Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC

État: 15 octobre 2019

Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données

Prise de connaissance et suite de la procédure

Table des matières

1 Résumé

Le 5 septembre 2018, le Conseil fédéral a pris connaissance du rapport final rendu par le groupe d'experts « Avenir du traitement et de la sécurité des données ». Il a chargé le DETEC d'analyser ce document – en particulier les 51 recommandations d'action – jusqu'à mi-2019 en collaboration avec tous les départements concernés, et de lui présenter les éventuels travaux de suivi pour décision en 2019. Le rapport a été préparé par un groupe interdisciplinaire, sous la présidence de l'ancienne conseillère nationale Brigitta Gadient. La majorité des 51 recommandations (31) sont acceptées; souvent, elles coïncident avec des activités ou des projets déjà en cours. 19 recommandations du groupe d'experts ne sont pas poursuivies, entre autres par manque de compétence fédérale, à cause de compétences régaliennes des cantons, des villes et des communes ou en raison de positions déjà publiées du Conseil fédéral ou du Parlement sur ce thème en contradiction avec les recommandations concernées. Dans le cas d'une recommandation, des enquêtes sont en cours, dont les résultats peuvent mener à l'acceptation ou au rejet de cette recommandation.

Les thèmes suivants sont acceptés mais requièrent des travaux supplémentaires. Ils devraient donc être examinés de manière approfondie dans un cadre approprié :

- **Contrats et contenus numériques : Examiner si des adaptations du droit des contrats sont nécessaires, en tenant compte de l'évolution de la situation internationale**
- Examiner la mise en place d'un **système de licences obligatoires sous l'angle de l'accès aux données techniques**
- Elaborer des **normes de sécurité informatiques vérifiables** (par la Confédération, les cantons, les associations professionnelles des TIC) et **instaurer pour les exploitants d'infrastructures critiques une obligation de les observer.**

Le présent rapport du DETEC résume les avis et commentaires des Départements sur les thèmes dont ils sont responsables.

2 Introduction

Le 5 septembre 2018, le Conseil fédéral a pris connaissance du rapport final rendu par le groupe d'experts « Avenir du traitement et de la sécurité des données »[1]. Le document a été préparé durant trois années par ce groupe interdisciplinaire composé de représentants de la communauté scientifique, des milieux économiques et de l'administration. Institué en réponse à la motion 13.3841 du Conseiller d'Etat Paul Rechsteiner, le groupe a été présidé par l'ancienne conseillère nationale Brigitta Gadient. Son rapport compte plus de 190 pages et contient 51 recommandations dans différents domaines concernant le traitement et la sécurité des données. Le 5 septembre 2018, le Conseil fédéral a chargé le DETEC d'analyser d'ici mi-2019 le rapport, en collaboration avec tous les départements concernés, en particulier les 51 recommandations d'action du groupe d'experts « Avenir du traitement et de la sécurité des données », et de lui soumettre en 2019 pour décision les éventuels travaux de suivi nécessaires.

Les recommandations s'adressent principalement à la Confédération et, dans certains cas, aux cantons et aux communes. En décembre 2018, la Direction opérationnelle Suisse numérique GDS, qui fait partie de l'Office fédéral de la communication, a lancé une enquête auprès des départements et de la Chancellerie fédérale. Ceux-ci devaient indiquer s'ils acceptaient ou rejetaient les recommandations les concernant et quelles étaient, à leur avis, les recommandations prioritaires. En cas de rejet, il leur était demandé d'en expliquer la raison. Ce rapport donne un aperçu des avis reçus.

3 Avis de l'Administration fédérale sur les recommandations

La majorité (31) des 51 recommandations du groupe d'experts sont acceptées. Elles coïncident souvent avec des activités ou des projets déjà en cours. 19 recommandations du groupe d'experts ne sont pas poursuivies, entre autres par manque de compétence fédérale, à cause de compétences régaliennes des cantons, des villes et des communes ou en raison de positions déjà publiées du Conseil fédéral ou du Parlement sur ce thème en contradiction avec les recommandations concernées. Dans le cas d'une recommandation (n° 39, Innovation – Démocratie participative), des travaux sont en cours, dont les résultats peuvent conduire à l'acceptation ou au rejet de la recommandation. La numérotation des recommandations ci-après ne préjuge pas de leur importance, mais suit celle des thèmes abordés dans le rapport.

Les sujets suivants sont acceptés par l'Administration fédérale. Leur mise en œuvre requiert toutefois des travaux supplémentaires. Ils devraient être examinés de manière approfondie dans un cadre approprié :

- Recommandation n°15 : La Confédération examine, en tenant compte des développements internationaux, la nécessité d'adapter le droit des contrats aux spécificités des contrats et des contenus numériques : Une fois que les discussions dans l'UE en la matière seront conclues et les résultats des travaux disponibles, il semble judicieux d'examiner si des mesures s'imposent en Suisse.

- Recommandation n°20 : La Confédération examine la création d'un système de licences obligatoires sous l'angle de l'accès aux données techniques.

- Recommandation n°25 : La Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques pouvant être auditées et obligent les exploitants d'infrastructures critiques à les observer.

[1] https://www.efd.admin.ch/efd/fr/home/dokumentation/nsb-news_list.msg-id-72083.html

3.1 Recommandations du groupe d'experts acceptées

N°2 : La Confédération veille, en collaboration avec les cantons, à ce que la technique de cryptage utilisée pour les données sensibles garantisse durablement la sécurité requise en matière d'information. Cette technique est mise à la disposition de tous les utilisateurs publics et privés.

Entités compétentes : DDPS, DFF

Avis DDPS : Acceptation partielle, priorité élevée, activité en cours
Avis DFF : Acceptation partielle

DDPS : Le service spécialisé en cryptologie de la Confédération fait partie de la Base d'aide au commandement (BAC) du DDPS. Grâce à ses contrôles et recommandations en matière de cryptologie, il veille à ce que, pour les données sensibles, des systèmes cryptographiques sécurisés soient acquis. Il prend en considération les éventuelles menaces futures ainsi que la recherche et les développements dans le domaine. Au besoin, il peut également conseiller les cantons et les exploitants d'infrastructures critiques. Il n'était pas représenté dans le groupe d'experts chargé de l'élaboration du rapport, et le rapport n'a pas tenu compte de ses connaissances.

Pour répondre à un besoin de protection élevé, la Confédération recourt déjà à des solutions éprouvées, basées sur les technologies et les recherches les plus récentes. Lorsque de nouvelles exigences apparaissent, le service de cryptologie soutient la conception et le développement de modules cryptographiques sécurisés, en étroite collaboration avec les hautes écoles et l'industrie.

La recommandation relative à un réseau de communications sûr et hautement disponible (voir aussi la recommandation n°3) exige des infrastructures de communications sécurisées par cryptographie. Ces dernières années, la longueur des clés utilisées dans les procédés de cryptage symétriques a été augmentée à 256 bits, à des fins de protection contre les attaques d'ordinateurs quantiques. En effet, dans 10 à 15 ans, les procédés asymétriques actuels ne seraient plus sûrs si un ordinateur quantique de taille correspondante était conçu. Ce problème concerne le monde entier et pas seulement la Suisse. C'est pourquoi des efforts sont déployés un peu partout pour créer et mettre en œuvre des procédés asymétriques de protection contre les ordinateurs quantiques. La probabilité que de nouvelles technologies de cartes à puce supportant ces nouveaux procédés soient disponibles d'ici 5 ans est beaucoup plus grande que celle de voir, dans 10 à 15 ans, un ordinateur quantique capable de décoder les procédés asymétriques utilisés de nos jours. En outre, le service de cryptologie de la BAC veille depuis longtemps à ce que seuls des procédés symétriques avec de grandes longueurs de clé soient utilisés pour protéger les secrets stratégiques à long terme.

DFF ET DDPS : Il n'est pas donné suite à la deuxième partie de la recommandation : « Cette technique de cryptage est mise à la disposition de tous les utilisateurs publics et privés ». Mettre ce genre de technologies largement à disposition d'utilisateurs privés et publics n'est pas simple. D'une part, le traitement des demandes (helpdesk) nécessiterait la mise en place et la gestion d'une infrastructure coûteuse. D'autre part, les technologies de cryptage ne sont utiles que lorsqu'elles peuvent être intégrées dans une infrastructure TIC donnée, ce qui n'est souvent pas le cas avec les ordinateurs personnels d'utilisateurs privés. Il convient aussi de se demander s'il est raisonnable d'implanter des techniques de cryptage dans des systèmes TIC non fiables (comme les ordinateurs personnels justement), car celles-ci peuvent facilement être contournées.

Se posent enfin également des questions d'ordre concurrentiel, réglementaire et de droit des marchés publics. Ainsi, il n'existe ni base juridique ni mandat légal pour une large mise à disposition de technologies et de solutions de cryptage. Il faudrait commencer par les créer.

N°3 : La Confédération examine, en collaboration avec les cantons, les possibilités de mettre à la disposition des utilisateurs publics et privés un réseau de communication sûr et hautement disponible.

Entités compétentes : DFF, DETEC, DDPS

Avis DFF : Acceptation, pas urgent, important
Avis DETEC : Acceptation
Avis DDPS : Acceptation, activités en cours

DFF : Le 21 novembre 2018, le Conseil fédéral a adopté le message relatif à un crédit d'engagement pour un réseau national de données sécurisé. L'objectif du projet est de mettre en place pour la Confédération et les cantons un système de communication efficace en cas de crise. Il convient toutefois de distinguer la mise à disposition d'un réseau de communication sûr et hautement disponible destiné à un usage privé, laquelle devrait être assurée en imposant des obligations et des exigences appropriées aux fournisseurs de services de télécommunication. En effet, le rapport suggère que la performance du réseau devrait devenir une tâche fédérale, alors qu'elle devrait être laissée au secteur privé, comme c'est le cas actuellement.

Acceptation de la recommandation : pas urgent, car à long terme; important

DETEC : La référence faite dans le rapport à la technologie SCION (*Scalability, Control and Isolation on Next Generation Networks*) mérite d'être examinée[2]. Cette tâche pourrait être confiée au nouveau délégué ou à la nouvelle déléguée à la cybersécurité (« M. Cyber / Mme Cyber ») et devrait être prise en charge dans le contexte du Centre de compétences pour la cybersécurité. Il est essentiel de trouver un accord avec les fournisseurs de services de télécommunication.

DDPS : Comme l'explique la BAC, le réseau de conduite suisse doit être à la disposition non seulement des forces armées, mais aussi des organisations civiles remplissant des tâches liées à la sécurité. Des pourparlers sont en cours avec le Réseau national de sécurité (RNS), qui regroupe toutes les organisations et les moyens permettant à la Suisse de faire face aux menaces et aux dangers en matière de sécurité. La sous-stratégie informatique Défense 2012-2025 prévoit que la sécurité des infrastructures informatiques doit être adaptée aux nouvelles menaces. Si la topologie le permet, le réseau de conduite suisse sera co-utilisé.

Pour la Confédération et les cantons, un réseau suisse de données sécurisé sera créé, qui comprendra les composants suivants : RDS (réseau de données sécurisé); système d'accès aux données Polydata; LVS (Système cordonné de suivi de la situation). L'ancien système de communication des données Vulpus doit être remplacé.

D'un point de vue de politique de sécurité, le projet SCION devrait continuer à être observé, et si nécessaire soutenu et développé, en collaboration avec le DEFR – du côté des autorités – et avec les hautes écoles – aux niveaux scientifique et technique. (SCION signifie *Scalability, Control and Isolation on Next Generation Networks* : plus de sécurité sur internet, contrôle des routes, isolation des pannes contre les erreurs de route et de configuration, et informations explicites de confiance pour une communication de bout en bout)

Dans les secteurs public, privé ou technique, de nombreuses prestations dépendent de l'internet mondial. En cas d'attaque majeure de l'internet aujourd'hui, la souveraineté de ce réseau n'est pas assurée à l'échelle nationale. Dans l'internet classique, les expéditeurs et les destinataires n'ont aucun contrôle sur les itinéraires de transport. Au vu de la densité actuelle des réseaux, il conviendrait d'identifier quels services notre pays peut encore fournir sans l'internet (p. ex. support SAP, com-

[2] Rapport d'experts « Avenir du traitement et de la sécurité des données », p. 60

mande de composants matériels, logiciels, etc.). Une connaissance approfondie des chaînes d'approvisionnement est indispensable (fournisseurs de matériel, de logiciels, d'informations, de connaissances, etc.).

N°4 : La Confédération vérifie, en tenant compte des développements internationaux, s'il y a lieu de soumettre la mise sur le marché de composants informatiques au respect de normes ou à l'obtention d'une certification, et si oui dans quels domaines, et définit le cadre juridique nécessaire.

Entités compétentes : DFF, DETEC, DDPS

Avis DFF : Acceptation; important, pas urgent
Avis DETEC : Acceptation
Avis DDPS : Acceptation

DFF : Tâche du Centre de compétences pour la cybersécurité à créer

DDPS : Armasuisse pourrait faire office de centre d'achat et de contrôle. Pour les contrôles et homologations dans le domaine de la cryptologie, le service spécialisé en la matière doit être consulté, en coordination avec le Cyber-Defense Campus d'armasuisse. Quiconque souhaite procéder de manière absolument sûre peut vérifier lui-même la sécurité informatique tout au long de sa chaîne de processus numérisée (*supply chain security*).

N°5 : La Confédération crée les bases légales nécessaires à l'emploi d'identités numériques sûres reconnues par l'État (pour les personnes physiques et morales et pour les infrastructures numériques).

Entité compétente : DFJP; entité intéressée : DFAE

Avis DFJP : Acceptation partielle

DFJP : La recommandation peut être acceptée, à condition que l'identité numérique soit possible uniquement pour les personnes physiques. C'est d'ailleurs exactement ce que prévoit la loi sur l'identification électronique. Dans le monde analogique non plus les personnes morales n'ont pas leur propre identité personnelle, car leurs actions sont toujours induites par des personnes physiques. Elles peuvent être identifiées par une inscription au registre du commerce ou au registre IDE, mais ne peuvent agir indépendamment des personnes physiques. En Suisse, toute personne morale dispose aujourd'hui d'un numéro IDE qui « l'identifie », mais il n'est pas possible d'établir une sorte de carte d'identité numérique, d'autant moins avec des infrastructures numériques. Même les infrastructures analogiques n'ont pas d'identité propre; elles aussi ne peuvent être décrites qu'avec des attributs et, le cas échéant, être inscrites dans des répertoires.

DFAE : Il faut veiller à ce que les besoins des Suisses et Suissesses de l'étranger qui bénéficient de prestations en Suisse soient également pris en considération.

N°6 : La Confédération examine la possibilité d'instaurer, pour autant que l'identification ne soit pas indispensable, des accréditations anonymes (« anonymous Credentials »), en particulier pour les relations entre les particuliers et les autorités, mais aussi comme outil pour les internautes.

Entités compétentes : DFF, DFAE

Avis DFF : Acceptation
Avis DFAE : Acceptation

DFAE : Le DFAE se félicite de la recommandation pour la raison suivante. Les services consulaires sont soumis à un changement constant et profond, auquel ils participent activement avec leur projet à long terme « Développement des services consulaires », qui s'inscrit en parallèle et en complément au groupe de travail AVIS28. De nombreux pans de ce projet concernent l'échange numérique d'informations entre autorités, le transfert numérique d'informations, etc. Il ne sera probablement pas nécessaire dans tous les cas que les autorités connaissent l'identité *complète* des utilisateurs – selon le service, une seule information obligatoire peut suffire, par exemple la citoyenneté du client qui obtient une information sur les visas. Selon nous, cette possibilité est offerte par les accréditations anonymes.

N°7 : La Confédération veille à la constitution d'un réseau national visant à promouvoir la recherche dans les domaines de la transformation numérique, en donnant la priorité à la sécurité de l'information, et du transfert de connaissances entre la recherche et l'économie.

Entités compétentes : WBF, Conseil des EPF, innosuisse, entité intéressée : DFAE

Avis DEFR : Acceptation
Avis DDPS : Acceptation

DEFR : Le Fonds national suisse (FNS) vient de lancer le « Programme national de recherche (PNR) 77 « Transformation numérique" » sur mandat du Conseil fédéral. Ce programme vise à examiner les interdépendances et les effets concrets de la transformation numérique en Suisse. Ses trois axes sont l'éducation et l'apprentissage, l'éthique, la fiabilité et la gouvernance, ainsi que l'économie et le marché du travail. Il s'étend sur 5 ans et dispose d'un budget de 30 millions de francs.

Innosuisse soutient également les réseaux thématiques nationaux (RTN) dans le but de stimuler le transfert de connaissances et de technologies. En particulier, l'un des dix réseaux actuels – *Swiss Alliance for Data-intensive Services* (data+services) – s'engage à promouvoir la coopération entre les entreprises innovantes et les hautes écoles qui combinent leurs connaissances dans des domaines en lien avec les données tels que l'informatique, l'intelligence artificielle, le commerce et la psychologie et qui les développent en produits et services commercialisables.

DDPS : Dans le cadre du plan d'action du DDPS pour la cyberdéfense, des activités sont déjà en cours, qui vont dans le sens de la recommandation des experts. Le Cyber-Defence Campus d'armasuisse S+T est en cours de création avec les deux sites supplémentaires EPFZ (T3-2019) et EPFL (T2-2019). La coopération avec les partenaires de recherche, l'industrie et les fournisseurs de services est ancrée dans le Cyber-Defence Campus. Ce Campus met en place un réseau national de recherche dans le domaine de la cyberdéfense.

N°8 : La Confédération s'engage en faveur du renforcement de l'autodétermination en matière d'information, encourage notamment les technologies respectueuses de la sécurité des données et, dans le cadre du droit de la protection des données et en dehors, examine la pertinence d'approches complémentaires ainsi que d'autres approches en tenant compte des développements internationaux et du progrès technique.

Entités compétentes : DFJP, PFPDT, DFAE

Avis DFJP/OFJ : Acceptation
Avis PFPDT : Acceptation

DFJP : Cette recommandation concerne une tâche permanente que l'OFJ accomplit déjà. Elle est largement suivie dans le cadre de la révision totale de la loi sur la protection des données. Le projet du Conseil fédéral (P-LPD) prévoit, entre autres, le principe de la protection des données dès la conception *(privacy by design*), la promotion de l'autorégulation dans le domaine de la protection des données par des codes de conduite et une certification volontaire à l'échelle de la branche, ainsi que l'augmentation de la transparence du traitement des données. Le P-LPD tient particulièrement compte de l'évolution de la situation dans l'UE et au Conseil de l'Europe. Le Conseil fédéral veut faire en sorte

que la Suisse puisse ratifier le plus rapidement possible la convention STE 108 modernisée du Conseil de l'Europe sur la protection des données. En outre, les développements internationaux dans le domaine de l'intelligence artificielle sont suivis de près par un groupe de travail interne à l'administration fédérale.

Toutefois, nous ne pouvons pas soutenir ni comprendre toutes les « mesures complémentaires s'inscrivant dans le cadre traditionnel de la protection des données » proposées dans le rapport du groupe d'experts « Avenir du traitement et de la sécurité des données ». En particulier, l'assouplissement (proposé dans le cadre de l'approche dite « du bac à sable ») du principe de la finalité nous semble problématique pour la protection des données.

N°10 : La Confédération et les cantons adaptent les pouvoirs et les ressources des autorités de protection des données de manière à leur permettre d'accomplir pleinement et efficacement leurs tâches légales de sensibilisation, de conseil et de surveillance.

Entités compétentes : DFJP, PFPDT

Avis DFJP : Acceptation partielle
Avis PFPDT : Acceptation

DFJP :

Confédération : Le Conseil fédéral a déjà largement tenu compte de cette recommandation dans son message sur la révision totale de la LPD. D'une part, le P-LPD renforce les compétences du PFPDT, qui disposera de pouvoirs d'enquête accrus et pourra prendre des décisions directement contraignantes, au lieu d'une recommandation (art. 44 et 45 P-LPD). Le Conseil fédéral estime cependant que le PFPDT ne devrait pas (du moins à l'heure actuelle) être habilité à infliger des sanctions (voir toutefois le postulat 18.4100 de la Commission des institutions politiques du Conseil national « Régime général de sanctions administratives pécuniaires », dont le Conseil fédéral recommande l'adoption). D'autre part, le PFPDT devrait obtenir davantage de ressources. Etant donné que le P-LPD introduit une série de mesures impliquant de nouvelles tâches pour le PFPDT (p. ex. consultation sur les analyses d'impact en matière de protection des données), le Conseil fédéral est d'avis que celui-ci a besoin de plus de ressources en personnel et en moyens informatiques. Selon le message sur le P-LPD, les besoins supplémentaires en personnel du PFPDT sont estimés à dix postes. Le Conseil fédéral propose que les ressources en personnel soient octroyées progressivement et réévaluées au plus tard cinq ans après l'entrée en vigueur de la loi. Leur financement devrait être possible en partie par des émoluments. Toujours selon le message sur le P-LPD, le PFPDT a également besoin de moyens informatiques additionnels (FF 2017 6565, 6789 ss.). Une part de ces ressources (trois postes) doit être attribuée au PFPDT en 2020 déjà, en lien avec la nouvelle loi fédérale sur la protection des données dans le cadre de l'application de l'acquis de Schengen en matière pénale.

Cantons : Etant donné que, en vertu de la Constitution fédérale (art. 47, al. 2, Cst.), les cantons sont autonomes en matière d'organisation, l'allocation de ressources à l'autorité de surveillance de la protection des données relève essentiellement de leur compétence; la marge de manœuvre de la Confédération est limitée. Toutefois, les cantons sont soumis à des exigences minimales qui découlent de l'art. 37 LPD, du protocole additionnel à la convention STE 108 du Conseil de l'Europe sur la protection des données et de la directive UE 2016/680 relative à la protection des données en matière pénale. La convention STE 108 modernisée du Conseil de l'Europe sur la protection des données, que la Suisse n'a pas encore ratifiée, oblige également (si nécessaire) les cantons à renforcer les compétences et les ressources affectées à la surveillance de la protection des données.

PFPDT : Le message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017 6565ss) indique explicitement que le PFPDT a besoin de personnel supplémentaire. D'autant plus qu'avec le développement de la numérisation, le PFPDT s'est vu confier de plus en plus de tâches, indépendamment du projet de révision

(voir p. 6788 du message). Dans son 26e rapport d'activité 2018/2019, le PFPDT lui-même souligne que la densité des contrôles est faible. De même, il a été recommandé à la Suisse, dans le cadre de l'évaluation Schengen, d'allouer des ressources financières et en personnel suffisantes au PFPDT afin qu'il puisse remplir toutes ses tâches en la matière. Certes, le PFPDT a reçu trois postes supplémentaires dans le cadre de la LPD de Schengen, qui est entrée en vigueur le 1er mars 2019, mais il n'est pas certain qu'il se verra attribuer les postes nécessaires à l'accomplissement des autres tâches prévues dans le P-LPD. En outre, la loi Schengen sur la protection des données, qui confère de nouvelles tâches au PFPDT, est entrée en vigueur le 1er mars 2019, sans qu'il soit certain que le PFPDT recevra les postes supplémentaires nécessaires. Dans ces conditions, il n'est pas possible pour le PFPDT de mener à bien l'ensemble de ses tâches et l'échelonnement proposé du processus n'est nullement approprié.

N°11 : La Confédération crée, en collaboration avec les cantons, des formes de coopération entre autorités de surveillance de la protection des données (centre de compétence, par ex.).

Entités compétentes : DFJP, PFPDT

Avis DFJP : Acceptation
Avis PFPDT : Acceptation

DFJP : Nous attirons l'attention sur le catalogue des tâches du PFPDT, inscrit à l'art. 52 P-LPD, en vertu duquel le PFPDT est notamment tenu de collaborer avec les autorités cantonales chargées de la protection des données (al. 1, let. b).

PFPDT: Il y a aujourd'hui déjà l'association « privatim » (Conférence des préposés cantonaux à la protection des données). En tant que membre associé, le PFPDT a le droit de participer aux séances du Bureau avec voix consultative.

Une collaboration existe également dans le cadre du Groupe de coordination des autorités suisses de protection des données dans le cadre de Schengen. Ce groupe est composé d'un représentant de chaque autorité de protection des données cantonales ainsi que d'un représentant du PFPDT, qui en assure le secrétariat.

N°12 : La Confédération vérifie, dans l'optique de la protection et de la sécurité des données, s'il y a lieu d'instaurer des paramétrages par défaut conformes aux exigences de la protection des données, conformément aux développements internationaux et compte tenu du potentiel de risque et des domaines d'application.

Entités compétentes : DFJP, DEFR, DFAE

Avis DFJP : Acceptation
Avis DEFR : Acceptation
Avis DFAE : Acceptation

DFJP : Dans le domaine de la législation sur la protection des données, cette recommandation sera mise en œuvre par le biais dans le cadre de la révision totale de la LPD. Le projet du Conseil fédéral ancre les principes de la protection des données dès la conception et par défaut (*Privacy by Design and by Default*) dans l'art. 6 P-LPD. En outre, l'art. 12 P-LPD prévoit que les fabricants de systèmes ou de programmes de traitement des données, ainsi que les responsables du traitement des données et les mandataires assurant le traitement des données peuvent faire certifier volontairement leurs systèmes, produits et services. En revanche, le P-LPD ne réglemente pas les exigences en matière d'autorisation de mise sur le marché.

DEFR : Ce principe est prévu à l'art. 6 P-LPD. En outre, il est manifestement déjà souvent appliqué de manière volontaire en Suisse.

DFAE : Acceptation de la recommandation.

N°15 : La Confédération examine, en tenant compte des développements internationaux, la nécessité d'adapter le droit des contrats aux spécificités des contrats et des contenus numériques.

Entités compétentes : DFJP, DFAE

Avis DFJP : Acceptation
Avis DFAE : Acceptation

DFJP : Une fois les travaux et les discussions en la matière terminés dans l'UE, il faudra examiner si une intervention est nécessaire en Suisse.

N°20 : La Confédération examine la création d'un système de licences obligatoires sous l'angle de l'accès aux données techniques.

Entité compétente : DFJP

Avis DFJP (IPI) : Acceptation

IPI : L'accès aux données techniques peut être complexe ou trop coûteux pour les PME, les universités ou la société civile. En outre, certains détenteurs de très grandes et volumineuses collections de données peuvent abuser de leur position sur le marché. Dans ces situations, les obstacles à l'accès, à l'utilisation et à la réutilisation des données sont des obstacles au développement économique, scientifique et social. C'est pourquoi la Commission européenne a publié une série d'études intitulée « *Data Economy Package for non-personal data* », dont l'objectif est de garantir la libre circulation des données technique dans le marché intérieur. Elle est parfois perçue comme étant pratiquement la cinquième liberté fondamentale de l'Union. L'élaboration d'un système de licences obligatoires compte parmi les propositions qui ont été examinées pour assurer la libre circulation des données. Cette institution juridique est bien connue en droit de la propriété intellectuelle et en droit antitrust et couvre un large éventail de réalités. Il s'agit d'un thème sensible, notamment en ce qui concerne l'Accord concernant les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord ADPIC).

Un système de licences obligatoires n'est pas la seule solution recherchée par la Commission. Celle-ci a notamment proposé d'établir un ensemble de règles contractuelles non contraignantes pour les contrats B2B (*business to business*) lors de l'octroi de droits d'accès, d'utilisation et de réutilisation des données, ou de promouvoir une culture des données ouvertes (*open data*). Le problème est le même pour la Suisse que pour l'Union européenne. Plusieurs solutions identifiées par la Commission pourraient intéresser notre pays. Nous recommandons donc que ce mandat soit accepté pour autant qu'il soit reformulé afin de fournir un cadre de recherche plus large : « Accès aux données techniques : Analyse de la situation actuelle et identification de solutions possibles ». Cela permettra au mandat de s'appuyer sur les résultats des travaux de l'UE sur le *« Data Economy Package for non-personal Data »* et de tenir compte des évolutions internationales.

N°21 : La Confédération complète la législation sur la protection des données par des dispositions régissant la portabilité des données, en tenant compte des évolutions observées sur le plan international.

Entité compétente : DFJP

Avis DFJP : Acceptation

DFJP : (Réserve : conformément au mandat du Conseil fédéral du 9 mai 2018). Le droit à la portabilité des données prévu par le règlement général de l'UE sur la protection des données 2016/679 n'est pas prévu dans le P-LPD du Conseil fédéral. Le Conseil national devra se prononcer sur l'introduction d'un tel droit dans le projet de révision lors de la session d'automne 2019 sur la base d'une proposition de majorité de la commission. En outre, le 9 mai 2018, le Conseil fédéral a chargé l'OFJ d'analyser le besoin de réglementation pour introduire la portabilité des données selon le secteur ou la branche et de soumettre d'éventuelles propositions de modalités juridiques au Conseil fédéral au plus tard mi-2020. Ce délai permet de se référer aux premières expériences faites dans l'UE avec l'instrument de la portabilité des données ainsi qu'aux résultats du débat parlementaire sur la révision totale de la LPD. Contrairement à ce qu'indique le rapport du groupe d'experts « Avenir du traitement et de la sécurité des données », nous estimons qu'il faudrait également envisager d'autres solutions que le rattachement de la portabilité des données au droit d'accès prévu par la législation sur la protection des données.

N°25 : La Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques pouvant être auditées et obligent les exploitants d'infrastructures critiques à les observer.

Entités compétentes : DFF, DDPS, DETEC

Avis DFF : Acceptation; urgent, important
Avis DDPS : Acceptation; activités en cours
Avis DETEC : Acceptation

DFF, DDPS, DETEC : L'élaboration de normes de sécurité vérifiables en matière de TIC s'effectue dans le cadre des projets définis par le plan de mise en œuvre de la SNPC en étroite collaboration avec les offices spécialisés. Pour ces travaux, le standard minimum pour l'amélioration de la résilience des TIC de l'OFAE est pris en compte. Le Centre de Compétence Cyber Sécurité coordonne les travaux. Toutefois, il reste à voir comment les exploitants d'infrastructures critiques seront obligés de se conformer à ces normes, et comment le suivi et la surveillance du respect de ces normes seront effectués. Il sera peut-être nécessaire d'adopter une nouvelle législation sectorielle.

N°26 : La Confédération crée un centre de compétence (ou un service rattaché à un centre de compétence en matière de cybersécurité) chargé des questions de normalisation dans le domaine de la sécurité informatique.

Entités compétentes : DFF, DDPS

Avis DFF : Acceptation; urgent, important (sans justifications)
Avis DDPS : Acceptation; priorité élevée

DDPS : L'idée adoptée par le Parlement de créer un centre de compétences devrait se concrétiser en 2019 (sur la base de MELANI). Un Délégué à la cybersécurité de la Confédération a été nommé en juin 2019[3]. Celui-ci rend compte directement au chef du DFF. Pour le centre de cyberdéfense rattaché au DDPS, une coopération étroite avec le poste nouvellement créé sera importante et permettra de coordonner au mieux les contenus en vue de la mise en œuvre de la stratégie nationale.

[3] https://www.efd.admin.ch/efd/fr/home/dokumentation/nsb-news_list.msg-id-75421.html

N°27 : La Confédération encourage, en étroite collaboration avec les associations faîtières, les associations de branche, les associations de prestataires de services informatiques et les entreprises intéressées, le lancement de programmes d'amélioration de la sécurité de l'information dans l'économie.

Entités compétentes : DFF, DEFR

Avis DFF : Acceptation; urgent, important
Avis DEFR : Pas d'avis

EFD : L'amélioration de la sécurité de l'information dans l'économie est un objectif stratégique de la SNPC. La mise en œuvre des mesures 8, 9, 13 et 29 permettra d'atteindre cet objectif.

N°28 : La Confédération soumet les exploitants d'infrastructures critiques à une obligation de notifier les cyberincidents. Elle élabore la base légale nécessaire à cet effet en collaboration avec les autorités compétentes, l'économie privée et les associations concernées, compte tenu également des développements internationaux en la matière.

Entités compétentes : DFF, DEFR, DDPS, DFAE

Avis DFF : Acceptation, activités en partie en cours
Avis DDPS : Acceptation; priorité élevée, activités en partie en cours
Avis DFAE : Acceptation

DFF : Les régulateurs concernés devraient également être consultés sur la recommandation; des clarifications sont en cours (voir Plan de mise en œuvre[4] de la Stratégie nationale de protection de la Suisse contre les cyberrisques – SNPC).

DDPS : Les signalements des cyberincidents sont importants pour dresser un tableau de la menace. Les signalements se font aujourd'hui sur une base volontaire. La SNPC traite de cet aspect avec la mesure 9 « Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction ». Les signalements importants en terme de stratégie ou de politique de sécurité devront être traités au niveau du Groupe Sécurité et, le cas échéant, de la Délégation pour la cybersécurité (Délégation Cyber) du Conseil fédéral.

DFAE : Le DFAE est concerné dans tous les cas qui présentent une composante diplomatique, stratégique ou relative à la politique en matière de sécurité. Ces cas doivent être traités au sein du Groupe Sécurité (et de la Délégation du Conseil fédéral pour la sécurité – Délséc); par conséquent, les organes du Groupe Sécurité doivent être directement impliqués dans l'aménagement de l'obligation de notifier (au DFAE, le SIS assure, en tant qu'entité responsable des organismes de politique de sécurité, l'échange d'informations à l'interne, en particulier avec le bureau de sécurité sur le cyberespace pour ce qui est des tendances et des conséquences sur la politique étrangère de la Suisse en matière de sécurité, et avec la DDIP pour les questions et développements de droit international)

Avis supplémentaire DFJP/OFJ : Nous tenons à souligner que si la recommandation 28 est mise en œuvre, l'obligation générale de signaler les violations de la sécurité des données nouvellement prévue dans le P-LPD (art. 22) devrait également être prise en compte : en cas de violation de la sécurité des données (voir définition art. 4, let. g, P-LPD), s'il existe un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, le responsable du traitement des données doit l'an-

[4] https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/umsetzungsplan.html; https://www.isb.admin.ch/isb/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-70482.html

noncer au PFPDT le plus rapidement possible. Dans certaines circonstances, il doit également informer les personnes concernées, afin que celles-ci puissent prendre elles-mêmes des mesures pour protéger leurs données.

N°29: La Confédération veille, en collaboration avec les cantons, l'économie et les instituts de recherche, à ce que le développement de MELANI débouche sur la création d'un centre national de prévention et de gestion des cyberincidents (par ex. sous la forme d'un service rattaché à un centre de compétence en matière de cybersécurité, cf. recommandation 26).

Entités compétentes: DFF, DFAE

Avis DFF: Acceptation, activités en cours
Avis DFAE: Acceptation

DFAE : Le DFAE (SIS) et/ou le Groupe Sécurité doivent absolument être impliqués afin d'assurer la congruence entre la direction de la politique de sécurité et les organes s'occupant de cybersécurité (en particulier le service spécialisé en cybersécurité).

N°31 : La Confédération mène un débat de politique de sécurité portant spécifiquement sur la cybersécurité et visant à déterminer si et, le cas échéant, dans quelle mesure la Suisse doit développer ses propres moyens de défense ou établir d'étroites coopérations avec d'autres États. La question de la cyberrésilience doit être au cœur de ce débat.

Entités compétentes : DDPS, DFAE

Avis DDPS : Acceptation, activités en cours
Avis DFAE : Acceptation

DDPS : Le débat nécessaire de politique de sécurité sur la cyberdéfense et sur les possibilités de coopération avec l'étranger devra être mené au niveau de la Délégation Cyber ou du Groupe Cyber nouvellement créés par le Conseil fédéral (avec la participation du DFAE).

DFAE : Le rapport traite du débat sur la politique de sécurité ainsi que de la coopération avec d'autres Etats. La participation du DFAE et des responsables de la politique de sécurité (Groupe Sécurité/Délséc et DDPS, DFJP, DFAE) à cette discussion est impérative (au moins traitement préalable dans le Groupe Sécurité et Délséc).

N°32 : La Confédération prend les mesures nécessaires pour que l'armée et l'administration militaire soient à même de mettre à la disposition des autorités civiles, à titre subsidiaire, des moyens relevant du cyberespace et permettant de soutenir les exploitants d'infrastructures critiques lors de situations extraordinaires.

Entité compétente : DDPS; autre entité intéressée : DFF

Avis DDPS : Acceptation, activités en cours

DDPS : Pour pouvoir remplir sa mission à tout moment, l'armée doit protéger ses systèmes informatiques contre les cyberattaques. Afin qu'elle dispose des instruments nécessaires à sa propre protection, le Conseil fédéral a fixé dans une nouvelle ordonnance[5], lors de sa séance du 30 janvier 2019, l'organisation et les compétences pour garantir la sécurité militaire dans le cyberespace. L'ordonnance est entrée en vigueur le 1er mars 2019. Toutefois, l'armée n'a aucune responsabilité globale pour la

[5] Ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (OCMil), RS 510.921

Suisse dans le domaine de la cybersécurité; cette ordonnance ne lui confère que des pouvoirs d'autoprotection et d'autodéfense. Elle décrit cependant en détail comment l'armée suisse exerce son autoprotection et son autodéfense dans le cyberespace. Elle réglemente également les tâches du Conseil fédéral et de la personne à la tête du DDPS, et contient des dispositions d'exécution dans les domaines de l'engagement, de l'instruction et de la recherche.

À ce sujet, il convient de relever les deux points suivants de la motion Dittli 17.35076, adoptée en mars 2018 :

- apporter un soutien subsidiaire aux exploitants d'infrastructures essentielles;
- apporter un soutien subsidiaire aux autorités civiles de la Confédération et des cantons en matière de cybercriminalité.

La mesure 24 de la SNPC prévoit la garantie de la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et la réglementation de son rôle subsidiaire consistant à appuyer les autorités civiles.

DFF : Concertation nécessaire avec le centre de compétence en matière de cybersécurité

N°33 : La Confédération précise les critères propres à garantir que l'engagement de l'armée dans le cyberespace respecte toujours le principe de proportionnalité.

Entités compétentes : DDPS, DFAE

Avis DDPS : Acceptation, activités en cours
Avis DFAE : Acceptation

DDPS : Est traité par le centre de cyberdéfense rattaché au DDPS, en coopération avec la BAC, dans le cadre du plan d'action pour la cyberdéfense adopté par le DDPS.

DFAE : Engagement de l'armée dans le cyberespace selon le principe de proportionnalité. L'engagement de l'armée dans le domaine cybernétique est toujours un engagement dans le (cyber)espace international. Les aspects de sécurité et de politique étrangère ou diplomatique nécessitent la participation directe du DFAE (DDIP, Division politique de sécurité/SIS).

N°35 : Pour permettre la transformation numérique des activités administratives, la Confédération et les cantons créent des conditions générales uniformes permettant d'assurer un traitement des données sans rupture de média, aussi convivial que possible, bien coordonné, interconnecté et répondant aux exigences de la protection des données, y compris pour les particuliers et les entreprises; si cela paraît judicieux, la Confédération et les cantons étendent l'application des solutions adoptées à tout le pays.

Entités compétentes : DFF, DFI; autre entité intéressée : DFAE

Avis DFF : Acceptation

DFF, DFI : Mise en œuvre de la Déclaration de Tallinn, selon le principe « une seule fois » (*once-only*)

[6] Motion 17.3507 Dittli Josef du 15 juin 2017 Création d'un commandement de cyberdéfense dans l'armée suisse, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507

DFAE : Correspond aux principes internes du DFAE pour un parcours client sans rupture (*Seamless customer journey*) ainsi qu'aux travaux effectués sur les pages internet du département.

N°36 : Lors de la mise en œuvre de la stratégie suisse de cyberadministration, la Confédération et les cantons veillent à ce que la numérisation ne soit pas un facteur d'exclusion pour le groupe de population qui ne désire pas recourir aux services en ligne.

Entité compétente : DFF; autre entité intéressée : DFAE

Avis DFF : Acceptation

DFF : La Confédération suit le principe « le numérique d'abord » (*digital first*) et non « le numérique seulement » (*digital only*). Ce faisant, elle doit absolument tenir compte des considérations coûts-avantages : Quel serait le coût de l'intégration des personnes qui ne souhaitent pas recourir aux services en ligne (*offliners*).

DFAE : Cette recommandation s'applique également aux Suisses de l'étranger et aux personnes voyageant en Suisse.

N°37 : La Confédération et les cantons créent les bases légales permettant que les données collectées par des moyens publics soient mises à disposition en vue de leur réutilisation, sous réserve des prescriptions relevant de la législation sur la protection des données.

Entité compétente : DFI

Avis DFI/SG : Acceptation

DFI: Dans le cadre de la mise en œuvre de la Stratégie Open Government Data 2019-2023[7], le DFI a reçu le mandat de déterminer, jusqu'à mi-2020, les mesures juridiques et organisationnelles nécessaires permettant de définir des conditions générales plus contraignantes et, si possible, optimales pour un développement de l'OGD dans le sens de la stratégie (principe 4.2.3). Outre l'examen d'un éventuel projet de loi, il s'agit de mettre en place les conditions d'utilisation établies au niveau international (voir mesure 1) et d'introduire un monitoring permanent des critères de qualité (voir mesure 2). Conformément à la stratégie, les services de l'administration fédérale centrale doivent en principe publier leurs nouvelles données en libre accès, à moins qu'un intérêt légitime ou des dispositions légales ne s'y opposent. Les cantons sont invités à collaborer étroitement, entre autres dans le forum des pouvoirs publics, à la mise en application de la stratégie et des solutions juridiques développées.

N°38 : La Confédération et les cantons créent un service spécialisé chargé d'élaborer des normes techniques et opérationnelles relatives au traitement des OGD et de fournir une assistance technique à toutes les unités administratives concernées.

Entité compétente : DFI

Avis DFI /SG : Acceptation de la responsabilité pour la mise en œuvre

DFI: La Stratégie Open Government Data 2019-2023 confie au DFI la gestion globale des travaux de mise en œuvre. L'une des mesures préconise la mise en place d'un « Secrétariat Open Government Data » dans le Département, au sein de l'Office fédéral de la statistique (principe 4.2.1, objectifs 4.3.1-

[7] Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2019 à 2023 (Stratégie Open government data, OGD)

5, ressources 6.2). Le secrétariat basé à l'OFS est opérationnel dès le 1.1.2019. Il coordonne les mesures de la stratégie relatives à la mise en œuvre pratique, notamment les questions de normalisation et de standardisation prévues dans le plan de mesures annexé à la stratégie (p. ex. les mesures sur la standardisation et la qualité des données OGD publiées (mesure 2) ou des synergies technico-opérationnelles (mesure 3).

Le Secrétariat OGD de la Confédération est directement en réseau avec les services équivalents, mis en place au niveau cantonal et développe en commun avec ceux-ci des thèmes tels que la normalisation et la standardisation. Comme le prévoit la stratégie (Organisation 6.1), des groupes de travail appropriés sont constitués ou reconduits (p. ex. le groupe de travail Portail et métadonnées).

N°40 : La Confédération, les cantons et les communes encouragent les systèmes et les processus ouverts et participatifs (par ex. données ouvertes, libre accès, science ouverte, innovation ouverte, science citoyenne, marathons de programmation, ateliers ou espaces de fabrication numérique, laboratoires de la gouvernance et défis urbains), afin d'accélérer à la fois la transformation numérique, le gain de résilience et le développement durable.

Entités compétentes : DFF, DETEC, DFAE

Avis DFF : Acceptation
Avis DETEC : Acceptation
Avis DFAE : Acceptation

DFF : Travaux à coordonner avec E-Government Schweiz.

DETEC : Travaux déjà partiellement en cours dans le cadre de la Stratégie Suisse numérique[8]

DFAE : Voir également le projet du DFAE « Développement de la démocratie sur la base d'une autodétermination numérique »[9]

N°42 : La Confédération et les cantons s'assurent que des solutions blockchain ne soient appliquées à des domaines sensibles au sein de l'administration et dans les secteurs réglementés que lorsque leur sécurité à long terme sera garantie (moyennant par ex. des mises à jour régulières).

Entité compétente : DFF

Avis DFF : Acceptation

DFF : Les régulateurs concernés devraient également être impliqués.

N°43 : La Confédération procède, compte tenu de l'évolution de la réglementation à l'étranger, aux modifications du droit en vigueur requises par la gestion des « paquets de données » (jetons ou tokens), par la tenue de registres numériques et par la protection des données.

Entité compétente : DFJP

Avis DFJP : Acceptation partielle

---

[8] https://strategy.digitaldialog.swiss/fr/plan-d-action

[9] https://strategy.digitaldialog.swiss/fr/plan-d-action/4

DFJP : Le 7 décembre 2018, le Conseil fédéral a adopté un rapport sur le cadre légal régissant la blockchain et la *distributed ledger technology* dans le secteur financier.[10] Les analyses montrent qu'aucune modification fondamentale du cadre suisse ne s'impose, mais qu'il faut tout de même y apporter des modifications ponctuelles. Le Conseil fédéral a chargé le DFF et le DFJP d'élaborer un projet de consultation au cours du premier trimestre 2019, notamment afin d'accroître, dans le droit civil, la sécurité juridique en matière de transfert de droits au moyen de registres numériques, de clarifier davantage, dans le droit de l'insolvabilité, la question de la disjonction des cryptoactifs et d'examiner la possibilité de créer un droit de disjonction des données sans valeur patrimoniale.

Nr. 44 : La Confédération et les cantons veillent à ce que tous les élèves de l'école obligatoire et tous les étudiants acquièrent et développent les aptitudes fondamentales et les compétences requises pour se préparer à la transformation numérique et maîtriser les technologies numériques.

Entités compétentes : Compétence pour les écoles obligatoires : cantons; compétence pour les hautes écoles : hautes écoles, cantons et Confédération

Avis DEFR : Acceptation

DEFR : Confédération et cantons sont déjà très actifs dans ce domaine. Le rapport « Défis de la numérisation pour la formation et la recherche en Suisse »[11] souligne à plusieurs reprises que le système de formation suisse doit s'adapter à l'évolution numérique. À cette fin, le plan d'action propose différentes mesures visant à améliorer et intensifier l'acquisition de compétences numériques à tous les niveaux de la formation, en collaboration avec les cantons. Certaines de ces mesures ont déjà été mises en place, d'autres sont en cours. Dans le secteur de l'enseignement supérieur, la transmission des compétences d'application numériques sera encouragée dans les années 2019-2020 par des contributions liées à des projets.

À noter qu'avec l'adoption de sa « Stratégie pour la gestion de la transition numérique dans le domaine de l'éducation » du 21 juin 2018[12], la CDIP a aussi reconnu l'importance d'agir dans ce domaine. Enfin, dans le cadre du Comité de coordination Numérisation de l'éducation (CC N), Confédération et cantons assurent la coordination et la cohérence entre leurs stratégies respectives.

N°46 : La Confédération et les cantons s'attachent à promouvoir une culture qui traite davantage de la transformation numérique et créent des lieux publics qui permettent d'utiliser les technologies numériques à des fins créatrices.

Entité compétente : DFI

Avis DFI : Acceptation partielle

DFI: La recommandation s'adresse à la Confédération et aux cantons. Dans le projet de consultation du 29 mai 2019 sur le message concernant l'encouragement de la culture pour la période 2021-2024 (message culture)[13], le Conseil fédéral a indiqué vouloir mettre l'accent, dans les prochaines années, sur les mesures qui résultent pour la culture des défis de la numérisation. Par contre, la Confédération n'a aucune influence directe sur la politique culturelle des cantons.

---

[10] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-73398.html
[11] https://www.sbfi.admin.ch/sbfi/fr/home/le-sefri/numerisation.html
[12] http://www.edk.ch/dyn/31426.php
[13] Documents relatifs à la consultation sur le Message culture 2021-2024

N°47 : La Confédération et les cantons s'engagent à ce que les valeurs fondamentales, les droits de l'homme et la dignité humaine restent garantis à l'ère du numérique et à favoriser l'autodétermination en matière d'information.

Entités compétentes : DFJP, DFAE

Avis DFJP : Acceptation
Avis DFAE : Acceptation

DFJP : Cette recommandation concerne une tâche permanente déjà remplie par l'OFJ. Celui-ci est actuellement impliqué dans plusieurs dossiers qui tiennent compte de cette recommandation, en particulier la révision totale de la LPD. La ratification prévue de la convention STE 108 modernisée du Conseil de l'Europe sur la protection des données vise aussi à renforcer l'autodétermination en matière d'information. Il convient également de mentionner la participation de l'OFJ au groupe de travail interne de l'administration fédérale sur l'intelligence artificielle.

DFAE : L'intérêt particulier du DFAE concerne la question du respect du droit international humanitaire et des droits de l'homme par les acteurs privés dans le domaine des applications et de la cybersécurité. A voir dans quelle mesure cet aspect spécifique pourra figurer dans ce cadre plus général.

N°50 : La Confédération veille à ce que les processus numériques et les algorithmes respectent parfaitement les exigences en matière de transparence, de traçabilité, de compréhension et de responsabilité (*accountability*).

Entité compétente : DEFR

DEFR : Le sujet est traité en lien avec le mandat sur l'intelligence artificielle octroyé au DEFR par le Conseil fédéral (Groupe de travail interdépartemental Intelligence artificielle, GTID IA). Un rapport est attendu en novembre 2019[14].

3.2 Recommandations du groupe d'experts rejetées

N°1 : La Confédération s'engage pour que

- **les écoles polytechniques fédérales, les universités, les hautes écoles spécialisées et les institutions de formation professionnelle développent et mettent en réseau la sécurité de l'information par des offres de formation dans le domaine informatique et fixent les contenus didactiques minimaux correspondants, et**

- **la sécurité de l'information soit intégrée à la formation de base dans les écoles polytechniques fédérales, les universités, les hautes écoles spécialisées et les institutions de formation professionnelle.**

Entités compétentes : DEFR, Conseil des EPF; autre entité intéressée : DDPS

Avis DEFR: Rejet
Avis DDPS : Rejet

DEFR : De l'avis du SEFRI, et en accord avec le Secrétariat général de la Conférence des recteurs des hautes écoles suisses (*swissuniversities*), la première recommandation doit être rejetée sous cette

[14] https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/communiques-de-presse.msg-id-72053.html

forme. La création et la conception d'offres de formation et de perfectionnement dans le secteur de l'enseignement supérieur relèvent de l'autonomie des hautes écoles. Ni la Confédération ni les cantons ne peuvent prescrire aux hautes écoles d'offres de formation ni de contenus d'enseignement. Le SEFRI communiquera à swissuniversities le rapport d'experts et les recommandations concernant les hautes écoles. Dans le rapport « Défis de la numérisation pour la formation et la recherche en Suisse », le Conseil fédéral a établi qu'il était nécessaire d'intervenir dans tous les domaines au niveau de la transmission des compétences en matière de technologies numériques (*digital skills*). Dans les années 2019-2020, les universités mettront notamment en œuvre des projets de coopération relatifs à l'évolution des exigences curriculaires. En outre, la Conférence suisse des hautes écoles a déjà chargé swissuniversities d'intégrer le thème de la numérisation dans la planification stratégique des hautes écoles pour les années 2021-2024.

Dans l'enseignement professionnel de base, l'enseignement de culture générale (ECG) transmet les compétences de base. La Confédération est responsable du plan d'études cadre correspondant, mais il appartient aux cantons de le mettre en œuvre concrètement. La recommandation doit également être rejetée du point de vue de l'enseignement professionnel de base, car dans le cadre de l'élaboration de la stratégie « Formation professionnelle 2030 », le plan d'études cadre de l'ECG sera également abordé et révisé en tant que projet « Culture générale 2030 ». Les mesures nécessaires ont donc déjà été prises; elles se fondent sur le mandat inscrit dans le plan d'action « Numérisation pour le domaine FRI durant les années 2019 et 2020 ».

DDPS : Le DDPS rejoint les explications du DEFR. Il souligne que de nombreuses activités sont également menées à l'armée en vue d'une formation dans le domaine cybernétique, par exemple la création du cybercampus et l'introduction de la formation en cybernétique (voir aussi la remarque sur la recommandation 7).

N°9 : La Confédération vérifie si les dispositions pénales en vigueur sont suffisantes pour faire rendre des comptes aux responsables en cas de violation de secrets par des systèmes numériques (applications personnalisées, par ex.).

Entités compétentes : DFJP, DDPS; autre entité intéressée : DFAE

Avis DFJP : Rejet
Avis DDPS : Rejet
Avis DFAE : Intérêt

DFJP : Les règles du droit pénal relatives à la protection du secret sont suffisantes :

Quiconque utilise les ressources informatiques en tant que détenteur d'un secret doit analyser les risques de cette utilisation et, si nécessaire, adopter les mesures appropriées (obtention du consentement, cryptage, conclusion d'un accord de confidentialité, renoncement à l'utilisation et examen d'autres solutions, etc.). Si le détenteur d'un secret prend malgré tout de tels risques en connaissance de cause, cela doit être considéré comme un consentement implicite au regard du droit pénal. Les conséquences de la divulgation de secrets ne relèvent dès lors plus du droit pénal. Si le détenteur d'un secret prend de tels risques en connaissance de cause sans adopter les mesures nécessaires (notamment obtention du consentement ou cryptage), il est punissable. Selon le droit en vigueur, la violation de secret par négligence n'est pas punissable. En l'occurrence, elle ne semble pas non plus pertinente : Toute personne qui utilise ou fait utiliser des ressources TIC à titre professionnel sait que les données en question (« secrets ») sont souvent stockées par des tiers (éventuellement même à l'étranger). Le fait de croire que les tiers ne distinguent pas les informations protégées par le droit pénal n'est pas pertinent : Dans le cas de l'infraction de « divulgation », la possibilité que des personnes non autorisées aient connaissance des données est suffisante, c'est pourquoi il y a régulièrement dol éventuel.

Pour des raisons liées à l'Etat de droit (principe de culpabilité), le fait qu'une personne physique ou morale soit « l'auteur » (selon la formulation du groupe d'experts « Avenir du traitement et de la sécurité des données ») d'une violation du secret n'est pas suffisant pour la punir. En effet, il serait erroné de pénaliser les fabricants et les opérateurs de systèmes informatiques pour des violations de secret dont ils n'ont pas (ne peuvent pas avoir) connaissance. Le droit pénal suisse ne connaît pas la responsabilité causale. Toutefois, les fabricants et les exploitants de systèmes informatiques peuvent être poursuivis en tant qu'auxiliaires du détenteur du secret, en application de l'article 162 CP (pour les détenteurs de secrets commerciaux) ou de l'article 321 CP (pour les détenteurs de secrets professionnels). Selon le projet du Conseil fédéral sur la révision de l'art. 320 du CP, la punissabilité des auxiliaires doit également s'appliquer pour la protection des secrets de fonction – en particulier dans le domaine des TIC (voir le projet d'art. 320 CP dans l'objet 17.028 Loi sur la sécurité de l'information). Cette situation présente des similitudes avec la responsabilité pénale des fournisseurs d'hébergement due à leur complicité dans les délits commis par les utilisateurs.

Etant donné que les fournisseurs de TIC opèrent au-delà des frontières nationales, des problèmes se posent souvent dans l'application de la loi. Pour des raisons de droit international (principe de souveraineté et de territorialité) et pour des raisons pratiques (notamment en raison de la perte de la connaissance du lieu de localisation – *loss of knowledge of location*), les autorités pénales peinent à prouver que les membres d'une entreprise sont pénalement responsables des violations de secret qui peuvent résulter du fonctionnement de systèmes TIC. Toutefois, les dispositions contractuelles et techniques prévues par le mandant permettent de résoudre, du moins en partie, les difficultés pratiques. Dans le cadre de la mise en œuvre de la motion 18.3379 CAJ -E (Accès des autorités de poursuite pénale aux données conservées à l'étranger), le Conseil fédéral proposera au Parlement une réglementation visant à améliorer l'application de la loi dans les affaires transfrontalières; il œuvre également dans ce but au niveau international.

DDPS : Le DDPS partage en principe l'avis du DFJP. Dans tous les cas, les interfaces avec la police militaire (armée) et la justice militaire (auditeur en chef du SG DDPS) doivent être prises en compte.

DFAE : Egalement intéressé en raison de liens possible avec les affaires internationales.

N°13 : La Confédération s'engage, en collaboration avec l'économie, en faveur de l'instauration d'instruments visant à garantir au consommateur une protection appropriée dans les conditions générales de vente en ligne.

Entités compétentes : DFJP, DEFR

Avis DFJP : Rejet
Avis DEFR : Rejet

DFJP : L'inclusion et le contrôle de conditions générales dans les contrats avec les consommateurs sont déterminés par les règles du Tribunal fédéral ainsi que par l'art. 8 LCD, en vigueur depuis le 1er juillet 2012 (contrôle du contenu). Bien qu'il n'y ait guère de décisions de justice relatives à l'art. 8 LCD, cette disposition a un effet sur la pratique contractuelle. Il ne s'agit pas d'un problème spécifique au commerce en ligne et il n'y a pas de raison que des règles spéciales doivent s'y appliquer. Le régime actuel est suffisant. De plus, la décision est hautement politique; toute modification nécessite un mandat clair du Parlement.

DEFR : Il n'existe pas de base légale permettant au SECO de s'engager, en collaboration avec l'économie, en faveur de l'instauration d'instruments visant à garantir au consommateur une protection appropriée dans les conditions générales de vente en ligne.

D'une manière générale, la Confédération, représentée par le SECO, peut, sur la base de l'art. 10, al. 3, LCD (Loi fédérale contre la concurrence déloyale; RS 241), si elle le juge nécessaire à la protection de l'intérêt public, engager uniquement des poursuites civiles et, dans les cas visés à l'art. 23, al.

1, LCD, des poursuites pénales contre toute personne ou entreprise qui, par ses pratiques commerciales déloyales, menace la réputation de la Suisse à l'étranger ou les intérêts collectifs en Suisse, ou y porte atteinte. En principe, le SECO n'exerce ce droit que s'il reçoit des plaintes qui font état d'une menace ou d'une atteinte aux intérêts publics. Quant à l'art. 10, al. 3, LCD, il ne constitue pas une base juridique qui permettrait à la Confédération ou au SECO, en collaboration avec l'économie, d'introduire des instruments visant à garantir au consommateur une protection appropriée dans les conditions générales de vente en ligne.

En outre, il convient de garder à l'esprit que l'art. 8 LCD ne prévoit qu'une protection dont le champ d'application est limité aux cas réels d'abus; il précise simplement quand les conditions générales sont abusives. Le SECO peut avertir les utilisateurs des conditions générales abusives au sens de l'art. 8 LCD et, le cas échéant, les poursuivre au civil uniquement si les conditions de l'art. 10 al. 3, de la loi sur la concurrence déloyale sont remplies.

N°14 : La Confédération vérifie s'il y a lieu d'instaurer un droit de révocation pour les transactions en ligne.

Entité compétente : DFJP

Avis DFJP : Rejet

DFJP : Dans le cadre des débats menés en 2013 sur l'IP 06.441[15], le Parlement a rejeté en connaissance de cause l'adoption d'un droit de rétractation pour les contrats à distance basés sur le modèle du droit européen. Depuis, aucun changement n'est survenu qui pourrait impliquer de revenir sur cette décision. En outre, il s'agit d'une décision hautement politique; toute modification requiert un mandat clair du Parlement.

N°16 : La Confédération vérifie s'il y a lieu de prévoir à moyen terme des règles spécifiques à certains secteurs, par exemple dans le droit de la concurrence (LCD), dans l'ordonnance sur l'indication des prix ou dans le droit des assurances.

Entité compétente : DEFR

Avis DEFR : Rejet

DEFR : L'ordonnance sur l'indication des prix (OIP) a pour but d'assurer une indication claire des prix, permettant de les comparer et d'éviter que l'acheteur ne soit induit en erreur. Elle s'applique également aux prix dynamiques; en particulier, les prix effectifs à payer doivent être annoncés et spécifiés. Si les dispositions de l'OIP sont respectées, la différenciation des prix fondée sur l'analyse des données n'a donc aucun effet négatif sur la clarté et la comparabilité des prix ni sur la prévention des prix trompeurs. Seules des durées de validité extrêmement courtes pour les prix dynamiques pourraient entrer en conflit avec le but de l'OIP. Toutefois, à l'heure actuelle, la fixation d'une durée minimale n'est guère indiquée. Aujourd'hui, la durée de validité des prix dynamiques est suffisamment longue pour assurer la comparabilité; la réglementer pourrait au contraire entraîner un raccourcissement général. En outre, la durée de validité des prix n'est pas directement liée au problème de la différenciation des prix fondée sur l'analyse des données. Une réglementation complète dans l'OIT n'est pas nécessaire. D'éventuelles réglementations sectorielles devraient être envisagées dans les lois spéciales et non dans l'OIP.

---

[15] 06.441 Initiative parlementaire Pour une protection du consommateur contre les abus du démarchage téléphonique, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20060441

N°17 : La Confédération encourage les mécanismes de règlement en ligne des plaintes et des litiges (Online Dispute Resolution, ODR), en tenant compte des offres privées.

Entités compétentes : DFJP, DEFR

Avis DFJP/OFJ : Rejet
Avis DEFR : Rejet

DFJP et **DEFR :** Les mécanismes de règlement en ligne des plaintes et des litiges (*Online Dispute Resolution* – ODR) sont reconnus comme étant des instruments efficaces de résolution extrajudiciaire des litiges, qui complètent de manière significative la protection juridique. Dans le secteur des télécommunications, l'ombudscom est un exemple d'organe de conciliation prévu par la loi (https://de.ombudscom.ch/gesetzliche-grundlagen/). Il s'agit d'une fondation, qui ne fait donc pas partie de l'administration fédérale, même si elle est supervisée par l'OFCOM. Toutefois, faute d'une base juridique suffisante dans la législation existante, la recommandation 17 est rejetée pour le moment. Il faudrait d'abord clarifier si et sous quelle forme l'administration fédérale peut et doit promouvoir ce type de mécanismes de règlement des différends.

N°18 : La Confédération vérifie s'il y a lieu de prévoir dans le droit des cartels, comme critère d'intervention lors du contrôle des concentrations d'entreprises, la valeur des transactions, en plus des seuils de chiffres d'affaires.

Entité compétente : DEFR

Avis DEFR : Rejet

DEFR : Le Conseil fédéral a déjà abordé ce sujet dans son « Rapport sur les principales conditions-cadre pour l'économie numérique » de 2017[16]. Une étude[17] commandée par le SECO s'est penchée sur cette question; à une exception près, les experts interrogés rejettent une réforme des critères d'intervention qu'ils trouvent précipitée. Par conséquent, le SECO ne voit actuellement pas la nécessité d'en faire davantage.

N°19 : La Confédération vérifie, en tenant compte des développements internationaux, s'il y a lieu de réglementer plus précisément dans la loi sur les cartels le risque d'ententes tacites dues à des algorithmes de prix.

Entité compétente : DEFR

Avis DEFR : Rejet

DEFR : La loi sur les cartels couvre également les faits relatifs à la coordination au moyen d'algorithmes de prix. Pour l'heure, il n'y a pas lieu de modifier la législation. Les remarques sur les considérations de l'administration fédérale en matière d'algorithmes de prix sont également incorrectes. Le SECO et les autorités responsables du domaine de la concurrence ont déjà mené des réflexions approfondies à cet égard (notamment lors de divers séminaires).

---

[16] https://www.seco.admin.ch/seco/fr/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html
[17] https://www.seco.admin.ch/seco/fr/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Wettbewerb_Service_Public/Kartellgesetz/revision-fusionskontrolle---studie-zur-fusionskontrolle.html

N°22 : La Confédération étudie la possibilité de réglementer la portabilité des données techniques, en tenant compte des évolutions observées sur le plan international.

Entité compétente : DFJP

Avis DFJP : Rejet

DFJP: La problématique de l'accès aux données non personnelles sera examinée de manière assez large dans le cadre de la recommandation 20 (voir ci-dessus). Il n'est dès lors pas judicieux à ce stade de mener en parallèle des travaux concernant le portage des données non personnelles. À cela s'ajoute que le rapport d'experts apporte très peu d'éléments à l'appui de cette recommandation. Les développements internationaux auxquels il est fait allusion ne vont pas jusqu'à introduire des droits ou des obligations: le Règlement 2018/1807 de l'UE du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne prévoit uniquement que la Commission européenne encourage et facilite l'élaboration des codes de conduite par autorégulation afin de faciliter le portage de données. Il ne semble donc guère judicieux d'examiner le besoin de réglementer en droit suisse, alors que l'UE privilégie l'autorégulation. Enfin, il se pose la question de savoir s'il n'est pas plus indiqué que les départements examinent le besoin de réglementation dans leurs domaines respectifs (énergie, véhicules, etc.) en tenant compte des spécificités de ces domaines plutôt que d'introduire des dispositions de nature générale. Nous proposons par conséquent de ne pas poursuivre l'examen de cette recommandation plus avant pour l'instant, car cela représenterait vraisemblablement un travail inutile, d'autant qu'au niveau international les codes de conduite prévus par le règlement européen n'en sont vraisemblablement qu'à leurs débuts. Il convient également d'attendre le résultat des travaux concernant la recommandation 20.

N°23 : La Confédération comble les lacunes en matière de protection juridique des personnes concernées, notamment en adaptant la loi fédérale sur la poursuite pour dettes et la faillite et le droit des successions.

Entité compétente : DFJP

Avis DFJP : Rejet

DFJP : Les travaux dans ce domaine sont déjà en cours. Dans la LP, une disposition spéciale relative au tri des données est mise en consultation dans le cadre du projet de blockchain. En droit successoral, la question est traitée dans le cadre du postulat 14.3782[18]. La recommandation est également partiellement prise en considération dans la révision totale de la LPD, à l'art. 16 P-LPD. Cette disposition régit à quelles conditions l'accès aux données personnelles d'une personne décédée est accordé et à quelles conditions les héritiers ou l'exécuteur testamentaire peuvent exiger la suppression ou la destruction des données personnelles d'une personne décédée.

N°24 : La Confédération examine, en tenant compte des évolutions observées sur le plan international et en particulier dans l'UE, les mesures à prendre dans le domaine du droit de la responsabilité extracontractuelle (responsabilité du fait des produits, responsabilité de la sécurité des produits, responsabilité des prestataires et responsabilité de l'infrastructure numérique). Elle se penche également sur la possibilité d'introduire de nouveaux concepts de responsabilité.

Entité compétente : DFJP

[18] Postulat 14.3782 Schwaab Jean Christophe du 24.09.2014 Des règles pour la « mort numérique », https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20143782

Avis DFJP/OFJ : Rejet

DFJP : Pour le moment, on ne voit aucune nécessité d'intervenir. Les différents aspects de la question ont par ailleurs déjà été partiellement examinés. Si des problèmes se posent dans la pratique, ils sont traités de manière spécifique; des solutions générales ne semblent pas appropriées.

En ce qui concerne la responsabilité de l'infrastructure du réseau et la responsabilité des fournisseurs, une nouvelle fois abordées par le groupe d'experts « Avenir du traitement et de la sécurité des données », il convient de se référer aux travaux du Conseil fédéral et du Parlement sur la lutte contre la cybercriminalité et au rapport du Conseil fédéral sur la responsabilité civile des fournisseurs. Selon ces documents, il n'est pas nécessaire d'introduire de nouveaux concepts de responsabilité dans ce domaine car ceux-ci ne présenteraient aucun avantage par rapport aux règles en vigueur aujourd'hui. On ignore si les conclusions du groupe d'experts auraient changé quelque chose à cette conclusion. En droit pénal, les modifications ponctuelles des lois relatives à la sécurité des produits ou à la responsabilité du fait des produits doivent être examinées accessoirement lors d'une éventuelle révision de ces lois.

N°30 : La Confédération examine :

- **si les exploitants d'infrastructures critiques doivent présenter une déclaration de sécurité relative aux entreprises;**
- **si la procédure de sécurité relative aux entreprises doit aussi être ouverte aux services externes à la Confédération et à l'administration lors de la conclusion de marchés sensibles et, le cas échéant, comment.**

Entité compétente : DDPS

Avis DDPS : Rejet

DDPS : Les entreprises qui sont surtout importantes en tant que fournisseurs font également partie des infrastructures critiques. Les opérateurs d'infrastructures critiques ne peuvent pas tous être logés à la même enseigne. Hormis pour quelques domaines spécifiques et quelques législations spéciales, cette approche ne promet guère de valeur ajoutée ni de rapport coûts-utilité intéressant, qu'il s'agisse d'entités qui contrôle ou d'entités qui sont contrôlées.

N°34 : La Confédération examine avec les cantons l'éventuelle harmonisation nationale de la réglementation de droit public de la protection des données.

Entités compétentes : DFJP, PFPDT

Avis DFJP/OFJ : Rejet

DFJP : Comme l'explique le groupe d'experts « Avenir du traitement et de la sécurité des données » dans son rapport (p. 138), la question de savoir si l'actuelle répartition des compétences entre la Confédération et les cantons en matière de protection des données est toujours indiquée ou s'il ne vaut pas mieux viser une harmonisation a déjà été examinée dans le cadre des travaux de révision totale de la LPD. Une consultation menée en automne 2013 par la Conférence des gouvernements cantonaux a révélé qu'une nette majorité des cantons étaient opposés à ce que l'harmonisation de la législation générale sur la protection des données relève de la compétence de la Confédération. La révision totale de la LPD ne prévoit donc pas de modifier la répartition des compétences entre la Confédération et les cantons (ni, par conséquent, de réviser préalablement la Constitution). Nous doutons que la situation ait changé depuis. En outre, la Confédération n'est pas la seule à réviser sa législation

en matière de protection des données pour tenir compte des nouvelles normes européennes; les cantons le font aussi, ce qui devrait rapprocher les contenus. Dans ce contexte, nous sommes d'avis que les considérations relatives à l'harmonisation du droit public en matière de protection des données ne sont pas appropriées pour l'instant.

N°41 : La Confédération et les cantons n'étendent les projets de vote électronique que s'il peut être démontré que ce vote ne présente pas plus de risques que les formes actuelles de participation démocratique aux élections et aux votations. Les résultats des élections et des votations doivent rester vérifiables.

Entité compétente : ChF; autre entité intéressée : DFAE

Avis ChF : Rejet
Avis DFAE : Intérêt

ChF : La recommandation exigerait une comparabilité avec les risques des « formes existantes de démocratie participative », c'est-à-dire le vote par correspondance et le vote dans l'urne. Cette partie de la recommandation ne peut être mise en œuvre car les critères de comparaison des risques ne sont pas clairs et les risques des « formes existantes de démocratie participative » ne sont pas quantifiés. L'objectif doit continuer à être de maintenir les risques spécifiques de tous les canaux de vote aussi bas que possible. Les exigences légales fédérales concernant le recours au vote électronique (en particulier la vérifiabilité, la certification, la transparence) tiennent donc compte des risques spécifiques de ce canal de vote. Seuls sont autorisés les systèmes de vote électronique qui répondent aux exigences fédérales élevées en matière de sécurité. L'article 3 du OVotE (ordonnance de la ChF sur le vote électronique du 13 décembre 2013; RS 161.116) exige une évaluation continue des risques dans le cadre de l'autorisation générale et de l'agrément nécessaires pour recourir au vote électronique. Les risques liés à une utilisation plus large du vote électronique sont également évalués. Le vote électronique ne peut être utilisé que si tous les risques de sécurité sont suffisamment faibles. La vérifiabilité (art. 4 et 5 OVotE) garantit la transparence du scrutin, sur la base de procédures cryptographiques spéciales, tout en préservant le secret du vote. Ainsi le vote électronique est vérifiable (deuxième partie de la recommandation) et particulièrement efficace contre les manipulations passées inaperçues. En outre, la consultation relative à la modification de la loi fédérale sur les droits politiques (ODP; RS 161.1) visant à faire du vote électronique le troisième canal de vote à part entière a montré qu'une nette majorité des cantons et des partis étaient favorables au principe de l'introduction du vote électronique, mais trouvent l'exploitation de ce système prématurée. Lors de sa séance du 26 juin 2019, le Conseil fédéral a donc décidé de renoncer pour le moment à la révision partielle de l'ODP et a chargé la Chancellerie fédérale de collaborer avec les cantons pour réorienter la phase d'essai d'ici fin 2020.

DFAE : Le vote électronique a aussi une grande importance pour les Suisses de l'étranger.

N°45 : En étroite collaboration avec tous les acteurs concernés de la société et de l'économie, la Confédération et les cantons mettent en place les structures requises pour permettre aux professionnels de tous les domaines de suivre une formation ou un perfectionnement qui leur permettront de gérer la transformation numérique.

Entité compétente : DEFR

Avis DEFR : Rejet

DEFR : Le SEFRI demande le rejet de cette recommandation. Avec la loi sur la formation professionnelle et la loi sur la formation continue, la Confédération a déjà fixé les conditions et les responsabilités structurelles qui s'appliquent dans ces domaines. La définition du contenu d'une formation professionnelle ou continue relève de la responsabilité des milieux économiques concernés. S'agissant des mesures et des questions proposées au chapitre 10.3.3, il convient aussi de relever tout particulièrement l'art. 5 de la loi sur la formation continue.

N°48 : En collaboration avec les autorités compétentes et les prestataires de la formation professionnelle, la Confédération et les cantons veillent à ce que l'éthique fasse partie intégrante des formations initiale et continue et incluent ces aspects dans leurs attentes en matière de responsabilité des entreprises.

Entité compétente : DEFR

Avis DEFR : Rejet

DEFR : Le SEFRI rejette la recommandation, qui a déjà été suivie. Le programme-cadre correspondant relève de la responsabilité de la Confédération, mais sa mise en œuvre concrète est du ressort des cantons. L'éthique fait déjà partie du programme-cadre prévu pour le domaine de l'apprentissage social. S'agissant de la formation continue, la Confédération n'est pas responsable du contenu.

N°49 : La Confédération et les cantons créent les conditions requises pour que les hautes écoles et les établissements de formation continue intensifient la recherche et l'enseignement dans les domaines de l'innovation responsable (*responsible innovation*) et de la conception axée sur les valeurs (*design for values*).

Entité compétente : DEFR, Conseil des EPF

Avis DEFR : Rejet

DEFR : Le SEFRI, en accord avec le Secrétariat général de swissuniversities, rejette cette recommandation. La conception des programmes de formation et de perfectionnement ainsi que les formes d'enseignement et d'apprentissage adoptées dans l'enseignement supérieur relèvent de l'autonomie des hautes écoles. Le SEFRI portera le rapport d'expertise et les recommandations concernant les universités à la connaissance de swissuniversities.

N°51 : La Confédération crée les bases légales nécessaires pour garantir qu'il soit clairement spécifié à la personne qui recourt à une forme de communication électronique interactive si elle est en communication avec un être humain ou non.

Entités compétentes : DEFR, DETEC

Avis DEFR : Rejet
Avis DETEC : Rejet

DEFR et DETEC : Il n'est pas clair dans quelle mesure le « problème » décrit dans la recommandation existe réellement dans la pratique aujourd'hui. On ignore d'une part si cette communication « machine » est répandue et d'autre part si elle ne se fait pas volontairement de manière transparente. Aucune réglementation anticipée ne devrait être introduite aussi longtemps que des preuves n'ont pas été apportées.

3.3 Activités en cours, acceptation ou rejet possibles

N°39 : La Confédération, les cantons et les communes prennent les mesures appropriées pour encourager les projets pilotes fondés sur des approches innovantes de la démocratie participative, telles que les délibérations en ligne massives et ouvertes (*massive open online deliberation, MOOD*), et pour créer les bases nécessaires à leur évaluation.

Entité compétente : ChF; autre entité intéressée : DFAE

Avis ChF : Acceptation ou rejet selon les travaux en cours

ChF : La ChF prépare actuellement le rapport en réponse aux postulats 17.3149 Hausammann19 et 17.4017 Müller Damian[20]. Ce document montrera, entre autres, quel rôle la Confédération peut et doit jouer dans la promotion des instruments numériques de participation. Jusqu'à présent, rien n'indique qu'il existe une forte demande non satisfaite de plateformes de délibération en ligne. Le rapport devrait être adopté par le Conseil fédéral d'ici mi-2019.

DFAE : La problématique concerne aussi les Suisses de l'étranger. Il existe éventuellement des synergies avec les travaux sur la mesure "Développement de la démocratie sur la base d'une autodétermination numérique", placée sous l'égide du DFAE dans le cadre de la Stratégie « Suisse numérique ».

[19] Postulat 17.3149 Hausammann Markus du 16.03.2017 Uniformiser et rendre plus efficace la procédure de consultation, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173149

[20] Postulat 17.4017 Müller Damian du 04.12.2017 Profiter des opportunités offertes par les technologies civiques, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017

4 Liste des abréviations

Al.	Alinéa
FF	Feuille fédérale
OFJ	Office fédéral de la justice
ChF	Chancellerie fédérale suisse
Let.	Lettre
CYD	Cyber-Defence, défense dans l'espace virtuel
DDIP	Direction du droit international public (au DFAE)
DFAE	Département fédéral des affaires étrangères
DFI	Département fédéral de l'intérieur
P-LPD	Droit sur la protection des données
DFF	Département fédéral des finances
E-Gov	Cyberadministration, services électroniques
Loi e-ID	Identité électronique
DFJP	Département fédéral de justice et police
EPFL	Ecole polytechnique fédérale de Lausanne
EPFZ	Ecole polytechnique fédérale de Zurich
UE	Union européenne
BAC	Base d’aide au commandement de l’armée
Gov Lab	Laboratoire de la gouvernance, laboratoire d'innovation pour le secteur public
CdG-E	Commission de gestion du Conseil des Etats
TIC	Technologies de l'information et de la communication
SECO	Secrétariat d’Etat à l’économie
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
PNR	Programme national de recherche
ODR	Online Dispute Resolution, mécanismes de règlement en ligne des plaintes et des litiges

IP	Interventions parlementaires
OIP	Ordonnance sur l'indication des prix
CAJ-E	Commission des affaires juridiques – Conseil des Etats
SEFRI	Secrétariat d'Etat à la formation, à la recherche et à l'innovation
SCION	Scalability, Control and Isolation on Next Generation Networks
MELANI	Centrale d’enregistrement et d’analyse pour la sûreté de l’information
SEV 218	Convention sur une approche intégrée de la sécurité, de la sûreté et des services lors des matches de football et autres manifestations sportives
Délséc	Délégation du Conseil fédéral pour la sécurité
FNS	Fonds national suisse
CE	Conseil des Etats
CP	Code pénal
IDE	Numéro d’identification d’entreprises
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
LCD	Loi fédérale contre la concurrence déloyale
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche