



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA JUSTICE

**DIRECTION DE
L'ADMINISTRATION PÉNITENTIAIRE**

**CIRCULAIRE RELATIVE À L'ACCÈS DES DÉTENUS À
L'INFORMATIQUE**

VERSION COMMUNICABLE

TABLE DES MATIÈRES

1. INTRODUCTION – ACCÈS DES DÉTENUS A L'INFORMATIQUE : SÉCURITÉ ET RÉINSERTION	3
1.1. CONTEXTE	4
1.2. OBJET DE LA PRÉSENTE CIRCULAIRE.....	4
1.3. RAPPEL DU CADRE LÉGAL.....	5
1.4. RISQUES	6
1.5. PRINCIPE D'UTILISATION DE L'INFORMATIQUE PAR LES DÉTENUS ...	8
1.6. MISE EN ŒUVRE ET SUIVI	8
2. MESURES GÉNÉRALES	9
2.1. CADRE GÉNÉRAL D'UTILISATION DE L'INFORMATIQUE EN DÉTENTION	9
2.2 Publications informatiques.....	9
2.3. ÉCHANGE DE SUPPORTS D'INFORMATIONS AMOVIBLES.....	10
2.3.1. Échange interne.....	10
2.3.2. Échange avec l'extérieur	10
2.3.3. Accès Internet.....	10
3. INFORMATIQUE EN CELLULE	12
3.1. ACQUISITION DU MATÉRIEL.....	12
3.1.1. Autorisation d'achat.....	12
3.1.2. Fournisseurs agréés	13
3.1.3. Unicité des matériels.....	13
3.1.4. Technologies autorisées / interdites	14
3.2. UTILISATION ET COMPORTEMENT.....	15
3.3. MOTS DE PASSE SUR LES ORDINATEURS EN CELLULE.....	15
3.4. GARANTIE, RÉPARATION ET MAINTENANCE	16
4. INFORMATIQUE EN SALLE D'ACTIVITÉ.....	17
4.1. CONTEXTE D'UTILISATION.....	17
4.2. CADRE CONTRACTUEL DES ACTIVITÉS COLLECTIVES.....	17
4.3. CONDITIONS D'ACCÈS	18
4.4. TECHNOLOGIES AUTORISÉES / INTERDITES	18
4.5. MATÉRIELS FOURNIS PAR LES ASSOCIATIONS	21

4.6. MOTS DE PASSE DES EQUIPEMENTS INFORMATIQUES EN SALLE D'ACTIVITÉ.....	21
5. MESURES DE CONTRÔLE.....	22
5.1. RAPPEL DU CADRE LÉGAL.....	22
5.2. INVENTAIRE	22
5.3. SCHELLEMENT DES BOITIERS	22
5.4. FOUILLES PHYSIQUE ET LOGIQUE DES ORDINATEURS ET DES SUPPORTS D'INFORMATION.....	23
5.5. TRANSFÈREMENT	24
5.6. LIBÉRATION.....	24
5.7. SURVEILLANCE DES ACTIVITÉS	25
6. FORMATION ET INFORMATION DES PERSONNELS	26
6.1. CONTEXTE	26
6.2. MODULE POUR LES ÉQUIPES INFORMATIQUES RÉGIONALES ET LOCALES.....	27
6.3. MODULE PERSONNELS DE SURVEILLANCE, TECHNIQUE ET DE DIRECTION.....	28
6.4. MODULE PERSONNELS D'INSERTION ET DE PROBATION	29
ANNEXES	30
ANNEXE 1 Liste des technologies autorisées et interdites en cellule.....	31
ANNEXE 2 : Liste des technologies autorisées et interdites en salle d'activités encadrées	34
ANNEXE 4 : références juridiques	39
ANNEXE 5 : Convention cadre fournisseur.....	44

1. INTRODUCTION – ACCÈS DES DÉTENUS A L'INFORMATIQUE : SÉCURITÉ ET RÉINSERTION

1.1. CONTEXTE

L'administration pénitentiaire se trouve aujourd'hui confrontée à une forte augmentation du nombre d'ordinateurs possédés ou utilisés par les détenus au sein des établissements pénitentiaires, et particulièrement au sein des maisons centrales et des centres de détention.

Les ordinateurs sont désormais mis à disposition des détenus dans deux contextes différents :

- lors d'activités collectives assurées par des intervenants extérieurs (*formation professionnelle, enseignement, programmation culturelle et socioculturelle*) et dans le cadre du travail rémunéré des personnes détenues ;
- en cellule où, au-delà d'un grand nombre de consoles de jeux, le nombre d'ordinateurs installés est important et augmente fortement. Ces demandes sont plus fortes dans les maisons centrales et centres de détention où les détenus souhaitent accéder à l'informatique en dehors des heures de travail ou d'activités encadrées.

L'administration pénitentiaire souhaite accompagner cette évolution.

L'article 1 de la loi du 22 juin 1987 relative au service public pénitentiaire lui fait obligation de mettre en œuvre toutes les dispositions utiles pour assurer une formation et une activité professionnelle aux personnes incarcérées qui le souhaitent.

Pour assurer ces missions de formation et de réinsertion des personnes détenues les outils informatiques sont des vecteurs privilégiés pour l'acquisition de connaissances à tous les niveaux de formation, pour de nombreuses professions, et pas uniquement à destination des métiers de l'Informatique.

C'est aussi un moyen de motivation pour des publics qui manquent souvent d'un accès facile à l'écrit et acquièrent par ce support un apprentissage large de savoirs de base, de connaissances et de modes de communication qui structurent la vie sociale contemporaine.

La politique de réinsertion suppose de permettre à la fois l'acquisition de connaissances et compétences nouvelles mais aussi d'offrir des activités diversifiées, les plus proches possible de la société contemporaine où il s'agit de se réinsérer. C'est pourquoi on ne peut établir une frontière stricte entre une utilisation pédagogique et une utilisation ludique très répandue dans la société. Cependant, si l'usage de l'outil informatique se révèle être un support performant dans l'acquisition des connaissances ou d'un métier, il n'en demeure pas moins vrai que l'introduction de l'ordinateur en détention constitue un risque spécifique qu'il convient également de mesurer et de maîtriser.

Ainsi, il ne saurait être question de banaliser l'utilisation de cet instrument de travail, d'éducation et de loisirs.

Le domaine très **évolutif** dans lequel se situe l'informatique entraînera nécessairement et inévitablement des **actualisations** qui tiendront compte notamment des avis et observations formulés par les chefs d'établissement pénitentiaire.

1.2. OBJET DE LA PRÉSENTE CIRCULAIRE

Le terme « informatique » comprend, dans la présente circulaire, tout composant matériel ou logiciel permettant de recueillir et stocker, de traiter ou de diffuser des informations. Il comprend ainsi principalement les unités de traitement (*Poste de travail, consoles de jeux, lecteur multimédia, Pocket PC et PDA, SmartPhones, ...*), les unités de stockage d'information (Cédérom par exemple).

La présente circulaire a pour but d'encadrer l'utilisation par les personnes détenues du matériel informatique en tenant compte d'une part des impératifs sécuritaires et d'autre part de la mission de réinsertion qui incombe à l'administration pénitentiaire.

En matière d'informatique il convient de distinguer **plusieurs niveaux d'utilisation** :

1. **par les personnes détenues en cellule.** On rappellera dans le présent texte le pouvoir du chef d'établissement de répondre favorablement ou non à une demande du détenu d'ordinateur en cellule en fonction du profil de la personne. Viennent ensuite des prescriptions strictes sur le matériel autorisé ou interdit, prescriptions sur lesquelles les services locaux et régionaux d'informatique seront obligatoirement consultés.
2. **par les personnes détenues en salle d'activités encadrées.** La présente circulaire définit strictement les matériels utilisables par les personnes détenues quel que soit le type d'activités collectives concerné.

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes]

Compte tenu des difficultés soulevées par la présence d'ordinateurs en détention, il est rappelé que **seul le chef d'établissement, usant de son pouvoir d'appréciation et garant de la conformité de son fonctionnement, peut autoriser ou non l'introduction d'ordinateurs dans son établissement.** Pour ce qui concerne les demandes d'achat des matériels informatiques pour les détenus ou de participation à des activités informatiques, il s'appuie sur l'avis de la commission de classement (*Cf. processus décrits au chapitre 3.1.1*), en relation avec le SPIP et les équipes informatiques régionales.

1.3. RAPPEL DU CADRE LÉGAL

Acquisition :

Les détenus bénéficient :

- du droit au travail, à la formation professionnelle, à l'enseignement et aux activités socio-culturelles en vertu des articles 717-3, D95, à D440 à D 449, D450 à D459, et D573 du CPP ;
- du droit d'acquérir un ordinateur par l'intermédiaire de l'administration et selon les modalités qu'elle détermine pour les équipements informatiques (article D 449-1 du Code de Procédure Pénale issu du décret du 20 mars 2003).

Utilisation :

L'utilisation est réglementée par l'article D 449-1 du code de procédure pénale.

- article D449-1 (*décr. n° 2003 -59 du 20 mars 2003, art. 19*).

Les détenus peuvent acquérir par l'intermédiaire de l'administration et selon les modalités qu'elle détermine des équipements informatiques.

Une instruction générale détermine les caractéristiques auxquelles doivent répondre ces équipements, ainsi que leur utilisation.

En aucun cas, les détenus ne sont autorisés à conserver des documents, autres que ceux liés à des activités socioculturelles ou d'enseignement ou de formation ou professionnelles, sur un support informatique.

Ces équipements ainsi que les données qu'ils contiennent sont soumis au contrôle de l'administration. Sans préjudice d'une éventuelle saisie par l'autorité judiciaire, tout équipement informatique appartenant à un détenu peut, au surplus, être retenu, pour lui être restitué qu'au moment de sa libération, dans les cas suivants :

1° pour des raisons de sécurité;

2° en cas d'impossibilité d'accéder aux données informatiques, du fait volontaire du détenu.

1.4. RISQUES

[Partie occultée, car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

1.5. PRINCIPE D'UTILISATION DE L'INFORMATIQUE PAR LES DÉTENUS

L'administration pénitentiaire autorise l'utilisation de l'informatique par les détenus sous réserve du respect des principes suivants :

1. la mise en œuvre de ces outils informatiques ne doit en aucun cas mettre en péril la sécurité pénitentiaire.
2. les règles présentées dans la présente circulaire doivent être rigoureusement respectées.

Les règles énoncées ci-après sont issues de réflexions qui ont privilégié une **approche globale** des difficultés soulevées par l'informatique en détention. Elles ont été élaborées pour éviter toute dépendance à une technologie trop spécifique et pour faciliter les prises de décisions des chefs d'établissement.

Il est toutefois recommandé à ces derniers, en cas de doute sur l'adoption de telle ou telle mesure, de prendre l'attache des services de la direction régionale afin d'estimer le dispositif à prendre en compte pour une gestion maîtrisée des ordinateurs en détention.

3. **Tout ce qui n'est pas explicitement autorisé est interdit.**
4. L'utilisation des ordinateurs par les détenus doit pouvoir être contrôlée à tout moment.

1.6. MISE EN ŒUVRE ET SUIVI

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

2. MESURES GÉNÉRALES

2.1. CADRE GÉNÉRAL D'UTILISATION DE L'INFORMATIQUE EN DÉTENTION

Dans le respect de la réglementation en vigueur le chef d'établissement dispose d'un pouvoir d'appréciation et demeure le décisionnaire final quant aux mesures relatives à l'informatique en détention.

Une utilisation abusive (gêne causée à des codétenus, par exemple) ou détournée de l'outil informatique telle que prévues par l'article D 249-3 10°, peuvent justifier des sanctions disciplinaires, sans préjudice de poursuites pénales éventuelles. La sanction consistant à priver le détenu de son appareil, telle que prévue par l'article D251-1, alinéa 3 du Code de Procédure Pénale peut notamment être infligée au contrevenant.

Les prescriptions relatives aux procédures d'achat de matériel informatique, aux modalités d'utilisation de ce matériel, aux règles à respecter pour son usage et aux sanctions applicables en cas d'utilisation abusive ou détournée doivent être précisées dans le **règlement intérieur** de l'établissement pénitentiaire.

2.2 Publications informatiques

La presse informatique est achetée par les détenus, soit par l'intermédiaire de l'administration pénitentiaire (en cantine), soit au moyen d'un abonnement autorisé.

Les dispositions concernant les publications doivent être indiquées dans le règlement intérieur de l'établissement pénitentiaire qui doit déterminer de manière précise les modes d'acquisition des journaux.

Pour des raisons de sécurité, les objets joints aux revues ne sont pas remis. Ils sont déposés au vestiaire du détenu ou remis à sa demande à un membre de sa famille ou à une personne titulaire d'un permis de visite.

La réception de journaux informatiques par le courrier personnel est prohibée, comme est prohibé l'envoi suivant le même mode de disquettes informatiques ou de disques compacts, conformément aux articles D-444 et D-423 du code de procédure pénale.

En ce qui concerne les revues de piratage informatique : celles-ci peuvent être retenues sur la base de l'article D-444 alinéa 2 du code de procédure pénale, lequel prévoit que les publications contenant des menaces précises contre la sécurité des personnes ou celles des établissements pénitentiaires peuvent être, à la demande des chefs d'établissement, retenues sur décision du ministre de la justice.

Si une procédure de retenue est envisagée, le détenu concerné doit être mis à même de présenter ses observations écrites, et le cas échéant sur sa demande, ses observations orales. Il doit avoir la possibilité de se faire représenter par un avocat ou un mandataire de son choix. Il convient de se reporter sur ce point à la circulaire du 9 mai 2003 relative à l'application pour l'administration pénitentiaire de l'article 24 de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

Les revues saisies sont déposées au vestiaire du détenu.

De la même manière, il convient de ne pas remettre les CD Rom et disquettes joints aux revues non spécialisées en informatique, qui peuvent présenter des risques quant à leur utilisation ou leur contenu.

2.3. ÉCHANGE DE SUPPORTS D'INFORMATIONS AMOVIBLES

2.3.1. ÉCHANGE INTERNE

Il convient de s'assurer :

- que le détenu ne transporte aucun support informatique (disquette, cédérom, DVD... entre la salle d'activités ou les ateliers et sa cellule, et vice-versa) ;
- qu'il ne réalise aucune copie illicite de programme ou logiciel ;
- qu'il n'utilise pas le matériel mis à sa disposition à d'autres fins.

L'échange de supports d'informations, quels qu'ils soient, entre détenus est rigoureusement interdit.

Le chef d'établissement doit prévoir, dans le règlement intérieur, des modalités particulières concernant ces échanges, en application de l'article D249-2, alinéa 8 (échanges non autorisés entre codétenus) CPP. Seuls les échanges ou prêts de livres personnels entre détenus sont autorisés en vertu du dernier alinéa de l'art D-444 CPP.

2.3.2. ÉCHANGE AVEC L'EXTERIEUR

L'échange ou la communication par un détenu de tout support d'informations (disque dur, bande magnétique, disquette ou CÉDÉROM) avec l'extérieur est **strictement interdit**.

La remise de matériel informatique est prohibée aux parloirs.

Seules sont autorisées les sorties de disquettes ou de supports optiques ayant fait l'objet d'une convention entre les organismes de formation et l'administration pénitentiaire. Cette convention doit stipuler que ces supports à caractère pédagogique ne contiennent pas d'informations prohibées. Ces supports autorisés doivent pouvoir être contrôlés à tout moment par les personnels pénitentiaires [*fin de phrase occultée car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes*]-

2.3.3. ACCES INTERNET

Aucun détenu ne doit avoir accès à Internet, ni être physiquement en contact avec un équipement le permettant.

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

3. INFORMATIQUE EN CELLULE

3.1. ACQUISITION DU MATÉRIEL

3.1.1. AUTORISATION D'ACHAT

Avant l'achat ou l'utilisation de matériels informatiques, le détenu doit obligatoirement faire une **demande d'autorisation auprès du chef d'établissement.**

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

L'autorisation d'achat ne doit porter que sur des matériels **neufs**. Il est en effet trop difficile d'assurer une parfaite vérification des matériels d'occasion : la conservation de données prohibées sur la mémoire de masse représente le principal danger des anciens appareils. **Il est dès lors interdit de permettre à un détenu de faire entrer dans l'établissement pénitentiaire le matériel informatique qu'il peut posséder à l'extérieur.**

De même sont interdites la vente ou la cession de matériel informatique entre détenus.

En cas d'autorisation effective, le détenu concerné doit être formellement identifié comme possédant un ordinateur auprès du personnel de surveillance [*fin de phrase occultée car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes*]

Le chef d'établissement dispose de la possibilité de retirer une autorisation d'acquisition d'un ordinateur préalablement accordée en cas d'usage manifestement abusif ou illégal. Ce retrait d'autorisation devra être motivé et notifié au détenu concerné après qu'ait été mise en oeuvre la procédure contradictoire telle que prévue à l'article 24 de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

3.1.2. FOURNISSEURS AGREES

Afin de garantir l'homogénéité du parc informatique et surtout l'application des règles de sécurité en la matière, il est établie une convention cadre qui lie l'administration pénitentiaire avec un ou plusieurs fournisseurs de matériels informatiques, laquelle précise les modalités d'acquisition de ces matériels informatiques par les détenus.

Les conventions peuvent être établies sur initiative des directions régionales (cf. modèle en annexe). Elles doivent au préalable avoir été validées par l'administration centrale.

Cette convention prévoit notamment :

- un engagement de confidentialité :

les fournisseurs doivent toujours rester dans l'ignorance de l'identité des détenus ayant acheté du matériel informatique. L'établissement constitue le seul interlocuteur des fournisseurs.

De même, le nom du fournisseur ainsi que les éléments permettant de l'identifier ne doivent pas être connus du détenu acquérant. Toutefois la garantie les stipule. Par conséquent, il convient de ne faire parvenir au détenu qu'une photocopie de la facture établie par le prestataire en masquant au préalable le nom du fournisseur ainsi que sa raison sociale.

- un engagement à ne pas fournir de matériels dits « dangereux », c'est-à-dire présentant des risques du point de vue de la sécurité pénitentiaire ou incluant des technologies interdites par la circulaire.
- la communication des éléments par les fournisseurs vers l'administration pénitentiaire listant les composants et caractéristiques des matériels fournis, permettant d'attester de la conformité de ces matériels au regard des dispositions de sécurité de la convention cadre.

3.1.3. UNICITE DES MATERIELS

Le détenu qui demande le remplacement d'un ancien matériel doit en accepter le dépôt à son vestiaire. Il peut aussi éventuellement en faire don à une association d'insertion de l'établissement. Le matériel concerné sera dans ce cas préalablement contrôlé.

Le principe dit de l'échange « un contre un » est systématiquement appliqué. Il vise à interdire la mise en place d'un trafic ou d'un système de racket liés au matériel d'occasion.

Cela impose notamment :

- un unique ordinateur par détenu ;
- un unique disque dur par ordinateur ;**
- un unique type de périphérique par catégorie et par ordinateur.

Le détenu ne doit jamais disposer de périphériques en double et tout remplacement doit faire l'objet d'une consignation au vestiaire de l'ancien matériel, qu'il soit ou non en état de marche. **Aucune exception ne saurait être acceptée.**

3.1.4. TECHNOLOGIES AUTORISEES / INTERDITES

Les technologies interdites par la présente circulaire mais intégrées en standard à la carte mère (modem RTC, carte réseau Ethernet, WIFI, ...) peuvent être autorisées par le chef d'établissement pour un usage en cellule *uniquement après destruction physique irréversible des fonctions prohibées.*

Pour éviter toute contestation de la part des détenus, cette destruction doit être opérée par le fournisseur du matériel informatique avec lequel l'administration a signé une convention et clairement figurer dans les caractéristiques techniques du catalogue et du bon de commande signé par le détenu. *Elle ne doit pas obérer la garantie due par le constructeur.*

Les services de l'administration pénitentiaire ne sont pas juridiquement habilités à modifier les caractéristiques techniques des matériels acquis par les détenus. Une autorisation écrite d'intervention signée par le détenu n'a en effet aucune valeur juridique.

Concernant les consoles de jeux, du fait des nouvelles fonctionnalités, il convient de considérer ce type d'équipement au même titre que tout autre ordinateur. Par conséquent, les personnels pénitentiaires se doivent d'être particulièrement vigilants quant aux capacités de communication offertes (cartes réseau Ethernet, WiFi ou CPL) par certains modèles d'équipements ludiques de ce type.

Les établissements devront mettre en place une procédure permettant aux détenus ayant un besoin réel de sauvegarde de bénéficier ponctuellement d'une solution de sauvegarde à l'aide d'un matériel de sauvegarde appartenant à l'administration pénitentiaire. La procédure suivie doit alors impérativement garantir que les supports mis à disposition du détenu seront vierges avant la sauvegarde.

Le tableau présenté en annexe 1 détaille les technologies autorisées et interdites dans le cadre de l'informatique en cellule. La personne détenue sera informée avant achat des fonctions interdites et détruites. Cet accord de destruction de fonctions dangereuses sera alors annexé à la demande d'achat.

Cette liste sera régulièrement mise à jour par l'administration pénitentiaire. Elle fait l'objet d'un «cahier technique», annexé à la présente circulaire et illustrant chaque technologie par des représentations de produits du marché. Ce cahier permet notamment au personnel pénitentiaire d'optimiser la réalisation des fouilles.

Les principales technologies autorisées et interdites pour un usage en cellule sont les suivantes (***liste non exhaustive, Cf. annexe 1 pour la liste exhaustive***) :

Principales technologies autorisées	Principales technologies interdites
<ul style="list-style-type: none"> • PC non portable et non communicant et consoles de jeux non communicantes 	<ul style="list-style-type: none"> • PC portables ou « de poche », PC communicants, consoles communicantes, assistants personnels
<ul style="list-style-type: none"> • Lecteur de CD ou de DVD 	<ul style="list-style-type: none"> • Graveurs de CD ou de DVD
<ul style="list-style-type: none"> • Lecteur de disquettes standard 	<ul style="list-style-type: none"> • Lecteur de disquettes « haute densité »
<ul style="list-style-type: none"> • Souris et manette de jeux avec fil 	<ul style="list-style-type: none"> • Périphérique de technologie « sans fil »
<ul style="list-style-type: none"> • CD et DVD pressés, disquettes 	<ul style="list-style-type: none"> • Tout autre support vierge (CD, DVD, clé USB, baladeur MP3 ...)
<ul style="list-style-type: none"> • Imprimantes jet d'encre 	<ul style="list-style-type: none"> • Imprimantes laser, scanners, télécopieurs, photocopieurs, Webcam, matériel de photo numérique
	<ul style="list-style-type: none"> • Tout périphérique et technologie de communication
<ul style="list-style-type: none"> • Systèmes d'exploitation, outils bureautiques et de développement, CAO, antivirus • Tout outil de graphisme livré « en standard » avec le système d'exploitation Windows 	<ul style="list-style-type: none"> • Logiciels de sécurité autres qu'antivirus, outils de numérisation, graphisme • Logiciels professionnels PAO ou DAO

3.2. UTILISATION ET COMPORTEMENT

L'autorisation d'utilisation et de possession de matériel informatique par un détenu nécessite de la part du personnel pénitentiaire de faire preuve d'une vigilance particulière au regard de l'usage qui est fait de ce matériel.

La personnalité du détenu, ses antécédents judiciaires, ses compétences techniques particulières peuvent conduire le chef d'établissement à prescrire des modalités spécifiques de surveillance de l'intéressé et de contrôle de l'utilisation du matériel.

3.3. MOTS DE PASSE SUR LES ORDINATEURS EN CELLULE

L'administration pénitentiaire doit toujours être en mesure de connaître et de vérifier le contenu du disque dur de l'ordinateur du détenu. Dès lors, ce dernier doit communiquer à l'administration pénitentiaire les différents mots de passe d'accès à son ordinateur personnel (au niveau du démarrage, du système d'exploitation ou des diverses applications).

Le refus de communiquer un mot de passe doit être considéré comme un refus d'obtempérer aux ordres des personnels pénitentiaires ou comme un usage non conforme de l'outil informatique. Il relève des sanctions disciplinaires telles que le retrait de l'autorisation d'utiliser un ordinateur ou la privation de son utilisation pendant une période d'un mois (article D-251-1 3° du Code de Procédure Pénale).

Une mention doit en être faite au règlement intérieur.

3.4. GARANTIE, RÉPARATION ET MAINTENANCE

L'achat de matériels informatiques par un détenu rend celui-ci **propriétaire de plein droit** et de manière **définitive**.

Le détenu acquéreur de matériels informatiques doit ainsi bénéficier des garanties accordées à tout acquéreur. Ni l'intermédiation de l'établissement dans l'acte d'achat, ni les spécificités de la vie en détention ne peuvent altérer ou annuler ces assurances. Ces dispositions doivent être clairement acceptées par le fournisseur avant son agrément.

Le nom du fournisseur ne doit pas être connu du détenu acquérant. Toutefois la garantie le stipule. Par conséquent, l'établissement veillera à ne fournir au détenu qu'une photocopie de la facture établie par le prestataire en masquant au préalable le nom du fournisseur.

Dans le cas d'une intervention exigeant un retour sur site, le matériel peut être retourné au fournisseur agréé, après accord de la direction de l'établissement. Chaque intervention donne lieu à une fiche qui est conservée à la fouille du détenu.

La réparation des matériels est confiée :

- aux fournisseurs initiaux pour les matériels encore sous garantie au moment de la mise en application de la présente circulaire ;
- à des prestataires de service agréés par les directions régionales, pour les matériels hors garantie.

Dans le cadre de la garantie des matériels, les fournisseurs proposent généralement, et pour une période limitée, une maintenance sur site. Au sein de l'établissement pénitentiaire, le chef d'établissement met, si cela est possible, à la disposition du technicien de maintenance habilité relevant d'un fournisseur agréé, une pièce réservée à cet effet et dans laquelle est apporté le matériel nécessitant une intervention. Cette opération doit se dérouler en présence d'un personnel pénitentiaire.

Les maintenances sur site sont préférables aux maintenances extérieures.

4. INFORMATIQUE EN SALLE D'ACTIVITÉ

4.1. CONTEXTE D'UTILISATION

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

4.2. CADRE CONTRACTUEL DES ACTIVITÉS COLLECTIVES

Toute activité collective doit être obligatoirement encadrée par les documents suivants :

- procédure d'agrément des solutions logicielles et matérielles utilisées,
- convention cadre entre la personne morale partenaire et l'administration pénitentiaire,
- avenant à la convention cadre entre la personne morale partenaire et l'administration pénitentiaire pour chacun de ses intervenants,

Il couvrira les sujets suivants :

responsabilités et obligations incombant à l'intervenant,
engagement de ne pas faire entrer et utiliser en détention du matériel prohibé,
circulation de l'information et échanges de fichiers avec l'extérieur,
fourniture et acquisition des matériels nécessaires aux formations,
respect de la réglementation en vigueur (références),
sanction envisagée dans le cadre du non-respect des engagements contractuels
(suspension sans délai de l'activité),
gestion et communication des mots de passe.

Tout intervenant doit être sensibilisé aux engagements précités.

4.3. CONDITIONS D'ACCÈS

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

4.4. TECHNOLOGIES AUTORISÉES / INTERDITES

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

4.5. MATÉRIELS FOURNIS PAR LES ASSOCIATIONS

Tout matériel fourni par une association doit garantir le respect des règles suivantes :

- mise en place d'une convention entre l'association donatrice ou mettant à disposition et l'administration pénitentiaire afin d'empêcher l'introduction de matériels prohibés en détention,
- mise en place de procédures de contrôle du matériel par l'administration pénitentiaire,
- dans le cas où ces matériels en seraient pourvus, démontage ou annihilation des matériels communicants intégrés par l'association ou sortie de ces matériels de l'établissement selon le choix des membres associatifs,
- pose de scellés (cf. §5.3),

4.6. MOTS DE PASSE DES EQUIPEMENTS INFORMATIQUES EN SALLE D'ACTIVITÉ

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

5. MESURES DE CONTRÔLE

5.1. RAPPEL DU CADRE LÉGAL

L'article D-449-1 du Code de Procédure Pénale – créé par le décret du 20 mars 2003 – confère à l'administration pénitentiaire une base légale concernant le contrôle des ordinateurs des détenus.

L'article D-449-1 du Code de Procédure Pénale permet aux personnels d'effectuer le contrôle des ordinateurs des détenus (contenant et contenu) sans risquer de contrevenir au principe de confidentialité des échanges avec l'avocat. En effet les détenus ne sont autorisés à conserver dans leur ordinateur que des documents liés à des activités socio-culturelles, d'enseignement, de formation professionnelle, à l'exclusion de tout autre document (notamment la correspondance avec leur avocat).

5.2. INVENTAIRE

L'inventaire complet des matériels informatiques à disposition des détenus est obligatoire et constitue un préalable à toute possibilité de gestion et de contrôle efficace. Cet inventaire doit être annexé au classeur de sécurité informatique.

Lors des fouilles, transferts ou réclamations, la fiche d'inventaire devient un moyen de preuve de l'appartenance d'un objet et du bien fondé de sa possession.

Dès lors, cet inventaire doit concerner tous les biens possédés par le détenu dans sa cellule, et plus particulièrement les biens informatiques. A cet égard, l'inventaire conservé au vestiaire du détenu doit être accompagné des pièces justificatives de propriété ou de garantie (logiciels, matériels).

La tenue d'une fiche d'inventaire, comprenant les références des matériels informatiques et des logiciels possédés par le détenu, doit permettre au chef d'établissement, notamment au moment de la libération ou du transfert d'un détenu, de s'assurer qu'il n'y a pas de trafic ou de matériel illicite.

5.3. SCCELLEMENT DES BOITIERS

Les dispositifs de plombage et scellement des matériels informatiques sont obligatoires pour tout ordinateur en cellule ou en salle d'activité.

Le détenu ne doit en aucun cas avoir accès à l'intérieur du boîtier de son ordinateur, de son écran et des autres périphériques. Le fonctionnement de l'ordinateur en cellule avec le boîtier de l'unité centrale ouvert est formellement proscrit.

L'ouverture, même occasionnelle, de l'unité centrale est interdite, exceptée dans le cadre d'une réparation ou d'une maintenance qui doit être réalisée en présence d'un personnel de l'administration pénitentiaire afin que soit constatée la régularité de l'opération.

La mesure consiste à faire apposer sur les boîtiers des unités centrales et sur les périphériques, par le personnel dédié à l'informatique :

- obligatoirement** : un scellement papier autocollant afin de détecter toute ouverture frauduleuse;

- **dans la mesure du possible** : un cadenas sécurisé afin d'interdire la possibilité d'ouverture;

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

5.4. FOUILLES PHYSIQUE ET LOGIQUE DES ORDINATEURS ET DES SUPPORTS D'INFORMATION

A l'arrivée du matériel un inventaire doit être réalisé, cet inventaire doit être mis à jour et le matériel doit être contrôlé régulièrement.

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

Après une fouille d'ordinateur, le personnel de l'administration pénitentiaire ayant effectué le contrôle demande au détenu de signer un procès verbal précisant la non détérioration du matériel informatique inspecté.

Si le détenu refuse de signer car il considère qu'il y a eu détérioration à l'issue du contrôle, il le signale dans le procès verbal en cochant la case appropriée du formulaire.

Le cas échéant, une retenue à titre conservatoire du matériel permet de faire réaliser un contrôle plus approfondi par un personnel tiers compétent. Le détenu portant réclamation à la suite de la détérioration de son matériel inspecté peut se voir indemnisé au titre du préjudice subi.

Des fouilles et contrôles sont également organisés dès que le matériel informatique est amené à quitter l'établissement pénitentiaire pour quelque raison que ce soit (réparation, transfert ou libération).

Les fouilles peuvent être réalisées en l'absence du détenu comme en dispose l'article D-269 du CPP.

En application de l'article 40 et de l'article D-281 du code de procédure pénale, le chef d'établissement doit signaler aux autorités judiciaires toute infraction découverte à l'occasion de ces fouilles et contrôles, en particulier les copies illégales d'œuvres protégées par la propriété intellectuelle (copie de logiciels, de fichiers musicaux, de films...).

Outre, ce signalement aux autorités judiciaires, il convient de noter qu'une procédure administrative est également prévue en la matière. Il peut être fait application des dispositions du code de procédure pénale en matière disciplinaire.

Le détenu peut par ailleurs potentiellement essayer de dissimuler des informations [*Fin de phrase occultée car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes*]

Ce comportement de la part du détenu impose la **confiscation systématique par l'instance de contrôle des fichiers rendus inaccessibles à l'administration pénitentiaire (support informatique ou unité centrale selon les cas).**

Cette confiscation ne peut avoir lieu qu'après constat que le détenu refuse de communiquer les éléments permettant d'accéder à un fichier [*mots occultés car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes*], ou s'il y a suspicion de camouflage d'informations, [*fin de phrase occultée car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes*]

La décision de confiscation d'un matériel informatique demeure du ressort du chef d'établissement.

L'administration pénitentiaire ne doit pas détruire les documents licites élaborés par le détenu, en respect de ses droits d'auteurs éventuels.

[*§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.*]

Rappel : Le chef d'établissement dispose de la possibilité de retirer une autorisation de détention d'un ordinateur préalablement accordée en cas d'usage manifestement abusif ou illégal. Ce retrait d'autorisation devra être motivé et notifié au détenu concerné après qu'ait été mise en oeuvre la procédure contradictoire, telle que prévue à l'article 24 de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

5.5. TRANSFÈREMENT

Le transport des matériels informatiques appartenant au détenu est effectué, dans la mesure du possible, par l'administration pénitentiaire, avec **ses moyens logistiques**, garantissant ainsi la maîtrise de l'acheminement du matériel informatique. Cette solution doit être privilégiée.

En cas d'impossibilité, notamment au regard de l'importance du paquetage du détenu, le transport des matériels est réalisé aux frais du détenu, conformément à l'article D-340 du Code de Procédure Pénale, par un transporteur privé. Le choix de ce transporteur incombe à l'administration pénitentiaire.

Il n'en reste pas moins que la fouille matérielle et logique de l'appareil doit être d'autant plus vigilante qu'une personne extérieure à l'administration pénitentiaire a pris en charge l'appareil pendant le temps de son transport d'un établissement à l'autre.

5.6. LIBÉRATION

La libération d'un détenu propriétaire d'un ordinateur en cellule fait l'objet de mesures permettant de contrôler qu'aucun fichier non accessible ou non autorisé n'est sorti.

Les personnels formés de l'établissement sont ainsi chargés :

- d'identifier avec le détenu les fichiers devant être sortis,
- de les contrôler et de les sauvegarder si leur contenu est jugé licite,
- de formater l'ordinateur avant sa sortie effective.

[§ occulté, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

5.7. SURVEILLANCE DES ACTIVITÉS

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

6. FORMATION ET INFORMATION DES PERSONNELS

6.1. CONTEXTE

Dans le cadre de la mise en place de la présente circulaire, un programme d'information et de formation des personnels amenés à intervenir en établissement a été élaboré :

- information et formation des personnels de l'administration pénitentiaire ;
- information et sensibilisation des intervenants « externes ».

La formation est placée sous l'égide de l'École Nationale d'Administration Pénitentiaire (ENAP) qui a en charge la formalisation, l'uniformisation et la mise à jour des supports, *en s'appuyant sur la veille technologique réalisée en amont.*

Le programme de formation du personnel pénitentiaire, abordant les risques et les mesures sécuritaires liés à l'Informatique mis à disposition des détenus, se décline en trois modules distincts en fonction des publics identifiés suivants :

- les personnels dédiés à l'informatique aux échelons locaux et régionaux ;
- les personnels de surveillance et de direction ;
- les personnels d'insertion et de probation ;
- les personnels techniques.

Ces formations sont obligatoires dans le cadre du cursus de formation initial des personnels pénitentiaires. Elles s'inscrivent dans le programme de formation à l'informatique.

La mise en œuvre d'un processus de **formation continue** ou d'information régulière est recommandée aux échelons régionaux et locaux, par exemple par la diffusion de brochures d'information et de sensibilisation et de messages de sensibilisation diffusés lors de réunions internes.

Par ailleurs, les enseignants devront recevoir une formation lors de leur cursus au sein de l'ENAP. Cette formation devra leur permettre :

- de connaître les risques encourus en cas d'usage inapproprié de l'informatique par les détenus ;
- de connaître le cadre légal et réglementaire concernant l'informatique en détention ;
- de connaître, de comprendre et de savoir appliquer l'ensemble des procédures de sécurité leur incombant.

Enfin, la formation des intervenants externes doit être réalisée aux échelons locaux et régionaux en rappelant les risques (*cf. § 1.4*) et en expliquant les droits et obligations des intervenants.

6.2. MODULE POUR LES ÉQUIPES INFORMATIQUES RÉGIONALES ET LOCALES

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

6.3. MODULE PERSONNELS DE SURVEILLANCE, TECHNIQUE ET DE DIRECTION

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

6.4. MODULE PERSONNELS D'INSERTION ET DE PROBATION

[§§ occultés, car non communicables au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

Pour le garde des Sceaux, ministre de la Justice,
et par délégation :
Le Directeur de l'administration pénitentiaire

Claude d'HARCOURT

ANNEXES

ANNEXE 1 Liste des technologies autorisées et interdites en cellule

CONFIGURATIONS STANDARDS

Ordinateur de bureau non communicant	Autorisé
Console de jeux non communicante	Autorisé
Ordinateur portable	Interdit
Console de jeux communicante	Interdit
Ordinateur de poche (Pocket PC)	Interdit
Assistant personnel numérique (PDA)	Interdit
Ordinateur « tablette » (Tablet PC)	Interdit

EXTENSIONS STANDARDS / LECTEURS / GRAVEURS

Mémoire vive	Autorisé
Carte vidéo	Autorisé
Carte SCSI	Autorisé
Lecteur de disquette format standard (1,44 Mo)	Autorisé
Lecteur de DVD	Autorisé
Lecteur de CD	Autorisé
Lecteur de disquette à forte capacité	Interdit
Graveur de CD	Interdit
Graveurs de DVD	Interdit
Lecteur de carte multimédia	Interdit
Lecteur de carte à puce	Interdit
Lecteur de bande magnétique de sauvegarde	Interdit

PERIPHERIQUES DE CONTROLE

Clavier et souris	Autorisé
Manette de jeux	Autorisé
Clavier et souris sans fil	Interdit
Manette de jeux sans fil	Interdit
Tablette graphique	Interdit

PERIPHERIQUES D'EDITION ET DE NUMERISATION

Imprimante jet d'encre	Autorisé
Imprimante laser	Interdit
Cartouche d'encre / toner	Interdit
Scanner et photocopieur	Interdit
Fax	Interdit
WebCam	Interdit
Appareil photo numérique	Interdit

PERIPHERIQUES MULTIMEDIAS ET D'ACQUISITION

Cartes son	Autorisé
Enceintes	Autorisé
Casque audio	Autorisé
Amplificateur sonore	Interdit
Carte tuner télévision	Interdit
Carte d'acquisition vidéo	Interdit

SUPPORT D'INFORMATIONS

Support d'informations optique

CD / DVD pressé (pédagogique / culturel)	Autorisé
CD-ROM vierge	Interdit
DVD vierge	Interdit
Mini CD vierge	Interdit
Mini DVD vierge	Interdit

Support d'informations magnétique

Disquette format standard (1,44 Mo)	Autorisé
Disquette à forte capacité	Interdit
Bande magnétique de sauvegarde	Interdit

Unité de stockage amovible

Clé USB	Interdit
Baladeur MP3	Interdit
Support de stockage sur port FireWire (IEEE 1394)	Interdit
Disque dur externe ou sur rack amovible	Interdit
Carte mémoire multimédia miniaturisée	Interdit
Autre support de stockage	Interdit

PERIPHERIQUES ET TECHNOLOGIES DE COMMUNICATION

Liaison par réseau filaire

Modem ADSL	Interdit
Modem RTC	Interdit
Modem RNIS (ISDN / Numéris)	Interdit
Modem fax	Interdit
Carte réseau Ethernet	Interdit
CPE LAN (courant porteur électrique)	Interdit
Autre technologie	Interdit

Liaison sans fil (hertzienne / radio ou optique)

WiFi	Interdit
Bluetooth	Interdit
Infrarouge (IrDA)	Interdit
Autre technologie	Interdit

Liaison téléphonie mobile

GSM	Interdit
WAP	Interdit
GPRS	Interdit
i-Mode	Interdit
UMTS	Interdit
Autre technologie	Interdit

LOGICIELS

Systemes d'exploitation	Autorisé
Bureautique	Autorisé
Developpement	Autorisé
Tout outil de graphisme livré « en standard » avec le système d'exploitation Windows.	Autorisé
Conception assistée par ordinateur (CAO)	Autorisé
Creation multimedia / audiovisuelle	Autorisé
Steganographie	Interdit
Chiffrement	Interdit
Numérisation	Interdit
Graphisme / retouche	Interdit
Publication assistée par ordinateur (PAO)	Interdit
Dessin assisté par ordinateur (DAO)	Interdit

RESEAU

Concentrateur (hub)	Interdit
Commutateur (switch)	Interdit
Routeur	Interdit

DIVERS

Parasurtenseur	Autorisé
Livre électronique	Autorisé
Onduleur	Interdit

ANNEXE 2 : Liste des technologies autorisées et interdites en salle d'activités encadrées

[Annexe 2 occultée, car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]

ANNEXE 3 : convention sur l'accès et l'utilisation des ressources informatiques par les détenus en salle d'activité*[Annexe 3 occultée, car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]*

ANNEXE 4 : références juridiques

Publication au JORF du 23 juin 1987

LOI n°87-432 du 22 juin 1987

LOI relative au service public pénitentiaire

NOR : JUSX8700042L

Article 1

Le service public pénitentiaire participe à l'exécution des décisions et sentences pénales et au maintien de la sécurité publique. Il favorise la réinsertion sociale des personnes qui lui sont confiées par l'autorité judiciaire. Il est organisé de manière à assurer l'individualisation des peines.

CODE DE LA PROPRIETE INTELLECTUELLE (Partie Législative)

Article L122-4

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque.

Article L335-3

(Loi n° 94-361 du 10 mai 1994 art. 8 Journal Officiel du 11 mai 1994)

(Loi n° 98-536 du 1 juillet 1998 art. 4 Journal Officiel du 2 juillet 1998)

Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.

Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6.

Article L335-4

(Loi n° 94-102 du 5 février 1994 art. 2 Journal Officiel du 8 février 1994)

(Loi n° 98-536 du 1 juillet 1998 art. 4 Journal Officiel du 2 juillet 1998)

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi n° 2003-517 du 18 juin 2003 art. 1 Journal Officiel du 19 juin 2003 en vigueur le 1er août 2003)

(Loi n° 2004-204 du 9 mars 2004 art. 34 II Journal Officiel du 10 mars 2004)

Est punie de trois ans d'emprisonnement et de 300 000 € d'amende toute fixation, reproduction, communication ou mise à disposition du public, à titre onéreux ou gratuit, ou toute télédiffusion d'une prestation, d'un phonogramme, d'un vidéogramme ou d'un programme, réalisée sans l'autorisation, lorsqu'elle est exigée, de l'artiste – interprète, du producteur de phonogrammes ou de vidéogrammes ou de l'entreprise de communication audiovisuelle.

Est punie des mêmes peines toute importation ou exportation de phonogrammes ou de vidéogrammes réalisée sans l'autorisation du producteur ou de l'artiste - interprète, lorsqu'elle est exigée.

Est puni de la peine d'amende prévue au premier alinéa le défaut de versement de la rémunération due à l'auteur, à l'artiste - interprète ou au producteur de phonogrammes ou de vidéogrammes au titre de la copie privée ou de la communication publique ainsi que de la télédiffusion des phonogrammes.

Est puni de la peine d'amende prévue au premier alinéa le défaut de versement du prélèvement mentionné au troisième alinéa de l'article L. 133-3.

Lorsque les délits prévus au présent article ont été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 € d'amende.

CODE DE PROCEDURE PENALE (Partie Législative)

Article 40

*(Loi n° 85-1407 du 30 décembre 1985 art. 1 et 94 Journal Officiel du 31 décembre 1985 en vigueur le 1er février 1986)
(Loi n° 98-468 du 17 juin 1998 art. 27 Journal Officiel du 18 juin 1998)
(Loi n° 2004-204 du 9 mars 2004 art. 74 Journal Officiel du 10 mars 2004)*

Le procureur de la République reçoit les plaintes et les dénonciations et apprécie la suite à leur donner conformément aux dispositions de l'article 40-1.

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.

CODE DE PROCEDURE PENALE (Partie Réglementaire - Décrets simples)

Article D66

(Décret n° 73-281 du 7 mars 1973 art. 1 Journal Officiel du 16 mars 1973 rectificatif JORF 7 avril 1973)

Il est interdit au personnel de l'administration pénitentiaire et à toute personne qui apporte sa collaboration à cette administration d'agir de façon directe ou indirecte auprès des détenus pour influencer sur leurs moyens de défense et sur le choix de leur défenseur.

Pour l'exercice de ce choix, le tableau des avocats inscrits dans les barreaux du département est affiché au greffe et tenu à la disposition des détenus.

Article D67

(Décret n° 98-1099 du 8 décembre 1998 art. 147 Journal Officiel du 9 décembre 1998)

Conformément aux dispositions des articles 145-4 et 716, les prévenus peuvent communiquer librement avec leur conseil verbalement ou par écrit, et toutes facilités compatibles avec les exigences de la discipline et de la sécurité de l'établissement pénitentiaire leur sont accordées pour l'exercice de leur défense. Ni l'interdiction de communiquer visée à l'article 145-4, ni les punitions de quelque nature qu'elles soient, ne peuvent supprimer ou restreindre cette faculté de libre communication avec le conseil.

Article D68

Le défenseur régulièrement choisi ou désigné, agissant dans l'exercice de ses fonctions, et sur présentation d'un permis portant mention de sa qualité, communique librement avec les prévenus, en dehors de la présence d'un surveillant, et dans un parloir spécial.

A moins de dérogations motivées par l'urgence, les visites du conseil peuvent avoir lieu tous les jours, aux heures fixées par le règlement intérieur de l'établissement après avis du bâtonnier de l'ordre des avocats.

Article D69

Les lettres adressées sous pli fermé par les prévenus à leur défenseur, ainsi que celles que leur envoie ce dernier, ne sont pas soumises au contrôle visé à l'article D416, s'il peut être constaté sans équivoque qu'elles sont réellement destinées au défenseur ou proviennent de lui.

A cet effet, les mentions utiles doivent être portées sur leur enveloppe pour indiquer la qualité et l'adresse professionnelle de leur destinataire ou de leur expéditeur.

Article D249-2

*(Décret n° 96-287 du 2 avril 1996 art. 1 et 2 Journal Officiel du 5 avril 1996)
(Décret n° 98-1099 du 8 décembre 1998 art. 187 et 190 Journal Officiel du 9 décembre 1998)*

Constitue une faute disciplinaire du deuxième degré le fait, pour un détenu :

1. De proférer des insultes ou des menaces à l'égard d'un membre du personnel de l'établissement ou d'une personne en mission ou en visite au sein de l'établissement pénitentiaire ;
2. De participer à des actions collectives de nature à perturber l'ordre de l'établissement, hors le cas prévu au 2 de l'article D. 249-1 ;
3. De commettre ou tenter de commettre des vols ou toute autre atteinte frauduleuse à la propriété

- d'autrui ;
4. De causer délibérément un dommage aux locaux ou au matériel affecté à l'établissement, hors le cas prévu au 7 de l'article D. 249-1 ;
 5. D'imposer à la vue d'autrui des actes obscènes ou susceptibles d'offenser la pudeur ;
 6. De refuser de se soumettre à une mesure de sécurité définie par les règlements et instructions de service
 7. De se soustraire à une sanction disciplinaire prononcée à son encontre ;
 8. De se livrer à des trafics, des échanges non autorisés par les règlements ou tractations avec des codétenus ou des personnes extérieures ;
 9. De détenir des objets ou substances non autorisés par les règlements ou de se livrer à leur trafic, hors le cas prévu au 3 de l'article D. 249-1 ;
 10. De se trouver en état d'ébriété ou d'absorber sans autorisation médicale des substances de nature à troubler son comportement ;
 11. De provoquer un tapage de nature à troubler l'ordre de l'établissement ;
 12. De mettre en danger la sécurité d'autrui par une imprudence ou une négligence ;
 13. De tenter d'obtenir d'un membre du personnel de l'établissement ou d'une personne en mission au sein de l'établissement un avantage quelconque par des offres, des promesses, des dons ou des présents
 14. D'inciter un codétenu à commettre l'un des manquements énumérés au présent article.

Article D249-3

(Décret n° 96-287 du 2 avril 1996 art. 1 et 2 Journal Officiel du 5 avril 1996)

(Décret n° 98-1099 du 8 décembre 1998 art. 187 et 190 Journal Officiel du 9 décembre 1998)

Constitue une faute disciplinaire du troisième degré le fait, pour un détenu :

1. De formuler des outrages ou des menaces dans les lettres adressées aux autorités administratives et judiciaires ;
2. De formuler dans les lettres adressées à des tiers, des menaces, des injures ou des propos outrageants à l'encontre de toute personne ayant mission dans l'établissement ou à l'encontre des autorités administratives et judiciaires, ou de formuler dans ces lettres des menaces contre la sécurité des personnes ou de l'établissement ;
3. De proférer des insultes ou des menaces à l'encontre d'un codétenu ;
4. De refuser d'obtempérer aux injonctions des membres du personnel de l'établissement ;
5. De ne pas respecter les dispositions du règlement intérieur de l'établissement ou les instructions particulières arrêtées par le chef de l'établissement ;
6. De négliger de préserver ou d'entretenir la propreté de sa cellule ou des locaux communs ;
7. D'entraver ou de tenter d'entraver les activités de travail, de formation, culturelles ou de loisirs ;
8. De jeter des débris ou tout autre objet par les fenêtres de l'établissement ;
9. De communiquer irrégulièrement avec un codétenu ou avec toute autre personne extérieure à l'établissement ;
10. De faire un usage abusif ou nuisible d'objets autorisés par le règlement intérieur ;
11. De pratiquer des jeux non autorisés par le règlement intérieur ;
12. De multiplier, auprès des autorités administratives et judiciaires, des réclamations injustifiées ayant déjà fait l'objet d'une décision de rejet ;
13. D'inciter un codétenu à commettre l'un des manquements énumérés au présent article.

Article D251-1

(Décret n° 75-402 du 23 mai 1975 art. 1 Journal Officiel du 27 mai 1975)

(Décret n° 96-287 du 2 avril 1996 art. 1 et 2 Journal Officiel du 5 avril 1996)

(Décret n° 98-1099 du 8 décembre 1998 art. 187 et 190 Journal Officiel du 9 décembre 1998)

Peuvent être prononcées, en fonction des circonstances de la faute disciplinaire, les sanctions disciplinaires suivantes :

1. La mise à pied d'un emploi pour une durée maximum de huit jours lorsque la faute disciplinaire a été commise au cours ou à l'occasion du travail ;
2. Le déclassement d'un emploi ou d'une formation, lorsque la faute disciplinaire a été commise au cours ou à l'occasion de l'activité considérée ;
3. La privation pendant une durée maximum d'un mois de tout appareil acheté ou loué par l'intermédiaire de l'administration lorsque la faute disciplinaire a été commise à l'occasion de l'utilisation de ce matériel ou lorsque la sanction accompagne une décision de confinement en cellule individuelle ordinaire ;
4. La suppression de l'accès au parloir sans dispositif de séparation pour une période maximum de quatre

- mois lorsque la faute a été commise au cours ou à l'occasion d'une visite ;
5. L'exécution d'un travail de nettoyage des locaux pour une durée globale n'excédant pas quarante heures lorsque la faute disciplinaire est en relation avec un manquement aux règles de l'hygiène ;
 6. La privation d'activités de formation, culturelles, sportives et de loisirs pour une période maximum d'un mois lorsque la faute disciplinaire a été commise au cours de ces activités ;
 7. L'exécution de travaux de réparation lorsque la faute disciplinaire est en relation avec la commission de dommages ou de dégradations.
- La mise à pied et le déclassement d'un emploi prévus aux 1 et 2 ainsi que la privation d'activités de formation ne sont pas applicables aux mineurs de seize ans.
- Les sanctions prévues aux 5 et 7 ne peuvent être prononcées que pour se substituer aux sanctions prévues aux 4 et 5 de l'article D. 251. Le consentement du détenu doit alors être préalablement recueilli.

Article D269

(Décret n° 98-1099 du 8 décembre 1998 art. 54 et 190 Journal Officiel du 9 décembre 1998)

Les surveillants procèdent, en l'absence des détenus, à l'inspection fréquente et minutieuse des cellules et locaux divers où les détenus séjournent, travaillent ou ont accès. Les systèmes de fermetures sont périodiquement vérifiés et les barreaux contrôlés quotidiennement.

Article D281

(Décret n° 98-1099 du 8 décembre 1998 art. 190 Journal Officiel du 9 décembre 1998)

Le chef de l'établissement dans lequel a été commis un crime ou un délit doit dresser rapport des faits et en aviser directement et sans délai le procureur de la République, conformément aux dispositions de l'article 40.

Article D340

(Décret n° 98-1099 du 8 décembre 1998 art. 85 Journal Officiel du 9 décembre 1998)

Au moment de la libération, les bijoux, valeurs, vêtements et effets personnels sont remis au détenu qui en donne décharge. Si l'intéressé refuse de les recevoir, il en est fait remise à l'administration des domaines. Lorsque le détenu est transféré, les objets lui appartenant sont déposés contre reçu entre les mains de l'agent de transfèrement s'ils ne sont pas trop lourds ou volumineux ; sinon, ils sont expédiés à la nouvelle destination du détenu aux frais de ce dernier ou sont remis à un tiers désigné par lui, après accord du chef d'établissement.

Article D444

*(Décret n° 75-402 du 23 mai 1975 art. 1 Journal Officiel du 27 mai 1975)
(Décret n° 77-1294 du 25 novembre 1977 Journal Officiel du 27 novembre 1977)
(Décret n° 98-1099 du 8 décembre 1998 art. 119 et 120 Journal Officiel du 9 décembre 1998)*

Les détenus peuvent se procurer par l'intermédiaire de l'administration les journaux, les périodiques et les livres français et étrangers de leur choix n'ayant pas fait l'objet d'une saisie dans les trois derniers mois. Toutefois, les publications contenant des menaces précises contre la sécurité des personnes ou celle des établissements pénitentiaires peuvent être, à la demande des chefs d'établissement, retenues sur décision du ministre de la justice.

Les détenus peuvent se procurer par l'intermédiaire de l'administration et selon les modalités qu'elle détermine un récepteur radiophonique et un téléviseur individuels.

Le règlement intérieur détermine les caractéristiques auxquelles doivent répondre ces appareils, ainsi que les conditions de leur utilisation.

Les échanges et les prêts de livres personnels entre détenus sont autorisés

Article D449-1

(inséré par Décret n° 2003-259 du 20 mars 2003 art. 19 Journal Officiel du 22 mars 2003)

Les détenus peuvent acquérir par l'intermédiaire de l'administration et selon les modalités qu'elle détermine des équipements informatiques.

Une instruction générale détermine les caractéristiques auxquelles doivent répondre ces équipements, ainsi que les conditions de leur utilisation. En aucun cas, les détenus ne sont autorisés à conserver des documents, autres que ceux liés à des activités socioculturelles ou d'enseignement ou de formation ou professionnelles, sur un support informatique.

Ces équipements ainsi que les données qu'ils contiennent sont soumis au contrôle de l'administration. Sans préjudice d'une éventuelle saisie par l'autorité judiciaire, tout équipement informatique appartenant à un détenu peut, au surplus, être retenu, pour ne lui être restitué qu'au moment de sa libération, dans les cas suivants :

1. Pour des raisons d'ordre et de sécurité ;
2. En cas d'impossibilité d'accéder aux données informatiques, du fait volontaire du détenu.

ANNEXE 5 : Convention cadre fournisseur

[Annexe 5 occultée, car non communicable au titre de l'article 6 de la loi du 17 juillet 1978 : informations dont la communication serait susceptible de mettre en cause la sécurité publique ou des personnes.]