ANNEXE A LA DELIBERATION
CHARTE DU BON USAGE DES MOYENS INFORMATIQUES ET DE TELECOMMUNICATION D'ESTUAIRE ET SILLON

Communauté de Communes Estuaire et Sillon

Charte Informatique Et Téléphonique

SOMMAIRE

Contenu

PREAMBULE

✓ Le contexte et les enjeux

Les différents outils technologiques utilisés offrent au personnel des collectivités une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles.

A l'inverse, une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves. En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'intégrité et à la sécurité des fichiers de données.

De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.

L'application des nouvelles technologies informatiques et de communication permettent de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun.

✓ L'objectif

La présente charte informatique est un code de déontologie formalisant les règles légales de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de la collectivité : applications métiers, bureautique, messagerie, micro-ordinateurs fixes et portables, périphériques, téléphones fixes et portables, Internet … (liste non exhaustive). Elle vise autant à sécuriser la collectivité que l'agent dans sa pratique et permet également de poser les règles de fonctionnement et l'obligation de la collectivité.

✓ Le champ d'application

La présente charte s'applique à l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire. Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte. Dès l'entrée en vigueur de la présente charte, chaque agent de la collectivité s'en verra remettre un exemplaire, il devra en prendre connaissance et devra s'engager à la respecter.

I.LES REGLES GENERALES D'UTILISATION

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues ainsi que des règles élémentaires de courtoisie et de bienséance.

Tout manquement, selon sa gravité, est susceptible d'entraîner pour l'utilisateur des sanctions disciplinaires, et ce sans exclusion d'éventuelles actions pénales ou civiles à son encontre. L'utilisateur pourra, en outre, voir ses droits d'accès aux ressources et système d'information et de communication suspendus ou supprimés, partiellement ou totalement.

A. Les droits et les devoirs des utilisateurs

1) UN ACCÈS AUX RESSOURCES RÉGLEMENTÉ

Toute personne travaillant dans la collectivité dispose ou disposera à terme d'un droit d'accès au système d'information.

Ce droit d'accès est :

- **Strictement personnel**
- **Incessible**

Toutes les connexions réalisées à l'aide de son identifiant engagent la responsabilité de son propriétaire. En conséquence de quoi, il convient de respecter les règles de sécurité suivantes :

- Ne pas inscrire ses identifiants et mots de passe sur support papier ou électronique à proximité des outils informatiques mis à disposition ou sur ceux-ci, ainsi que de les stocker en clair dans un registre, un programme ou un fichier.
- Ne jamais confier son identifiant / mot de passe, même à son supérieur hiérarchique (exception faite du chef de projet informatique dans le cadre de sa mission).
- Ne jamais demander l'identifiant / mot de passe d'un collègue ou d'un collaborateur (exception faite du chef de projet informatique dans le cadre de sa mission).

- Ne pas utiliser ou essayer d'utiliser les moyens d'authentification autres que les siens et / ou masquer sa véritable identité.

2) UNE UTILISATION PROFESSIONNELLE DES RESSOURCES

Les ressources informatiques mises à disposition constituent un outil de travail. Elles relèvent d'un strict usage professionnel. Il est entendu ici qu'elles ne pourront être mises à disposition ou prêter à un tiers autre qu'un agent de la collectivité.

Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter l'intégrité et la confidentialité des données. Cette règle s'applique tant pour le traitement des informations que pour leur communication interne et externe.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi " informatique et liberté " du 06/01/1978). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives.
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Ne pas introduire de "ressources extérieures" matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information.
- Respecter les contraintes liées à la maintenance du système d'information.
- Respecter le plan de nommage des fichiers dès lors qu'il aura été défini au sein de la collectivité.

B. Les droits et les devoirs de la collectivité

La collectivité doit veiller à la disponibilité et à l'intégrité du système d'information. En ce sens, elle s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources…) du système d'information susceptibles d'occasionner une perturbation.
- Respecter la confidentialité des "données utilisateurs" auxquelles elle pourrait être amenée à accéder pour diagnostiquer ou corriger un problème spécifique.
- Définir les règles d'usage de son système d'information et veiller à leur application.

C. L’analyse et le contrôle

Pour des nécessités de sécurité, de maintenance et de gestion technique, l’utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du chef de projet informatique, de la direction générale des services et de l’autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l’informatique, aux fichiers et aux libertés.

D. Les sanctions

La loi, les textes réglementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout utilisateur du système d'information de la collectivité n'ayant pas respecté la loi pourra être poursuivi pénalement.

En outre, tout utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à la collectivité et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l’autorité territoriale.

E. Les évolutions

Cette charte est un guide qui s'impose à tous les utilisateurs, validée par le Comité Social Territorial et le Conseil Communautaire.

Son application au quotidien est l'affaire de tous, dans l'intérêt de chacun.

Elle pourra être complétée ou modifiée par l'autorité territoriale, l'avis du C.S.T sera préalablement sollicité et la charte soumise à l'approbation du Conseil Communautaire sera à nouveau demandé.

II. LES POSTES INFORMATIQUES

A. Les règles d'utilisation des postes

Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition de chaque utilisateur :

- Matériel : unité centrale, écran, clavier, souris…,
- Système d 'exploitation: Windows (10 Pro, 11 …), Android, …,
- Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le chef de projet informatique doit être informé au moins 15 jours à l'avance de l'arrivée d'un nouvel agent, le temps de pouvoir créer, session, licence office365 et autorisations d'accès et faire préparer par le prestataire le matériel nécessaire à la mission de l'agent.

Lors du départ d'un agent de la collectivité, le responsable de service doit en informer le chef de projet informatique afin de pouvoir libérer les licences utilisées préalablement et tenir à jour l'inventaire du matériel.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention notamment pour les écrans plats.

Les tablettes doivent être mises sous clef à la fin de la journée.

Toute installation logicielle est à la charge de la personne compétente et désignée par l'autorité territoriale.

Les téléchargements à l'initiative de l'utilisateur et sans l'autorisation du chef de projet informatique sont interdits.

En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches "Windows + L")

En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller systématiquement son PC.

A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran.

Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (au moins une fois par an).

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations.

L'utilisateur doit signaler tous dysfonctionnements ou anomalies au référent informatique selon la procédure définie par la collectivité.

Rappel de la **procédure** :

Envoyez un mail à ***assistance.informatique@estuaire-sillon.fr*** en précisant :

- L'objet de l'incident informatique
- Le n° de téléphone où vous êtes joignable
- Pour certains sites avec des horaires atypiques (par exemple médiathèques, accueils périscolaires…), merci de préciser également les horaires où vous êtes disponible.

L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés dans le but de préserver la capacité de stockage.

L'agent qui quitte définitivement la collectivité doit restituer ses équipements informatiques et téléphoniques au chef de projet informatique pour maintenance et remise à zéro.

B. Sécurité

Les supports amovibles **personnels** (clé USB, disque dur externe etc.) sont formellement interdits.

Des clés USB destinées à un usage strictement professionnel ainsi que des clés USB sécurisées sont disponibles. (demande à faire auprès du chef de projet informatique).

III.LA MESSAGERIE

A. Les règles d'utilisation de la messagerie électronique (@estuaire-sillon.fr)

L'utilisation de la messagerie est réservée à des fins professionnelles.

L'utilisateur est tenu de la consulter au minimum une fois par jour, hormis en période d'absence. Il doit accorder la même importance aux messages électroniques qu'aux courriers postaux et se doit de les traiter.

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'autorité territoriale ou le référent informatique. Les courriers à caractère privé doivent expressément porter la mention « [PRIVÉ] » dans leur objet. Ces derniers ne pourront alors être ouverts par l'autorité territoriale ou le référent informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la loi.
L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel. Elle comportera obligatoirement :

- Le nom et prénom de l'expéditeur sauf dérogation expresse de l'autorité territoriale.
- Son entité de rattachement.
- Les coordonnées téléphoniques de la collectivité.

L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles.

Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue.

B. Rappel des bonnes pratiques de sécurité

La messagerie est devenue l'un des premiers vecteurs de propagation de virus. Il est en effet très simple de diffuser, sous forme de fichier attaché ou de lien internet par exemple, un programme infecté.

Des outils ont été mis en place pour prémunir la collectivité contre ce type d'attaque. Toutefois il est impossible de garantir un niveau de sécurité totale, il est donc nécessaire de respecter les précautions simples décrites ci-dessous :

- Les fichiers attachés ayant une extension de type « .exe » ne doivent jamais être ouverts. Il est indispensable de prévenir le prestataire informatique (mail à assistance.informatique@estuaire-sillon.fr) pour analyse, ou de les supprimer directement.
- Les messages suspects (ayant un objet douteux, une pièce jointe inhabituelle, ou encore provenant d'une personne ou d'une institution connue nous demandant des informations inhabituelles ou employant un ton inusité…) ne doivent pas être ouverts, ils seront directement transmis au prestataire informatique pour analyse ou destruction.
- Préférez Smash à WeTransfer pour l'envoi des fichiers volumineux jusqu'à 2Go, (https://fr.fromsmash.com/) Smash est un service français et sécurisé.

IV.L'INTERNET

Cette présente partie a pour objectif d'établir les règles d'utilisation de l'Internet.

L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel. Toutefois, la consultation des e-mails personnels (Exemple : Laposte.net, Orange.fr, Wanadoo.fr, Free.fr, Gmail.com … etc.) reste interdite sur le réseau de la CCES.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pornographie, pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée…).

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

Le streaming (Radio, TV, Musique …) est interdit sur le réseau professionnel de la CCES afin de réduire l'encombrement de la bande passante.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.

Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

Toute procédure d'achats personnels sur Internet est formellement interdite.

L'utilisation de forums de discussion est autorisée pour un usage professionnel. Tout utilisateur participant à un forum fait figurer en bas de chacun des messages publiés la mention suivante : « Le contenu de ce message n'engage que son auteur et en aucun cas la Communauté de Communes Estuaire et Sillon ».

V.LE WIFI

Le réseau wifi « CC_Estuaire&Sillon » est au même titre qu'une connexion filaire un moyen d'accéder au réseau professionnel.

Il sert uniquement à connecter nos équipements professionnels.

Par mesure de sécurité, les périphériques personnels (téléphone portable, tablette par exemple) ne doivent pas être connectés à ce réseau.

Le mot de passe ne doit pas être partagé avec le public, ni avec les entreprises venant travailler dans nos bâtiments.

VI.LE TELEPHONE

Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.

L'utilisation des téléphones fixes, portables et leurs numéros est réservée à des fins professionnelles.

L'utilisation d'une carte SIM privée dans un téléphone de la CCES n'est pas autorisée.

Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle.

L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.

L'agent qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel ainsi que la carte SIM au chef de projet informatique.

L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

VII. DEMATERIALISATION

Les utilisateurs s'engagent à maîtriser la production des documents et privilégier la dématérialisation :

- Travailler dans la mesure du possible à l'écran pour limiter l'usage papier.
- N'imprimer ou ne photocopier que si nécessaire : l'impression des e-mails est à éviter, **sauf besoin indispensable**.
- Imprimer en noir et blanc et recto/verso sauf si besoin couleur (Carte, Plan …).
- Eviter d'imprimer les courriels, les devis et les documents projetés en réunion (hormis dispositions réglementaires).
- Déposer les documents de travail sur le serveur et envoyer un lien plutôt que d'envoyer un document.
- Utiliser l'aperçu avant impression pour éviter les erreurs.

VIII. Données personnelles à caractère sensible

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, l'ordonnance n°2018-1125 du 12 décembre 2018, ainsi que le règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

A cet égard, les utilisateurs s'engagent à :

- Ne pas utiliser les données auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions.
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales.
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution des fonctions de l'agent.
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données.
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données.
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données.

En cas de cessation des fonctions de l'utilisateur, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Tous les utilisateurs du système d'information et particulièrement les agents sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées.

IX. LES BASES LEGALES

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

A. Les textes législatifs

Loi du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

Loi du 17/07/1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

Loi du 03/07/1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.

Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

Loi du 05/01/1988 sur la fraude informatique.

Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :

- Les accès ou maintien frauduleux dans un système d'information.
- Les atteintes accidentelles ou volontaires au fonctionnement.
- La falsification des documents informatiques et leur usage illicite.
- L'association ou l'entente en vue de commettre un de ces délits.

Loi du 10/07/1991 relative au secret des correspondances émises par voie des télécommunications.

Loi du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Loi du 21/06/2004 pour la confiance dans l'économie numérique. Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

B. Le droit disciplinaire

Loi n°84-53 du 26 janvier 1984 (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.

Décret n°92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.

Décret n°88-45 du 15 février 1988 (art. 36 et 37) relatif aux agents non titulaires.

Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

C. Le code pénal

Article 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1 : 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 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4 : La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs

des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5 : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1) L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
2) L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
3) La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
4) La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.
5) L'exclusion, pour une durée de cinq ans au plus, des marchés publics.
6) L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.
7) L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6 : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7 : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

D. La réglementation européenne

La convention européenne du 28/01/1991 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel.

Elle définit les principes de base de la protection des données que les Etats parties doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les Etats parties.

Elle règle la coopération entre Etats pour la mise en œuvre de la Convention, en particulier l'assistance qu'un Etat partie doit prêter aux personnes concernées ayant leur résidence à l'étranger. Enfin, elle met en place un Comité consultatif chargé en particulier de faciliter et d'améliorer son application.

La directive 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données, publiée au Journal Officiel des Communautés Européennes du 23 novembre 1995.

Cette directive vise à réduire les divergences entre les législations nationales sur la protection des données afin de lever tout obstacle à la libre circulation des données à caractère personnel à l'intérieur de l'Union européenne.

La directive de la CEE du 21/12/1988 sur l'harmonisation de la protection juridique des logiciels. Elle protège les droits d'auteur, elle interdit en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, **l'ordonnance n°2018-1125 du 12 décembre 2018**, ainsi que le Règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

GLOSSAIRE

(A compléter, le cas échéant, par l'autorité territoriale lors de toute modification)

SYSTEME D'INFORMATION : Ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation (de la collectivité).

RESSOURCES INFORMATIQUES :

- Le matériel.
- les logiciels et les procédures.
- les données et les fichiers.

INTERNET : Interconnexion mondiale de réseaux reposant sur un protocole appelé « Internet » et dont les applications les plus utilisées sont le courriel et les consultations de sites (Web).

INTRANET : Utilisation des technologies liées à Internet au sein d'un réseau local. Les principaux intérêts sont de faciliter et de rendre plus conviviale l'accès aux données par l'utilisation du navigateur et de la messagerie interne.

COURRIEL : message électronique.

RESEAU : Ensemble d'ordinateurs et de machines informatiques qui communiquent grâce à une technique commune de transmission.

PERIPHERIQUES : Matériels connectés à un poste de travail ou directement sur le réseau local (exemples : imprimante, scanners…)