Session ordinaire 2012-2013

AT/vg P.V. ERMCE 18

Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

Procès-verbal de la réunion du 25 février 2013

Ordre du jour :

1. Motion de Monsieur Eugène Berger relative au développement d'une charte de sécurité pour la sécurisation de bases de données à caractère personnel en fonction de la sensibilité des données et d'une charte de déontologie auprès de l'Etat (demande de M. Eugène Berger du 6 février 2013)

2. 6487 Projet de loi portant création de l'établissement public « Autorité luxembourgeoise indépendante de l'audiovisuel » et modification 1. de la loi modifiée du 27 juillet 1991 sur les médias électroniques ; 2. de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat et 3. de la loi du 20 avril 2009 relative à l'accès aux représentations cinématographiques publiques
   - Rapporteur : Monsieur Serge Wilmes
   - Examen de l'avis du Conseil d'Etat

3. JOIN(2013) 1 : COMMUNICATION CONJOINTE AU PARLEMENT EUROPEEN, AU CONSEIL, AU COMITE ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS
   Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

   Le document précité ne relève pas du contrôle du principe de subsidiarité.

   - Désignation d'un rapporteur

   COM(2013) 48 : Proposition de DIRECTIVE DU PARLEMENT EUROPEEN ET DU CONSEIL concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

   Le document précité relève du contrôle du principe de subsidiarité. Le délai de subsidiarité a débuté le 13 février 2013 et prendra fin le 10 avril 2013

   - Désignation d'un rapporteur

   COM(2013) 40 : Proposition de REGLEMENT DU PARLEMENT EUROPEEN ET DU CONSEIL modifiant le règlement (UE) n° 912/2010 établissant l'Agence du GNSS européen

Le document précité relève du contrôle du principe de subsidiarité. Le délai de subsidiarité a débuté le 7 février 2013 et prendra fin le 4 avril 2013

- Désignation d'un rapporteur

4. Divers

*

Présents : Mme Diane Adehm, M. Eugène Berger, Mme Anne Brasseur, M. Ben Fayot, M. Marcel Oberweis, M. Serge Wilmes

Mme Michèle Bram, du Service des Médias et des Communications
M. Pierre Zimmer, du Centre des Technologies de l'Information de l'Etat

Mme Anne Tescher, de l'Administration parlementaire

Excusés : M. Claude Adam, M. Jean Colombera, Mme Claudia Dall'Agnol, Mme Christine Doerner, M. Claude Haagen, M. Norbert Haupert

*

Présidence : M. Marcel Oberweis, Président de la Commission

*

1. Motion de Monsieur Eugène Berger relative au développement d'une charte de sécurité pour la sécurisation de bases de données à caractère personnel en fonction de la sensibilité des données et d'une charte de déontologie auprès de l'Etat (demande de M. Eugène Berger du 6 février 2013)

M. Eugène Berger rappelle qu'il avait déposé la motion sous rubrique le 7 mars 2012 dans le contexte de l'affaire « Medicoleak » où il y a eu une fuite de données de la base de donnés du Centre Médico-sportif en janvier 2012. L'orateur renvoie en outre à l'attaque de cyberespionnage du réseau « Red October » en janvier 2013 de sorte que le contenu de la motion reste d'actualité (cf. question parlementaire n°2508 de M. Eugène Berger du 17 janvier 2013).

- Explications de M. le Ministre

En juillet 2011, le Gouvernement a mis en place le CERT gouvernemental (Computer Emergency Response Team) de même que le Cybersecurity board. Le Cybersecurity board, présidé par le Ministre des Communications et des Médias, a eu comme mission d'élaborer une stratégie nationale de lutte contre les cyberattaques.

Le CERT gouvernemental est donc une structure publique ayant pour mission la prévention et la réponse aux incidents pour les systèmes d'informations de l'Etat et des infrastructures critiques qui touchent à la sécurité nationale. Le CERT gouvernemental est aussi reconnu comme point de contact au niveau international et représente le Luxembourg à l'étranger.

Il existe au Luxembourg également un CERT national, à savoir le groupement d'intérêt économique SMILE (« Security made in Luxembourg ») qui gère les trois pôles d'activités suivants : CIRCL (Computer Incident Response Center Luxembourg), CASES et BEE SECURE. Ces instances réalisent notamment des missions de sensibilisation et de réponse aux incidents dont le périmètre d'intervention sont les entreprises du secteur privé ainsi que le grand public et les communes.

En ce qui concerne les 6 points de la motion, M. le Ministre confirme que les travaux afférents sont en cours. Rappelons que les 6 revendications de la motion sont les suivantes :

1) procéder endéans les six mois à un relevé des bases de données à caractère personnel auprès de l'Etat ;

2) développer dans la même période une charte de sécurité pour la sécurisation de bases de données à caractère personnel en fonction de la sensibilité des données ;

3) développer dans la même période une charte de déontologie définissant clairement les données à caractère sensible ne devant pas être stockées dans des bases de données ;

4) mettre en place des systèmes de retraçage pour toutes les bases de données à caractère personnel de l'Etat jusqu'à l'échéance 2014 ;

5) désigner au sein de chaque ministère un responsable à la protection des données susceptible de contrôler une exploitation adéquate des bases de données ;

6) augmenter les effectifs de la CNPD afin de garantir qu'elle puisse assurer sa mission de contrôle de la collecte et de l'utilisation de données à caractère personnel.

- Quant au point 1 de la motion

Le Cybersecurity board a décidé en date du 26 janvier 2012 d'identifier les bases de données de l'Etat qui sont sensibles. M. le Ministre rappelle que dans les années 90 il a été proposé de créer une base de données centrale de l'Etat qui serait localisée auprès du CTIE. Cette idée a cependant été rejetée au motif de la protection des données.

Le Cybersecurity board est donc en charge de l'élaboration d'une liste des bases de données. L'inventaire, qui est d'ailleurs presque achevé, montre que le nombre des bases de données est élevé. De plus, des banques de données à caractère hautement sensible ne sont pas localisées auprès de l'Etat. Il s'agit notamment du secteur de la santé et en particulier des bases de données des hôpitaux privés. Les mesures et les recommandations prônées par le Cybersecurity board ne sont donc pas applicables à ces banques de données. A souligner que le Ministère de la Santé envisage une action de sensibilisation en parallèle.

En mai 2011, chaque ministre s'est vu adresser une demande afin de communiquer au Cybersecurity board les informations sur les bases de données de son ministère. Une lettre de rappel vient d'être envoyée aux ministères afin de pouvoir arrêter cette liste de manière définitive. D'une manière provisoire, on peut estimer qu'il y a plus de 700 bases de données auprès de l'Etat.

- Quant à la sensibilisation et la formation au sujet de la protection des données

Le sujet de la protection des données fait désormais partie intégrante de la formation des fonctionnaires-stagiaires à l'INAP. Les fonctionnaires sont sensibilisés au fait que des abus au niveau de l'utilisation des banques de données peuvent être retracés et entraîneront une poursuite pénale voire disciplinaire.

M. le Ministre envisage en outre une séance de sensibilisation et de formation des membres du Conseil de Gouvernement.

D'une manière générale, il s'agit de développer une culture de sécurité au sein de l'administration gouvernementale. Plusieurs ministères ont d'ailleurs déjà entamé des mesures de sensibilisations à cet égard.

La fiche d'impact relative aux projets de loi contient désormais une rubrique sur la protection des données. En effet, il y a lieu de constater que la CNPD n'a pas été consultée systématiquement au sujet des projets de loi. M. le Ministre suggère que l'avis de la CNPD devra accompagner tous les avant-projets de loi.

- Quant à l'inventaire des banques de données de l'Etat

Le Cybersecurity board envisage de mettre en place une liste des bases de données laquelle sera régulièrement mise à jour. Il s'agit également d'homogénéiser les niveaux de sécurité. Voilà pourquoi dans le cadre du recensement des bases de données, les ministères se sont vu adresser un questionnaire exhaustif. Les renseignements portent entre autres sur les éléments suivants (cf. présentation du CTIE sur le recensement en annexe 1 du présent procès-verbal) :

- Il s'agit de savoir si les bases de données ont une base légale, s'il elles sont autorisées par la CNPD ou notifiées à la CNPD ;
- la finalité du traitement de même que le responsable de ce traitement voir le responsable technique ou encore le sous-traitant ;
- le volume des données ;
- la nature et la sensibilité des données traitées ;
- la description des opérations et notamment la question de savoir s'il y a des transferts de données vers d'autres entités ;
- le type d'accès à la banque de données (interne ou externe via Internet) ;
- l'interconnexion éventuelle avec d'autres banques de données ;
- les mesures de sécurité mises en place, en particulier la sécurisation des accès par mot de passe ou par authentification forte, le niveau de traçabilité (logging) et l'exercice d'audits de sécurité (p.ex. des tests d'intrusion) ;
- la formation continue obligatoire des personnes ayant accès aux données.

A noter que la CNPD est également représentée au sein du groupe de travail en charge du recensement des banques de données.

Le représentant du CTIE explique qu'il est impérieux d'appliquer un langage et une approche susceptibles d'être soumis à un audit. A noter que le CTIE fait régulièrement l'objet d'audits par différents acteurs. Il faut que l'auditeur se retrouve dans un cadre standardisé.

Quant à la mise à jour, le CTIE développera une application informatique qui permette aux responsables désignés de mettre à jour régulièrement les informations sur leurs banques de données. Alors que les responsables devront notamment implémenter des recommandations de sécurité, le CTIE pourra faire le suivi de la mise en œuvre par le biais de cette application.

Dans une première étape, les banques de données doivent être catégorisées selon des critères standardisés, comme par exemple l'intégrité des données, la confidentialité et la traçabilité.

Une première conclusion de cet inventaire est que l'utilisation des bases de données à caractère sensible nécessite désormais l'authentification forte de Luxtrust.

Certaines banques de données existaient déjà avant la mise en vigueur de la loi du 2 août *2002* relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Or, cette loi impose pour la première fois le traçage dans le cadre du traitement des banques données. Toutes les banques de données créées après 2002 sont évidemment conformes aux exigences de la loi. Les banques de données plus vieilles devront être adaptées au fur et à mesure.

- Quant au point 2 de la motion

Le CTIE dispose d'ores et déjà d'un code de conduite (cf. annexe 2 du procès-verbal) qui sera adapté pour être applicable à d'autres entités de l'Etat. Ce code de conduite du CTIE, avisé par la CNPD, sera régulièrement évalué et adapté aux nouveaux standards.

A noter que ce code de conduite doit être conforme à certains critères standardisés. Le terme « charte de sécurité » de la motion n'est donc pas adéquat.

- Quant au point 5 de la motion

Dès que la liste élaborée par le Cybersecurity board sera disponible, elle sera analysée afin d'identifier les bases de données à caractère sensible. C'est uniquement pour ce type de base de données qu'un responsable sera désigné et qui sera l'interlocuteur du Cybersecurity board et de la CNPD.

- Quant au point 6

L'effectif de la CNPD compte actuellement 12 personnes. Un nouveau poste d'ingénieur-informaticien a été attribué à la CNPD l'année dernière. M. le Ministre est train d'examiner la revendication de postes supplémentaires par la CNPD cette année.

- *Echange de vues*

- Le projet de loi 6475 relative à la Protection nationale, déposé le 3 septembre 2012 et renvoyé à la Commission des Institutions et de la Révision constitutionnelle, introduit en droit positif les infrastructures critiques. En vertu de ce projet de loi, le Haut-Commissariat à la Protection nationale est l'organe coordinateur des mécanismes de protection nationale.

- M. le Ministre regrette que pour des raisons de sécurité il ne puisse fournir des détails supplémentaires sur l'attaque de cyberespionnage « Red October ». L'information concernant le département de l'Etat visé est une information qui ne peut être divulguée. Il propose cependant de fournir des statistiques quant à la fréquence et à la nature des cyberattaques.

- M. le Ministre est d'avis que la protection informatique est essentielle, tout en estimant que le facteur humain, c'est-à-dire les précautions de l'utilisateur d'une banque de données, est souvent l'élément faible. Ceci est d'ailleurs bien illustré par l'exemple du Centre Médico-

sportif où la fuite de données a été engendrée par une faute de l'agent. Voilà pourquoi il est fondamental de sensibiliser les agents de l'Etat d'autant plus que des mesures disciplinaires peuvent être engagées à l'encontre du fonctionnaire fautif.

- En ce qui concerne le retraçage, M. le Ministre explique que dans le cadre de l'affaire « Médicoleak », il a été impérieux à l'Etat de déposer plainte afin de pouvoir vérifier quel agent avait accédé à la banque de données. En effet, il n'est pas permis de retracer dans tous le cas les personnes ayant consulté la base de données mais il faut une poursuite pénale du Parquet.

- En revanche, le retraçage ne doit pas être confondu avec le droit d'accès des citoyens. Le droit d'accès permet à chaque citoyen de se renseigner à propos de la consultation de ses données personnelles par une administration. Ce droit d'accès fait notamment l'objet d'une proposition de Règlement de l'UE[1] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Pour de plus ample détails au sujet des réformes en matière de protection des données au niveau européen il est renvoyé au discours de M. le Ministre à la *Spring Conference* organisée en mai 2012 par la CNPD, et repris en annexe 3 du présent procès-verbal.

- Le projet de loi 6330 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques dispose dans son article 38 que toute personne, dont les données font l'objet d'une inscription sur le registre national, a le droit d'obtenir la liste des autorités, administrations, services, institutions ou organismes qui ont, au cours des six mois précédant sa demande, consulté ou mis à jour ses données au registre national. Il est important que le citoyen sache qui a consulté ses données ou qui a procédé à une modification de ses données. L'information qui lui sera fournie ne révélera pas le nom du fonctionnaire ayant consulté les données, mais uniquement le service pour lequel il travaille.

- Le représentant du groupe LSAP rappelle que les travaux parlementaires au sujet du projet de loi n°6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves, dont il a été le rapporteur, n'ont pas été évidents. Il a fallu plusieurs étapes avant qu'un consensus ait pu être trouvé entre la Chambre, la CNPD, le Conseil d'Etat et le Gouvernement. Il est assez complexe de mettre en pratique des règles générales en matière de protection des données.

- L'expert du CTIE explique que l'exportation des données d'une administration à une autre n'est plus pratiquée. L'interconnexion concerne en fait uniquement les banques de données plus anciennes où les réseaux n'étaient pas encore développés. Une interconnexion entre deux banques de données n'était d'ailleurs possible que sous condition d'une base légale adéquate et d'une autorisation de la CNPD. Les utilisateurs se voient désormais attribuer un accès contrôlé à certaines données d'une banque de données par le réseau de l'Etat. De plus, il ne s'agit pas d'un accès direct aux données, mais d'un accès à un programme qui permet un certain traitement prédéfini des données.

2. 6487 Projet de loi portant création de l'établissement public « Autorité luxembourgeoise indépendante de l'audiovisuel » et modification 1. de la

[1] COM (2012) 11 final Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)

loi modifiée du 27 juillet 1991 sur les médias électroniques ; 2. de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat et 3. de la loi du 20 avril 2009 relative à l'accès aux représentations cinématographiques publiques

Ce point n'a pas été abordé.

3. **JOIN(2013) 1 : COMMUNICATION CONJOINTE AU PARLEMENT EUROPEEN, AU CONSEIL, AU COMITE ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS**
Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

Mme Diane Adehm est nommée rapportrice du document sous rubrique.

COM(2013) 48 : Proposition de DIRECTIVE DU PARLEMENT EUROPEEN ET DU CONSEIL concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

Le document précité relève du contrôle du principe de subsidiarité. Le délai de subsidiarité a débuté le 13 février 2013 et prendra fin le 10 avril 2013

Mme Diane Adehm est nommée rapportrice du document sous rubrique.

COM(2013) 40 : Proposition de REGLEMENT DU PARLEMENT EUROPEEN ET DU CONSEIL modifiant le règlement (UE) n° 912/2010 établissant l'Agence du GNSS européen

Le document précité relève du contrôle du principe de subsidiarité. Le délai de subsidiarité a débuté le 7 février 2013 et prendra fin le 4 avril 2013

M. Marcel Oberweis est nommé rapporteur du document sous rubrique.

Luxembourg, le 14 mars 2013

La secrétaire,
Anne Tescher

Le Président,
Marcel Oberweis

Annexes :

1. Présentation du CTIE sur le recensement des banques de données

2. Code de conduite du CTIE

3. Spring Conference : The reform of EU data Protection – Discours du Ministre des Communications et des Médias

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Centre des technologies de l'information de l'Etat

Informations demandées

- Base légale, banque de données autorisée par /notifiée à la CNPD
- Dénomination / Descriptif
- Finalité du traitement
- Responsable du traitement (selon la loi de 2002) + contacts nominatifs
- Responsable technique / sous-traitant (au sens de la loi de 2002),
- Nature/type/catégorie/sensibilité des données traitées
- Volume de données
- Description des opérations (aussi les transferts vers d'autres entités)

Informations demandées

- Type d'accès à la banque de données (interne/externe-internet)
- Interconnexion avec d'autres banques de données
- Mesures de sécurité mises en place :
  - Sécurisation des accès (authentification forte, mot de passe)
  - Niveau de traçabilité / logging
  - Audit de sécurité (test d'intrusion etc)
- Formation continue obligatoire des personnes ayant accès aux données
- Evolutions futures planifiées

Critères de qualification du projet en terme de sécurité :									
	Disponibilité DMIA (D)		Perte PMIA (P)		Intégrité des données (I)		Confidentialité des données (C)		Traçabilité (T)
1	≥5j	1	≥5j	1	Tolérance	1	Public	1	Besoin non requis
2	>24h	2	> 48h	2	Correction	2	Restreint	2	Besoin analytique
3	4 h < DMIA ≤ 24h	3	24 h < PMIA ≤ 48h	3	Arrêt et correction	3	Confidentiel	3	Besoin métier
4	0h < DMIA ≤ 4h	4	0h < PMIA ≤ 24h	4	Certification	4	Secret	4	Obligation légale
Qualification du projet									
	D1		P2		I2		C4		T3

Disponibilité DMIA (D)	*Disponiblité Maximale d'Interruption Admissible*
Perte PMIA (P)	*Perte Maximale d'Informations Accpetable*
Intégrité	*L'intégrité définit l'erreur maximale acceptable du système.*
Confidentialité	*La confidentialité définit le public de personnes autorisé à y accéder.*
Traçabilité	*La traçabilité définit le niveau d'information nécessaire et suffisant pour justifier les traitements du système.*

Disponibilité								
		Très basse		Basse		Moyenne		Haute
Disponibilité		≥5j		>24h		4 h < DMIA ≤ 24h		0h < DMIA ≤ 4h
Impact		Nuisances insignifiantes		Nuisance à l'organisation locale		Impact négatif sur l'ensemble du système, les personnes, et le public ; peut induire des dettes financières ou juridiques, et atteinte à l'image		Impact très négatif sur l'ensemble du système, les personnes, et le public ; induit de fortes dettes financières ou juridiques, et atteinte forte à l'image et la réputation
Exemples		Site Web Public d'information non sensible		Horaires, agenda		Accès à des informations réglementaires		Informations d'urgences, données personnelles ou médicales

Perte de données								
		Très basse		Basse		Moyenne		Haute
Perte de données		≥5j		> 48h		24 h < PMIA ≤ 48h		0h < PMIA ≤ 24h
Impact		N/A		Nuisance à l'organisation		Impact négatif sur l'ensemble du système, les personnes, et le public ; peut induire des dettes financières ou juridiques, et atteinte à l'image		Impact très négatif sur l'ensemble du système, les personnes, et le public ; induit de fortes dettes financières ou juridiques, et atteinte forte à l'image et la réputation
Exemple		Site Web Public d'information non sensible		Horaires, agenda		Accès à des informations réglementaires		Informations d'urgences, données personnelles ou médicales

Intégrité				
	Très basse	Basse	Moyenne	Haute
Intégrité	Tolérance	Correction	Arrêt et Correction	Certification
Définition	Perte momentanée d'intégrité tolérée, sous réserve qu'elle soit signalée et qu'elle ne remette pas en cause le service fourni	Perte d'intégrité devant être signalée et corrigée dans un délai déterminé, sans conséquence sur le service fourni	Perte d'intégrité nécessitant un arrêt des opérations jusqu'à la correction de l'anomalie dans un délai conforme aux exigences de disponibilité	Préservation pérenne et opposable de l'intégrité (par vérification et signature des opérations)
Impact	Nuisances insignifiantes	Nuisance à l'organisation locale	Impact négatif sur l'ensemble du système, les personnes, et le public ; peut induire des dettes financières ou juridiques, et atteinte à l'image	Impact très négatif sur l'ensemble du système, les personnes, et le public ; induit de fortes dettes financières ou juridiques, et atteinte forte à l'image et la réputation
Exemple	Site Web Public d'information non sensible	Horaires, agenda	Accès à des informations réglementaires	Informations d'urgences, données personnelles ou médicales

Traçabilité				
	Très basse	Basse	Moyenne	Haute
Traçabilité	Besoin non critique	Besoin analytique	Besoin métier	Obligation légale
Impact	N/A	Nuisance à l'organisation	Impact négatif sur l'ensemble du système, les personnes, et le public ; peut induire des dettes financières ou juridiques, et atteinte à l'image	Impact très négatif sur l'ensemble du système, les personnes, et le public ; induit de fortes dettes financières ou juridiques, et atteinte forte à l'image et la réputation
Exemples	Logs systèmes de postes de travail	Logs systèmes de postes de serveurs	Accès aux systèmes sensibles d'un système d'information	Conservation des traces pour les Fournisseurs d'Accès Internet (FAI)

Confidentialité							
		Très basse		Basse		Moyenne	Haute
Confidentialité		Public		Interne		Confidentiel	Secret
Accès		Public		Disponible aux employés et aux non employés approuvés		Disponible aux employés et les non employés autorisés avec un accord de non divulgation	Disponible à une sélection d'employés et non employés autorisés, avec un accord de non divulgation, accordé sur base de nécessité. Une liste d'accès doit être maintenue
Impact		N/A		Nuisance à l'organisation		Impact négatif sur l'ensemble du système, les personnes, et le public ; peut induire des dettes financières ou juridiques, et atteinte à l'image	Impact très négatif sur l'ensemble du système, les personnes, et le public ; induit de fortes dettes financières ou juridiques, et atteinte forte à l'image et la réputation
Exemple		Site Web Public		Documents Internes au CTIE		Accès à des informations réglementaires	Informations d'urgences, données personnelles ou médicales

Code de Conduite du CTIE

Centre des technologies de l'information de l'Etat

Version 2.0

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Centre des technologies de l'information de l'Etat

Le mot du directeur

Chères et Chers collègues,

Depuis sa création **le Centre des technologies de l'information de l'Etat** s'est donné comme objectif principal de fournir des services informatiques de qualité, innovants et performants.

L'informatique gouvernementale est un des piliers sur lesquels reposent les initiatives de diversification de l'économie luxembourgeoise et de ce fait le CTIE se doit de contribuer aux efforts de développement du Luxembourg en tant qu'acteur majeur sur la scène internationale du commerce électronique.

Ainsi, pour maintenir la confiance qui est placée en nous, il est capital que chacun de nous adhère à des valeurs déontologiques communes, mais aussi à certains principes qui ont pour objectif de nous guider dans le déroulement de nos activités quotidiennes.

C'est dans ce contexte que notre Code de Conduite a été conçu.

Il permet donc d'énoncer clairement notre vision, nos valeurs et nos engagements sur le comportement que nous devons adopter en tant que collaborateurs du CTIE, vis-à-vis du respect des lois, des relations avec nos interlocuteurs, d'une utilisation responsable de nos ressources, et de l'application de mesures de sécurité et environnementales.

L'engagement de tous envers notre Code de Conduite est primordial, car il nous permet d'exposer à l'ensemble des utilisateurs de nos services, ainsi qu'aux autres institutions gouvernementales nationales et internationales, que nous sommes une organisation solide, unie et possédant des valeurs fortes.

C'est de cette manière que nous continuerons d'améliorer les services à nos utilisateurs et par cette voie que nous obtiendrons la reconnaissance qui nous est due.

Je compte sur vous pour avoir la patience et la motivation pour lire et promouvoir les principes de ce Code de Conduite.

Pierre Zimmer,
Directeur

Table des matières

1. Introduction

Le **Centre des technologies de l'information de l'Etat (CTIE)** a été institué par *la loi modifiée du 20 avril 2009* portant création du Centre des technologies de l'information de l'Etat ; son organisation et ses attributions étant fixées par le *règlement grand-ducal modifié du 7 mai 2009* déterminant l'organisation du Centre des technologies de l'information de l'Etat.

Outre son rôle de support technique, le CTIE a une vocation de **prestataire de services informatiques pour l'ensemble de l'Etat**, mais assure également des tâches de coordination, de planification et d'assistance des instances gouvernementales.

Ainsi, tout dysfonctionnement de service informatique, d'élément de système ou de réseau peut porter un préjudice sérieux à des tierces parties comme les administrations ou autres clients du CTIE. Il en va de même des éventuels incidents susceptibles d'avoir un impact sur l'intégrité, la disponibilité et la confidentialité des informations traitées par le CTIE.

En conséquence, il existe un besoin vital de **protéger les informations** et de **gérer la sécurité des systèmes d'information** au sein de chacune des entités du CTIE.

Pour ce faire, le CTIE met en œuvre une **gouvernance informatique** qui repose sur les lois et réglementations luxembourgeoises, mais aussi sur un cadre de sécurité solide permettant de transcrire de manière formelle les volontés stratégiques et opérationnelles du CTIE en matière de **gestion de la sécurité des systèmes d'information.**

Ce cadre de sécurité est composé de politiques de sécurité de l'information, de documents formalisant les besoins de sécurité, de procédures opérationnelles, mais aussi de ce présent Code de conduite.

De ce fait, pour garantir la pérennité de la sécurité de l'information, l'application du Code de conduite est **rendue obligatoire** pour tout le personnel du CTIE (personnel internes et collaborateurs externes).

De plus, chaque agent du CTIE doit veiller à ce que le personnel temporaire, les visiteurs mais aussi les entités en interaction avec les systèmes d'information du CTIE ou manipulant des informations circulant au sein du CTIE respectent les dispositions de sécurité qui seraient d'application en la circonstance.

Chaque agent du CTIE dispose de manière individuelle de l'opportunité d'améliorer cette sécurité ou au contraire de la compromettre. Dans ce contexte, chaque responsable hiérarchique est invité à revoir régulièrement le mode de fonctionnement de son entité, afin de s'assurer qu'il est parfaitement compatible avec les dispositions du cadre de sécurité.

Les objectifs de sécurité seront donc atteints par la mise en pratique du cadre de sécurité. Chaque personne concernée par les activités du CTIE devra contribuer à l'**effort général de sécurité**. Le cadre de sécurité doit devenir le modèle commun de comportement individuel et spontané.

Pour conserver le niveau de sécurité nécessaire, le Code de conduite et les autres composants du cadre de sécurité seront revus périodiquement et adaptés aux situations rencontrées.

2. Préserver les valeurs

Les membres du personnel du CTIE doivent préserver les valeurs du CTIE en respectant la loi, les règlements et les politiques internes applicables au CTIE, en agissant de manière honnête et intègre dans toutes les relations professionnelles et en maintenant un environnement de travail sain.

Les membres du personnel du CTIE sont tenus de traiter les clients, les fournisseurs, les collaborateurs et les collègues avec **respect, dignité, honnêteté, équité et intégrité.**

2.1. Egalité

Le CTIE et son personnel s'engagent à traiter toutes les personnes avec égalité, sans faire de distinction relative à la race, la couleur, la religion, le sexe, l'orientation sexuelle, l'âge, l'origine nationale, le handicap, l'état matrimonial, le statut professionnel et de faire abstraction de toute autre sorte de discrimination.

2.2. Discrimination & harcèlement

Le CTIE appliquera une politique de **tolérance zéro envers toute forme de harcèlement** qu'il soit d'ordre sexuel ou d'ordre discriminatoire reposant sur la race, la couleur, la religion, le sexe, l'orientation sexuelle, l'âge, l'origine nationale, le handicap, l'état matrimonial, le statut professionnel ou de toute autre nature.

Toute forme de discrimination ou de harcèlement doit être signalée au supérieur hiérarchique ou au service secrétariat et personnel (ressources

humaines) ou à la Commission spéciale en matière de harcèlement, telle que défini par la Loi du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat, telle qu'elle a été modifiée.

2.3. Violence

Le CTIE ne tolérera aucun comportement abusif, hostile ou menaçant envers quiconque sur le lieu de travail et, en conséquence, prendra immédiatement les mesures nécessaires contre les contrevenants. Des mesures disciplinaires et juridiques pourront être entamées.

La possession et l'utilisation d'arme ou de tout autre élément composant pour arme (munitions, par exemple) sont **strictement interdites** sur les lieux appartenant au CTIE. Il est interdit de posséder une arme ou tout autre élément composant pour arme dans son véhicule lorsque celui-ci est dans l'enceinte du CTIE ou est utilisé pour des besoins professionnels.

2.4. Sécurité physique au travail

Le CTIE s'engage à mettre à disposition de l'ensemble de son personnel un espace de travail sécurisé et respectant les dispositions de sécurité environnementales. Pour cela, le CTIE a mis en œuvre et mène des politiques de sécurité physique et environnementale précises (tous les documents applicables sont disponibles sur le site http://www.ctie.etat.lu).

Pour chacun de ses bâtiments, le CTIE a identifié des délégués à la sécurité physique en charge de la gestion de la sécurité physique dans les locaux (les noms et contacts des délégués à la sécurité sont disponibles sur le site http://www.ctie.etat.lu).

L'ensemble du personnel doit s'engager à travailler de manière responsable, sécurisée et dans le respect de l'environnement et à appliquer **les politiques de sécurité** mises en œuvre au CTIE.

Si un membre du personnel pense qu'il y a un risque de sécurité physique, environnemental ou lié à la santé, il doit le signaler à son supérieur hiérarchique ou au délégué à la sécurité physique (sécuritéphysique@ctie.etat.lu) ou encore à la division Sécurité et Audit.

Le CTIE enregistre et conserve les preuves des accidents de travail. Si un membre du personnel est impliqué dans un **accident lié au travail**, il doit immédiatement le signaler à son supérieur hiérarchique et suivre le processus défini pour déclarer les accidents et les blessures.

2.5. Substances illicites, drogues, alcool

Le CTIE s'engage à maintenir un environnement sain et sans drogue pour tout son personnel. Il est interdit de posséder, consommer, échanger, vendre ou fabriquer des drogues illégales (y compris des substances réglementées qui n'ont pas été prescrites par un médecin). Il est interdit d'être sous l'influence d'une drogue ou d'une substance illicite pendant le travail.

Il n'est pas autorisé de servir, de boire ou d'être sous l'influence de l'alcool sur le lieu de travail et pendant l'utilisation d'un véhicule pour des raisons professionnelles. Les seules exceptions où l'alcool peut être servi ou consommé sont lors d'événements externes (conférences, …) ou lors d'événements internes spécifiques, mais uniquement après accord d'au moins un chef de division. Bien que l'alcool puisse être servi à de tels événements, la consommation devra y être entièrement volontaire, soumise à modération, et jamais d'une manière qui pourrait gêner ou nuire au CTIE.

2.6. Trouble du comportement

Si un membre du personnel a, ou est susceptible de présenter, un trouble au niveau de son comportement (exemples : consommation de médicament spécifique affectant la perception ou la réceptivité, migraine aiguë, …), pouvant altérer ses dispositions à mener ses activités professionnelles dans le cadre normal de ses fonctions il doit le signaler à son supérieur hiérarchique, afin de convenir d'un rendez-vous à la médecine du travail.

2.7. Vie privée

Le CTIE enregistre et conserve des renseignements personnels de tous les employés dans le cadre normal de ses activités professionnelles et dans le respect des lois et réglementations en vigueur pour des besoins d'identification et de gestion des ressources humaines ou salariale.

Le CTIE s'engage à mettre en œuvre les mesures de sécurité adéquates pour protéger tous les renseignements personnels des employés qu'il conserve. Pour des besoins de sécurité gouvernementale, mais également pour protéger le personnel et les actifs du CTIE, pour assurer un environnement de travail sain et sûr, et pour pouvoir détecter une mauvaise utilisation des ressources ou des tentatives d'accès non autorisées, le CTIE surveille et conserve les traces de l'utilisation des dispositifs de communication et des systèmes (y compris l'utilisation de l'Internet et de la messagerie électronique), dans les limites fixées par la loi et par la Commission nationale pour la protection des données (CNPD).

En outre, pour autant que la loi et la CNPD le permette, le CTIE se réserve le droit d'inspecter, de surveiller et d'enregistrer l'utilisation de tous les biens de l'entreprise.

2.8. Qualité

2.8.1. Qualité de représentation

L'ensemble du personnel du CTIE s'attachera à véhiculer dans le cadre de ses missions internes et externes, les valeurs de qualité, d'intégrité, de compétences, et de dynamique propres au CTIE.

Au-delà des compétences intrinsèques requises pour lesquelles il est affecté, le personnel du CTIE entretient une relation courtoise, d'écoute, d'analyse et de support et de services aves ses interlocuteurs externes et internes.

Par ailleurs - comme stipulé au paragraphe 4.1 relatif à la Confidentialité – sauf si requis pour des besoins métiers ou des besoins spécifiques liés au statut du membre du personnel du CTIE, le membre du personnel s'engage à un devoir de discrétion et de réserve totale, quant aux informations de fonctionnement interne du CTIE vis-à-vis des acteurs externes avec lesquels il est amené à collaborer.

2.8.2. Qualité d'exécution des travaux

Dans le cadre de l'ensemble de ses activités, le CTIE analyse, conçoit, évalue, développe, met en œuvre et assure la disponibilité, la sécurité, et la pérennité de systèmes d'information complexes et multiples.

Dans ce contexte, il a défini des **standards et normes d'exécution** visant à garantir la qualité, l'opérabilité, la sécurité et l'homogénéité de ces travaux.

Le CTIE s'engage à fournir des prestations de qualité pour l'ensemble des administrations auxquelles il délivre des services et fournitures.

Pour ce faire, le CTIE s'appuie sur des outils, des méthodologies et des processus, applicables notamment **dans les domaines suivants** :

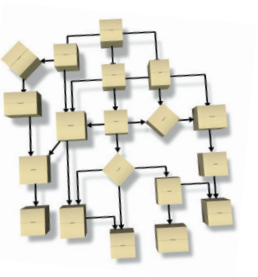
- Démarche qualité pour l'ensemble des projets de technologies de l'information et de la communication déterminée via le référentiel **QUAPITAL-HERMES**, référentiel de gestion de projet (http://extranet.quapital.etat.lu/fr/guide-quapital-hermes/index.html)
- Démarche qualité pour l'élaboration de portails web déterminée via le référentiel **Renow**, référentiel de normalisation pour la présence Web du Gouvernement luxembourgeois
- Démarche qualité pour la gestion, modélisation et optimisation des processus, réglée par **PROMETA**
- Démarche qualité dans le cadre de la gestion des services informatiques (processus standardisés dont notamment les processus de gestion des incidents, des changements, etc.) centralisés au sein d'un seul outil (**solution ITSM**)
- …

Ces éléments sont au cœur de la qualité des services produits par le CTIE, par conséquent l'ensemble du personnel a donc le devoir de les respecter, appliquer et soutenir.

3. Protéger les ressources

3.1. Organisation

3.1.1. Organisation de la sécurité



Un système de gestion de la sécurité de l'information est mis en œuvre au sein du CTIE.
Des groupes de gestion de la sécurité et de gestion des risques, impliquant la direction, sont établis afin d'approuver les politiques de sécurité de l'information, l'attribution des rôles et pour coordonner la mise en œuvre de la sécurité de l'information au sein du CTIE :

La **Division Sécurité et Audit (DSA)** est en charge de la gestion de la sécurité de l'information.

Pour accomplir ses missions, la DSA s'appuie sur les deux leviers suivants :

Le **Comité de Sécurité de l'Information (CSI)** qui est chargé d'assurer :

- l'identification des risques informatiques ;
- la définition et la cohérence d'un cadre de sécurité ;
- le suivi de l'évolution de la sécurité ;
- le suivi des incidents de sécurité et les décisions concernant les mesures de remédiation ;
- la surveillance de l'efficacité des mesures de sécurité ;
- la garantie que des actions de correction et de protection sont prises pour minimiser les risques associés à la sécurité.

Le **Comité de gestion des Risques et Audits (CRA)** qui est chargé d'assurer :

- la gestion des risques (opérationnels relatifs aux systèmes d'information) ;
- le maintien d'une matrice de risques et de contrôles ;
- la gestion des audits internes et externes ;
- la cohérence entre la gouvernance informatique et les objectifs métiers ;
- la conformité vis-à-vis des lois et des réglementations.

Le système de gestion de la sécurité de l'information mis en œuvre suit le modèle de la roue de Deming, le **Plan-Do-Check-Act**.

Ainsi toutes les mesures de sécurité mises en œuvre au CTIE s'inscrivent dans ce cycle et de ce fait supportent une phase de planification, une phase d'implémentation, une phase de contrôle et une phase d'amélioration.

3.1.2. Risques et audits

Le CTIE procède périodiquement à des analyses de risques (initiées par le CRA) qui permettent l'élaboration d'un plan d'action sécurité.

En complément, pour contrôler la mise en œuvre des mesures de sécurité permettant de couvrir les risques, le CTIE (incité par le CRA) se réserve le droit de procéder périodiquement à des contrôles et de commanditer des **audits externes** (sans obligation de prévenir auparavant tout le personnel) de la bonne application du présent Code de Conduite et du cadre de sécurité.

Le personnel fournira toute l'aide nécessaire au bon déroulement de ces évaluations.

Durant celles-ci, il est demandé au personnel du CTIE de préserver autant que possible la confidentialité des informations sensibles autres que celles nécessaires à l'évaluation de la sécurité, sauf si le descriptif de la mission d'audit prévoit explicitement la communication de telles informations.

3.2. Responsabilité de chacun

3.2.1. Ressources informatiques et de télécommunications mises à disposition (ordinateurs, logiciels, téléphones, …)

Les ressources informatiques du CTIE (ordinateurs, imprimantes, téléphones, …) et les fonctionnalités associées mises à disposition des utilisateurs doivent être **utilisées à des fins professionnelles**.

Le CTIE tolère cependant une utilisation privée des ressources en bon père de famille et dans le respect des conditions suivantes :

- l'impact sur les ressources informatiques demeure limité (puissance des processeurs, bande passante, coût engendré, …) ;
- l'utilisation ne perturbe pas les tâches professionnelles ;
- l'utilisation ne viole aucune règle de ce présent Code de Conduite.

3.2.2. Anomalies de fonctionnement et incidents de sécurité

Doit être considéré comme incident de sécurité, toute concrétisation d'un risque qui menace la confidentialité, l'intégrité ou la disponibilité d'une ressource d'information et qui met en péril, selon sa sévérité, le déroulement des activités du CTIE.

Ainsi, les événements ci-dessous ne sont que quelques exemples d'incidents de sécurité :

- copies illégales de logiciels ;
- intrusion physique dans un bâtiment ;
- contournement des dispositifs de sécurité (Firewall, Proxy, Antivirus, …) ;
- logiciels malveillants sur un poste de travail (virus, vers, chevaux de Troie, ...) ;
- perte, altération et fuite d'informations sensibles ;
- vol de matériel ;
- phishing ;
- …

Les incidents de sécurité doivent être rapportés le plus rapidement possible au responsable hiérarchique, et en cas d'absence, au chef de la DSA. Concernant la perte ou le vol de matériel, une déclaration au commissariat de Police doit également être établie dans les délais les plus brefs (pour la perte et le vol de matériel au-delà des frontières du Luxembourg, voir le §3.4.15 - Déplacement à l'étranger).
Lors de la découverte d'anomalies sur un poste de travail, les symptômes et les erreurs doivent être communiqués au Help Desk. L'utilisateur ne doit pas essayer d'enlever le programme suspect.

3.2.3. Port du badge

Toute personne (interne ou externe) doit porter un badge d'identification visuelle dès lors qu'elle se trouve dans les locaux appartenant au CTIE.

3.2.4. Visiteurs

Tout visiteur du CTIE doit être enregistré au moment de son arrivée et à sa sortie du bâtiment.
Pour les bâtiments possédant un système de gardiennage, c'est le gardien qui est en charge de l'enregistrement du visiteur. Pour les bâtiments ne possédant pas de système de gardiennage, c'est la personne en charge du visiteur qui a le devoir d'enregistrer le visiteur.
Tout visiteur doit porter un badge d'identification visuelle (fourni par le gardien ou par la personne en charge du visiteur) et n'est pas autorisé à circuler librement dans les bâtiments. C'est à la personne en charge du visiteur de s'assurer que le visiteur porte correctement le badge d'identification visuelle et que ce dernier ne circule pas librement.

3.2.5. Sensibilisation

Le CTIE s'engage à mener auprès du personnel « interne » une campagne de sensibilisation continue à la sécurité des systèmes d'information. Ainsi l'ensemble du personnel doit être sensibilisé au besoin de sécurité dans les systèmes d'information. La compréhension de ce document constitue une première partie de cette sensibilisation.

3.3. Protection des informations

L'utilisateur doit protéger les informations et les données du CTIE afin d'éviter une divulgation accidentelle ou non autorisée, une mauvaise utilisation, une altération ou une destruction inappropriée.

3.3.1. Classification[1]

Les informations peuvent présenter des degrés divers de sensibilité et de criticité.

Certaines informations peuvent nécessiter un niveau de protection spécial ou une manipulation particulière. Il est donc nécessaire de classifier les documents dont le CTIE est propriétaire et qui sont créés et utilisés pour conduire les activités opérationnelles du CTIE (ainsi, les documents produits en chaîne pour les différentes administrations ne sont pas concernés).

Quelques exemples de documents à classifier :

- procédure ;
- compte rendu de réunion ;
- rapport d'audit ou d'expertise ;
- cahier des charges ;
- document ou dossier d'architecture technique ;
- …

Pour réaliser cette classification, le CTIE définit **trois niveaux de confidentialité** :

Informations publiques

- informations disponibles dans la presse, sur Internet, … ;

[1] La politique de classification menée au CTIE ne se substitue pas aux directives prévues par la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, mais vient compléter son application.

Informations non publiques à usage interne : CTIE USAGE INTERNE

- informations devant être connues par le personnel du CTIE (personnel interne et collaborateurs externes) en fonction de leur besoins métiers (principe du « *need to know* ») ;

Informations non publiques confidentielles : CTIE CONFIDENTIEL

- informations restreintes à un très petit groupe de personnes.

Toute information non publique doit être considérée comme interne ou confidentielle.

Le niveau de confidentialité de toute information doit être connu par les personnes y accédant sous n'importe quelle forme que ce soit (électronique, papier ou orale). Hormis les membres de la direction, seuls les propriétaires de l'information peuvent décider de modifier le niveau de confidentialité de l'information.

Les questions relatives à la classification adéquate de la valeur d'une information doivent être adressées aux propriétaires de l'information ou au responsable hiérarchique.

Sur l'ensemble des documents contenant des informations non publiques doit être inscrit le niveau de classification. Les propriétaires de l'information sont chargés de s'en assurer.

La diffusion vers l'extérieur d'informations à usage interne est interdite, sauf autorisation par les propriétaires. Les informations confidentielles ne doivent pas être divulguées à d'autres personnes que les destinataires prévus.

3.3.2. Bureau

Afin de réduire les risques d'accès non autorisés, de perte et d'endommagement des informations pendant les heures de travail comme en dehors des heures de travail, il est demandé au personnel du CTIE d'adopter une **politique de « bureau propre »**.

Ainsi, chacun a le devoir de ranger les supports d'information (documents papiers, CD-ROM, clés USB, …), contenant des informations non publiques dès lors qu'il quitte son poste de travail.

En outre, pour des raisons de sécurité physique, les membres du personnel du CTIE ne doivent jamais fermer à clé la porte de leur bureau.

3.4. Utilisation des ressources

Les ressources mises à disposition des utilisateurs pour réaliser les tâches professionnelles qui leur sont attribuées sont des biens précieux pour le CTIE et doivent être protégées par tous les utilisateurs.

Pour toute question concernant l'utilisation des ressources, les utilisateurs doivent contacter le Help Desk du CTIE ou leur responsable hiérarchique.

3.4.1. Limites dans l'utilisation des ressources

Il est strictement interdit d'utiliser les ressources de communication du CTIE pour des activités illégales, violant les politiques de sécurité, ou entraînant la responsabilité du CTIE.

Il est **strictement interdit de pratiquer les activités suivantes** :

- utilisation des ressources à des fins qui auraient des caractéristiques offensantes, insultantes, racistes, pornographiques, pédophiles, diffamatoires ;
- utilisation des ressources pour violer les droits de propriété intellectuelle d'autrui ;
- utilisation de logiciels malveillants dans le but de compromettre la sécurité du CTIE.

3.4.2. Postes de travail

Les postes de travail sont des éléments clés du système d'information du CTIE. La modification de la configuration tant logicielle que matérielle et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système d'information du CTIE.

Les postes de travail doivent être utilisés pour accomplir des tâches professionnelles, et en aucun cas à des fins qui pourraient ternir l'image du CTIE.

Il est strictement interdit de tenter de modifier, modifier ou contourner les paramètres de sécurité informatique qui ont été spécifiquement mis en place, comme par exemple : désactiver le logiciel antivirus, modifier les droits d'accès ou encore supprimer les traces d'audit fournies par les systèmes.
Les utilisateurs doivent verrouiller leur poste de travail lorsqu'ils quittent leur place de travail, même momentanément, en activant le blocage d'accès **(+ L ou CTRL + ALT + DELETE)**.

De manière générale, les utilisateurs doivent stocker leurs données sur les serveurs prévus à cet effet (serveurs de fichiers, GED, …) et sont tenus de les épurer régulièrement. Les espaces disques disponibles sur les postes de travail peuvent être utilisés temporairement mais ne doivent en aucun cas être utilisés comme des espaces de stockage. Les informations contenues sur les espaces disques des postes de travail ne sont pas sauvegardées par les systèmes de sauvegarde du CTIE. En outre, en aucun cas, le CTIE ne pourra être tenu responsable de la sauvegarde et de la perte des informations se trouvant sur les postes de travail.

Une utilisation privée des applications installées sur le poste de travail est tolérée, dans la mesure où elle ne constitue pas un abus et notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne viole pas la loi, le cadre de sécurité et les règles établies dans ce présent Code de Conduite.

Il est interdit de modifier la configuration matérielle des postes de travail en retirant des composants ou en installant de nouveaux (par exemple, graveur, disque supplémentaire, lecteur DVD, CD-ROM, modem, ...). Ces actions sont uniquement réservées aux personnes désignées de l'équipe bureautique. Sauf raison professionnelle justifiable, il est interdit de modifier la configuration logicielle des postes de travail en retirant des programmes ou en installant des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source. L'utilisateur modifiant la configuration logicielle de son poste de travail doit agir en bon père de famille et est prié de notifier à l'équipe bureautique un tel acte. Il est rappelé que les logiciels sont soumis à des licences d'installation et d'utilisation. L'utilisateur a pour obligation de les respecter.

3.4.3. Ordinateurs portables

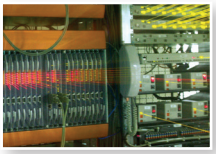
En sus des règles relatives aux postes de travail, les ordinateurs portables utilisés dans le cadre du travail sont soumis aux **règles suivantes** :

- les ordinateurs portables ne doivent être utilisés que par le salarié affecté (cette déclaration ne s'applique pas aux ordinateurs portables spécifiquement désignés, autorisés et documentés pour le partage) ;
- les utilisateurs ayant le besoin professionnel de posséder un ordinateur portable doivent au préalable recevoir une sensibilisation aux risques liés à l'informatique mobile ;
- les utilisateurs d'ordinateurs portables doivent désactiver toutes les connexions sans fil dès qu'elles ne sont plus requises à des fins professionnelles. Ces connexions sans fil incluent, mais ne se limitent pas au WiFi, infrarouge et Bluetooth ;
- les utilisateurs d'ordinateurs portables doivent éviter d'utiliser ceux-ci dans des zones où des personnes mal intentionnées pourraient lire sur l'écran de l'ordinateur ;
- les ordinateurs portables ne doivent pas être laissés sans surveillance dans les lieux publics et ne doivent pas être visibles lorsqu'ils sont laissés sans surveillance dans une voiture ;
- les ordinateurs portables fournis aux membres du personnel du CTIE sont sous la responsabilité de l'utilisateur. Des mesures de protection doivent être prises pour minimiser les risques de vols et d'endommagements lorsqu'ils ne sont pas dans l'enceinte de l'établissement ;

- le télétravail et l'accès à distance aux installations par le personnel du CTIE doivent être réalisés avec les ordinateurs portables fournis et configurés par le CTIE selon les standards de configuration approuvés.

3.4.4. Utilisation des serveurs de fichiers

Les serveurs de fichiers permettent d'enregistrer, de manipuler et de partager une multitude d'informations pouvant parfois être critiques. C'est pourquoi les serveurs de fichiers constituent une ressource clé du CTIE.



En outre, il est demandé à tous les utilisateurs d'adopter une conduite responsable vis-à-vis de l'utilisation de serveurs de fichiers et ainsi de respecter au minimum les règles de bonne conduite suivantes :

- Afin d'éviter toute **fuite de données** :
  - Etre très vigilant quant aux répertoires utilisés pour stocker les données ;
  - S'assurer de connaître les personnes qui disposent d'un accès aux répertoires et aux informations contenues.

- Afin de **ne pas saturer** les serveurs de fichiers :
  - Stocker uniquement ce qui est nécessaire ;
  - Epurer régulièrement les fichiers qui ne sont plus utilisés.

L'équipe bureautique peut être contactée pour plus d'informations sur l'utilisation des serveurs de fichiers.

3.4.5. Utilisation de la GED

L'objectif de la GED (gestion électronique de documents) est d'être le point central de classement, de stockage et d'archivage de l'ensemble du patrimoine informationnel du CTIE. Ainsi, dès sa mise à disposition, tous les utilisateurs devront considérer et utiliser la GED comme outil principal pour entreposer les documents du CTIE.

L'ensemble des règles d'utilisation de la GED sera défini dans un catalogue de procédures et d'instructions de travail. Pour plus d'informations, un manuel d'utilisation de la GED ainsi qu'une équipe de contact seront également mis à disposition des utilisateurs.

3.4.6. Dispositifs informatiques mobiles[2]

Les dispositifs informatiques mobiles comprennent des ordinateurs de poche, assistants numériques personnels (PDA) et téléphones.

Seuls les appareils fournis par le CTIE peuvent être connectés aux ressources du CTIE. Il est interdit à toute personne non autorisée au préalable de connecter sur les postes de travail, sur les ordinateurs portables ou sur le réseau du CTIE, tout dispositif informatique mobile privé.

3.4.7. Manipulation des supports d'information

Tous les supports d'information (mobiles et papier) contenant des informations non publiques doivent être entreposés dans une armoire verrouillée lorsqu'ils sont laissés sans surveillance.

Manipulation des supports mobiles

Les utilisateurs doivent mettre en œuvre les mesures de protection adéquates pour les supports mobiles de stockage (DVD, CD, clés USB, disques durs externes, ...) qu'ils utilisent.
Toutes les informations à usage interne contenues sur des supports mobiles doivent être chiffrées lorsqu'elles transitent en zone publique (hors des locaux du CTIE).
Toutes les informations confidentielles doivent être chiffrées, dès lors qu'elles se situent sur un support mobile. Le chiffrement doit être effectué avec des logiciels fiables et les méthodes de chiffrement doivent être en conformité avec la législation et les règlements en vigueur.
Pour faciliter la mise en œuvre, le CTIE propose aux utilisateurs des solutions de chiffrement et met notamment à disposition des utilisateurs des clés USB chiffrées.

Tous les supports mobiles contenant des informations internes ou confidentielles doivent être complètement effacés ou écrasés (et non simplement supprimés) de manière à rendre l'information qu'ils contiennent irrécupérable, avant leur destruction ou leur réutilisation.
Tous les supports mobiles qui ne sont plus nécessaires doivent être complètement déchiquetés, purgés et/ou détruits (et non simplement jetés) de manière à rendre l'information qu'ils contenaient avant élimination irrécupérable. Des broyeurs de CD-ROM sont disponibles dans les locaux du CTIE.

Manipulation des supports papiers

Tous les supports papiers contenant des informations internes ou confidentielles, qui ne sont plus nécessaires, doivent être complètement

déchiquetés (et non simplement jetés) de manière à rendre l'information qu'ils contenaient avant élimination irrécupérable. Des destructeurs de papiers et des poubelles fermées à clé sont disponibles dans les locaux du CTIE.

3.4.8. Utilisation d'Internet

Internet doit être utilisé pour la recherche et la diffusion d'informations à but professionnel. Une utilisation privée est tolérée, dans la mesure où elle ne constitue pas un abus, et notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne viole pas les autres règles de sécurité et de bonne conduite énoncées dans le présent document. Il est interdit à l'utilisateur de transmettre à des collègues ou à des tiers, à l'extérieur, tout document à caractère indécent, obscène, profanateur, menaçant, frauduleux ou illégal. Il est tenu de signaler immédiatement à son supérieur hiérarchique tout incident relatif à l'usage abusif d'Internet.

Le CTIE se réserve le droit de bloquer, sans préavis, l'accès à certaines catégories de **sites Internet**, notamment ceux **qui représentent un risque** pour lui, comme :

- sites dits à risques (phishing, hacking, …) ;
- sites à caractère pornographique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit ;
- sites qui sollicitent trop fortement les systèmes d'information (par ex. connexion à des sites radiophoniques) ;
- sites de jeux et de paris ;
- sites de réseaux sociaux ;
- sites de transactions financières (notamment les sites boursiers) ;
- sites de messagerie non professionnelle, y compris sites de messagerie instantanée (« chat »).

Il est proscrit de contourner les dispositifs ou le matériel assurant les contrôles de sécurité.

L'utilisateur s'engage à ne pas copier illégalement des logiciels ou des fichiers protégés par un « copyright » (musique, film, ...) et à ne pas diffuser des informations appartenant à des tiers sans leur autorisation.

Il s'engage à mentionner ses sources lors de l'utilisation d'informations. L'utilisateur n'est pas autorisé à s'abonner à des services d'information payants sous le nom et l'adresse du CTIE, sauf autorisation préalable.

L'utilisateur n'est pas autorisé à révéler des informations concernant le CTIE ou ses systèmes d'information sur des forums publics.

L'utilisateur doit être conscient que tout accès à Internet génère des traces au niveau de l'architecture d'accès à Internet.
Ces traces comportent les informations suivantes
:

- date et heure de l'accès ;
- durée de l'accès ;
- volumétrie de l'accès ;
- noms des sites visités et des fichiers transmis ;
- adresses IP source et destination ;
- ports IP utilisés.

Ces données sont stockées pour une durée de six mois. Après cette période de rétention, les informations relatives à la source sont écrasées.

3.4.9. Réseaux sociaux

Lorsque des personnes se rassemblent, il est important que chacun respecte certaines règles de bonne conduite et d'éthique. Les sites de réseaux sociaux n'en sont pas exclus.

L'utilisateur naviguant sur les sites de réseaux sociaux doit être conscient des risques associés à cette pratique et, par conséquent, doit impérativement connaître et respecter les règles suivantes :

- **Etre responsable**
  - L'utilisateur est responsable pour toutes les activités qu'il conduit sur le site et est donc responsable pour tout ce qu'il laisse comme messages, commentaires.
  - Le CTIE se réserve le droit de bloquer, sans préavis, l'accès à la cible en question, à toute personne qui violerait les présentes règles énoncées dans le Code de Conduite.
- **Respecter autrui**
  - L'utilisateur s'engage à ne pas publier des propos intolérants, hostiles, haineux ou tout autre propos diffamatoire. L'utilisateur s'engage également à être courtois.
- **Respecter la confidentialité**
  - L'utilisateur s'engage à ne publier aucune information non publique relative au CTIE ou à son travail au CTIE.

3.4.10. Utilisation de la messagerie électronique

L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est tolérée, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et qu'elle ne viole pas la loi, le cadre de sécurité et les règles établies dans ce présent Code de Conduite.

L'utilisateur doit être attentif à l'absence de garantie relative à l'acheminement, à l'authenticité et à l'intégrité des messages véhiculés par Internet.

Les utilisateurs doivent faire usage d'une extrême vigilance lorsqu'ils reçoivent un e-mail provenant d'Internet avec un fichier attaché ou contenant un lien vers un autre site, surtout si celui-ci est de provenance inconnue ou douteuse, qui pourrait contenir des virus ou des chevaux de Troie.

Les envois de messages par les utilisateurs depuis leur adresse e-mail doivent être accompagnés d'une signature ainsi que d'une décharge de responsabilité standardisée.

En cas d'incapacité à gérer le courrier électronique pendant une durée prolongée, l'utilisateur doit activer la fonction de notification. Afin de minimiser les risques liés à ce type d'action, le CTIE met à disposition des utilisateurs de la messagerie, un message de notification générique. Ce message devra être utilisé par les utilisateurs de la messagerie électronique du CTIE. En cas de doute, quant à l'utilisation du message de notification générique, l'utilisateur peut s'adresser à la DSA. De plus, afin de favoriser la continuité de service durant l'absence d'un ou de plusieurs membres du personnel du CTIE, la Direction du CTIE encourage fortement les équipes à mettre en œuvre des adresses de messagerie électronique génériques.

Il est strictement interdit de transférer des courriers électroniques à caractère professionnel de son adresse professionnelle à son adresse privée. L'utilisateur s'engage à ne pas diffuser des informations qui peuvent porter atteinte à la réputation du CTIE.

Si un utilisateur reçoit un courrier électronique à caractère violent, raciste ou pornographique, il est prié d'en avertir rapidement la DSA. Cette dernière prendra les mesures nécessaires, afin de stopper ces réceptions non sollicitées.

3.4.11. Utilisation des réseaux

Pour renforcer la sécurité des accès à l'information, le CTIE a mis en œuvre plusieurs réseaux informatiques dont l'accessibilité est attribuée et limitée selon les besoins métiers et de la sensibilité des informations pouvant y circuler. En complément, le CTIE a mis en œuvre pour les consultants et les visiteurs un réseau « GUEST » séparé et sécurisé (périmètre d'action très limité). Ce réseau GUEST ne doit pas être utilisé par les membres du personnel interne.
L'utilisation du réseau sans fil doit être limitée aux visiteurs et uniquement aux personnes autorisées.

3.4.12. Utilisation des imprimantes

L'utilisation des imprimantes représente un coût financier élevé et a un impact non négligeable sur l'environnement. L'utilisation des imprimantes est réservée aux besoins professionnels et l'impression de documents ne doit se faire que lorsqu'elle est utile.

L'utilisateur se doit de respecter les autres usagers des imprimantes mais également de veiller à protéger la confidentialité des informations qu'il imprime ; il est demandé aux utilisateurs de retirer les documents imprimés de l'imprimante le plus rapidement possible.

3.4.13. Communication téléphonique

L'utilisation de la téléphonie fixe et mobile est réservée aux besoins professionnels.
Cependant, l'utilisation de la téléphonie à usage privé est tolérée. Les conversations privées doivent rester brèves et se limiter au plus petit nombre possible.
L'utilisation de services payants est interdite, sauf autorisation de la direction.

3.4.14. Protection des ressources à l'extérieur du CTIE

Lorsqu'un utilisateur quitte les locaux du CTIE pour une mission de service, il doit faire preuve de vigilance quant aux ressources et aux informations qu'il transporte.

Ainsi tout utilisateur quittant le CTIE pour une mission de service doit s'assurer au minimum :

- que les informations qu'il transporte sont sauvegardées sur un autre support d'information restant dans les locaux du CTIE ;
- que les informations qu'il transporte correspondent aux besoins de la mission et ainsi éviter de sortir et manipuler des informations inutiles à la mission ;
- que les informations non publiques soient chiffrées ;
- que les ressources et les informations sont conservées en sécurité durant la mission de service (ne pas laisser l'ordinateur portable de manière visible dans une voiture, …).

3.4.15. Déplacement à l'étranger

Lorsqu'un utilisateur est en déplacement à l'étranger, la protection des ressources et des informations est jugée hautement critique.

En sus des mesures de protection des ressources décrites ci-dessus, l'utilisateur doit en plus appliquer les consignes suivantes :

- Éviter de connecter des périphériques externes ou de se connecter à des réseaux qui ne sont pas de confiance ;
- En cas de perte ou de vol de matériel, prévenir au plus vite la DSA et établir une déclaration au commissariat de Police du pays dans lequel l'incident s'est produit ;
- En cas d'inspection par les autorités locales, prévenir au plus vite la DSA ;
- Au retour, ne pas hésiter à changer les mots de passe et à demander une analyse du matériel.

3.5. Accès aux systèmes

3.5.1. Comptes utilisateurs

Tous les utilisateurs reçoivent personnellement un code utilisateur et un mot de passe. Les utilisateurs doivent garder ces informations d'identification confidentielles et ne pas les partager avec une autre personne. Les utilisateurs ne doivent en aucun cas permettre à une autre personne (collègue ou autre), d'utiliser un système ou une application avec leurs identifiants.

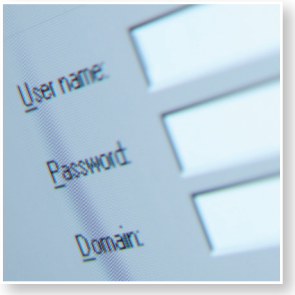
Les utilisateurs sont responsables de l'utilisation qui est faite sur les systèmes avec leurs identifiants. Les mots de passe des utilisateurs ne doivent jamais être écrits.

3.5.2. Authentification

Les utilisateurs doivent respecter les systèmes d'authentification mis en œuvre par le CTIE et en aucun cas essayer de les contourner.
Les utilisateurs ne doivent en aucun cas tenter d'utiliser ou d'accéder à un système/application avec les identifiants d'un autre utilisateur.

3.5.3. Mot de passe

Les utilisateurs doivent choisir leurs mots de passe avec soin. Un bon mot de passe est difficile à deviner et facile à mémoriser. Les mots de passe ne doivent pas figurer dans un dictionnaire et ne doivent pas contenir des informations personnelles comme la date de naissance par exemple. Un bon mot de passe contient des lettres minuscules et majuscules ainsi que des chiffres.



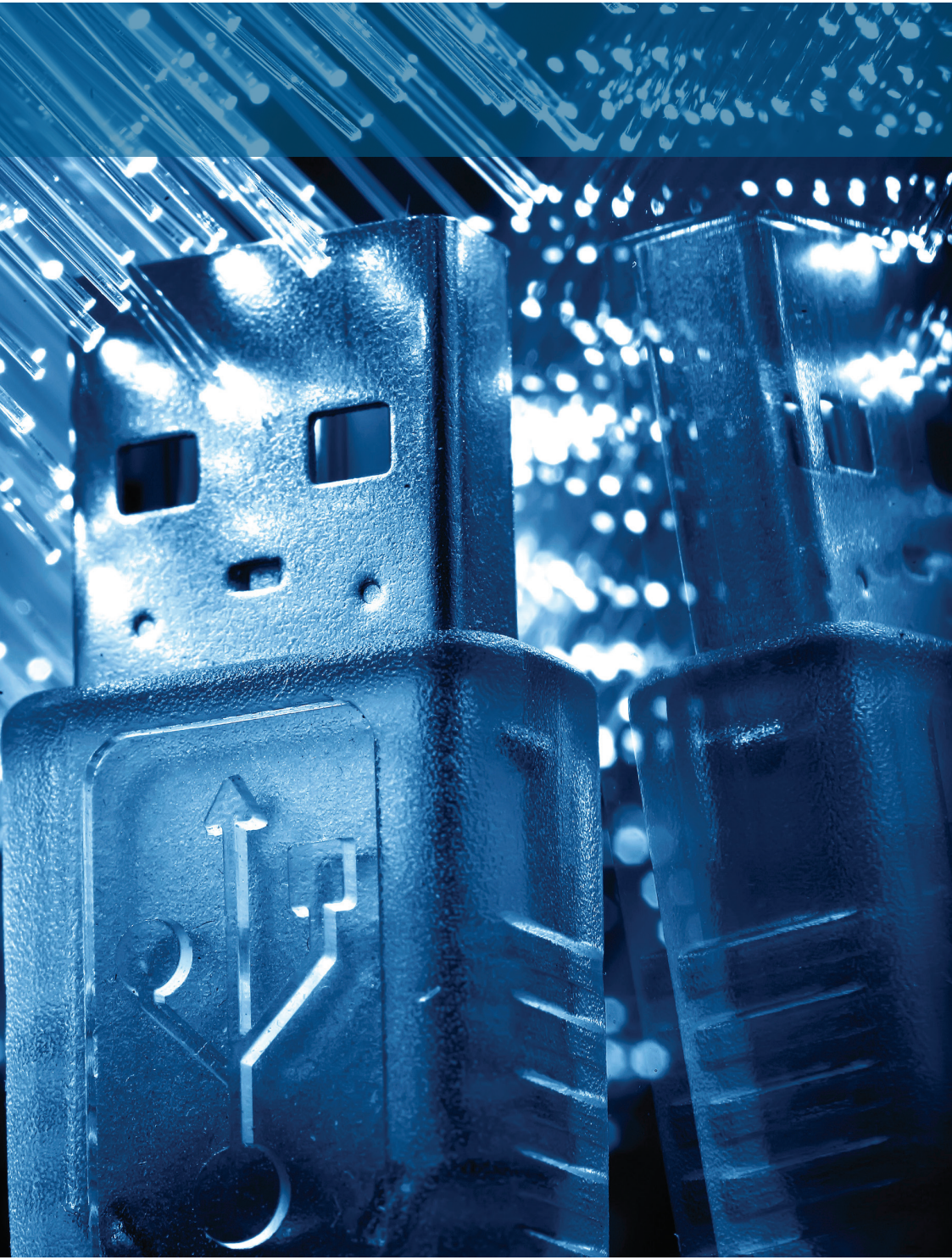
La réutilisation des mêmes mots de passe personnels pour accéder aux systèmes du CTIE et pour accéder à des comptes privés est interdite (par exemple, les utilisateurs ne doivent pas utiliser les mots de passe personnels du CTIE pour s'authentifier sur leur messagerie électronique privée, newsgroup, forums ou pour accéder à des services bancaires en ligne).

3.5.4. Accès à distance (VPN)

Par défaut, il n'est pas permis aux utilisateurs de se connecter aux ressources informatiques internes du CTIE à distance. Les utilisateurs devant se connecter à des ressources informatiques du CTIE à distance pour des besoins professionnels doivent avoir reçu une autorisation formelle de la part de leur chef de division et du chef de la DSA.

Ces utilisateurs doivent avoir reçu une sensibilisation à la sécurité précisant les risques liés aux accès à distance.
Ces utilisateurs doivent obligatoirement utiliser les outils mis à leur disposition, et uniquement ces derniers, pour assurer la connexion à distance.

Les mesures et dispositifs de sécurité mis en œuvre par le CTIE pour assurer la sécurité des connexions à distance ne doivent en aucun cas être contournés ou faire l'objet d'une tentative de contournement.



4. Relations avec l'extérieur

4.1. Confidentialité

Toute information apprise pendant l'exécution de son travail au CTIE qui n'est pas à la disposition du public doit être conservée de manière confidentielle.
Chaque membre du personnel est chargé de protéger la confidentialité des informations et ainsi être prudent lors des conversations, l'utilisation du courrier électronique, et lors de la création, la manipulation, la copie, la télécopie, et l'élimination des informations.

Toutes les politiques et procédures relatives à l'autorisation, l'accès et la manipulation des supports doivent être suivies.

4.1.1. Ingénierie sociale

Le terme d'« ingénierie sociale » désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations par téléphone, courrier électronique, courrier traditionnel ou contact direct de la part de certaines personnes cibles travaillant pour l'entreprise visée.

L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des personnes cibles en se faisant passer pour une personne de cette entreprise, un technicien, un administrateur, etc.

Il est demandé à l'ensemble des personnes travaillant pour le CTIE de faire attention à ce type de pratique. Pour ce faire, il est demandé de respecter **les consignes minimales suivantes** :

- de se renseigner sur l'identité des interlocuteurs en leur demandant des informations précises (nom et prénom, société, numéro de téléphone) ;
- de vérifier éventuellement les renseignements fournis ;
- de s'interroger sur la criticité des informations demandées.

4.2. Relations avec les tiers

4.2.1. Relations avec les administrations

Sauf si requis pour des besoins métiers ou des besoins spécifiques liés au statut du membre du personnel du CTIE, il est interdit de divulguer à des collègues ou des tierces personnes toute ou partie de conversation ou d'information apprise lors de collaboration avec les administrations.

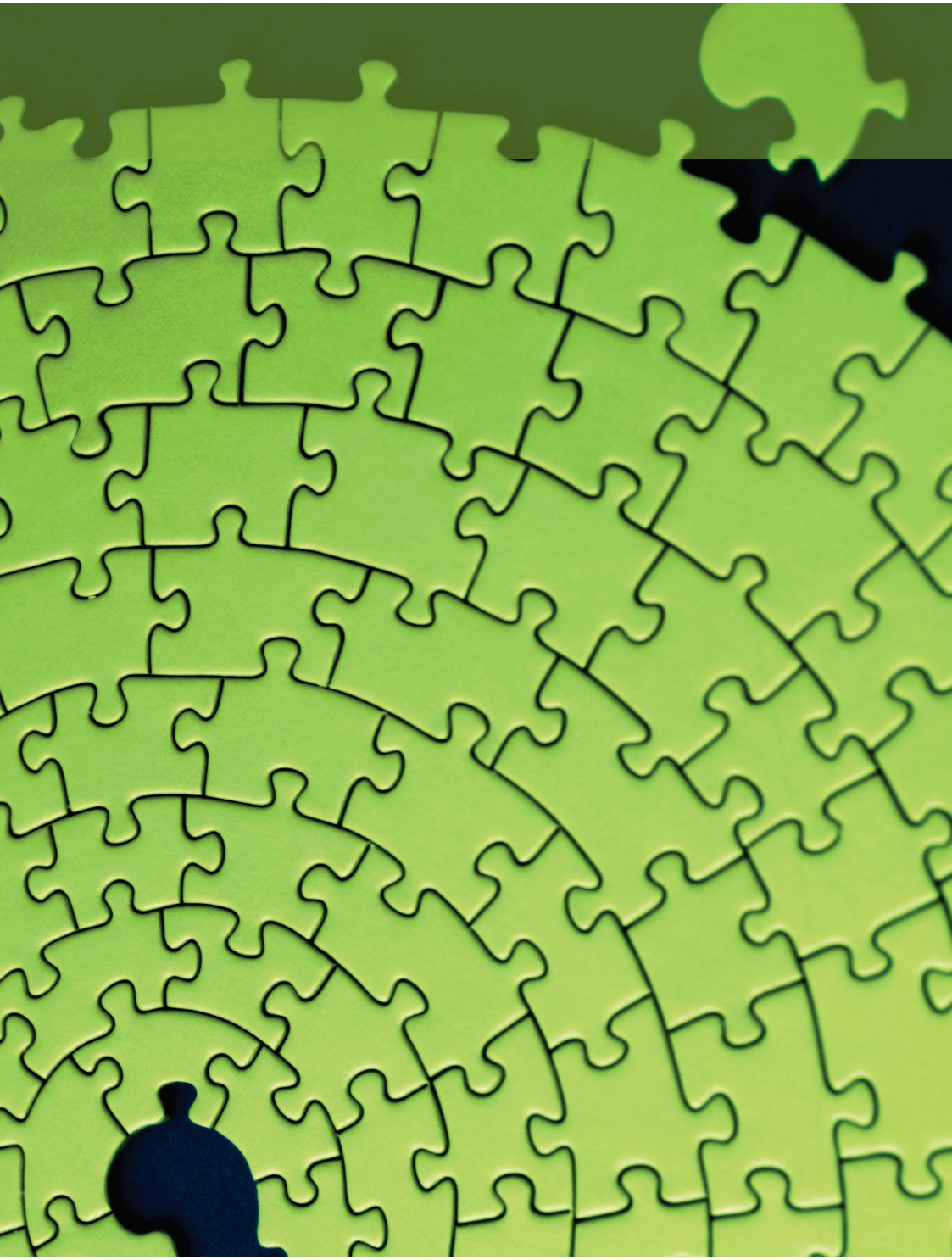
Hormis la protection des communications avec les administrations, chacun a également le devoir de protéger les renseignements concernant les administrations. Ainsi, l'accès, l'affichage, l'utilisation, la modification, le partage ou la distribution des informations concernant les administrations ne sont pas autorisés sans raisons métiers valables.

4.2.2. Relations fournisseurs

Toute personne du CTIE ayant des relations avec un fournisseur de service doit faire preuve de prudence, notamment si elle est impliquée dans le processus de sélection.

Ainsi, les règles suivantes **doivent être respectées** :

- connaître le niveau d'engagement du fournisseur : relation commerciale, engagement par SLA, … ;
- s'assurer que les fournisseurs sont informés de leur obligation de respecter le cadre de sécurité et les méthodes de travail du CTIE ;
- ne jamais divulguer d'informations confidentielles sur le CTIE à un fournisseur ou à quiconque en dehors du CTIE. La divulgation de telles informations doit uniquement se limiter à ce qui est nécessaire et suffisant ;
- ne jamais divulguer d'informations confidentielles sur un fournisseur à un autre fournisseur ou à quiconque en dehors du CTIE. La divulgation de telles informations doit uniquement se limiter à ce qui est nécessaire et suffisant.



5. Conclusion

Il n'est pas possible de décrire toutes les pratiques illégales ou contraires à l'éthique dans le détail. Cependant, les meilleures lignes directrices de bonne conduite restent **la conscience individuelle**, la **considération d'autrui** et **le respect de toutes les politiques du CTIE**, des lois, des règlements et des obligations contractuelles.

La violation de ce présent Code de Conduite, des politiques du CTIE, des procédures, des instructions peuvent entraîner des mesures disciplinaires ou juridiques. Nul ne peut justifier un acte illicite ou abusif en faisant valoir qu'il a été ordonné par quelqu'un.

Les éléments suivants sont des exemples d'actions considérées comme illégales ou inacceptables :

- le vol, l'accès non autorisé, l'utilisation ou la divulgation des dossiers, des données, des ressources ou des informations du CTIE ;
- le travail sous l'influence de l'alcool ou de substances illégales ou l'abus de substances licites ;
- la mauvaise utilisation d'un véhicule de service ou la conduite sous l'influence de drogue ou d'alcool ;
- l'utilisation de tout programme informatique de manière non autorisée ;
- le recours à toute forme de violence au travail, mais aussi à tout acte d'intimidation physique ou d'agression.

Le présent Code de Conduite sera revu et actualisé au moins tous les deux ans. En cas d'amendements, la nouvelle version sera communiquée au personnel selon le même procédé que pour la version initiale.

Suite à toute modification du Code de Conduite, le personnel sera invité à prendre connaissance de la dernière version du document et à confirmer la compréhension des changements survenus ainsi que de leurs effets éventuels.

S'il survient des événements (ex. : modification législative ou détection de nouveaux types d'attaque à la sécurité) ou que l'actualité justifie des modifications urgentes, le comité de direction pourra diffuser des avenants à ce présent document à l'ensemble du personnel.

Ces avenants seront intégrés dans le Code de Conduite lors de sa prochaine révision.

Glossaire

A	**Antivirus**	Logiciel conçu pour identifier, neutraliser et éliminer les logiciels malveillants (dont les virus ne sont qu'un exemple).
	Audit	Inspection et vérification formelle permettant de s'assurer qu'une politique, un standard, une procédure ou un ensemble de principes a bien été suivi, que les enregistrements sont précis ou que les objectifs d'efficience et d'efficacité ont été atteints. Un audit peut être effectué par des groupes internes ou externes.
	Authentification	Procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes informatiques, réseaux, applications...). L'authentification permet donc de valider l'authenticité de l'entité en question.
C	**Compte utilisateur**	Ensemble des ressources informatiques attribuées à un utilisateur. Il ne peut les utiliser qu'en s'authentifiant sur le système avec son nom d'utilisateur et son mot de passe.
	Chiffrement	Procédé utilisé en cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
	Classification	Schéma qui subdivise l'information en catégories comme la criticité, la potentialité de fraude ou la sensibilité, de telle manière que des mesures de sécurité appropriées puissent être appliquées.
	Collaborateur externe	Personne affiliée à une entreprise et travaillant sous contrat pour le CTIE pour une durée déterminée.
	Confidentialité	Propriété d'une information qui ne doit pas être accessible ou divulguée à des personnes, entités ou processus non autorisés.
D	**Disponibilité**	Propriété d'être accessible ou utilisable par une entité autorisée.
	Donnée	Représentation d'une information, codée dans un format permettant son traitement par ordinateur.

	Données à caractère personnel	Toute information concernant un individu. Ces données comprennent le nom, l'adresse, le numéro de téléphone, l'adresse, le numéro de sécurité sociale, le numéro de permis de conduire, les détails personnels des transactions commerciales, ...
G	**Gouvernance IT**	Processus de management fondé sur les bonnes pratiques, permettant à l'entreprise de maîtriser son système d'information dans le but de : • Soutenir ses objectifs de création de valeur ; • Accroître la performance des processus du système d'information et leur orientation clients ; • Maîtriser les aspects financiers du système d'information ; • Assurer que les risques liés au système d'information sont gérés.
I	**Identifiant**	Code technique permettant à un utilisateur de s'identifier auprès d'un système d'information.
	Impact	Mesure de l'effet d'un incident, problème ou changement sur les processus métiers.
	Incident de sécurité	Un ou plusieurs événements liés à la sécurité de l'information indésirables ou inattendus présentant une forte probabilité de compromettre les opérations liées aux activités de l'organisme ou de menacer la sécurité de l'information.
	Information sensible	Information qui, si elle est révélée à des personnes mal intentionnées, peut entraîner la perte ou une dégradation du niveau de sécurité. Elle exige des précautions spéciales pour la protéger contre toute divulgation non autorisée, modification ou suppression.
	Intégrité	Propriété assurant qu'une donnée ne peut être altérée ou détruite d'une manière non autorisée.
M	**Menace**	Tout ce qui peut exploiter une vulnérabilité. Toute cause potentielle d'incident peut être considérée comme une menace. Par exemple, un incendie est une menace pouvant exploiter la vulnérabilité des revêtements de sol inflammables.

P	**Personnel (du CTIE)**	Ensemble des personnes regroupant le personnel interne et les collaborateurs externes.
	Personnel interne	Ensemble des agents de l'Etat (ayant le statut de fonctionnaire, d'employé ou d'ouvrier) et travaillant pour le CTIE.
	Politique de sécurité de l'information	Document définissant des directives relatives à la sécurité de l'information d'une organisation et généralement ratifié par la direction générale ou par des responsables de haut niveau hiérarchique.
	Poste de travail	Elément du bureau qui permet à l'utilisateur d'avoir accès aux ressources et applications accessibles en local ou à distance via le réseau informatique.
	Procédure	Regroupement d'instructions détaillées étape par étape pour accomplir une tâche.
	Propriétaire de l'information	Personne qui crée ou qui provoque la création ou le stockage de l'information. Dans une organisation comportant des unités telles que des divisions, des départements et des sections, le responsable de l'unité devient le propriétaire de l'information.
R	**Ressource**	Toute donnée, quelle que soit sa forme ou son mode d'enregistrement et tout composant lié à l'informatique dont l'entreprise est le propriétaire, héberge ou loue. Exemples : • réseaux et équipements réseaux ; • ordinateurs (serveurs, postes de travail et ordinateurs portables) ; • imprimantes ; • logiciels et applications ; • clés USB, papier, … ; • tout autre équipement informatique ou électronique permettant d'accéder, de stocker, de transmettre ou d'interfacer avec une autre ressource.

Réseau social

Site Web ou application permettant à un individu :

- de construire un profil public ou semi-public au sein d'un système ;
- de définir une liste d'utilisateurs (appelés souvent « contact » ou « ami ») avec lesquels il partage une connexion ;
- et de visualiser et de parcourir les informations saisies par d'autres utilisateurs du système.

Roue de Deming

La roue de Deming est une illustration de la méthode de gestion de la qualité dite «PDCA» (Plan-Do-Check-Act) et constitue un moyen mnémotechnique permettant de repérer avec simplicité les étapes à suivre pour améliorer la qualité (d'un produit, d'un service, de la sécurité) dans une organisation.
La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux :

- *plan* : préparer, planifier (ce que l'on va réaliser)
- *do* : développer, réaliser, mettre en œuvre (le plus souvent, on commence par une phase de test)
- *check* : contrôler, vérifier
- *act* : agir, ajuster, réagir

Risque

Événement possible pouvant causer une déficience, une perte, ou affecter la possibilité d'atteindre des objectifs. Un risque se mesure par la probabilité d'une menace, la vulnérabilité d'une ressource à cette menace et l'impact qu'il aurait s'il se produisait.

S

Sécurité physique

Mise en vigueur d'un ensemble de mesures de sécurité informatique permettant d'assurer la sécurité des personnes dans un centre informatique, ainsi que la protection de l'environnement et des biens informatiques matériels contre toute forme de menace physique, accidentelle ou humaine.

Support mobile

Support de stockage pouvant facilement être transporté. Exemples : clé USB, DVD, CD, bande magnétique, disque dur externe, ordinateur portable, …

Support papier

Support de stockage (non informatique) au format papier. Exemples : document imprimé, archive, post-it

	Standard de sécurité	Exigences minimales et spécifiques destinées à traiter certains risques afin d'être en conformité avec les politiques de sécurité de l'information et les autres standards de sécurité. Ils fournissent une base pour vérifier la conformité aux travers d'audits et d'évaluations. Toutes les divisions doivent respecter les standards de sécurité qui ont aussi pour but de soutenir et de faciliter l'implémentation des politiques de sécurité de l'information.
U	**Utilisateur**	Tout membre du personnel du CTIE faisant appel aux ressources informatiques pour mener à bien ses activités.
V	**Visiteur**	Tout individu ne faisant pas partie du personnel du CTIE et ayant un besoin de pénétrer dans l'enceinte du CTIE.
	Vulnérabilité	Une vulnérabilité est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à la disponibilité, à la confidentialité et l'intégrité des données qu'il contient.

Centre des technologies de l'information de l'Etat

1, rue Mercier
B.P. 1111
L - 2144, Luxembourg
Grand-Duché de Luxembourg

Tél. : (+352) 49925-1
Fax : (+352) 48 23 88
http://www.ctie.public.lu

Spring Conference : The reform of EU data Protection
3 – 4 Mai 2012

Discours du Ministre des Communications et des Médias, François Biltgen
Seul le discours prononcé fait foi

Merci beaucoup Monsieur le Président, c'est en effet un très grand plaisir pour moi de vous souhaiter tous aujourd'hui la bienvenue à cette conférence organisée par notre petite, j'y reviendrai, autorité nationale pour la protection des données. Cette conférence permettra de débattre ensemble pendant deux journées consécutives d'un sujet d'une actualité brûlante, à savoir la protection des données personnelles qui représente une valeur fondamentale de notre société démocratique et un droit fondamental en Europe depuis la mise en vigueur de la Charte des droits fondamentaux avec son article 8 sans oublier l'article 16 du nouveau traité.

Même si je suis en ordre principal Ministre de la Justice, je m'adresse aujourd'hui à vous en ma qualité de Ministre des Communications et des Médias, car au Luxembourg la matière de la protection des données relève non pas des attributions du ministre de la Justice, comme c'est le cas dans d'autres Etats membres de l'Union Européenne, mais appartient au domaine de compétence du ministre des Communications et des Médias.

En effet, lorsque je suis devenu membre du Gouvernement en 1999, d'ailleurs ensemble avec mon ami Henri Grethen, qui a quitté le Gouvernement depuis, lorsque je suis devenu ministre en 1999, le Ministre de la Justice de l'époque, qui se voyait encore toujours confronté à la transposition en droit national de la directive de 1995, s'est adressé à moi et a dit : « Ecoutes, tu es connu dans notre parti comme le « Computerfreak » donc tu t'intéresses certainement à cette matière, est-ce que tu ne veux pas que le ministre de la Justice cède cette compétence au Ministre des Communications et des Médias parce que cela a aussi quelque chose à voir avec le domaine des communications électroniques ». Et c'est ainsi qu'en 1999 j'ai hérité de ce dossier dont je peux bien témoigner parce que je suis peut-être un des hommes politiques de l'Europe qui a une des plus longues expériences dans ce domaine. Effectivement, comme Gérard Lommel le rappelle, j'étais le père de la première législation luxembourgeoise. J'ai fait quelque chose qu'en général on ne fait pas au Luxembourg : j'ai plaidé pour que la législation transposant la directive aille au-delà du niveau de protection prévu par la directive. J'ai essayé de renforcer la législation luxembourgeoise par rapport à l'acquis de la directive. C'est en 2002 que la loi sur la protection des données à caractère personnel a été adoptée et que notre toute petite Commission nationale de la protection des données a été créé.

C'est aussi un avatar de cette discussion que cette équipe reste encore et toujours très, voire trop petite parce qu'à l'époque on ne voulait même pas créer de véritable commission parce qu'on avait encore des difficultés au Luxembourg de comprendre ce système d'autorité indépendante qui depuis lors a quand même aussi trouvé son entrée dans le droit luxembourgeois.

Donc l'équipe voulue toute petite l'est restée mais cette équipe est aussi très efficace. Elle fêtera d'ailleurs ses 10 années d'expériences en automne et je suis sûr que ce ne sera pas le dernier anniversaire qu'on fêtera, vu l'importance croissante que les autorités de protection des données sont appelées à jouer à l'avenir. D'ailleurs, mon amie la commissaire Viviane Reding me dit

toujours : « C'est bien que tu appuies notre initiative parce que ça te forcera aussi de renforcer l'équipe. » Permettez-moi ici devant vous tous de féliciter Gérard Lommel et son équipe de leur travail efficace.

J'ai enfin réussi depuis quelques années à convaincre mes amis au Gouvernement de demander avant toute nouvelle législation un avis préalable à cette Commission, ce qui commence maintenant à se faire, on a d'ailleurs adopté vendredi dernier au Conseil de Gouvernement enfin une modification de la fiche technique qui accompagne tout projet de loi et qui doit désormais renseigner sur la question si le projet a une implication au niveau de la protection des données et si la commission a été demandée en son avis. Et je crois que mes collègues au Gouvernement apprécient tous la proactivité de cette commission qui au lieu de faire traîner les dossiers essaie de donner des avis circonstanciés pour mettre en œuvre des lois efficaces qui tiennent compte d'une façon adéquate de la protection des données. Je crois que suite à la mise en vigueur du nouveau paquet j'aurai peut-être moins de problèmes à demander un renforcement de la commission nationale de la protection des données que je n'avais au moment de sa création.

En effet, vous le savez, vous êtes largement ici pour en discuter, début 2012, donc il y a à peine quelques semaines, la Commission européenne a entamé la révision tant attendue de la législation européenne en matière de protection des données à caractère personnel datant de 95, avec notamment l'objectif de moderniser les règles en vigueur, de renforcer les droits des citoyens, d'accroître la sécurité juridique des traitements de données et de consolider le rôle des autorités nationales compétentes.

Je ne peux que féliciter la Commission pour avoir pris cette initiative ambitieuse car la matière est complexe et les défis sont considérables.

Je peux vous assurer que Viviane Reding trouve en moi et notre gouvernement des défenseurs acharnés de l'entreprise. Je crois que nous aurons des discussions sur des questions de détails mais sur le principe et le choix des instruments retenus - un règlement d'une part et une directive d'autre part, j'y reviendrai, - nous appuyons fortement Viviane Reding et cela pas seulement parce que Viviane Reding et moi, nous sommes issus de la même ville et que nos destins politiques se sont toujours croisés. Ce n'est pas non plus par sympathie à l'égard de Viviane Reding mais pour des raisons de fond que nous appuierons ce paquet.

Mesdames, Messieurs, nous nous situons aujourd'hui au début d'une nouvelle ère, à un moment charnière pour la future orientation de notre société en générale. Dans un monde globalisé où l'évolution technologique est très rapide, où les flux de données connaissent une croissance quasi exponentielle et où les échanges d'informations traversent dans la plupart des cas les frontières, le traitement de données permanent n'est pas l'exception mais plutôt la règle – tant pour les entreprises que pour les citoyens eux-mêmes. On est sur Internet non plus « anywhere, anytime » mais plutôt « everywhere, all the time ».

De cette abondance de données et d'informations qui circulent, il est de plus en plus difficile de faire d'emblée une distinction claire entre celles qui sont sensibles et celles qui ne le sont pas, entre celles qui risquent d'engendrer un impact néfaste sur la révélation de l'identité d'une personne et celles

qui sont anodines d'autant plus que les citoyens semblent être de moins en moins réticents à divulguer sur les plateformes publiques des données personnelles, voire même intimes

Ce qui importe plutôt est le contexte dans lequel les données sont traitées et la finalité de ce traitement, la mise en lien entre différentes données – souvent aussi à l'insu de la personne concernée. L'intérêt ou la sensibilité d'une donnée peut donc changer en fonction du responsable du traitement, en fonction de la finalité, en fonction du contexte, en fonction des risques encourus par le traitement.

Mais ne cachons pas que derrière ces dangers évidents qu'il faut appréhender, derrière ces dangers se cache quand même également une opportunité énorme pour notre économie et pour notre société.

L'exploitation commerciale ou indirectement commerciale des données personnelles est aujourd'hui devenue un élément clé de l'économie numérique. Elle est l'une des sources majeures de financement à travers la publicité ciblée, le marketing viral et les services géolocalisés.

Au Luxembourg, nous avons très tôt reconnu le potentiel de croissance du secteur de nouvelles technologies qui est aujourd'hui un des principaux moteurs de la croissance économique au Luxembourg, et nous avons entrepris de diversifier notre économie qui jusqu'à présent reposait sur le secteur industriel il y a cinquante ans, et sur le secteur des services notamment des services bancaires. Nous avons il y a quelques années, adopté une stratégie de haut débit qui encourage et soutient le déploiement de réseaux et d'infrastructures de communications performants en termes de qualité et de vitesse. Notre objectif est de doter par le « fiber to the home » sans oublier les satellites et d'autres technologies de doter tous les ménages d'ici 2020 d'un débit d'1 GB

La réalisation de cette stratégie est d'ailleurs une des priorités du programme du gouvernement actuel, car l'existence d'une infrastructure à la pointe du progrès est une condition préalable pour garantir la diversification et le développement du secteur des nouvelles technologies de l'information et de la communication. Dans ce contexte, j'aimerais d'ailleurs souligner que les nouvelles technologies de communication et d'information figurent parmi les priorités nationales de la recherche et que notre Université dispose d'un centre renommé pour la sécurité et la confiance dans le monde numérique.

Je peux vous dire que je ne suis pas uniquement Ministre de la Justice, et non pas uniquement Ministre des Communications et des Médias mais également Ministre de la Recherche et de l'Université ainsi que Ministre de la Fonction Publique et de la Réforme Administrative qui héberge notre Centre Technologique de l'Information de l'Etat. Ce qui fait que même si je ne touche qu'un seul traitement, le secret de la richesse du Luxembourg est que les ministres travaillent plus que dans d'autres pays ! J'ai donc plusieurs compétences qui dans le cas qui nous intéresse aujourd'hui se chevauchent très, très bien.

Nos efforts de développement ont été récompensés car au cours des dernières années, le secteur des services liés au stockage, au traitement et à la gestion des données a connu une forte croissance : une vingtaine de centres de calcul (*data centers*) d'une surface totale de près de 40.000

ont été déployés. Le Luxembourg est l'un des rares pays dans le monde pouvant se prévaloir de 3 centres de calcul certifiés Tier4, qui sont le plus sécurisés.

Avec ces infrastructures de pointe, nous disposons au Luxembourg d'une grande expertise en gestion des données. Mais dans le cas de la gestion de données et je viens de citer les data center de très haut niveau, des plus sécurisés, un point nous intéresse particulièrement.

Notre pays veut se démarquer par sa culture de confiance et de sécurité. La sécurisation des données est d'ailleurs un élément clé de notre stratégie en matière de cyber-sécurité que le Gouvernement a adoptée en 2011 et dont la mise en œuvre a été confiée au Cyber Security Board que j'ai l'honneur de présider suite à mon chevauchement de différentes compétences.

Le cyber security board s'est prononcé en faveur d'une politique de sécurité très stricte de protection des données gérées par les autorités publiques, recommandation qui a été entérinée par le Gouvernement. Si dans les années 80 certaines banques de la place financière ont fait de la publicité en avançant l'argument que les comptes étaient très sécurisés et sûrs au Luxembourg aujourd'hui, en matière de technologie de l'information nous voulons faire une politique qui met l'accent sur l'aspect sécuritaire des données. Pour nous ce n'est pas en bradant les données personnelles mais justement en assurant la sécurité des données personnelles qu'on peut développer un secteur qui est bâti sur la confiance.

Voilà pourquoi aussi nous avons mis en œuvre d'ores et déjà un groupe de travail en matière de Cloud computing. Le Cloud computing offre de nouvelles opportunités énormes mais peut comporter un certain nombre de risques potentiels pour les clients. Or Cloud computing n'a pas seulement à faire avec la simple technique mais aussi à faire avec des questions de droit. Une question par exemple qui m'occupe en tant que Ministre de la Justice est de savoir, en cas de faillite d'une société établie au Luxembourg, à qui appartiennent les données qui sont centralisées sur un ordinateur ?

Ce sont des questions très épineuses qui sont très transversales. C'est pour ça que nous avons mis en œuvre un groupe de travail sur le Cloud computing pour nous doter aussi rapidement que possible d'une législation complète permettant de développer le Cloud computing mais permettant de le développer dans la sécurité la plus complète possible.

En effet, le développement de l'économie numérique ne doit pas se faire au détriment des citoyens dont les données personnelles sont au centre des activités des acteurs économiques. Il est indispensable de faire coexister et respecter différents principes et droits fondamentaux pour apporter tant aux citoyens qu'aux entreprises la confiance, la sécurité juridique qu'ils réclament et dont ils ont besoin.

Réussir cet exercice délicat consiste à trouver un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel. Trouver le juste équilibre entre la protection des données personnelles et le besoin d'innovation, entre la nécessité d'accroître la confiance dans l'économie numérique et une certaine simplification de l'environnement légal. C'est donc le grand défi que nous a également confié le traité de Lisbonne et notamment l'article 16.

Je suis en faveur d'une approche pragmatique et moderne et en adéquation avec les droits fondamentaux. C'est pourquoi nous appuyons l'initiative de la Commission Européenne.

Au niveau européen, cette approche se traduit par la nécessité de disposer des mêmes règles dans tous les Etats membres. Ces règles se doivent d'être des plus claires si nous voulons renforcer la protection des données personnelles de tous les citoyens européens tout en établissant un marché intérieur complet en matière d'économie numérique, il faut que chacun sache à quoi s'en tenir - les citoyens aussi bien que les entreprises. Evitons donc des règles trop complexes, divergentes et obscures. La même réflexion vaut pour les citoyens et pour les entreprises.

Voilà pourquoi nous pensons que l'adoption de règles claires et pragmatiques à travers le marché intérieur, associées au « one stop shop » tant pour les entreprises que pour les citoyens, n'apportera que des avantages pour tous les concernés. Il s'agit d'une véritable situation *win-win*. C'est la protection des données personnelles de nos citoyens qui en sortira gagnante avec un même niveau de protection élevé et avec les mêmes droits sur l'ensemble du territoire de l'Union. D'où encore une fois, et je le répète, notre appui à la solution du règlement pour justement établir l'équilibre entre protection des données et libre circulation.

En gardant donc en mémoire le principe « less is more » j'espère qu'on pourra faire émerger une véritable culture de la protection des données. Dans cette nouvelle culture les autorités nationales doivent jouer un rôle clé comme le prévoit le projet de la Commission. La protection des données est devenue un réel sujet de débat dans la société civile, les enjeux quotidiens et la prise de conscience des citoyens augmentée, je m'en félicite.

En conséquence nous devons œuvrer pour doter les autorités de moyens juridiques, financiers et humains adéquats pour leur accorder les instruments juridiques appropriés qui leur permettront d'accomplir les missions complexes avec efficacité et circonspection.

Monsieur le Président Lommel, malheureusement la presse nationale n'est pas ici pour enregistrer ma promesse Mais vous l'avez tous entendue : on va essayer de vous doter de moyens plus efficaces parce que équiper toutes les autorités nationales de la même manière permettra une application efficace et uniforme des règles européennes sur base du principe du pays d'origine tout en permettant une coopération accrue entre les différentes autorités compétentes.

Mesdames, Messieurs, j'ai parlé de l'équilibre entre la protection des données personnelles et la libre circulation des données, j'aimerais toucher quelques mots quant à l'équilibre entre la liberté individuelle et la sécurité publique.

C'est en effet un dossier qui me tient particulièrement à cœur en tant que Ministre de la Justice, un Ministre de la Justice qui a quand même tenu - lorsque la compétence en matière de justice lui a été confiée - de ne plus être, comme son prédécesseur, à la fois Ministre de la Justice et de la Police. Je voulais séparer les deux, justement parce que je suis d'avis qu'il faut toujours avoir une bonne balance entre sécurité et liberté. Je préfère avoir deux ministres qui essaient d'établir cette balance, le Ministre de l'Intérieur qui est responsable de la police et le Ministre de la Justice est responsable de la liberté, et je suis d'avis qu'en matière de balance il faut toujours dire que la sécurité publique

doit constituer l'exception nécessaire - c'est toujours nécessaire - mais doit constituer l'exception par rapport au principe de la liberté individuelle et non pas l'inverse.

C'est pour ça aussi que je peux vous dire que nous appuyons la proposition de la directive de la Commission qui permet justement de fixer pour chaque Etat membre un niveau minimal de protection des libertés tout en donnant aux différents Etats membres la latitude nécessaire pour mettre en œuvre leur politique de sécurité. Avoir des socles minimaux communs, je crois, est très important si nous voulons vraiment mettre en œuvres les dispositions de la charte et du traité.

Les problèmes concrets sont évidents, nous étions un des derniers pays à mettre en œuvre la directive en matière de rétention des données et nous avons essayé de la mettre en œuvre - et c'était peut-être dû au fait que je suis à la fois Ministre des Communications et de la Justice – d'une façon minimaliste, en nous inspirant notamment de l'arrêt du Bundesverfassungsgericht, c'était un peu la chance que nous avions que ce dossier avait trainé aussi un certain temps.

C'est aussi une des raisons pour lesquelles la semaine passée nous n'avons pas appuyé la proposition de la Commission Européenne en matière de PNR européen, parce que nous avons trouvé que la solution proposée n'est pas suffisamment proportionnée, efficace comme elle devrait l'être. Nous avons notamment plaidé pour donner d'avantage de compétences à Europol au lieu d'établir de nouvelles structures et nous avons surtout critiqué la durée de rétention des données.

J'étais peut être un peu long et j'ai peut-être abusé un peu du temps de parole que le Président Lommel m'avait accordé. Mais je voulais saisir l'occasion pour vous faire part de la politique et de l'attitude du Gouvernement luxembourgeois face aux dossiers qui sont en cours de négociation actuellement.

Mesdames, Messieurs, je n'ai qu'à vous souhaiter un très, très bon travail. J'essaierai de rester encore une demi-heure avec vous avant de devoir m'occuper d'autres domaines. Je souhaite aussi au Président Lommel et à sa petite équipe une bonne satisfaction, je sais que vous avez investi énormément de temps et d'énergie dans l'organisation de cette conférence mais je crois que c'est aussi une reconnaissance de vos confrères et consœurs en Europe par rapport à votre travail. Soyez assurés que notre reconnaissance vous l'avez acquise depuis longtemps.

Bon travail !