Directives relatives à l'usage des ressources informatiques et de télécommunication

Le Gouvernement de la République et Canton du Jura,

vu la loi sur le personnel de l'Etat du 22 septembre 2010;

vu la Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE);

vu l'article 38, alinéa 2, de la loi d'organisation du Gouvernement et de l'administration cantonale du 26 octobre 1978;

arrête :

TITRE PREMIER
Dispositions générales

Buts

Article premier Les présentes directives poursuivent les buts suivants:

a) fixer les modalités d'utilisation des ressources informatiques et de télécommunication de l'Etat mises à disposition des utilisateurs;

b) préciser les moyens de contrôle mis en place pour garantir notamment la protection des ressources informatiques et des données en tenant compte des intérêts de l'Etat et de la protection de la personnalité des utilisateurs;

c) définir la procédure lors de soupçons d'utilisation des ressources informatiques et de télécommunication contraire aux présentes directives, ou d'abus.

Terminologie

Art. 2 Les termes utilisés dans les présentes directives pour désigner des personnes s'appliquent indifféremment aux femmes et aux hommes.

Champ d'application

Art. 3 Sont régis par les présentes directives les utilisateurs au sens de l'article 4, lettre a.

Définitions

Art. 4 Dans les présentes directives, le terme :

a) *utilisateur* désigne la personne, quel que soit son statut, qui accède aux ressources informatiques ou de télécommunication;

b) *activité professionnelle* désigne les activités nécessaires à l'accomplissement des tâches de l'Etat;

c) *responsable hiérarchique* désigne le chef de service et, pour un chef de département, le Gouvernement; pour un chef de service, son chef de département; pour un magistrat au sens de la loi d'organisation judiciaire,

le président du Conseil de surveillance de la magistrature; pour un autre magistrat, le président du Parlement;

d) *ressources* désigne les ressources informatiques et de télécommunication;

e) *ressources informatiques* désigne les moyens informatiques (matériel, logiciel et télématique) et de gestion centraux ou locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade, à partir des réseaux administrés par l'Etat;

f) *ressources de télécommunication* désigne la mise à disposition par l'Etat, par le biais d'un téléphone fixe ou mobile ou d'un ordinateur, d'un service de téléphonie ou de télécommunication.

Réserve

Art. 5 [1] Les utilisateurs demeurent soumis notamment aux législations spéciales suivantes:

a) la législation fédérale sur le droit d'auteur;

b) la législation sur la protection des données;

c) en fonction de leur statut, la législation sur le personnel de l'Etat et sur l'organisation judiciaire.

[2] Les dispositions de procédure pénale, civile et administrative sont réservées.

TITRE II

Modalités d'utilisation des ressources

CHAPITRE PREMIER
Généralités

Principe

Art. 6 Les ressources sont destinées à l'activité professionnelle.

Usage à des fins privées

Art. 7 [1] Les ressources peuvent être employées brièvement à des fins privées, notamment pour des travaux ou des communications privés, s'ils sont urgents ou s'ils ne peuvent être effectués à un autre moment.

[2] Cet usage est admis pour autant qu'il respecte les dispositions légales et réglementaires et les devoirs de service, qu'il ne surcharge pas les ressources, et que son coût soit modique.

[3] Les présentes directives, notamment en matière de traces d'utilisation et de restriction d'accès, s'appliquent lors d'un usage à des fins privées.

Obtention des ressources

Art. 8 [1] Les ressources sont accordées de manière strictement personnelle. Elles sont liées à la fonction et incessibles.

[2] L'obtention des ressources fait l'objet d'une demande que l'utilisateur adresse à sa hiérarchie pour préavis, puis au Service de l'informatique qui statue.

Protection de la personnalité

Art. 9 La personnalité de l'utilisateur est strictement protégée, notamment lors de la mise en œuvre des moyens de contrôle destinés à assurer la sécurité des ressources.

Devoirs généraux de sécurité

Art. 10 [1] Chaque utilisateur est responsable des ressources mises à sa disposition.

[2] Il doit, à son niveau, contribuer à la sécurité générale des ressources.

[3] A ce titre, il lui est notamment interdit de:

a) perturber le bon fonctionnement des ressources;

b) modifier les paramètres des ressources mises à sa disposition qui régissent la sécurité;

c) contourner, de quelque façon que ce soit, les mesures de sécurité;

d) se livrer, depuis des systèmes appartenant à l'Etat, à des actes mettant sciemment en péril la sécurité ou le bon fonctionnement de systèmes ou de réseaux de télécommunication;

e) consulter, enregistrer et diffuser des données à caractère raciste, pornographique ou violent. Demeurent réservés les besoins liés aux procédures administratives et judiciaires;

f) connecter au réseau informatique un équipement, matériel ou virtuel, qui n'est pas agréé au sein de l'Etat. En cas de doute, l'utilisateur consulte le Service de l'informatique;

g) installer ou utiliser d'autres logiciels que ceux agréés au sein de l'Etat. En cas de doute, l'utilisateur consulte le Service de l'informatique;

h) effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde prévue par un contrat d'achat à des conditions admises par le Service de l'informatique.

Droits d'accès

Art. 11 Chaque utilisateur:

a) choisit des mots de passe sûrs, selon le type défini par l'application concernée ou par le Service de l'informatique, et ne les communique pas à des tiers;

b) signale à sa hiérarchie et au Service de l'informatique toute tentative de violation de son compte et, de manière générale, toute anomalie particulière qu'il constate;

c) ne met pas à disposition de personnes non autorisées un accès aux ressources;

d) veille à ce que les données ne puissent pas être accessibles à des personnes non autorisées;

e) est personnellement responsable du bon usage de ses droits d'accès aux ressources;

f) verrouille son poste de travail et ses accès lors des pauses et des absences;

g) détruit ou efface de manière sécurisée tout document sensible ou confidentiel présent sur un support amovible lorsqu'il n'en a plus besoin.

L'utilisateur peut en charger le Service de l'informatique s'il n'est pas muni d'outils appropriés.

Installation de logiciels

Art. 12 [1] Seul le Service de l'informatique installe les logiciels sur les ressources.

[2] Le Gouvernement ou le chef de département auquel est rattaché le Service de l'informatique peut déléguer cette compétence à une autre entité.

Confidentialité

Art. 13 Chaque utilisateur s'abstient de prendre connaissance d'informations détenues par des tiers et auxquelles il n'est pas autorisé à accéder.

Abus

Art. 14 L'usage contraire aux présentes directives ou abusif des ressources est régi par le titre IV.

CHAPITRE 2
Messagerie

Utilisation

Art. 15 [1] Les abonnements à des lettres d'information ou à des listes de distribution doivent présenter un lien avec l'activité professionnelle de l'utilisateur.

[2] Il est interdit à l'utilisateur de procéder, au moyen des ressources mises à sa disposition :

a) à des envois de masse à des fins non professionnelles, à la propagation de messages en chaîne et de fausses rumeurs, ainsi qu'à l'envoi de messages à des fins privées contenant des pièces jointes volumineuses;

b) à la diffusion et à la redistribution à des fins privées de tout ou partie des annuaires électroniques de l'Etat;

c) à l'ouverture de messages et de pièces jointes suspects reçus d'un expéditeur inconnu ou dont l'extension de la pièce jointe est inusitée ou peu plausible. En cas de doute, l'utilisateur consulte le Service de l'informatique avant l'ouverture;

d) à la redirection automatique des messages émis ou reçus vers un compte de messagerie personnelle.

[3] Pour des motifs de sécurité et de bon fonctionnement des ressources, le Service de l'informatique peut prohiber l'utilisation, par le biais des ressources, de messageries personnelles ou associatives, ainsi que de forums de discussion.

Droits d'accès

Art. 16 [1] Seul l'utilisateur qui en est titulaire peut accéder à sa messagerie et à l'espace informatique privé que l'Etat met à sa disposition.

[2] Il peut déléguer ses droits d'accès par écrit.

[3] Les exceptions prévues dans les présentes directives sont réservées.

[4] Les droits d'accès à la messagerie d'un service sont déterminés par son responsable.

CHAPITRE 3
Internet

Utilisation

Art. 17 [1] L'utilisation de l'Internet est réservée à l'activité professionnelle. Elle peut avoir lieu à des fins privées aux conditions de l'article 7.

[2] En tous les cas, elle n'est permise que sur des sites autorisés et connus de l'utilisateur comme étant sûrs.

[3] Sous réserve de besoins professionnels et, pour les lettres d, f, g, k et l, de l'accord préalable du responsable hiérarchique, il est notamment interdit à l'utilisateur :

a) de procéder à des opérations boursières et financières;

b) de regarder des émissions ou des films;

c) de télécharger de la musique ou des vidéos;

d) de faire des achats en ligne;

e) d'écouter la radio ou de la musique;

f) de jouer;

g) de passer du temps sur des sites sociaux;

h) de passer ou recevoir des appels téléphoniques ou vidéo par l'Internet;

i) d'utiliser des fonctions de messagerie instantanée ou de dialogue ("chat") en ligne;

j) de participer à des forums de discussion;

k) de consulter des sites de vente aux enchères en ligne;

l) de déporter des ressources informatiques par l'Internet, notamment par l'utilisation de logiciels de prise de contrôle à distance; dans ce dernier cas, l'accord préalable du Service de l'informatique est également nécessaire.

Données protégées

Art. 18 [1] L'utilisateur ne doit pas rendre accessibles par l'Internet des données protégées par la législation spéciale mentionnée à l'article 5, notamment par les dispositions relatives au secret de fonction.

[2] En particulier, l'utilisateur s'abstient de traiter de telles données au moyen d'une messagerie privée ou d'un outil privé de stockage de données en ligne.

[3] L'utilisation des identifiants professionnels (login, mot de passe, courriel) est interdite pour un usage d'Internet à titre privé, même en dehors des horaires de travail.

CHAPITRE 4

Station de travail

Art. 19 [1] L'utilisateur ne dispose pas de droits d'administrateur sur sa station de travail, sauf décision contraire de son responsable hiérarchique.

[2] L'usage de l'Internet et de la messagerie est interdit tant que l'utilisateur dispose de tels droits.

[3] L'utilisateur n'encombre pas les espaces de stockage de sa station de travail de fichiers volumineux n'ayant pas de caractère professionnel (musique, vidéos, jeux, photos).

[4] La confidentialité et la sauvegarde de tels fichiers ne sont pas garanties. En particulier, la confidentialité de tels fichiers n'existe pas pour une station de travail partagée entre plusieurs utilisateurs réguliers.

[5] L'utilisateur éteint sa station de travail à la fin de sa journée de travail.

CHAPITRE 5

Téléphones et terminaux mobiles

Art. 20 [1] Les téléphones mobiles, les équipements de télécommunication et les ordinateurs portables interconnectés au réseau informatique de l'Etat ou synchronisant des ressources et des données de l'Etat doivent avoir été préalablement approuvés par le Service de l'informatique.

[2] Le Service de l'informatique édicte les règles d'utilisation et en assure l'application par des moyens de contrôle.

[3] En cas de problème, les accès de l'utilisateur aux ressources pourront être suspendus par le Service de l'informatique.

[4] Au surplus, les règles des chapitres 1 à 4 s'appliquent par analogie.

CHAPITRE 6

Accès aux ressources à distance

Art. 21 [1] Le Service de l'informatique peut mettre à disposition de l'utilisateur situé en dehors des bâtiments de l'Etat des ressources informatiques par une connexion à distance, un déport d'affichage, un site web "extranet" ou tout autre moyen.

[2] Cas échéant, l'utilisateur ne communique pas ses identifiants d'accès ou tout paramètre associé aux accès qui lui ont été remis, et prend les mesures nécessaires afin d'assurer la sécurité de ceux-ci.

[3] L'utilisateur informe immédiatement le Service de l'informatique s'il dispose d'indices que ses accès ont été compromis.

[4] En cas d'accès aux ressources à distance via un ordinateur, un réseau ou un système n'étant pas sous contrôle du Service de l'informatique, l'utilisateur doit être vigilant, ne pas activer la mémorisation automatique des identifiants, veiller à se déconnecter, et, si possible, s'assurer que le système est pourvu de mécanismes de sécurité appropriés.

[5] Au surplus, les règles des chapitres 1 à 4 s'appliquent par analogie.

TITRE III

Moyens de contrôle techniques et organisationnels

CHAPITRE PREMIER
Messagerie

Moyens de contrôle

Art. 22 Pour la messagerie, le Service de l'informatique a recours aux moyens de contrôle suivants:

a) *protection antivirus et antispams;* tous les messages émis ou reçus sont analysés par un ou plusieurs logiciels antivirus et antispams. Les messages suspectés de contenir un logiciel malveillant ainsi que ceux dont l'analyse n'a pas été possible ou considérés comme spam sont traités en fonction de l'incident reconnu (nettoyés, remplacés par du texte ou par un fichier, supprimés, mis en quarantaine, remis dans la boîte aux lettres de l'utilisateur);

b) *vérification de la taille des messages;* tous les messages émis ou reçus dépassant la taille maximale autorisée définie par le Service de l'informatique sont rejetés. Dans la mesure du possible, l'expéditeur et le destinataire en sont avisés;

c) *contrôle du type de pièces jointes;* les messages reçus contenant une pièce jointe de type non autorisé par le Service de l'informatique sont traités en fonction de l'incident reconnu (supprimés, remplacés par du texte ou par un fichier, mis en quarantaine, remis dans la boîte aux lettres de l'utilisateur);

d) *vérification de la taille de la boîte aux lettres;* lorsque la taille maximale autorisée par le Service de l'informatique pour chaque boîte aux lettres est proche d'être atteinte, un message est envoyé automatiquement à l'utilisateur et l'invite à nettoyer la boîte aux lettres. Au-delà de cette limite, l'usage de la boîte aux lettres peut être restreint par le Service de l'informatique;

e) *enregistrement des transactions;* pour chaque message reçu ou envoyé, les données suivantes sont enregistrées et elles seules peuvent être utilisées à des fins de contrôle:

- adresse courriel de l'expéditeur;
- adresse courriel du destinataire;
- en-tête technique de courriel;
- catégorie (spam, virus, légitime);
- taille du message;
- objet du message;
- date et heure de la transaction;

f) *données statistiques;* pour une bonne gestion de la messagerie, des statistiques mensuelles d'utilisation issues de la journalisation des transactions au sens de la lettre e) peuvent être produites.

Conservation des données

Art. 23 [1] Les données enregistrées au sens de l'article 22, lettre e, sont conservées six mois.

[2] Au-delà de cette période, elles sont détruites.

[3] Dans le cadre d'une procédure administrative ou judiciaire, elles peuvent être conservées plus de six mois sur décision préalable de l'autorité compétente.

[4] Les données qui ne sont pas ou cessent d'être versées au dossier de la procédure sont détruites.

Statistiques

Art. 24 [1] Les statistiques au sens de l'article 22, lettre f, sont anonymes et ne peuvent pas être établies de manière plus précise que par unité administrative.

[2] De sa propre initiative ou à la demande du responsable hiérarchique, le Service de l'informatique peut lui communiquer les statistiques concernant son unité administrative.

Restauration des messages

Art. 25 La restauration d'une boîte aux lettres peut avoir lieu si les moyens techniques le permettent et si :

a) l'autorité de poursuite pénale compétente le demande dans le cadre d'une procédure;

ou

b) l'utilisateur de la boîte aux lettres le demande par écrit.

Accès au contenu de la boîte aux lettres
1. En général

Art. 26 [1] Afin notamment de garantir la poursuite des activités professionnelles, le responsable hiérarchique peut ordonner la consultation des messages professionnels reçus sur la messagerie d'un utilisateur absent pour une durée indéterminée ou pour une durée déterminée supérieure à trois semaines.

[2] A ce titre, le Service de l'informatique est autorisé à ouvrir la boîte aux lettres électronique, afin d'extraire ou d'ouvrir les messages professionnels et d'introduire une réponse automatique renseignant les futurs expéditeurs sur l'absence de l'utilisateur et l'adresse de son remplaçant. Il y procède en présence du responsable hiérarchique ou de la personne que celui-ci désigne.

[3] Les messages privés ne peuvent pas être extraits ou ouverts.

[4] Si une indication, notamment les éléments d'adresse, ne permet pas de déterminer le caractère professionnel ou privé d'un message, le Service de l'informatique peut présumer que le message est professionnel.

[5] Lorsqu'il a de sérieuses raisons de douter du caractère professionnel d'un message, il prend contact avec l'utilisateur afin de clarifier la situation. En pareil cas, il n'est pas autorisé à consulter le contenu du message avant cette prise de contact. Si celle-ci n'est pas possible ou si des doutes subsistent encore, le message n'est pas consulté.

2. Proportionnalité

Art. 27 La consultation n'est admise que si le but recherché ne peut être atteint par un autre moyen, compte tenu notamment de l'urgence.

3. Forme de la demande

Art. 28 La demande de consultation doit être écrite, motivée et adressée par le responsable hiérarchique de l'utilisateur au Service de l'informatique.

CHAPITRE 2
Internet

Moyens de contrôle

Art. 29 Pour l'Internet, le Service de l'informatique a recours aux moyens de contrôle suivants:

a) *filtrage;* l'accès depuis le réseau cantonal est bloqué, en fonction des moyens techniques à disposition, aux sites sans aucune pertinence ou utilité pour l'activité de l'Etat, notamment ceux ayant pour thème le racisme, la pornographie ou la violence;

b) *limitation sur les fonctionnalités;* l'accès à certaines fonctionnalités de l'Internet depuis le réseau cantonal peut être bloqué, en particulier si elles mettent en jeu la sécurité de celui-ci;

c) *enregistrement des transactions;* pour chaque échange avec l'Internet, les données suivantes sont enregistrées et elles seules peuvent être utilisées à des fins de contrôle:

- identifiant de l'utilisateur;
- date et heure de la transaction;
- adresse du site visité;
- nombre de transactions quotidiennes pour chaque site visité;

d) *données statistiques des accès;* pour une bonne gestion des accès à l'Internet, des statistiques mensuelles d'utilisation issues de la journalisation des transactions au sens de la lettre c peuvent être produites;

e) *statistiques de trafic;* le Service de l'informatique contrôle la quantité de données transitant vers l'Internet. Des statistiques journalières d'utilisation de la bande passante peuvent être établies.

Conservation des données

Art. 30 L'article 23 s'applique à la conservation des données enregistrées au sens de l'article 29, lettre c.

Statistiques

Art. 31 L'article 24 s'applique aux statistiques au sens de l'article 29, lettres d et e.

CHAPITRE 3
Station de travail

Moyens de contrôle

Art. 32 Pour les stations de travail, le Service de l'informatique a recours aux moyens de contrôle suivants:

a) *analyses de la configuration;* des analyses de la configuration de la station de travail pour en recenser les composants matériels, les périphériques et les logiciels sont effectuées périodiquement;

b) *analyses statistiques du contenu des espaces de stockage;* des contrôles sur le contenu des espaces de stockage (locaux et en réseau) sont effectués régulièrement en utilisant exclusivement à des fins de contrôle les données suivantes:

- la localisation du fichier;
- sa taille;
- son propriétaire;
- son type;
- sa date de création;
- sa date de dernière utilisation;

c) *enregistrement des sessions internes;* pour chaque connexion aux ressources internes du réseau, seules les données suivantes peuvent être utilisées à des fins de contrôle:

- l'identifiant de l'utilisateur;
- les date et heure du début et de la fin de la session;
- le volume des données sur les serveurs;

d) *enregistrement des sessions à distance;* lorsque des ressources internes du réseau sont accessibles depuis l'extérieur de l'Etat par une connexion à distance, seules les données suivantes peuvent être utilisées à des fins de contrôle:

- l'identifiant de l'utilisateur;
- les date et heure du début et de la fin de la connexion;
- le volume des données échangées lors de la connexion;
- l'adresse IP d'établissement de la connexion;

e) *enregistrement de données relatives à l'usage d'un pare-feu*; lorsque la station de travail est équipée d'un pare-feu dit applicatif agréé par le Service de l'informatique, seules les données suivantes peuvent être utilisées à des fins de contrôle:

- l'identifiant de l'utilisateur;
- le numéro d'inventaire du poste de travail;
- les date et heure;
- l'identifiant de l'application ou du périphérique (pare-feu applicatif);
- les adresses IP, ports source et destination (pare-feu réseau);
- l'identification du réseau utilisé;
- les volume et nature des données transférées;
- la nature de l'action détectée par le pare-feu;
- l'action effectuée par le pare-feu;

f) *données statistiques;* des statistiques mensuelles d'utilisation issues de la journalisation des sessions et des connexions externes, ainsi que des statistiques d'utilisation des espaces de stockage peuvent être établies aux fins d'évaluer les capacités des systèmes et de détecter les intrusions externes.

Traces du système d'exploitation et des applications

Art. 33 [1] Les traces laissées par le système d'exploitation et les applications sur la station de travail lors de son utilisation ne sont pas collectées.

[2] Toutefois, dans le cadre d'une procédure administrative ou judiciaire, elles peuvent l'être sur décision de l'autorité compétente.

[3] Les données qui ne sont pas ou cessent d'être versées au dossier sont détruites.

[4] En outre, en cas de défectuosité à large échelle justifiant une intervention urgente, ces traces peuvent être collectées pour des raisons techniques ou

de maintenance durant le temps nécessaire à résoudre le problème posé, sur décision du chef du Service de l'informatique; celui-ci en informe les utilisateurs dès que possible.

Conservation des données

Art. 34 [1] Les données collectées en application de l'article 32, lettre a, sont conservées tant que le poste est en service.

[2] Au surplus, l'article 23 s'applique à la conservation des données enregistrées au sens de l'article 32.

Statistiques

Art. 35 L'article 24 s'applique aux statistiques au sens de l'article 32, lettres b et f.

CHAPITRE 4
Ressources de télécommunication

Moyens de contrôle

Art. 36 Pour les ressources de télécommunication, le Service de l'informatique a recours aux moyens de contrôle suivants :

a) *enregistrement des numéros d'appel;* les numéros appelés par l'utilisateur sont enregistrées avec les données suivantes :
   - le numéro de téléphone appelé;
   - la date de l'appel;
   - sa durée;
   - son coût.

b) *facturation par numéro;* une facture détaillée des appels privés par numéro d'utilisateur est établie et contient les données mentionnées sous lettre a;

c) *données statistiques;* des statistiques d'usage de la télécommunication peuvent être établies.

Conservation des données

Art. 37 [1] Les données collectées en application de l'article 36 sont conservées douze mois.

[2] Au surplus, l'article 23 s'applique.

Statistiques

Art. 38 L'article 24 s'applique aux statistiques au sens de l'article 36, lettre c.

TITRE IV
Analyse nominative des données

Principes

Art. 39 [1] Les données enregistrées peuvent être analysées en rapport avec des personnes et de manière nominative dans les buts suivants:

a) élucider un soupçon concret d'utilisation abusive ou poursuivre un cas d'utilisation abusive, pour autant que les mesures d'information,

organisationnelles et techniques de prévention des abus ne permettent pas de remédier à ceux-ci;

b) analyser les perturbations des ressources, y remédier ou parer aux menaces concrètes qu'elle subit;

c) fournir les prestations indispensables;

d) saisir les prestations effectuées et les facturer;

e) contrôler le temps de travail de personnes déterminées.

[2] Une analyse nominative de données personnelles ne peut être effectuée que si cumulativement :

a) elle est ordonnée par :
   1. le Gouvernement, si les données concernent un employé de l'Etat ou un ministre; dans les cas de peu de gravité et ne concernant qu'un employé, le chef de département de celui-ci est compétent;
   2. le Conseil de surveillance de la magistrature, si elles concernent un magistrat au sens de la loi d'organisation judiciaire;
   3. le Bureau du Parlement, si elles concernent un autre magistrat;
   4. l'organe compétent pour engager l'utilisateur concerné au sein des entités paraétatiques;

b) elle suit une information écrite de la personne concernée.

[3] Selon les circonstances, l'autorité au sens de l'alinéa 2, lettre a, peut renoncer à une analyse nominative rétrospective et avertir en lieu et place l'employé ou les employés concernés qu'une analyse nominative sera opérée ultérieurement dans un délai qu'elle indique.

[4] Au surplus, le président du Gouvernement peut ordonner, à titre provisionnel, des mesures urgentes nécessaires, pouvant impliquer une analyse nominative de données personnelles, pour assurer la protection des ressources, en particulier en cas d'attaque informatique.

Signalement

Art. 40 Le responsable hiérarchique qui soupçonne que des ressources ne sont pas utilisées conformément aux présentes directives ou sont utilisées abusivement le signale à l'autorité compétente au sens de l'article 39, alinéa 2, lettre a.

Exécution

Art. 41 [1] Le Service de l'informatique exécute l'analyse nominative sur mandat de l'autorité compétente au sens de l'article 39, alinéa 2, lettre a.

[2] Il ne peut déléguer cette analyse à un tiers qu'avec l'accord de cette autorité.

Droit applicable

Art. 42 L'autorité au sens de l'article 39, alinéa 2, lettre a, donne suite à sa saisie conformément à la législation dont relève l'utilisateur concerné, en particulier à la législation sur le personnel de l'Etat et sur l'organisation judiciaire.

TITRE V

Dispositions finales

Abrogation

Art. 43 Les directives concernant les modalités d'utilisation d'Internet et de la messagerie au sein de l'Administration cantonale du 13 mars 2001 et les directives techniques relatives aux enregistrements et à la surveillance informatique au sein de la République et Canton du Jura du 13 mars 2001 sont abrogées.

Entrée en vigueur

Art. 44 Les présentes directives entrent en vigueur le 1er janvier 2014.

Delémont, le 4 mars 2014

AU NOM DU GOUVERNEMENT DE LA REPUBLIQUE ET CANTON DU JURA

Le président :

Charles Juillard

Le chancelier :

Jean-Christophe Kübler