revenge) et elle est moins accessible que le cadre législatif. Consultez le portail service-public.fr qui assure cette veille jurisprudentielle.

Quelle valeur accorder à un courriel ou à un "post" sur un réseau social ?

La jurisprudence accorde au courriel une valeur de preuve et elle peut constituer un élément suffisant, par exemple au Conseil des Prud'Hommes, pour statuer sur un licenciement. A l'inverse, un courriel, qui n'intègre pas une signature numérique, n'est pas une alternative à la lettre recommandée avec accusé de réception.

En ce qui concerne les publications sur les réseaux sociaux, la jurisprudence considère qu'elles peuvent être diffamatoires si l'accès est public (notion de faute grave pour un licenciement). Pensez à limiter vos publications à vos "amis" pour limiter ce risque.

Lycée Suscinio - Morlaix - janvier 2018

EPN ou établissement scolaire

ETRE NET SUR LE NET

Vous vous interrogez sur votre identité numérique, le droit à l'oubli, le droit à l'image, la liberté de panorama, le phishing, le rançonning, l'achat en ligne, le typosquattage... ce triptyque vous apporte une définition synthétique à ce vocabulaire spécifique du monde internet ; il vous apporte aussi quelques informations utiles pour une navigation tranquille.

Tout d'abord, prenons connaissance de l'article n° 1 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : "l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant."

Vos droits sur internet :

Le droit au déréférencement (droit à l'oubli) vous permet de demander à un moteur de recherche de supprimer certains résultats de recherche associés à vos noms et prénoms. Il consiste à supprimer l'association d'un résultat de votre nom et votre prénom. Cette suppression ne signifie pas l'effacement de l'information sur le site internet source (source CNIL) et l'utilisation courante de générateurs d'adresses IP à l'étranger rend ce déréférencement inefficace (Le Conseil d'Etat a interrogé, en février 2017, la Cour de justice de l'Union européenne sur ce point).
Le droit d'accès : vous pouvez demander directement au responsable d'un fichier s'il détient des informations sur vous, et demander à ce que l'on vous communique l'intégralité de ces données. (source CNIL).
Le droit d'opposition : vous pouvez vous opposer, pour des motifs légitimes, à figurer dans un fichier. Vous pouvez vous opposer à ce que les données vous concernant soient diffusées, transmises ou conservées (source CNIL).
Le droit de rectification : Vous pouvez demander la rectification des informations inexactes vous concernant. Le droit de rectification complète le droit d'accès (source CNIL).
Le droit à l'image est un droit exclusif que vous avez sur votre image (photo ou vidéo) qui en est faite.
Le droit d'opinion : c'est un droit majeur aux Etats-Unis mais, en France, il est limité à un emploi qui n'est pas contraire à nos valeurs républicaines (négationnisme, apologie du terrorisme, propos haineux racistes ou homophobes...) et sur ce point le code pénal est applicable aux usagers français du net.
Le droit d'auteur, qui porte sur les œuvres de l'esprit (écrits, photos, partitions, logiciels, etc.), confère à l'auteur un droit de propriété exclusif sur sa création, aussi bien en matière de droits moraux (divulgation, par exemple) que patrimoniaux (droit d'exploitation de l'œuvre : représentation, reproduction ou adaptation). Si le droit d'auteur s'applique dès la naissance de l'œuvre, la protection qu'il apporte suppose d'en prouver l'existence (source DILA).

Plusieurs droits sont en cours d'évolution (le droit à la portabilité des données intégré au règlement européen sur la protection des données qui sera effectif en mai 2018) ou attendent des décrets d'application :
La loi pour une République Numérique a créé de nouveaux droits : le droit au maintien de connexion (préserve un accès fonctionnel aux services de communication au public en ligne et aux services de courrier électronique) et la possibilité d'organiser le sort de ses données personnelles après la mort "testament numérique").
L'article 55 de la loi du 8 août 2016 dite « loi Travail » a introduit un droit à la déconnexion afin de mieux respecter les temps de repos et de congé mais aussi la vie personnelle et familiale des salariés connectés en dehors des heures de bureau (source DILA).
Consultez régulièrement le portail de la CNIL et sa rubrique actualités pour prendre connaissance des dernières évolutions.

Les risques sur internet :

L'usurpation d'identité numérique : une personne se fait passer pour vous et vous cause des préjudices. Après avoir vérifié qu'il ne s'agissait pas d'un homonyme, contactez le FAI ou le réseau social concerné puis, éventuellement, déposez une plainte pénale.
L'achat sur un site internet non sécurisé ou ne répondant pas aux critères réglementaires : la présence dans l'adresse URL d'un cadenas ou du HTTPS garantit la mise en place d'un protocole de sécurité. Ne réalisez pas de transaction si le vendeur ne propose pas ce protocole.
L'achat sur un site inernet qui n'intègre pas les mentions obligatoires liées à la vente à distance : le site, souvent situé en dehors de l'Europe, éphémère ou non, n'intègre pas les clauses obligatoires liées à la vente sur internet.
Le phishing : sur toutes les étapes de ce risque, vous pensez être en liaison avec une autre personne. Son but est de de bénéficier d'un virement bancaise (Transcash ou autre) à partir d'un scénario bâti pour vous tromper : les impôts (ou la CAF ou pôle emploi...) vous annoncent, qu'après vérification, ils vous doivent une petite somme et vous invitent à communiquer vos coordonnées bancaires. Le phishing peut être aussi produit à partir d'une adresse d'un de vos proches qui a été piratée et qui vous informe qu'il a besoin de vous car il lui est victime d'un accident. Le phishing n'est pas à inclure dans la catégorie des virus car il ne s'agit que de scénarios, souvent extrêmement élaborés, réalisés par des hackeurs qui maîtrisent les outils de communication numérique. La réponse la plus appropriée consiste à contacter directement l'expéditeur par téléphone ou à prendre avis auprès d''autres personnes sur l'action demandée par l'expéditeur. Le typosquattage consiste à vous faire croire que vous naviguez sur un site internet qui vous semble sûr : le hacker construit un site qui lui ressemble à l'identique et il utilise un nom de domaine très proche vous vous tromper : "votrecaf.com" au lieu "caf.fr", "impots-gouv.com" au lieu de "impots.gouv.fr".
Les virus : il en existe plusieurs familles et les plus dangereux peuvent collecter des données mais aussi les détruire ou les modifier. Ne télécharger pas n'importe quoi n'importe où et n'ouvrez pas les pièces jointes qui vous semblent suspectes.
Le rançongiciel : vos données ont été piratées (volées ou cryptées) et le hackeur vous demaine un paiement.
Le fake, le canular et le hoax : cet ensemble profite de votre naïveté et de votre manque de discernement. Ne propagez pas ces informations.
Les faux avis sur internet représentent le tiers des contributions. La DGCCRF propose, sur son site internet, une fiche pratique qui intègre les nouveaux cadres normatifs.
Les sites de propagante fondamentalistes agissent sur le manque de discernement de certains publics et bénéficient du cadre très protecteur des démocraties (toute entrave peut générer un délit d'opinion).
Les sites pornographiques sont aussi fréquentés par des enfants. Selon une étude menée par Bitdefender (antivirus), les enfants de moins de 10 ans représenteraient 10% des visiteurs de sites pornographiques dans le monde.

Le revenge-porn : le législateur a enfin intégré des mesures (loi pour une République Numérique du 7 octobre 2016) pour faciliter la défense des victimes (dans un établissement scolaire, parlez-en à l'infirmière ou à la CPE très rapidement si des éléments vous portent à croire que vous pourriez en être victime).

Limiter les risques : Soyez méfiants !

Sauvegardez vos données (sur un autre support physique ou, éventuellement, sur un cloud sécurisé européen).
Choisissez un mot de passe « fort » (recommandation ANSSI : il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe) et utiliser la double authentification en cas de modification de celui-ci (la modification nécessite la saisie d'un code fourni par SMS). L'ANSSI propose un outil, sur son site internet, pour mesurer la force de votre mot de passe.
Mettez à jour vos logiciels (Windows, Flash...). Utilisez des logiciels qui ne collectent pas vos données personnelles.
Paramétrez un pare-feu et installez un logiciel antivirus. Scannez les clés USB destinées à être connectées sur vos appareils numériques.
Téléchargez, sur internet, sur des sites sûrs. Vérifiez les adresses URL (adresses internet) des sites sur lesquels vous naviguez. Pour les sites de paiement en ligne, assurez-vous qu'ils soient en « HTTPS », ou précédés d'un cadenas sur la ligne URL et qu'ils comportent les mentions obligatoires : nom ou raison sociale, adresse de siège social, adresse de courrier électronique, coordonnées téléphoniques... .
Ne cliquez pas, dans votre messagerie, sur des liens proposés par des expéditeurs que vous ne connaissez pas. N'ouvrez pas non plus les pièces jointes d'expéditeurs connus sans avoir vérifié l'adresse de messagerie et la cohérence du texte. Posez-vous la question "la formulation utilisée par l'expéditeur (connu) est-telle habituelle ?
Ne confiez pas trop d'informations personnelles sur les réseaux sociaux : leurs collectes généreront, au mieux, des SPAM (messages non désirés) et, au pire, permettront à des hackers de produire des attaques visant à dérober vos mots de passe (technique dite par "ingénierie sociale" qui consiste à tester des mots de passe à partir de votre environnement personnel : prénoms de vos enfants, artistes préférés, club de football préféré, date de votre mariage... alternative à l'attaque par force brute ou par dictionnaire qui teste toutes les solutions. Attention les dictionnaires utilisés par les hackers comprennent "football" et "footb@ll".
Prenez conseil autour de vous en cas de doute (les hackers vous suggèrent très souvent "de n'en parler à personne" car une arnaque ne résiste pas longtemps à la collégialité...).
Dans les lieux publics, privilégiez la 4G au réseau Wifi.

Retenez cette formule de Guillaume Poupard
(directeur général de l'ANSSI) :
«Il faut une "saine paranoïa" face aux risques»
(propos recueillis par Amaelle Guiton
Journal Libération — 17 novembre 2016).