



Rectorat de l'académie de Créteil

Le Responsable de la Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information

Mél : rssi@ac-creteil.fr
4, rue Georges-Enesco
94 010 Créteil Cedex
www.ac-creteil.fr

Guide juridique

Note à la charte régissant
les usages des systèmes d'information et du numérique
par les personnels de l'académie de Créteil

Ref: ssi-guide_juridique_20240524

Date: 24/05/2024

Table des matières

I. Objet.....	2
II. La protection des personnes physiques à l'égard du traitement des données à caractère personnel. .	3
III. La protection des droits de propriété intellectuelle.....	4
III.1. Les règles de protection du droit d'auteur.....	4
III.2. Les règles de protection des logiciels.....	5
III.3. Les règles de protection des données et des bases de données.....	6
IV. La protection des marques.....	6
V. La protection des systèmes d'information.....	7
VI. Le secret des correspondances.....	8
VII. La responsabilité en matière de transmission des informations.....	8
VIII. Le respect de la vie privée.....	9
VIII.1. Le droit à la vie privée.....	9
VIII.2. Le droit à l'image.....	9
VIII.3. Le droit de représentation.....	9
IX. Les règles de preuve.....	10
X. L'obligation d'information.....	10

I. Objet

Le présent guide juridique de l'utilisateur s'inscrit dans le cadre de la politique de sécurité du ministère de l'éducation nationale et du ministère de l'enseignement supérieur et de la recherche (dénommés ci-après « l'institution »).

Le guide est pris en application des règles édictées dans la charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie de Créteil, dans le prolongement de laquelle il s'inscrit; il la complète.

Il a pour objet d'exposer aux "utilisateurs", les principales règles légales applicables, de manière non exhaustive.

Ces règles ne sont pas exclusives de celles qui s'imposent à tout agent public notamment en ce qui concerne l'obligation de neutralité (religieuse, politique et commerciale), de réserve, de discrétion professionnelle et de respect des secrets protégés par la loi.

Il a une vocation pédagogique.



II. La protection des personnes physiques à l'égard du traitement des données à caractère personnel

Les données à caractère personnel font l'objet d'une protection légale particulière dont la violation expose son auteur à des sanctions pénales.

Les textes applicables en la matière sont les suivants :

- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004;
- L'ordonnance n° 2018-1125 du 12 décembre 2018, publiée le 13 décembre 2018;
- La convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;
- La directive n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Ces règles s'appliquent à l'ensemble des systèmes de traitement de l'information dès lors que cette information permet d'identifier un ou plusieurs individus.

La loi du 6 janvier 1978 a créé un dispositif juridique pour encadrer la mise en œuvre des « traitements automatisés de données à caractère personnel » et ouvrir aux individus un droit d'accès et de rectification sur les données les concernant détenues et gérées par des tiers.

L'ordonnance n° 2018-1125 du 12 décembre 2018, publiée le 13 décembre 2018, achève, au niveau législatif, la mise en conformité du droit national avec le Règlement général sur la protection des données (RGPD) et la Directive « police-justice », applicable aux fichiers de la sphère pénale. Cette ordonnance améliore la lisibilité du cadre juridique en matière de protection des données.

Le RGPD supprime les déclarations de fichiers à effectuer auprès de la CNIL.

Seules certaines formalités préalables vont subsister (demande d'avis pour les secteurs police/justice, demande d'autorisation pour certains traitements de données de santé notamment).

En contrepartie de la disparition de l'accomplissement de démarches administratives auprès de la CNIL, les administrations, sociétés et associations traitant des données à caractère personnel, mais aussi leurs prestataires et sous-traitants, sont désormais pleinement responsables de la protection des données qu'ils traitent.



Il leur appartient d'assurer la conformité au RGPD de leurs traitements de données personnelles tout au long de leur cycle de vie et d'être en mesure de démontrer cette conformité.

Toute personne auprès de laquelle sont collectées (oralement ou par écrit) des informations destinées à être mises en œuvre dans un système automatisé de traitement doit être informée :

- du caractère obligatoire ou facultatif des réponses;
- des conséquences d'un défaut de réponse;
- de l'identité des destinataires des informations;
- de l'existence d'un droit d'accès et de rectification;
- de l'identité du responsable du traitement;
- des finalités du traitement auquel les données sont destinées:

Si les données sont destinées à être communiquées à des pays tiers à l'Union européenne, elle doit recevoir une information sur ce point ;

Si les données sont destinées à être utilisées à des fins de prospection, à être communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection, une information sur ce point doit lui être donnée, accompagnée d'une possibilité pour la personne de s'y opposer (au moyen d'une case à cocher ou à cliquer notamment).

III. La protection des droits de propriété intellectuelle

III.1. Les règles de protection du droit d'auteur

En vertu des règles du Code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création « d'un droit de propriété incorporel et exclusif opposable à tous ».

Cette disposition s'applique à toutes les œuvres de l'esprit quel qu'en soit le genre, la forme d'expression, le mérite ou la destination.

Sont notamment considérées comme des œuvres de l'esprit, au sens du Code de la propriété intellectuelle et en particulier de l'article L.112-2, les œuvres suivantes :

- les livres, brochures et autres écrits littéraires, artistiques et scientifiques;
- les conférences, allocutions et autres œuvres de même nature;
- les œuvres dramatiques ou dramatico-musicales;
- les œuvres chorégraphiques;
- les œuvres musicales avec ou sans paroles;
- les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images sonorisées ou non, dénommées ensemble œuvres audiovisuelles;



- les œuvres de dessins, de peintures, d'architectures, de sculptures, de gravures, de lithographies;
- les œuvres graphiques et typographiques;
- les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie;
- les œuvres d'art appliqué;
- les illustrations, les cartes géographiques;
- les logiciels, y compris le matériel de conception préparatoire.

Les actes de reproduction et de représentation des œuvres protégées en tout ou partie, par tout moyen et sous toute forme sont ainsi soumis à l'autorisation du/ou des titulaire(s) des droits sur les œuvres.

L'utilisation de ces œuvres suppose donc une acceptation préalable du/ou des titulaire(s) des droits.

L'utilisateur est donc informé qu'à défaut d'une autorisation expresse du/ou des titulaire(s) respectant les dispositions du Code de la propriété intellectuelle, il lui est interdit d'utiliser une telle œuvre.

A défaut, sa responsabilité civile et/ou pénale peut être engagée.

III.2. Les règles de protection des logiciels

Les logiciels sont protégés par le droit d'auteur.

Toute reproduction, adaptation et/ou distribution du logiciel n'est autorisée que sous réserve du consentement du titulaire des droits sur ledit logiciel.

L'étendue et les caractéristiques des droits conférés sont définies en général par des contrats de licence d'utilisation qui précisent les modalités selon lesquelles est autorisée l'utilisation des logiciels visés.

L'utilisation du logiciel, même à des fins d'essais, de démonstration de courte durée ou à des fins pédagogiques et à défaut d'autorisation expresse et écrite du titulaire des droits est en principe interdite.

L'utilisateur d'un logiciel s'expose à des sanctions civiles et pénales prévues et réprimées par le Code de la propriété intellectuelle lorsqu'il utilise un logiciel sans autorisation.

Afin de prévenir les risques liés à la contrefaçon de logiciel, une vigilance particulière des utilisateurs comme de leur autorité hiérarchique est indispensable.

Est un délit de contrefaçon puni par le Code de la propriété intellectuelle (article L.335-3 du Code de la propriété intellectuelle) toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur ainsi que la violation de l'un des droits de l'auteur d'un logiciel.



III.3. Les règles de protection des données et des bases de données

De la même façon, les données telles que les textes et, dès lors que ceux-ci présentent une certaine originalité, les images et les sons, sont protégés par le droit d'auteur.

L'autorisation écrite du titulaire des droits est ainsi nécessaire pour leur utilisation.

Le non-respect des dispositions relatives à la protection des droits de l'auteur sur ces données est constitutif de contrefaçon et il est donc civilement et/ou pénalement punissable.

D'une manière générale, la difficulté à connaître précisément l'origine des données transmises et donc les droits y afférent, en particulier avec le développement des moyens d'échanges d'informations en réseau ouvert comme Internet, oblige les utilisateurs à la plus grande prudence.

On entend par bases de données un recueil d'œuvres de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen.

Les bases de données sont protégées par le Code de la propriété intellectuelle indépendamment de la protection dont peuvent bénéficier les données au titre du droit d'auteur contenu dans ladite base.

Les bases de données qui, par le choix ou les dispositions des matières, constituent des créations intellectuelles, bénéficient des dispositions du Code de la propriété intellectuelle.

Les bases de données peuvent faire l'objet d'une extraction ou d'une réutilisation partielle ou en totalité, conformément à l'article L. 342-1 du Code de la propriété intellectuelle qui autorise des licences ou des utilisations subordonnées à l'accord du titulaire des droits.

L'utilisateur doit obtenir du producteur d'une base de données l'autorisation de :

- procéder à toute extraction par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle, du contenu de cette base sur un autre support, par tout moyen et sous toute forme que ce soit;
- réutiliser tout ou partie de cette base de données.

A ce titre, un utilisateur des bases de données de l'institution ne saurait s'autoriser à utiliser à des fins privées par exemple un fichier d'adresses, dont l'institution est propriétaire, et ne saurait le télécharger ou en faire toute utilisation contraire au Code de la propriété intellectuelle.

IV. La protection des marques

Le Code de la propriété intellectuelle protège « toute marque de fabrique, de commerce ou de service servant à distinguer les produits ou services d'une personne physique ou morale » (article L.711-1).

Peuvent être définis et utilisés à titre de marque, tous signes nominaux, figuratifs ou sonores, tels que les mots, assemblage de mots, nom patronymique, nom géographique, pseudonyme, lettre, chiffre, sigle, emblème, photographie, dessin, empreinte, logo ou la combinaison de certains d'entre eux.



Ces droits et leur protection sur une marque confèrent à son titulaire, par un enregistrement, un droit de propriété sur cette marque.

L'utilisateur ne peut, sauf autorisation du propriétaire, reproduire, utiliser ou apposer une marque, ainsi qu'utiliser une marque protégée, supprimer ou modifier une marque régulièrement déposée.

Les utilisateurs s'interdisent donc, sauf autorisation expresse du propriétaire, toute reproduction ou usage ou apposition d'une marque ainsi que l'usage d'une marque reproduite pour des produits ou services identiques à ceux désignés dans l'enregistrement, la suppression ou la modification d'une marque.

L'utilisateur ne saurait utiliser une marque sur laquelle l'institution ne détient pas l'autorisation expresse d'utilisation dans le cadre de ses fonctions.

Il lui sera en outre interdit d'utiliser à des fins privées toute marque dont l'institution est titulaire.

V. La protection des systèmes d'information

La protection des systèmes d'information est principalement mais non exclusivement organisée à travers les articles 323-1 et suivants du code pénal.

Les atteintes aux systèmes d'information en tant que systèmes de traitement automatisé de données sont sanctionnées au titre de la réglementation sur la fraude informatique contenue aux articles 323-1 et suivants du Code pénal.

Ce dernier interdit notamment :

- l'accès illicite, c'est-à-dire toute introduction dans un système informatique par une personne non autorisée (article 323-1 du Code pénal);

La notion d'accès s'entend de tout système de pénétration tel que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.

- le maintien frauduleux, c'est-à-dire le maintien sur le système informatique après un accès illicite et après avoir pris conscience du caractère « anormal » de ce maintien (article 323-3 du Code pénal);

Le maintien frauduleux est notamment caractérisé par des connexions, visualisations ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est « anormal ».

- le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 susvisés (article 323-3-1);



- l'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique (article 323-2 du Code pénal);
L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence « négative » sur le fonctionnement du système pour que le concept d'entrave soit retenu.
- l'altération des données, c'est-à-dire toute suppression, modification ou introduction de données « pirate », avec la volonté de modifier l'état du système informatique les exploitant et ce, quelle qu'en soit l'influence (article 323-1 du Code pénal).

Il en est ainsi pour les bombes logiques, l'occupation, la saturation de la capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.

Par ailleurs, la création de faux et leur usage, constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.

L'utilisateur doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires.

VI. Le secret des correspondances

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 45 000 euros d'amende « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination adressées à des tiers, ou d'en prendre frauduleusement connaissance, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises ou transmises par la voie de télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » (article 226-15 du Code pénal).

Il est également informé qu'est puni de trois ans d'emprisonnement et de 45 000 euros d'amende, « le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances... » (article 432-9 du Code pénal).

VII. La responsabilité en matière de transmission des informations

Les moyens informatiques mis à la disposition de l'utilisateur permettent l'accès à une communication et à une information importante et mutualisée.

Or, de tels moyens de communication ne doivent pas permettre de véhiculer n'importe quelle information ou donnée, dès lors que celle-ci serait susceptible de mettre en péril des mineurs.



Ainsi, le Code pénal, dans ses articles 227-23 et 227-24, sanctionne le fait de fabriquer, de transporter, de diffuser, par quelque moyen que ce soit et quel qu'en soit le support, un message à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, de trois ans d'emprisonnement et de 75000 euros d'amende.

Est également puni de cinq ans d'emprisonnement et de 75 000 euros d'amende, le fait de fixer, d'enregistrer ou de transmettre en vue de sa diffusion, l'image ou la représentation d'un mineur lorsque cette dernière présente un caractère pornographique.

Est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende, « le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit ».

VIII. Le respect de la vie privée

VIII.1. Le droit à la vie privée

Le principe est posé par l'article 9 du Code civil qui prévoit que "chacun a droit au respect de sa vie privée".

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre ou autres, propres à empêcher ou à faire cesser une atteinte à l'intimité de la vie privée.

VIII.2. Le droit à l'image

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 45000 euros d'amende, « le fait au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui :

- En captant, enregistrant ou transmettant, sans le consentement de leur auteur des paroles prononcées à titre privé ou confidentiel;
- En fixant, enregistrant ou transmettant sans le consentement de celle-ci l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés ci-dessus ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé » (article 226-1 du Code pénal).

VIII.3. Le droit de représentation

L'utilisateur est informé qu'est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention (article 226-8 du code pénal).



IX. Les règles de preuve

Le principe est celui de la liberté de la preuve qui peut donc être rapportée par tout moyen.

A ce titre, l'utilisateur est informé qu'un message électronique peut constituer une preuve susceptible d'engager la responsabilité de l'institution ainsi que la sienne.

En effet le Code civil reconnaît à travers les articles 1316 à 1316-4 une valeur juridique à l'écrit sous forme électronique. De même les articles 1369-1 et suivant du Code civil reconnaissent une valeur juridique aux contrats sous forme électronique.

Il est nécessaire que chaque utilisateur respecte scrupuleusement la législation en vigueur car le non-respect de cette obligation est passible de sanctions pénales.

X. L'obligation d'information

L'article 40 du code de procédure pénale précise que « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Il s'agit là d'une obligation forte attachée à la personne d'un fonctionnaire qui est tenu d'informer mais également de communiquer les éléments dont il dispose auprès du procureur de la République lorsqu'il a connaissance d'un crime ou d'un délit.