Accès à l'informatique
Administration pénitentiaire
Détenu
Personne placée sous main de justice (PPSM)
Règlement intérieur

Circulaire de la DAP en date du 13 octobre 2009 relative à l'accès à l'informatique pour les personnes placées sous main de justice

NOR : *JUSK0940021C*

Texte modifié : circulaire relative à l'accès à l'informatique pour les personnes placées sous main de justice du 9 avril 2009 NOR : JUSK094006C.

Le ministre d'Etat, garde des sceaux, ministre de la justice et des libertés à Messieurs les directeurs interrégionaux des services pénitentiaires (pour attribution) ; Madame la directrice de l'Ecole nationale de l'administration pénitentiaire (pour information).

1. Introduction. – Accès des détenus à 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.

L'administration pénitentiaire souhaite accompagner cette évolution.

L'article 1er 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 autres que les 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 ont la possibilité par ce support d'acquérir un accès aux 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 possibles 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.

[§§ 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.]

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'établissements pénitentiaires.

1.2. *Objet de la présente circulaire*

Le terme « informatique » s'applique, dans la présente circulaire, à tout composant matériel ou logiciel permettant de recueillir et stocker, de traiter ou de diffuser des informations. Il s'applique ainsi principalement aux unités de traitement et aux unités de stockage d'information dont, notamment, les postes de travail, les consoles de jeux, les Pocket PC et PDA, les disquettes et les Cédérom/Dévédérom. Les appareils électroniques non informatiques ne sont pas concernés par cette circulaire. Néanmoins, tout matériel disposant de port de communication (USB, Firewire...) devra être soumis aux mêmes règles que les équipements mentionnés ci-dessus (inhibition des ports de communication permettant d'exporter ou d'enregistrer de l'information...).

La présente circulaire a pour but de réglementer 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. Cette circulaire s'applique à tous les établissements pénitentiaires.

En matière informatique, il convient de distinguer quatre niveaux d'utilisation :

– par les personnes détenues en cellule. A cet égard, le rôle du chef d'établissement dans l'examen des demandes de détenus en vue de la détention d'ordinateur en cellule est essentiel et repose notamment sur le profil de la personne. Quant aux prescriptions strictes sur le matériel autorisé ou interdit, les services locaux et régionaux informatique, seront obligatoirement consultés ;

– par les personnes détenues en salle d'activités : locaux dans lesquels se trouvent des équipements informatiques en libre accès aux détenus, pour lesquels s'appliquent les dispositions concernant l'usage de l'informatique en cellule ;

– 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 concernées. Les activités encadrées doivent bénéficier d'un encadrement physique permanent ;

– par les personnes détenues en salle d'audience : la présente circulaire définit également les mesures qui doivent être mises en place pour que les détenus aient la possibilité d'accéder à leur dossier pénal dématérialisé.

La présente circulaire ne concerne donc pas les ordinateurs placés de la DAP ou des partenaires en détention qui ne sont pas accessibles aux détenus (par exemple GIDE, les réseaux de la RIEP ou des opérateurs privés) et qui sont traités par d'autres dispositions.

[§§ 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.]

Il est rappelé que seul le chef d'établissement, usant de son pouvoir d'appréciation, peut autoriser ou non l'introduction d'ordinateurs dans son établissement.

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, D. 95, D. 440 à D. 449, D. 450 à D. 459, et D. 573 du code de procédure pénale ;

– 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 D. 449-1 (décret 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.

La liste des matériels autorisés et interdits en annexe 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 une personne placée sous main de justice peut, au surplus, être retenu, pour lui être restitué qu'au moment de sa libération, dans les cas suivants :

– pour des raisons liées à la sécurité pénitentiaire et à la sécurité publique ;

– en cas de refus de présentation des données informatiques présentes sur son ordinateur.

1.4. *Risques*

[§§ 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.]

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 :

– la mise en œuvre de ces outils informatiques ne doit en aucun cas mettre en péril la sécurité pénitentiaire ;

– les règles présentées dans la présente circulaire doivent être rigoureusement respectées ;

[§§ 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.]

– toutes les technologies qui ne sont pas explicitement autorisées sont interdites. Cette règle doit également être appliquée pour les nouvelles technologies dans l'attente d'une révision de la liste des matériels autorisés et interdits par un groupe de travail piloté par le RSSI ;
– l'utilisation des ordinateurs par les détenus doit pouvoir être contrôlée à tout moment.

1.6. *Mise en œuvre et suivi*

Ainsi que cela a été rappelé en 1.1, l'utilisation de l'informatique par les détenus est de nature à faciliter leur formation et leur réinsertion. La nécessaire prise en compte des règles de sécurité applicables en la matière devra se concilier avec cet impératif.

[§§ 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 cadre 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 tel que prévue par l'article D. 249-3 10° peut justifier des sanctions disciplinaires, sans préjudice de poursuites pénales éventuelles. La sanction consistant à priver le détenu de son appareil, tel que prévu par l'article D. 251-1, 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 aux personnes placées sous main de justice. Pour ce faire, la présente circulaire dans sa version communicable pourra être jointe au règlement intérieur.

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 informatiques joints aux revues (CD, disquettes, clés USB) 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 en dehors des circuits de distribution gérés par l'administration pénitentiaire est prohibée, comme est prohibé l'envoi suivant le même mode d'objets informatiques, conformément aux articles D. 444 et D. 423 du code de procédure pénale.

L'article D. 444, alinéa 2, du code de procédure pénale prévoit que les publications contenant des menaces précises contre la sécurité des personnes ou celles des établissements pénitentiaires (exemple : revues sur le piratage informatique) 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.

2.3. *Echange de supports d'informations amovibles*

2.3.1. Echange interne

La personne détenue ne peut transporter que des supports amovibles informatiques nécessaires à l'activité et marqués par l'administration pénitentiaire ou par le responsable de l'activité (bibliothèque) ayant prêté le support entre la salle d'activité et sa cellule et vice-versa.

Elle ne peut réaliser aucune copie illicite de programme ou logiciel.

Elle ne peut pas utiliser le matériel mis à sa disposition à d'autres fins que celles définies au paragraphe 1.1.

L'échange de supports informatiques non modifiables (Cédérom et Dévédérom provenant d'éditeurs) est autorisé entre détenus dès l'instant où cet échange ne se fait pas au mépris des droits relatifs à la propriété littéraire et artistique des auteurs.

2.3.2. Echange avec l'extérieur

L'échange ou la communication par un détenu de tout support informatique avec l'extérieur est strictement interdit.

La remise de matériel informatique est prohibée aux parloirs. Seule les supports optiques (CD, DVD) audio et vidéo provenant d'éditeurs peuvent être remis aux personnes détenue après un contrôle par l'administration pénitentiaire.

Seules sont autorisées les entrées 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 être marqués et doivent pouvoir être contrôlés à tout moment par les personnels pénitentiaires.

Outre l'interdiction d'accès à internet en cellule, il est rappelé que les accès aux systèmes suivants sont interdits en cellule :

– aux systèmes d'information pénitentiaires ;
– aux systèmes d'information d'autres administrations ou de partenaires (réseaux de télémédecine, systèmes d'information des groupements privés ou de la RIEP) ;
– à des réseaux externes (réseaux de l'éducation nationale ou de facultés) ;
– de façon générale à tout dispositif de communication direct interne ou externe à l'établissement.

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.

La validation ou le refus d'une demande d'autorisation par le chef d'établissement s'appuie principalement sur deux critères :

– le profil du demandeur ;

[§§ 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.]

– les risques techniques encourus et les contraintes matérielles :

Le chef d'établissement tiendra notamment compte des caractéristiques du matériel informatique demandé au vu des installations électriques de l'établissement et de son éventuelle saturation et au vu du risque d'encombrement de la cellule du demandeur ;

[§§ 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.]

Ce processus d'autorisation s'applique tant lors de l'achat initial que du transfert d'un détenu déjà équipé d'un ordinateur.

L'autorisation d'achat ne doit porter que sur des matériels neufs. 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, le prêt 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 (dans le cadre de sa fonction de garde et de contrôle de la population pénale).

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'a été mise en œuvre 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 agréés

Afin de garantir l'homogénéité du parc informatique, d'offrir les meilleurs conditions d'achat et surtout l'application des règles de sécurité en la matière, il peut-être établi une ou plusieurs conventions (*cf.* annexe 4) qui lie les établissements pénitentiaires avec des fournisseurs de matériels informatiques locaux, régionaux ou nationaux en vente directe ou par correspondance, laquelle précise les modalités d'acquisition de ces matériels informatiques par les détenus.

Les conventions peuvent être établies sur initiative des établissements pénitentiaires et doivent être validées par les directions interrégionales.

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 ;

– 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 composantes 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. Garantie, réparation, 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'intervention de l'établissement dans l'acte d'achat, ni les spécificités de la vie en détention ne peuvent altérer ou annuler ces garanties. Ces dispositions doivent être clairement acceptées par le fournisseur avant son agrément.

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 incorporée à la fiche d'inventaire du matériel 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 interrégionales, 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. Les maintenances sur site sont préférables aux maintenances extérieures. Elles doivent néanmoins être organisées de sorte que l'anonymat des fournisseurs ne soit pas remis en cause.

Les services de l'administration pénitentiaires ne sont pas juridiquement habilités à modifier les caractéristiques techniques des matériels acquis par les détenus.

Avant de remettre l'ordinateur au détenu, un personnel de l'administration pénitentiaire devra contrôler l'ordinateur et devra ensuite replacer les scellés de sécurité manquants sur l'ordinateur du détenu.

3.2. *Unicité des matériels*

Le détenu qui demande le remplacement d'un matériel obsolète doit en accepter le dépôt à son vestiaire. Il peut aussi éventuellement en faire don à une association d'insertion de l'établissement avec l'accord préalable et écrit du chef d'établissement. Le matériel concerné sera dans ce cas préalablement contrôlé et devra subir une surcharge de sécurité (effacement sécurisé).

Un matériel dont l'achat date de moins de six mois n'est pas considéré comme un matériel obsolète et ne peut donc être remplacé.

[§§ 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.]

Cela impose notamment :

– un unique ordinateur par détenu ;

– un unique type de périphérique par catégorie et par ordinateur.

Le principe dit de l'échange « un contre un » est systématiquement appliqué.

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 et qu'il soit ou non raccordé à l'ordinateur. En revanche, afin de pouvoir sauvegarder ses informations, le détenu a la possibilité de posséder un second disque dur interne. La capacité totale des deux disques durs ne doit pas dépasser 500 Go.

3.3. *Technologies autorisées/interdites*

A l'exception du lecteur de disquette, toutes les technologies permettant d'enregistrer ou d'envoyer des informations numériques vers l'extérieur de l'ordinateur sont interdites. Ces technologies sont notamment :

– les technologies de communication filaires comme les cartes réseaux ethernet, les cartes modem, les cartes de sortie de flux numérique (IEEE1394), les cartes équipées de la technologie « CPL » ou encore les cartes équipées de la technologie USB ;

– les technologies de communication sans fil telles que les technologies « GSM », « GPRS », « Bluetooth », « Wifi » « Wimax » ou encore la technologie infrarouge ;

– les technologies d'enregistrement sur support amovible telles que les lecteurs de cartes mémoires, les graveurs de Cédérom et de Dévédérom.

Les supports amovibles, à savoir les Cédérom et Dévédérom provenant d'un fournisseur de matériel ou les disquettes, sont autorisés en cellule à condition que ceux-ci soient marqués par l'administration pénitentiaire.

Le chef d'établissement dispose de la possibilité de retirer une autorisation de possession d'un ordinateur préalablement accordée en cas de dégradation ou de retrait d'un scellé de sécurité. 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 (art. D. 251-1 [3°] du code de procédure pénale). Ce retrait d'autorisation devra être motivé et notifié au détenu concerné après qu'a été mise en œuvre 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.

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.

[§§ 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.]

Le tableau présenté en annexe I détaille les technologies autorisées et interdites dans le cadre de l'informatique en cellule. La personne détenue est informée des technologies autorisées et interdites avant de procéder à l'achat de son matériel.

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

PRINCIPALES TECHNOLOGIES AUTORISÉES	PRINCIPALES TECHNOLOGIES INTERDITES
Ordinateur compatible PC non portable et non communicant et consoles de jeux non communicantes	Ordinateur portables ou « de poche », ordinateurs communicants, consoles communicantes, assistants personnels
Lecteur de CD ou de DVD	Graveurs de CD ou de DVD
Lecteur de disquettes standard	Lecteur de disquettes « haute densité »
Souris et manette de jeux avec fil	Périphérique de technologie « sans fil »
Disquette CD DVD informatique de travail fournis et marqués par l'administration pénitentiaire ou un représentant ou CD et DVD provenant d'éditeurs	Tout autre support vierge (CD, DVD, clé USB, baladeur MP3, cartes mémoires…)
Imprimantes jet d'encre	Imprimantes laser, scanners, télécopieurs, photocopieurs, Webcam, matériel de photonumérique
	Tout périphérique et technologie de communication (Firewire, Ethernet.)
Systèmes d'exploitation, outils bureautiques et de développement, logiciels de conception assistée par ordinateurs (CAO), antivirus Tout outil de graphisme livré « en standard » avec le système d'exploitation Windows	Logiciels de chiffrement Logiciels de surcharge de sécurité Logiciels de numérisation Logiciels de graphisme Logiciels professionnels de publication assisté par ordinateur (PAO) et de dessin assisté par ordinateur (DAO) Logiciels utilisant des machines virtuelles et machines virtuelles (exemple : VMware) Logiciels utilisant des images de disques et images de disques (exemple : Ghost) Système d'exploitation pouvant être démarré sur un support externe à l'ordinateur.

3.4. *Mise en œuvre des scellés de sécurité*

La mise en place des scellés de sécurité sur les matériels informatiques sont obligatoires pour tout ordinateur en cellule.

Le détenu ne doit en aucun cas avoir accès à l'intérieur des boîtiers des ordinateurs et des autres équipements informatiques ou multimédia (imprimantes, consoles de jeux, chaîne hi-fi...). Ainsi, un ou plusieurs scellés devront être mis en place sur les unités centrales des ordinateurs et les équipements accessibles par les détenus, un ou plusieurs scellés devront également être placés sur les écrans des ordinateurs en cellule. 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 par un fournisseur agréé ou dans le cadre d'un contrôle physique ou logique. Lors d'une réparation ou d'une maintenance, l'ordinateur devra être contrôlé par un personnel de l'administration pénitentiaire afin que soit constatée la régularité de l'opération et que soient remplacés les scellés de sécurité qui auront été enlevés.

Les technologies filaires interdites par la présente circulaire mais intégrées en standard à la carte mère peuvent être autorisées en cellule uniquement après avoir été inhibées, via la mise en place de scellés de sécurité. De même, tous les périphériques autorisés par la présente circulaire peuvent être connectés à l'ordinateur du détenu via la technologie USB uniquement si un scellé de sécurité est placé à chaque extrémité du câble utilisé pour la connexion.

[§§ 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.]

Un inventaire des scellés de sécurité doit être mis en œuvre dans les établissements pénitentiaires. Cet inventaire comportera pour chaque nouveau scellé, le nom du propriétaire de l'ordinateur sur lequel le scellé a été placé, l'objet du nouveau scellé (attribution du matériel, ouverture de l'ordinateur, fouille informatique générale...), la date de pose du scellé et la personne de l'administration pénitentiaire ayant effectué la pose. Cet inventaire doit permettre, lors des fouilles, de vérifier le nombre de scellés mis en place sur l'ordinateur d'un détenu.

3.5. *Utilisation et comportement*

[§§ 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.]

3.6. *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 (art. D. 251-1 [3°] du code de procédure pénale).

Une mention doit en être faite au règlement intérieur.

4. **Informatique en salle d'activité**

4.1. *Utilisation du matériel*

On désigne par le terme « salle d'activité » tout local hébergeant une ou plusieurs des activités suivantes :

– services généraux assurés par des détenus ;
– bibliothèques ;
– salles de formation ;
– ateliers de travail ;
– salles d'activités socioculturelles ;
– salles d'activités audiovisuelles.

On distinguera les salles d'activités encadrées (par des enseignants, des intervenants d'associations, des personnels techniques de l'AP, des intervenants d'entreprise) pour lesquelles s'appliquent les dispositions décrites ci-dessous et pour lesquelles un encadrement physique permanent doit être prévu, des locaux dans lesquels se trouvent des équipements informatiques en libre accès aux détenus, pour lesquels s'appliquent les dispositions concernant l'usage de l'informatique en cellule.

Les activités de formation et de travail peuvent principalement concerner :

– les activités de numérisation/graphisme/retouche/dessin assisté par ordinateur (DAO)/créations multimédia ou audiovisuelle/création ou publication assistée par ordinateur (CAO/PAO) ;

– les activités sur outils bureautiques ou de développement.

Les ordinateurs concernés peuvent appartenir à l'administration pénitentiaire (établissement ou RIEP), aux groupements titulaires des marchés de fonctionnement des établissements en gestion mixte, aux entreprises concessionnaires, aux associations ou à d'autres administrations (par exemple l'éducation nationale). Les propriétaires des ordinateurs sont responsables, au même titre que l'administration pénitentiaire, du respect des règles énoncées ci-après.

4.2. *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.]

4.3. *Technologies autorisées/interdites*

Les technologies autorisées et interdites dans le cadre de l'informatique en salle d'activités concernent les matériels en salle d'activité, mis à disposition des détenus sous contrôle de personnel d'encadrement (personnels de l'administration pénitentiaire, des groupements dans les établissements à gestion mixte, formateurs, intervenants d'associations...).

Les principales technologies autorisées et interdites sont les suivantes (liste non exhaustive, *cf.* annexe II pour la liste exhaustive) :

PRINCIPALES TECHNOLOGIES AUTORISÉES dans le cadre d'activités encadrées	PRINCIPALES TECHNOLOGIES NTERDITES
Ordinateur compatible PC non portable, non communicant sans fil et consoles de jeux non communicantes	Ordinateur compatible PC portables ou « de poche », PC communicants sans fil, consoles communicantes, assistants personnels
Lecteur de disquettes standard (interne ou externe) et disquette marquée par l'administration pénitentiaire	
Lecteur de CD ou de DVD	
Souris et manette de jeux avec fil	Périphériques de technologie « sans fil »
Disquette CD,DVD informatique de travail fournis et marqués par l'administration pénitentiaire ou un représentant ou CD et DVD provenant d'éditeurs Graveurs de CD ou de DVD* *Sous réserve d'un accord de la DISP et uniquement dans le cadre des activités de travail pénal	Tout autre support vierge (CD, DVD, clé USB, baladeur MP3, cartes mémoires…)
Imprimantes jet d'encre, imprimantes laser	
Scanners Sous réserve d'un accord de la DISP et uniquement dans le cadre des activités de travail pénal	Webcam, matériel de photo numérique
Cartes réseau Ethernet	Tout périphérique et technologie de communication sans fil
Systèmes d'exploitation, outils bureautiques et de développement, CAO, anti-virus Outils de numérisation, graphisme, PAO ou DAO	Logiciels de chiffrement Logiciels de surcharge de sécurité Logiciels de numérisation Logiciels de graphisme Logiciels professionnels de publication assisté par ordinateur (PAO) et de dessin assisté par ordinateur (DAO) Logiciels utilisant des machines virtuelles et machines virtuelles (exemple : VMware) Logiciels utilisant des images de disques et images de disques (exemple : Ghost) Système d'exploitation pouvant être démarré sur un support externe à l'ordinateur

Les matériels soumis à l'accord de la DSIP ne devront être accessibles qu'aux personnes placées sous main de justice qui en auront la nécessité. Les accès à ce matériel devront être enregistrés de façon à permettre un contrôle à *posteriori* par la DISP.

4.4. *Mise en œuvre des scellés de sécurité*

La mise en place des scellés de sécurité sur les matériels informatiques est obligatoire pour tout ordinateur en salle d'activité.

Le détenu ne doit en aucun cas avoir accès à l'intérieur des boîtiers des ordinateurs et des autres périphériques. Ainsi, un ou plusieurs scellés devront être mis en place sur les unités centrales des ordinateurs accessibles par les détenus, un ou plusieurs scellés devront également être placés sur les écrans des ordinateurs en cellule.

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 par un personnel de l'administration pénitentiaire, un partenaire ou un fournisseur agréé et contrôlé par un personnel de l'administration pénitentiaire afin que soit constatée la régularité de l'opération et que soient remplacés les scellés de sécurité qui auraient été enlevés.

Un inventaire des scellés de sécurité doit être mis en œuvre dans les salles d'activités. Cet inventaire comportera pour chaque nouveau scellé, le nom de l'ordinateur sur lequel le scellé a été placé, l'objet du nouveau scellé (attribution du matériel, ouverture de l'ordinateur, fouille informatique générale...), la date de pose du scellé et la personne de l'administration pénitentiaire ayant effectué la pose. Cet inventaire doit permettre, lors des fouilles, de vérifier le nombre de scellés mis en place sur les ordinateurs des salles d'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.]

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 (*cf.* convention type pour la fourniture de matériel informatique au profit des personnes placées sous main de justice) entre l'association donatrice ou mettant à disposition et l'administration pénitentiaire afin d'empêcher l'introduction de matériels prohibés en détention et de respecter le principe d'anonymisation entre les fournisseurs et les bénéficiaires ;

– une surcharge de sécurité (multiples écritures) et un contrôle des éléments autorisés devront être appliqués par le correspondant local informatique de l'établissement sur le disque dur des ordinateurs fournis par l'association ;

– dans le cas où les matériels seraient pourvus de périphériques de communication sans fil, l'association donatrice devra procéder au démontage de ces matériels ;

– pose de scellés.

4.6. *Mots de passe des équipements informatiques en salle d'activité*

Les postes accessibles aux détenus en salle d'activité doivent être sécurisés.

Cette sécurisation impose notamment :

– au niveau du matériel : mise en place d'un mot de passe administrateur au niveau du BIOS. (Le BIOS est un composant faisant partie intégrante de la carte mère et gérant l'interface avec le matériel. C'est ce composant qui permet notamment de démarrer la machine sur un support amovible autre que le système d'exploitation de l'ordinateur.) Ce mot de passe ne doit être connu ni des détenus ni des intervenants ;

– au niveau du système d'exploitation ;

– mise en place d'un mot de passe d'administration connu uniquement de l'administration pénitentiaire et permettant notamment de modifier la configuration logicielle et matérielle de l'ordinateur. Un compte avec des privilèges d'administrateur pourra aussi être attribué à l'enseignant afin que celui-ci puisse installer les fichiers nécessaires à sa formation ;

– mise en place de mots de passe utilisateurs connus de l'administration pénitentiaire, de l'intervenant et des détenus concernés et permettant d'utiliser normalement l'ordinateur et les applications qu'il héberge en restreignant les risques d'utilisation frauduleuse ou détournée.

4.7. *Accès à des réseaux externes*

Hormis pour les salles dédiées, notamment les espaces Cyber Base, les connexions à des réseaux externes depuis les salles d'activités sont interdites. Les règles de sécurité suivantes concernent donc les salles d'activités connectées à des réseaux externes ayant reçu une validation de l'état-major de sécurité et du RSSI.

[§§ 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. **Accès au dossier de l'information dématérialisé**

5.1. *Rappel du cadre légal*

Conformément aux dispositions de l'article 114 du code de procédure pénale (CPP), l'avocat peut transmettre à son client une reproduction de tout ou partie des pièces et actes du dossier de l'information qui peut être dématérialisée sur un cédérom. Les modalités de transmission doivent être effectuées en application des dispositions prévues aux articles R. 15-42 et suivants du CPP. Ce cédérom doit donc être adressé par l'avocat au greffe de l'établissement chargé de le remettre au détenu et l'avocat doit donner connaissance au juge d'instruction de la liste des pièces ou actes dont il souhaite remettre reproduction à la personne placée sous main de justice.

En outre, il conviendra d'apposer un scellé de sécurité sur ce cédérom qui permettra, en cas de fouille informatique, de garantir la confidentialité du dossier. Par ailleurs, les magistrats instructeurs et les détenus pourront demander que ce cédérom soit conservé au greffe de l'établissement.

5.2. *Matériel informatique*

Les personnes placées sous main de justice qui ne disposent pas de matériel informatique en cellule pourront, s'ils en font la demande, accéder à un poste informatique dans une salle sécurisée en zone de détention de l'établissement. Les mesures de sécurité suivantes devront être mises en œuvre :

– en cas d'inutilisation, l'ordinateur de type unité centrale ou portable sera stocké dans une armoire fermée à clef ;
– l'ordinateur devra être équipé d'un lecteur de Cédérom/Dévédérom et des seuls logiciels nécessaires à la visualisation du dossier de l'information, notamment OpenOffice et Acrobat Reader ;
– cet ordinateur ne devra posséder aucun moyen de communication sans fil (Bluetooth, Wifi, infrarouge...) ;
– tous les périphériques d'entrées/sorties sur cet ordinateur devront être neutralisés à l'aide de scellés de sécurité qui devront être inventoriés dans le classeur de sécurité ;
– afin de garantir la confidentialité des informations liées au dossier dématérialisé du détenu, un outil de surcharge de sécurité (effacement sécurisé) sera mis en œuvre afin d'effacer les fichiers temporaires sur l'ordinateur ;
– la salle accessible au détenu pour consulter son dossier dématérialisé ne devra être équipée d'aucun dispositif de communication (prise réseau connectée au réseau de l'établissement, téléphone...).

6. **Mesures de contrôle**

6.1. *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 réglementaire concernant le contrôle des ordinateurs des détenus.

Il 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).

6.2. *Inventaire*

[§§ 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.]

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).

[§§ 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. *Contrôles physique et logique des ordinateurs et des supports d'information*

6.3.1. Contrôle physique des ordinateurs et des supports amovibles

[§§ 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.]

6.3.2. Contrôle logique des ordinateurs et des supports amovibles

[§§ 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.]

Ce contrôle doit être effectué à chaque entrée et sortie d'un matériel informatique en établissement. Cette condition est aussi valable lors d'un transfert d'une personne placée sous main de justice possédant du matériel informatique.

[§§ 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 un contrôle d'ordinateur :

– en cas de remise de la machine à la personne détenue : 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 et sa validation pour la suppression par l'administration pénitentiaire de tous les fichiers et logiciels illégitimes ou mettant en jeu la sécurité pénitentiaire retrouvés sur son ordinateur (l'administration pénitentiaire ne doit pas détruire les documents licites élaborés par le détenu sans son accord, en respect de ses droits d'auteurs éventuels). Si le détenu refuse de signer car il considère que des modifications ont été effectuées lors du contrôle ou qu'il n'autorise pas la suppression des fichiers interdits, il le signale dans le procès-verbal. Dans ce cas, 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 d'un matériel inspecté peut se voir indemnisé au titre du préjudice subi ;
– dans le cas contraire : en application de l'article 40 et de l'article D. 281 du code de procédure pénale le chef d'établissement peut signaler aux autorités judiciaires toute infraction découverte à l'occasion de ces fouilles et contrôles notamment les copies illégales d'œuvres protégées par la propriété intellectuelle (copie de logiciels, de fichiers musicaux, de films...). La décision de retenue d'un matériel informatique demeure du ressort du chef d'établissement. Il est important de noter qu'il peut être fait application des dispositions du code de procédure pénale en matière disciplinaire.

[§§ 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. Ce retrait d'autorisation devra être motivé et notifié au détenu concerné après qu'a été mise en œuvre 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.

6.4. *Libération*

La libération d'un détenu propriétaire d'un ordinateur en cellule fait l'objet de mesures permettant de contrôler qu'aucun fichier illégitime ou mettant en jeu la sécurité pénitentiaire ne sorte de l'établissement. Les supports achetés par le biais de l'administration pénitentiaire et/ou marqués par l'administration pénitentiaire pourront être fournis aux détenus au moment de sa libération, en revanche les autres supports non marqués (Cédérom, Dévédérom) seront conservés par l'administration pénitentiaire.

Les personnels de l'établissement sont ainsi chargés d'effectuer une fouille de l'ordinateur lors de la libération d'une PPSMJ.

6.5. *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.]

6.6. *Gestion des incidents de sécurité liés à la sécurité de l'information*

[§§ 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.]

ANNEXES

ANNEXE I

LISTE DES TECHNOLOGIES AUTORISÉES ET INTERDITES EN CELLULE

CONFIGURATIONS STANDARDS

Ordinateur compatible PC 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) (interne ou externe)	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

PÉRIPHÉRIQUES DE CONTRÔLE

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

PÉRIPHÉRIQUES D'ÉDITION ET DE NUMÉRISATION

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

PÉRIPHÉRIQUES MULTIMÉDIAS ET D'ACQUISITION

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

SUPPORT D'INFORMATIONS

Support d'informations optique

CD/DVD gravé et marqué par l'administration	Autorisé
CD/DVD pressé (pédagogique/culturel)	Autorisé
CÉDÉROM 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

PÉRIPHÉRIQUES 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

Systèmes d'exploitation Windows	Autorisé
Systèmes d'exploitation Linux/Unix/BSD	Autorisé*
Bureautique	Autorisé
Développement	Autorisé
Tout outil de graphisme livré « en standard » avec le système d'exploitation Windows.	Autorisé
Conception assistée par ordinateur (CAO)	Autorisé
Jeux qui ne nécessitent pas une connexion réseau internet	Autorisé

Création multimédia/audiovisuelle	Autorisé
Dissimulation de données	Interdit
Chiffrement	Interdit
Numérisation	Interdit
Graphisme/retouche	Interdit
Publication assistée par ordinateur (PAO)	Interdit
Exécution de machines virtuelles	Interdit
Surcharge de sécurité	Interdit
Création d'image disque	Interdit
Dessin assisté par ordinateur (DAO)	Interdit

RÉSEAU

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

DIVERS

Parasurtenseur	Autorisé
Onduleur	Interdit

* Sous réserve d'autorisation de la DISP

ANNEXE II

LISTE DES TECHNOLOGIES AUTORISÉES ET INTERDITES EN SALLE D'ACTIVITÉS ENCADRÉES

Configurations standards

Ordinateur compatible PC de bureau	Autorisé
Ordinateur portable	Interdit
Ordinateur de poche (Pocket PC)	Interdit
Assistant personnel numérique (PDA)	Interdit

Extensions standards/lecteurs/graveurs

Extension de mémoire vive	Autorisé
Carte vidéo	Autorisé
Carte SCSI	Autorisé
Lecteur de disquette format standard (1,44 Mo) (interne et externe)	Autorisé
Lecteur de disquette à forte capacité	Interdit
Lecteur de CD	Autorisé
Lecteur de DVD	Autorisé
Graveur de CD	Autorisé **
Graveur de DVD	Autorisé **
Lecteur de carte multimédia	Interdit
Lecteur de carte à puce	Interdit

Périphériques de contrôle

Clavier et souris filaires	Autorisé
Clavier et souris sans fil	Interdit
Tablette graphique	Autorisé

Périphériques d'édition et de numérisation

Imprimante jet d'encre	Autorisé
Imprimante laser	Autorisé
Cartouche d'encre/toner	Autorisé
Scanner * sous réserve d'autorisation de la DISP	Autorisé
Webcam	Interdit
Appareil photo numérique	Interdit

Périphériques multimédias et d'acquisition

Cartes son	Autorisé
Enceintes	Autorisé

Configurations standards

Amplificateur sonore	Autorisé
Casque audio	Autorisé
Micro	Autorisé
Carte tuner télévision	Autorisé *
Carte d'acquisition vidéo	Autorisé *

SUPPORTS D'INFORMATIONS

Support d'informations optique

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

PÉRIPHÉRIQUES 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	Autorisé
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

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

Logiciels

Systèmes d'exploitation	Autorisé
Stéganographie	Interdit
Chiffrement	Interdit
Numérisation	Autorisé
Bureautique	Autorisé
Graphisme/retouche	Autorisé
Développement	Autorisé
Publication assistée par ordinateur (PAO)	Autorisé
Création assistée par ordinateur (CAO)	Autorisé
Dessin assisté par ordinateur (DAO)	Autorisé
Création multimédia/audiovisuelle	Autorisé
Exécution de machines virtuelles	Interdit
Surcharge de sécurité	Interdit
Création d'image disque	Interdit

RÉSEAU

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

DIVERS

Onduleur	Autorisé **
Parasurtenseur	Autorisé

* Sous réserve d'autorisation du chef d'établissement.
** Sous réserve d'autorisation de la DISP.

ANNEXE III

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 1er

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 PROPRIÉTÉ INTELLECTUELLE

(Partie législative)

Article L. 122-4. – 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 L. 335-3 (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 L. 335-4 (loi n° 94-102 du 5 février 1994, art. 2, Journal officiel *du 8 février 1994) ; (loi n° 98-536 du 1er 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. 1er,* 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 même 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 PROCÉDURE PÉNALE

(Partie législative)

Article 40 (loi n° 85-1407 du 30 décembre 1985, art. 1er 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 PROCÉDURE PÉNALE

(Partie réglementaire – Décrets simples)

Article D. 66 (décret n° 73-281 du 7 mars 1973, art. 1er, 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 influer 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 D. 67 (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 D. 68. – 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 D. 69. – 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 D. 416, 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 D. 249-2 (décret n° 96-287 du 2 avril 1996, art. 1er 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 :

- 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 ;
- 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 ;
- de commettre ou tenter de commettre des vols ou toute autre atteinte frauduleuse à la propriété d'autrui ;
- 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 ;
- d'imposer à la vue d'autrui des actes obscènes ou susceptibles d'offenser la pudeur ;
- de refuser de se soumettre à une mesure de sécurité définie par les règlements et instructions de service
- de se soustraire à une sanction disciplinaire prononcée à son encontre ;
- de se livrer à des trafics, des échanges non autorisés par les règlements ou tractations avec des codétenus ou des personnes extérieures ;
- 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 ;
- de se trouver en état d'ébriété ou d'absorber sans autorisation médicale des substances de nature à troubler son comportement ;
- de provoquer un tapage de nature à troubler l'ordre de l'établissement ;
- de mettre en danger la sécurité d'autrui par une imprudence ou une négligence ;
- 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 ;
- d'inciter un codétenu à commettre l'un des manquements énumérés au présent article.

Article D. 249-3 (décret n° 96-287 du 2 avril 1996, art. 1er 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 :

- de formuler des outrages ou des menaces dans les lettres adressées aux autorités administratives et judiciaires ;

– 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 ;
– de proférer des insultes ou des menaces à l'encontre d'un codétenu ;
– de refuser d'obtempérer aux injonctions des membres du personnel de l'établissement ;
– de ne pas respecter les dispositions du règlement intérieur de l'établissement ou les instructions particulières arrêtées par le chef de l'établissement ;
– de négliger de préserver ou d'entretenir la propreté de sa cellule ou des locaux communs ;
– d'entraver ou de tenter d'entraver les activités de travail, de formation, culturelles ou de loisirs ;
– de jeter des détritus ou tout autre objet par les fenêtres de l'établissement ;
– de communiquer irrégulièrement avec un codétenu ou avec toute autre personne extérieure à l'établissement ;
– de faire un usage abusif ou nuisible d'objets autorisés par le règlement intérieur ;
– de pratiquer des jeux non autorisés par le règlement intérieur ;
– de multiplier, auprès des autorités administratives et judiciaires, des réclamations injustifiées ayant déjà fait l'objet d'une décision de rejet ;
– d'inciter un codétenu à commettre l'un des manquements énumérés au présent article.

Article D. 251-1 (décret n° 75-402 du 23 mai 1975, art. 1er, Journal officiel *du 27 mai 1975) , (décret n° 96-287 du 2 avril 1996, art. 1er 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 :

– 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 ;
– 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 ;
– 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 ;
– 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 ;
– 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 ;
– 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 ;
– 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 D. 269 (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 D. 281 (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 un rapport des faits et en aviser directement et sans délai le procureur de la République, conformément aux dispositions de l'article 40.

Article D. 340 (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 D. 423 (décret n° 83-48 du 26 janvier 1983, art 1er, Journal officiel *du 28 janvier 1983).* – L'envoi ou la remise de colis est interdit dans tous les établissements à l'égard de tous les détenus. Les seules exceptions qui peuvent être apportées

à ce principe, par décision du chef d'établissement, concernent la remise de linge et de livres brochés n'ayant pas fait l'objet d'une saisie dans les trois derniers mois et ne contenant aucune menace précise contre la sécurité des personnes et celle des établissements.

Article D. 444 (décret n° 75-402 du 23 mai 1975, art. 1er, 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 D. 449-1 (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 :

– pour des raisons d'ordre et de sécurité ;
– en cas d'impossibilité d'accéder aux données informatiques, du fait volontaire du détenu.

ANNEXE 4

Convention cadre fournisseur

[§§ 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.]