17 août 2018

Rapport du groupe d'experts concernant le traitement et la sécurité des données

Résumé

Mandat

En réponse à la motion Rechsteiner (13.3841), le Département fédéral des finances a institué le 27 août 2015 le groupe d'experts «Avenir du traitement et de la sécurité des données» pour une durée de trois ans. Celui-ci a été chargé de répondre aux questions suivantes:

1. D'un point de vue technologique et politique, comment évaluer l'état actuel du traitement des données?

2. Quels sont les effets sur l'économie suisse, la société et l'État?

3. Comment évaluer le cadre juridique actuel dans ce domaine?

4. Quelles conclusions en tirer pour la Suisse au niveau national? Quelles conclusions en tirer quant à d'éventuelles initiatives au niveau international?

Après une présentation des évolutions technologiques, le groupe d'experts répond aux questions posées dans la motion en tenant compte de la transformation numérique en cours et de ses implications pour l'ensemble de la société. Le rapport se concentre sur six domaines ou champs d'analyse: sécurité de l'information, relations entre les entreprises et les clients (Business to Consumer, B2C), relations entre les entreprises (Business to Business, B2B), relations entre l'État et les citoyens ou les entreprises (Government to Citizen/Business, G2Ci/B), information de la population en matière de numérique, développement des compétences et participation des utilisateurs ainsi que transformation numérique et éthique.

Défis et nouvelles possibilités

La transformation numérique touche tous les domaines de l'économie et de la vie quotidienne. Elle crée beaucoup de nouvelles possibilités, mais entraîne aussi une dépendance croissante de la société à l'égard de systèmes de plus en plus autonomes: compagnon de tous les instants, le smartphone permet de communiquer directement, d'accéder à des informations et d'ouvrir de nouvelles applications, mais aussi d'échanger de grandes quantités de données via Internet et de transmettre de nombreuses informations sur les utilisateurs. Compte tenu de la dépendance croissante de nos sociétés à l'égard des technologies numériques, l'homme risque de perdre toute possibilité de contrôle, d'intervention et de décision. Car la quantité d'informations, leur vitesse de transmission et leur degré de détail continueront à augmenter. De même, des matériels et logiciels faciles à utiliser sont désormais accessibles au plus grand nombre à un prix abordable, et les appareils pouvant être mis en réseau, équipés de capteurs et permettant de transmettre des données, sont omniprésents. À l'avenir, toujours plus d'objets du quotidien seront connectés à Internet. L'intelligence artificielle est capable de quantifier, d'analyser et d'évaluer d'énormes quantités de données sur la base d'algorithmes auto-apprenants. Par ailleurs, les ordinateurs quantiques, lorsqu'ils seront opérationnels, pourraient rendre obsolètes les systèmes de cryptage actuels.

Le recours aux outils numériques pour surveiller les comportements dans les lieux publics ou sur les réseaux sociaux ainsi que d'autres méthodes de traitement des données comme la manipulation numérique (*big nudging*) ou la modélisation prédictive, qui limitent l'autodétermination des individus, comportent des risques de dérive pour la société. L'éthique doit créer les bases qui permettront de détecter ces risques et de participer activement au développement d'innovations souhaitables.

Indépendamment de la dynamique de la transformation numérique, le groupe d'experts n'est pas favorable à une trop grande intervention réglementaire de l'État, d'autant que les règles de droit et les autres normes de comportement valables dans le monde analogique peuvent généralement contribuer de manière significative à la résolution des problèmes posés par le numérique. C'est pourquoi il est très important de combler les lacunes déjà identifiées et de développer de nouvelles solutions lorsque les solutions traditionnelles atteignent leurs limites.

Sécurité de l'information

Les systèmes étant de plus en plus complexes et interconnectés, le nombre de faiblesses non décelées dans le réseau continue à augmenter, ce qui peut causer d'importants dommages. Les attentes en matière de continuité de l'exploitation des infrastructures numériques sont plus élevées que ce que les exploitants sont en mesure de garantir.

La transformation numérique ne peut être durable que si elle repose sur la confiance dans une technologie sûre de traitement des données. Pour atteindre cet objectif, il faut tout d'abord développer les offres et les contenus de formation dans les domaines de l'informatique et de la sécurité de l'information. Par ailleurs, la Suisse doit créer des infrastructures de communication pérennes, sécurisées grâce à des techniques cryptographiques. C'est pourquoi la Confédération doit mettre en place un réseau national, afin de contribuer à promouvoir la recherche en sécurité de l'information et le transfert de savoirs entre la recherche et l'économie. Elle doit également examiner, conformément aux évolutions internationales, s'il y a lieu de définir les normes et les certifications concernant les logiciels et les appareils cyberphysiques comme des conditions préalables à l'accès au marché des composants informatiques, et, le cas échéant, dans quels domaines.

Relations entre les entreprises et les clients (Business to Consumer, B2C)

La numérisation génère une multitude de nouvelles offres avantageuses. Grâce aux méthodes de suivi et à l'analyse des *big data*, les entreprises établissent désormais des profils de personnalité. Ceux-ci offrent certes un plus en matière de confort et de service, mais ils peuvent aussi être utilisés à mauvais escient pour léser les clients, violer leur sphère privée et limiter leur autodétermination en matière d'information. Travaillant à concilier les intérêts des producteurs de biens et services et de leurs clients, tout en évitant d'enfreindre la liberté de chaque partie, les organismes chargés d'assurer la protection des consommateurs et des données ont constaté que les utilisateurs manifestaient des attentes accrues en matière d'information et de protection face aux réalités numériques.

Or, les autorités de surveillance de la protection des données ne disposent à l'heure actuelle que de bases juridiques dépassées, de pouvoirs restreints et de ressources insuffisantes. Elles sont donc de plus en plus confrontées à leurs limites lorsqu'elles s'efforcent de garantir un traitement des données dont l'intensité réponde non pas aux seules possibilités techniques, mais aux exigences légales par le recours à des technologies compatibles avec la protection des données. Il importe donc que le préposé fédéral à la protection des données et à la transparence (PFPDT) ainsi que les autorités cantonales de protection des données soient dotés au plus tôt des compétences et des ressources leur permettant d'assumer leurs tâches dans la réalité numérique de manière efficace et avec une densité de contrôle appropriée.

Abstraction faite de certaines réglementations commerciales et de prescriptions édictées par les cantons en matière de concessions, il n'existe aucune disposition réglementant la qualité en matière de protection des consommateurs. On part du principe que la concurrence assure le maintien du niveau de qualité requis. La transparence des prix ainsi que la protection contre la tromperie et les infractions contre le patrimoine constituent des piliers de la protection suisse des consommateurs. Actuellement, le groupe d'experts estime qu'il n'est pas nécessaire d'apporter des changements fondamentaux à ce niveau. Toutefois, il revient à la Confédération de recourir, conjointement avec les milieux économiques, aux outils adéquats pour garantir la protection appropriée des consommateurs, en particulier dans le domaine B2C et, par analogie, dans le cadre des relations B2B. Il s'agira également d'étudier l'opportunité d'instaurer des réglementations sectorielles visant à empêcher la discrimination par les prix, de prévoir un droit de révocation adéquat pour les transactions en ligne, de modifier le droit des contrats pour tenir compte de l'émergence des contrats et des contenus numériques ainsi que d'élaborer des mécanismes en matière de règlement des plaintes et des litiges en ligne (*Online Dispute Resolution*, ODR).

Relations entre les entreprises (Business to Business, B2B)

Dans le domaine B2B, la transformation numérique entraîne une mise en réseau accrue à l'échelle internationale et de profonds changements structurels. Cette évolution se traduit notamment par les nouveaux modèles d'affaires que l'on peut regrouper sous le nom d'économie collaborative. Dans ce contexte, la réglementation de la concurrence et la garantie de cette dernière revêtent une importance primordiale. Dans la mesure où des entreprises privées sont à même de traiter des quantités gigantesques de données, la Confédération doit examiner s'il est nécessaire de modifier le droit des cartels, notamment en édictant de nouveaux critères d'intervention pour les contrôles applicables aux fusions d'entreprises ou une réglementation des «ententes» entre algorithmes.

L'accès aux données et la propriété de ces dernières représentent par ailleurs des défis majeurs pour le domaine B2B (et également pour les rapports juridiques B2C).

Le droit en vigueur dans l'UE incite à compléter le droit d'accès dans le domaine de la protection des données par des dispositions régissant la portabilité des données et à étudier l'opportunité d'instaurer la portabilité des données techniques ainsi que de créer un système de licences obligatoires pour l'accès aux données techniques.

Il serait judicieux de combler, par la révision des diverses lois spécifiques, les lacunes existantes en ce qui concerne les droits des personnes concernées par la propriété des données.

La blockchain, technologie récente mais d'une importance croissante sur laquelle se fondent, entre autres, les cryptomonnaies et les contrats intelligents, pourrait offrir de nombreux gains d'efficacité notamment dans le domaine B2B, et fournir la base de nouveaux modèles d'affaires numériques. Toutefois, elle présente certains risques, en particulier en ce qui concerne la sécurité et la protection des données. Des mesures devraient être prises si les blockchains étaient utilisées pour la tenue de registres ou des procédures étatiques (élections). Le Conseil fédéral devrait observer de près les efforts de réglementation faits à l'étranger et, le cas échéant, lancer les procédures législatives nécessaires.

Relations entre l'État et les citoyens ou les entreprises (Government to Citizen/Business, G2Ci/B)

Le monde numérique étant considéré comme une extension de l'espace tant public que privé, l'État doit y assumer les mêmes tâches de protection que dans le monde analogique. Il lui incombe donc d'assurer à la société un accès aux données sécurisé et performant (service universel).

La Confédération et les cantons devront élaborer, en commun avec les associations professionnelles, des normes contraignantes en matière de sécurité informatique et en imposer l'application aux exploitants d'infrastructures d'importance vitale. La création d'un centre de compétence et d'un point de contact en matière de normalisation est donc nécessaire.

En outre, de nouveaux programmes visant à améliorer la sécurité de l'information auprès des entreprises, l'introduction d'une obligation pour les exploitants d'infrastructures d'importance vitale de notifier les cyberincidents et le développement de MELANI en tant que centre national pour la prévention et la lutte contre les cyberattaques devraient permettre de répondre aux défis à venir.

Une étude comparative au niveau international révèle que la Suisse doit elle aussi consentir des efforts dans ce domaine. En collaboration avec les associations et les entreprises, des mesures visant à protéger et à soutenir l'économie doivent être prises. Cela présuppose une réflexion en matière de politique de sécurité, portant sur la mise en place des ressources requises et la coopération avec d'autres États.

Depuis plus de dix ans, la Confédération, les cantons et les communes mènent une stratégie active de cyberadministration. La stratégie en matière de libre accès aux données publiques (stratégie OGD) vise à créer les conditions requises pour que l'administration puisse mettre à la disposition de la société les données qu'elle a collectées. À l'heure actuelle, cette stratégie ne peut être mise en œuvre par manque de bases juridiques, de normalisation dans le domaine du traitement des données et de ressources suffisantes. Les projets de cyberadministration en cours, notamment la création d'un cadre juridique pour un système e-ID reconnu par l'État et d'un portail administratif destiné aux entreprises, doivent être accélérés, poursuivis et développés au niveau national, tout comme ceux qui portent sur les infrastructures de base.

Notre système démocratique, avec ses normes et valeurs développées sur une longue durée, porte de plus en plus l'empreinte de la transformation numérique. Par conséquent, il incombe à la Confédération et aux cantons de créer les conditions générales permettant un traitement des données convivial et interconnecté tout en répondant aux exigences en matière de protection des données. Parallèlement, ils doivent veiller à ce que la partie de la population qui ne désire pas recourir aux services en ligne ne soit pas exclue de la société.

De nouvelles possibilités s'ouvrent notamment dans le domaine de la participation. Il conviendrait en particulier d'encourager, par le biais de projets pilotes, les approches innovantes en ce qui concerne la démocratie participative. En revanche, le vote électronique ne devrait être instauré que dans la mesure où il ne comporte pas de risques plus importants que les formes traditionnelles de participation aux votations et aux élections. Dans ce domaine, il importe particulièrement que les résultats des élections et des votations soient vérifiables.

Information de la population en matière de numérique, développement des compétences et participation des utilisateurs

À tous les niveaux, les domaines de la formation et du perfectionnement doivent préparer la population, tous âges confondus, aux défis que pose la transformation numérique. Ils doivent donc la doter des aptitudes et compétences qui lui permettront d'utiliser de manière responsable les possibilités offertes par la numérisation et d'affronter les défis de manière appropriée. Ce bagage comprend les connaissances de base en matière de traitement et d'utilisation des informations et la capacité de trouver les informations pertinentes et de les analyser.

Pour atteindre ces objectifs, tous les niveaux de formation doivent permettre de développer les capacités de base et les compétences en matière de maîtrise et de gestion des technologies numériques et de la transformation que celles-ci engendrent. Par ailleurs, le perfectionnement des professionnels doit être facilité dans tous les domaines.

Transformation numérique et éthique

L'éthique a un rôle fondamental à jouer dans le cadre de la transformation numérique. L'évolution actuelle du traitement des données bouleverse notre société et a des incidences profondes sur les valeurs et les principes centraux que sont la dignité humaine, la protection de la sphère privée, l'égalité, l'interdiction de la discrimination, l'autonomie, l'autodétermination, la transparence, la solidarité et la sécurité.

L'éthique se doit d'attirer l'attention sur les évolutions inopportunes et d'aborder avec esprit critique tant les espoirs que les peurs exagérés en la matière. Simultanément, il faudra faire connaître les solutions innovantes qu'offre la numérisation. Cela exige de mesurer les effets positifs et négatifs que cette évolution technologique peut avoir sur nos valeurs fondamentales.

Il appartient par conséquent à la Confédération et aux cantons d'assumer leur responsabilité en la matière et de s'engager à garantir, à l'ère du numérique, le respect des

valeurs fondamentales, des droits humains et de la dignité humaine, tout comme à renforcer la prise de conscience de l'importance de l'autodétermination en matière d'information. L'éthique doit donc faire partie intégrante de la formation et du perfectionnement.

Dans sa conclusion, le groupe d'experts constate que, au vu de la rapidité de l'évolution dans les domaines du traitement et de la sécurité des données, la Suisse doit en permanence analyser et évaluer quels sont les actions à engager et les changements à adopter.

Recommandations

L'ordre des recommandations ne préjuge pas de leur importance, mais suit celui des thèmes abordés dans le rapport.

Champ d'analyse sécurité de l'information

Formation dans le domaine de la sécurité de l'information

1. La Confédération veille à ce 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.

Infrastructure cryptographique sûre

2. La Confédération veille, en collaboration avec les cantons, à ce que la technique de chiffrement 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.

Infrastructure de communication sûre

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.

Normes et certification des logiciels et des appareils cyberphysiques, et création d'un cadre juridique

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.

Identités numériques sûres

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).

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

Mise en place d'un réseau national de promotion de la recherche et du transfert

de connaissances dans le domaine de la sécurité de l'information

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.

Champ d'analyse relations entre les entreprises et les consommateurs (B2C)

Protection de la sphère privée et de l'autodétermination en matière d'information

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.

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.).

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.

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.).

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.

Conditions de vente en ligne

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.

Droit de révocation en ligne

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

Contrats et contenus numériques

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.

Différenciation des prix

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.

Résolution en ligne des litiges

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.

Champ d'analyse relations entre les entreprises (B2B)

Droit des cartels

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.

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.

Thèmes communs aux champs d'analyse B2C et B2B: accès aux données, propriété des données et nouveaux enjeux liés à la responsabilité

Accès aux données techniques

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

Portabilité des données personnelles

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.

Portabilité des données techniques

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

Droit sur les données

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.

Enjeux liés à la responsabilité

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.

Champ d'analyse relations entre l'État et les citoyens ou les entreprises (G2Ci/B)

Normes de sécurité, standards et mesures de bonnes pratiques dans le domaine des infrastructures critiques

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.

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.

Normes de sécurité, standards et mesures de bonnes pratiques dans l'économie en général

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.

Obligations de notifier

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.

Organisation nationale centralisée de gestion des cyberincidents

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).

Procédure de sécurité relative aux entreprises pour les exploitants d'infrastructures critiques et les autres parties prenantes

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.

Limites des possibilités de défense de l'État

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.

Tâches de l'armée

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.

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

Harmonisation nationale de la protection des données dans l'administration

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

L'État comme prestataire de services

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.

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.

Libre accès aux données publiques et données ouvertes

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.

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.

Cyberdémocratie

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.

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 publics et défis urbains), afin d'accélérer à la fois la transformation numérique, le gain de résilience et le développement durable.

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.

Champ d'analyse blockchain

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).

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), par la tenue de registres numériques et par la protection des données.

Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche

École obligatoire et filières de culture générale jusqu'au degré tertiaire et aux hautes écoles

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.

Formation et perfectionnement professionnels

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.

Mesures en faveur du public ou de la culture

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.

Champ d'analyse transformation numérique et éthique

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.

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.

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 et de la conception axée sur les valeurs.

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)*.

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.

Table des matières

Remarque préliminaire: dans ce document, les termes désignant des personnes sont utilisés au sens générique; ils ont à la fois la valeur d'un masculin et d'un féminin. Par ailleurs, l'annexe 3 fournit un répertoire des abréviations et un glossaire des termes techniques.

1 Introduction

1.1 Contexte

Le 26 septembre 2013, le conseiller aux États Paul Rechsteiner a déposé la motion 13.3841 «Commission d'experts pour l'avenir du traitement et de la sécurité des données».

Cette motion charge le Conseil fédéral d'instituer une commission d'experts interdisciplinaire afin de répondre aux questions suivantes:

1. D'un point de vue technologique et politique, comment évaluer l'état actuel du traitement des données?
2. Quels sont les effets sur l'économie suisse, la société et l'État?
3. Comment évaluer le cadre juridique actuel dans ce domaine?
4. Quelles conclusions en tirer pour la Suisse au niveau national? Quelles conclusions en tirer quant à d'éventuelles initiatives au niveau international?

Développement de l'auteur de la motion:

Les révélations d'Edward Snowden montrent que, en Suisse également, les hypothèses sous-tendant le traitement et la sécurité des données ne sont plus fondées. L'ampleur des problèmes soulevés dépasse largement les frontières de notre pays. La Suisse, pays à l'économie hautement développée, ferait bien de se forger sa propre opinion; pour y parvenir, il lui faut recueillir les conseils avisés d'experts compétents avant de tirer d'éventuelles conclusions.

Avis des Chambres fédérales:

Le Conseil national et le Conseil des États ont tous deux reconnu que les mesures prises par le Conseil fédéral, en particulier la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), constituaient une première étape importante. Ils ont toutefois estimé que ces travaux étaient focalisés sur la protection de l'État et des infrastructures critiques et ne prenaient pas suffisamment en compte la signification du développement numérique pour la société dans son ensemble, la population et l'économie. Une commission d'experts pourrait selon eux examiner ces questions cruciales pour l'avenir numérique de la Suisse, et le rapport qu'elle rendrait permettrait de lancer un débat public.

Le Conseil des États a adopté la motion le 3 décembre 2013, le Conseil national, avec un ajout, le 13 mars 2014.

1.2 Composition du groupe d'experts

Le Département fédéral des finances (DFF), chargé de mettre en œuvre la motion, a, pour des raisons formelles, institué la commission sous la forme d'un groupe d'experts composé de douze personnes issues du monde scientifique, de l'administration et de l'économie (cf. liste à l'annexe 1). Il a confié la présidence du groupe d'experts à l'ancienne conseillère nationale Brigitta M. Gadient. Au point de vue administratif, le groupe d'experts est rattaché au Secrétariat général du DFF. Ses travaux étaient limités à trois ans et devaient prendre fin en 2018.

1.3 Priorités thématiques et délimitation

Compte tenu de l'ampleur du sujet et du caractère limité de ses ressources, le groupe d'experts a donné la priorité à la sécurité de l'information, à la protection des données, aux questions de responsabilité, à l'accès aux données et à la propriété des données.

Il a traité les champs d'analyse «information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche» et «transformation numérique et éthique» jusqu'à être en mesure d'élaborer une base de discussion et de formuler des recommandations générales. S'agissant des relations entre l'État et les citoyens ou les entreprises (G2Ci/B pour *Government to Citizen/Business*), il s'est focalisé sur les tâches de protection de l'État, sur les données d'administrations publiques librement réutilisables (OGD pour *Open Government Data*) et sur la cyberadministration. Il ne s'est intéressé que de façon marginale aux effets socioéconomiques de la transformation numérique (conséquences pour le marché du travail, économie de plateformes, etc.), qui relèvent en particulier du droit social, du droit du travail et du droit fiscal. Enfin, il n'a pas examiné les conséquences de la transformation numérique sur l'économie financière qui ne touchaient ni à des questions de sécurité ni au phénomène de la blockchain.

Dans le cadre de l'affaire RUAG qui a éclaté au printemps 2016, le groupe d'experts a par ailleurs été chargé d'examiner les mesures du Conseil fédéral et de présenter un rapport à ce sujet pour la fin 2016.

1.4 Méthodologie et structure du rapport

Le chapitre introductif (chap. 3) dégage, d'un point de vue général, les piliers du développement actuel et analyse les facteurs d'incitation (*push*) et d'attraction (*pull*) auxquels ils sont soumis de même que les possibilités et les risques qui s'y rattachent. Les chapitres 4 à 11 examinent les différents champs d'analyse en exposant la situation actuelle, l'évolution future, les possibilités et les risques, la réglementation et les mesures qui s'imposent à court ou à long termes. Le groupe d'experts a axé ses recommandations sur les objectifs suivants:

- garantir la dignité humaine et les droits, ou plus exactement la protection, de la personnalité;
- garantir le développement du numérique pour l'ensemble de la société;
- garantir la capacité d'action de l'État;
- garantir la protection des consommateurs;

- garantir la sécurité de l'information aux différents acteurs des différents secteurs économiques, à l'État et aux utilisateurs privés.

Le groupe d'experts a réparti ses importants travaux de clarification entre plusieurs groupes de travail. Il a par ailleurs confié l'exécution du mandat RUAG à un groupe de travail spécifique dont le rapport, destiné au Conseil fédéral, n'a pas été intégré au présent document.

Les groupes de travail ont consulté ou auditionné d'autres experts en fonction de leurs besoins, en particulier dans les domaines de la recherche, de la formation et de la sensibilisation, et dans ceux de la sécurité informatique et de la gestion des risques en vue de l'élaboration d'une éventuelle protection informatique de base pour l'économie au sens large.

1.5 Audition de représentants de groupes d'intérêts et d'experts

Le groupe d'experts a procédé à différentes auditions afin d'identifier les besoins et les préoccupations des différents groupes d'intérêts et secteurs économiques. Il a également consulté différents experts (cf. liste à l'annexe 2).

2 Analyse du mandat

2.1 Définition de l'objet de l'étude

L'évolution des technologies de l'information et de la communication a entraîné la colonisation par le numérique de tous les domaines de la vie: l'économie, la société, l'État et la grande majorité des personnes sont touchés dans une même mesure. Cette évolution se manifeste par l'enregistrement et le mesurage numériques du monde, quoique, en général, ce sont des valeurs analogiques que l'on transforme en données électroniques, qui sont ensuite traitées et enregistrées. Les données sont l'unité de base de la «révolution numérique», quelle que soit leur nature: données techniques ou personnelles, données de pilotage, informations, données de surveillance, données de communication, etc.

Cette évolution impressionne d'une part par la quantité des données dont il est question, d'autre part par la capacité des données à être mises en réseau et évaluées par de nouveaux instruments d'analyse, ainsi que par le fait qu'il n'existe pratiquement plus aucun domaine du monde réel qui ne soit concerné. L'augmentation du volume de données, qui était jadis le fait des seuls ordinateurs, est désormais exponentielle, principalement sous l'effet des terminaux mobiles et des objets connectés (l'Internet des objets [IdO, en anglais *Internet of Things*]).

Si le progrès technologique a jeté les bases de cette transformation, l'économie reste son principal moteur. Une multitude d'infrastructures et de services numériques sont à la disposition de tous, partout et à tout moment, dans tous les domaines de la vie. En voici quelques exemples significatifs: réseaux sociaux, commerce en ligne, jeux en ligne, *big data*, IdO, algorithmes et précurseurs de l'intelligence artificielle (apprentissage automatique, apprentissage profond), blockchain, réalité virtuelle et réalité augmentée, et agents conversationnels (*socialbots* et *chatbots*). De nouvelles infrastructures numériques telles que les ordinateurs quantiques ou des interfaces homme-machine ultra-sophistiquées sont en passe d'atteindre un niveau de développement commercialisable. Le potentiel économique est considérable. L'essence de ces développements reste le traitement de données. Aussi le groupe d'experts a-t-il étendu la première question de la motion, qui portait sur les aspects technologiques et politiques, aux aspects économiques.

Outre de nombreux avantages tels que gains de productivité et d'efficience, nouveaux services, confort, nouveaux modes de coopération (financement, production et savoir participatifs [*crowdfunding*, *crowdsourcing* et *crowdknowledge*]), ou encore possibilité de transformer une société de l'information en une société de la connaissance en vue d'une démocratisation du savoir, le traitement de données moderne et la transformation numérique comportent aussi des risques évidents. Les défis posés par le traitement de données sont les suivants:

1. Qu'est-ce qu'une donnée du point de vue juridique? Un support d'information ou un objet de valeur? Qui peut l'enregistrer, la modifier, la reprendre, l'exploiter, l'utiliser, se l'approprier, la copier ou la définir comme propriété intellectuelle, et à quel moment?
2. L'évolution du traitement des données a une influence considérable sur la protection de la sphère privée et de l'autodétermination en matière d'information. Il

s'agit là de droits de l'homme fondamentaux tels que la protection de la personnalité, la préservation de sa propre capacité d'action et le droit à la tranquillité. La transformation numérique est un enjeu de taille pour ces principes et ces valeurs fondamentales: elle crée des zones de tension entre la sécurité informatique et le confort des utilisateurs, entre la responsabilité personnelle et la protection des consommateurs, entre la réduction du coût des transactions et les exigences en matière de protection des données. Elle exige par conséquent une renégociation, éventuellement suivie d'une redéfinition, des relations de coopération et de confiance qui existent entre fournisseurs, utilisateurs, consommateurs et autorités.

3. Un traitement sûr suppose que soient réglés des aspects techniques et organisationnels tels que collecte, transformation, transport, enregistrement et archivage des données. Il convient à cet égard de respecter les quatre attributs de la sécurité informatique: confidentialité, disponibilité, intégrité et traçabilité, comme étant les conditions de base de la souveraineté des données.

4. Le numérique a généré une multitude de nouveaux modèles d'affaires dont certains, comme le transfert de la publicité sur Internet, se sont révélés disruptifs. Il est probable que les phénomènes disruptifs vont se multiplier, avec à la clé des défis majeurs pour bon nombre de structures normatives existantes telles que la protection des consommateurs, le droit du travail, le droit des assurances sociales, le droit fiscal, le droit de la propriété intellectuelle et le droit de la concurrence.

5. Le pouvoir que confère le contrôle des données et des flux d'information influe non seulement sur la souveraineté de chaque individu, mais aussi sur celle de la société tout entière, sur sa cohésion et sur ses structures démocratiques. Techniquement parlant, les moyens de surveillance et de manipulation vont déjà bien au-delà de ce que George Orwell avait imaginé dans son roman dystopique *1984*. Il faut par conséquent réduire le risque d'abus au strict minimum.

6. Les effets de la transformation numérique sur le traitement des données vont bien au-delà de simples questions de sécurité, de droit ou de réglementation. Le développement a atteint un stade où il remet en question des structures de valeurs et des principes juridiques que la société s'est constitués au fil des siècles. C'est pourquoi l'éthique revêt une importance décisive lorsqu'il s'agit de répondre à ces questions fondamentales.

Certains voient dans la révolution numérique une catastrophe qui se prépare, d'autres la possibilité, pour la société, de franchir la prochaine étape de son développement. Comme chaque progrès technique d'envergure, elle recèle des possibilités et des risques séparés par une fine frontière. Ces paramètres sont également pris en considération dans les différents champs d'analyse.

2.2 Champs d'analyse

La prise en compte de la société dans son ensemble a joué un rôle décisif dans les réflexions du Parlement concernant la motion. Aussi le groupe d'experts a-t-il adopté une perspective transversale, qui reflète toute la diversité des types de données et des infrastructures, de même que l'ensemble des acteurs concernés.

Pour discuter des implications de la transformation numérique pour l'ensemble de la société, le groupe d'experts a défini trois champs d'analyse portant sur les relations

mutuelles entre les différents groupes d'acteurs (citoyens, consommateurs, fournisseurs, producteurs, autorités), à savoir:

- les relations entre les fournisseurs ou les producteurs, d'une part, et les consommateurs et les utilisateurs, d'autre part (B2C);
- les relations entre les fournisseurs ou les producteurs (B2B);
- les relations entre l'État et les citoyens ou les entreprises (G2Ci/B).

Cinq champs d'analyse supplémentaires s'inscrivent dans une thématique transversale: «sécurité de l'information», «accès aux données et portabilité», «blockchain», «information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche» et «transformation numérique et éthique».

Cette approche a permis de répondre à la question 3 de la motion en tenant compte de tous les domaines juridiques pertinents.

2.2.1 Champ d'analyse sécurité de l'information

Pour observer cette question dans sa globalité, il faut la placer dans un contexte large, d'où l'emploi ici du terme très général de sécurité de l'information, étant entendu que l'accent sera mis sur la sécurité numérique. Les infrastructures numériques, depuis le smartphone jusqu'à l'écosystème Internet, constituant à l'heure actuelle la base du traitement de données, la sécurité et la résilience des données dépendent largement de la sécurité et de la résilience de ces infrastructures.

Dans le champ d'analyse sécurité de l'information, le groupe d'experts a débattu des menaces, des dangers, du potentiel de dommages, de la surface d'agression et des possibilités qui caractérisent les infrastructures numériques. Il a fait le point sur la sécurité de l'information, discutant de son évolution future et des défis à relever et exposant des pistes de solution.

Il a ainsi traité des thèmes aussi variés que le dilemme entre confort d'utilisation et sécurité, le défi que constitue la complexité alliée à un manque d'industrialisation de la sécurité informatique, les possibilités à exploiter, mais aussi les risques inhérents à une culture, une administration et une économie mues par la technologie, où ce qui est «faisable techniquement» et ce qui peut être «mis en œuvre d'une manière sûre» s'affrontent en permanence. Ce qui est en jeu, c'est l'avenir du monde analogique, qui est de plus en plus dominé par le traitement de données.

Le groupe d'experts a tenté de déterminer ce qu'on entend au juste par sécurité dans le monde du numérique. Cette sécurité est-elle tangible? Peut-on la mesurer? Existe-t-il des indicateurs qui permettent une gestion efficiente et efficace des risques?

Outre la question de la formation et du perfectionnement en matière de sécurité des experts informatiques, des secteurs professionnels concernés et de la population, le groupe d'experts a aussi traité en profondeur les sujets suivants: la cryptographie, la sûreté des authentifications et des identifications dans l'univers numérique, la nécessité d'édicter des normes pour les organisations et les produits, en particulier dans l'univers interconnecté des objets (IdO), et la nécessité de doter la Suisse d'un réseau de communication sûr.

2.2.2 Champ d'analyse relations entre les entreprises et les consommateurs (B2C)

Le champ d'analyse B2C porte sur les clients et les utilisateurs. Internet et des modèles d'affaires nouveaux ont modifié les rapports de dépendance, de connaissance et de pouvoir entre les propriétaires et les transformateurs de données d'une part, et les fournisseurs et les consommateurs d'autre part. Ce phénomène a des conséquences sur la protection à la fois de la sphère privée, de l'autodétermination en matière d'information et des consommateurs.

Le volume des données de clients et d'utilisateurs collectées et la densification de ces données représentent un défi croissant pour les principes actuellement en vigueur de l'autodétermination en matière d'information et pour la protection de la sphère privée. Compte tenu de cette évolution et du fait que la loi fédérale du 19 juin 1992 sur la protection des données (LPD) est en cours de révision (P-LPD), le groupe d'experts a tenté de savoir si la protection traditionnelle des données et son développement systématique dans le P-LPD seront à la hauteur à l'avenir, s'il existe d'autres solutions et quels pourraient être les points d'amorce de celles-ci. Pour déterminer dans quelle mesure les principes de la protection des données sont compatibles avec les méthodes modernes de traitement des données telles que l'analyse des *big data* et l'intelligence artificielle, le groupe d'experts a travaillé sur des scénarios d'évolution couvrant aussi une perspective à long terme.

L'enregistrement des utilisateurs et des clients au moyen de procédés de profilage et de notation (ou *scoring*) met la protection des consommateurs face à de nouveaux défis tels que l'absence de transparence et la discrimination en matière de prix et de constitution des offres. On ne peut pas ignorer non plus le fait que, sur les réseaux sociaux, la liberté de l'utilisateur d'aller voir ailleurs est entravée et les frais de transaction augmentent. Compte tenu de ces éléments, le groupe d'experts s'est penché sur différents aspects de la protection des consommateurs tels que les conditions de vente en ligne, la différenciation des prix, la conclusion de contrats dans le domaine du numérique, le blocage des accès et le blocage géographique. La question, également importante à cet égard, de la responsabilité est traitée dans le champ d'analyse «Thèmes communs aux champs d'analyse B2C et B2B: accès aux données, propriété des données et nouveaux enjeux liés à la responsabilité» (cf. ch. 2.2.4 et chap. 7).

2.2.3 Champ d'analyse relations entre les entreprises (B2B)

La transformation numérique entraîne un accroissement des interconnexions à l'échelle internationale particulièrement marqué dans le B2B. Dans ce champ d'analyse, le groupe d'experts a commencé par s'interroger sur les effets de l'économie collaborative. Ce phénomène fait naître de nouveaux modèles d'affaires pour lesquels la frontière entre fournisseurs professionnels et privés de produits et de services est toujours plus perméable. Le groupe d'experts s'est contenté d'identifier les besoins en matière de réglementation de ces nouveaux modèles d'affaires tels que plateformes d'hébergement et services de mobilité. Il n'a pas traité en détail les aspects relevant du droit du travail, du droit des assurances sociales, du droit fiscal, du droit du bail, etc., car le Conseil fédéral a chargé différents offices fédéraux (notamment le Secrétariat d'État à l'économie [SECO] et l'Office fédéral des routes [OFROU]) de procéder à des clarifications dans ces domaines.

Le groupe d'experts a ensuite examiné les rapports des entreprises entre elles. Dans le contexte des nouveaux marchés en ligne, cette question relève plus particulièrement de la loi du 6 octobre 1995 sur les cartels (LCart) et de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD). Le groupe d'experts s'est aussi attaché à expliquer certains aspects de la forte interconnexion internationale et leurs conséquences juridiques potentielles.

2.2.4 Thèmes communs aux champs d'analyse B2C et B2B: accès aux données, propriété des données et nouveaux enjeux liés à la responsabilité

L'un des aspects essentiels du traitement de données réside dans la question de savoir comment conférer aux personnes physiques et morales le statut juridique qui leur permette de disposer de leurs données (personnelles et techniques). On touche ici à la portabilité des données, à l'accès aux données et au débat sur les avantages et les inconvénients de la propriété des données. Du point de vue de la protection de la personnalité, de la protection des consommateurs (B2C), mais aussi du traitement économique des données (B2B), le transfert des droits d'utilisation, l'utilisation exclusive et la publication de données posent de nombreux problèmes qui rendent inutile le maintien d'une distinction stricte entre le B2C et le B2B.

Le passage au numérique crée de nouvelles responsabilités qui, au sens large, présentent généralement un rapport avec le thème de la sécurité de l'information, mais dont le contenu influe aussi sur de nouveaux modèles d'affaires. Les questions de responsabilité concernent aussi bien les fournisseurs de produits et services que les utilisateurs, qu'il s'agisse d'entreprises ou de particuliers. Le groupe d'experts a donc décidé de ne pas procéder à un examen différencié dans le cadre des rapports entre acteurs B2C et B2B.

2.2.5 Champ d'analyse relations entre l'État et les citoyens ou les entreprises (G2Ci/B)

Le champ d'analyse G2Ci/B ne vise pas à éclairer uniquement les rapports entre l'État et les citoyens au sens strict, mais aussi, selon une approche multi-acteurs, les rapports entre l'État et tous les autres acteurs de la société, des exploitants d'infrastructures critiques aux particuliers en passant par l'économie privée et les organisations.

Les révélations d'Edward Snowden ont fait prendre conscience au public que les services de renseignement de même que d'autres autorités publiques et des acteurs proches de l'État se servent du numérique et des nouveaux moyens techniques à des fins d'espionnage et pour collecter préventivement un maximum de données. Cette évolution est un défi pour la relation entre l'État, avec son appareil de sécurité, et l'individu, qui a droit au respect de sa sphère privée. En même temps, le cyberespace force l'État à assumer ses tâches de protection, à définir les prestations de soutien correspondantes pour la société et pour l'économie et à créer un cadre approprié.

Ces tâches comportent des aspects généraux tels que la sauvegarde de la souveraineté numérique: dans quelle mesure l'État doit-il et peut-il considérer la «toile» et les infrastructures numériques comme une extension de l'espace public et de l'espace privé où il doit assumer ses tâches (protection des libertés et de la sécurité, égalité

des chances, prospérité, ordre juste et pacifique)? Dans quelle mesure l'État (administration fédérale, cantons, communes) doit-il offrir aux citoyens des prestations numériques telles que services en nuage ou autres prestations informatiques dans le domaine de la sécurité? L'augmentation des risques affecte aussi les chaînes d'approvisionnement dans le domaine informatique, lorsque certains pays incitent, par la loi ou par d'autres moyens, leur industrie informatique à ne pas respecter vis-à-vis de leurs clients une obligation de garder le secret imposée par des dispositions contractuelles ou légales. Le groupe d'experts a par ailleurs examiné d'autres questions spécifiques telles que: l'informatique a-t-elle besoin de normes de sécurité? Faut-il imposer la notification des cyberincidents? Et il expose dans ce chapitre des mesures préventives et réactives que l'État pourrait prendre à l'échelle nationale pour améliorer la maîtrise des cyberrisques, de même que le rôle que joue l'armée à cet égard.

Le G2Ci/B ne concerne pas uniquement les tâches de protection de l'État mais aussi son rôle de fournisseur de services publics sous forme numérique (cyberadministration) et de promoteur d'une culture d'ouverture des données (*open data*), y compris celles du secteur public (OGD).

Pour conclure ce chapitre, le groupe d'experts s'est intéressé aux possibilités et aux risques liés à la transformation numérique, et à ses conséquences sur la démocratie sous sa forme actuelle: quelle est globalement l'importance des médias et des gros fournisseurs de services Internet dans les structures gouvernementales? Comment canaliser d'une manière compatible avec la démocratie les nouveaux moyens de propagande et de censure, aussi subtils que vastes, que génère le pilotage algorithmique des fils d'actualité sur les réseaux sociaux (manipulation numérique [*big nudging*] et *socialbots*)? Quelle est l'ampleur du risque de manipulation? Y a-t-il violation du droit «d'être laissé tranquille»? En fin de compte: comment une société de l'information potentiellement manipulable peut-elle se transformer en une société de la connaissance autodéterminée?

2.2.6 Champ d'analyse blockchain

La technologie de la blockchain doit sa notoriété à l'essor des cryptomonnaies, à commencer par le bitcoin. Également appelée technologie des registres distribués, elle offre par ailleurs un large éventail de possibilités d'application pour l'enregistrement numérique de transactions. Elle est sans doute appelée à jouer à terme un rôle majeur. C'est ce qui a incité le groupe d'experts à examiner à part, sous l'angle du droit et de la sécurité, cette nouvelle infrastructure numérique de traitement des données.

Les blockchains recèlent des possibilités: par exemple, les nouveaux modèles de financement et moyens d'allocation de capital sans intermédiaire dans le domaine de l'*initial coin offering* (levée de fonds grâce à la technologie des registres), et les systèmes de cryptomonnaies à frais de transaction réduits. Elles comportent aussi des risques: manque de transparence, insécurité juridique, blanchiment d'argent et perte de contrôle potentielle de l'État sur la masse monétaire et les flux monétaires transnationaux. Le groupe d'experts n'a pas été en mesure de traiter les possibilités et les risques dans le domaine financier dans le cadre restreint de son mandat.

2.2.7 Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche

Dans ce champ d'analyse, le groupe d'experts a identifié quatre caractéristiques majeures du passage au numérique:

- l'automatisation accélérée de nombreux processus dans le monde du travail;
- le mesurage numérique croissant de tous les domaines de la vie;
- la possibilité, décuplée par les technologies numériques, de créer, de diffuser et de modifier des contenus multimédias, et
- l'importance croissante des systèmes autonomes et de la dépendance à leur égard.

S'agissant de relever ces défis et d'inciter la population à prendre une part active à l'organisation du numérique, la formation revêt une grande importance. Le groupe d'experts s'est demandé quels étaient les changements nécessaires à chacun de ces niveaux, dans chacun de ces domaines. Les compétences aussi sont d'une importance fondamentale. Le groupe d'experts a formulé des recommandations visant à élaborer un processus qui permette d'identifier les compétences requises. Car la formation ne s'arrête pas à la fin de la scolarité obligatoire ou de la formation professionnelle initiale. La société doit être capable d'apprendre tout au long de la vie. Outre la formation, le groupe d'experts a réfléchi aux moyens de tirer parti de la culture ou de l'espace public pour sensibiliser la population aux thèmes du numérique et lui donner les moyens de se les approprier.

2.2.8 Champ d'analyse transformation numérique et éthique

Dans le champ d'analyse transformation numérique et éthique, le groupe d'experts a discuté des effets du numérique sur nos valeurs et sur les questions d'éthique qui s'y rattachent. Il a approfondi l'examen de problèmes, dont certains avaient déjà été abordés dans d'autres champs d'analyse, sous l'angle de valeurs fondamentales: dignité humaine et sphère privée, égalité et interdiction de discriminer, autonomie et autodétermination, ou encore transparence, solidarité et sécurité. Cette analyse visait notamment à déterminer dans quelle mesure la réflexion éthique peut éviter les évolutions inopportunes et favoriser les développements souhaitables.

Dans ce chapitre, le groupe d'experts s'est efforcé d'exposer les enjeux éthiques fondamentaux de la transformation numérique avec la brièveté requise, en étant bien conscient que les questions soulevées mériteraient une analyse beaucoup plus fouillée et qu'il pourrait, au mieux, relever des problématiques et ébaucher des solutions possibles et des recommandations. Il s'était fixé pour objectif de fournir, dans la mesure du possible, une base pour le nécessaire débat, sachant que l'éthique est un élément fondamental du travail législatif et de la réglementation.

Le groupe d'experts a défini les priorités suivantes:

- Comment faire en sorte que le débat sur les questions d'éthique ne reste pas à la traîne mais accompagne activement le développement de la technique?

- Comment une conception éthique (*value sensitive design*) peut-elle contribuer à garantir un développement technologique qui soit compatible avec les valeurs fondamentales de la société?
- Comment garantir que l'éthique acquière une importance appropriée dans la formation et le perfectionnement des experts qui exercent une influence déterminante sur le numérique?
- Par quelles mesures améliorer la protection des valeurs fondamentales de notre société?

3 Piliers du développement actuel

3.1 Facteurs d'incitation

3.1.1 Conditions techniques

Le principal facteur d'incitation est, depuis toujours, le développement technologique. Certains des principaux moteurs de la révolution numérique en cours ont commencé à déployer leurs effets il y a plus de cinquante ans: en particulier la puissance de calcul des processeurs, la stabilité et la rapidité des réseaux de transport de données et la possibilité de collecter et d'enregistrer des données. Leurs effets sur les modes de vie sont restés relativement faibles pendant des décennies malgré un déploiement progressif de l'ordinateur dans les bureaux et les sites de production et chez les particuliers. Au cours des quinze à vingt dernières années, ces moteurs ont atteint un niveau de développement et un coût qui ont permis leur utilisation de masse en réseau, avec un effet boule de neige sur l'évolution de la technologie en général.

3.1.1.1 Le progrès technologique en chiffres I: la puissance de calcul des ordinateurs

Le développement de circuits intégrés dans les puces informatiques commerciales est l'un des piliers de la révolution numérique. La capacité de ces puces est passée de 2300 transistors au début des années 1970 (Intel 4004) à plusieurs milliards aujourd'hui. Si la vitesse des voitures avait augmenté dans les mêmes proportions au cours des quarante dernières années, nous circulerions aujourd'hui à un dixième de la vitesse de la lumière. Chacun des quelque trois milliards de propriétaires de smartphone que compte la planète a dans la poche un ordinateur plus puissant que les super-ordinateurs de la taille d'une pièce d'habitation des années 1980. La loi de Moore, formulée en 1965, selon laquelle le nombre de transistors par circuit de même taille allait doubler tous les deux ans, s'est vérifiée. La puissance de calcul n'évolue cependant pas aussi vite que la capacité de stockage, qui double tous les dix-huit mois.

La miniaturisation des puces atteint toutefois ses limites: alors que les transistors des années 1970 faisaient la taille d'une cellule sanguine et étaient visibles au simple microscope, ils ont aujourd'hui la largeur de 100 atomes (environ 20 nanomètres, c'est-à-dire 20 millionièmes de millimètre), ce qui rend toujours plus difficile le pilotage des chargements et plus coûteuse la production. Cela dit, la fin prochaine de la loi de Moore a déjà mis en branle de nouveaux développements: nouveaux types de transistors, nouveaux matériaux, ordinateurs quantiques et utilisation de puces optimisées à des fins spécifiques dans le nuage. La mise en réseau des ordinateurs affranchit l'utilisateur final de la puissance de son propre ordinateur. Lorsqu'un GPS calcule aujourd'hui l'itinéraire le plus rapide, il ne fait qu'envoyer les données clés. Les calculs complexes sont effectués dans le nuage par des logiciels spécialisés. La plupart des services d'application reposent exactement sur ce principe, et cette tendance est appelée à se développer.

3.1.1.2 Le progrès technologique en chiffres II: la mise en réseau des ordinateurs

La mise en réseau des ordinateurs est le second pilier du passage au numérique. Sans les progrès révolutionnaires accomplis en matière de capacité et de qualité des transferts de données, il aurait été impossible d'atteindre le niveau de développement actuel. En 1977, le premier modem moderne affichait une vitesse de transmission de 300 bits par seconde (bit/s), ce qui correspond à environ 37 caractères. Aujourd'hui, la norme de téléphonie mobile LTE permet une vitesse de transmission théorique de 300 mégabits par seconde (Mbit/s), soit 300 000 000 bit/s. En Suisse, la vitesse moyenne du réseau était en 2016 de 18 Mbit/s (connexions à large bande), soit 60 000 fois supérieure à celle de 1977. Les vitesses actuelles de transmission par réseau mobile ou par câble dépassent même la vitesse de transmission interne des premiers PC. Sans cette capacité des ordinateurs à être mis en réseau, il n'aurait pas été possible de passer à l'Internet des objets et à l'Internet «de tout» (IdT, en anglais *Internet of Everything*) que nous connaissons aujourd'hui. Le premier réseau (ARPANET, ancêtre d'Internet) a été créé en 1969 entre quatre ordinateurs. Aujourd'hui, les ordinateurs en réseau sont une dizaine de milliards.

3.1.1.3 Le progrès technologique en chiffres III: l'évolution du prix du matériel

L'évolution des prix s'est révélée déterminante pour la généralisation des outils informatiques: la puissance de calcul que l'on obtient pour un franc est multipliée par cent tous les dix ans. Les moyens qui, en raison de leur coût et de leur complexité, étaient autrefois réservés à des experts de certains domaines de l'économie et de la recherche sont aujourd'hui compatibles avec une utilisation commerciale de masse.

3.1.2 Évolution future

Il reste difficile de prévoir les effets à long terme du progrès technologique sur la société et l'économie, même si les bases techniques sont connues. Citons l'exemple de la menace que constitue la collecte de données pour la sphère privée. Dès 2010, Eric Schmidt, qui fut longtemps le PDG de Google, déclarait quant à l'avenir de la sphère privée: «Nous savons où vous êtes. Nous savons où vous êtes allé. Nous sommes en mesure de connaître plus ou moins l'objet de vos pensées.» À l'époque, ceux qui ont saisi la signification de cette déclaration n'étaient sans doute pas nombreux. À l'heure actuelle, on voit apparaître dans différents domaines des innovations dont la portée a toutes les chances de devenir considérable: nouvelles interfaces entre l'homme et la machine, développement de l'ordinateur quantique et Internet des nano-objets. Les chiffres qui suivent y sont consacrés.

3.1.2.1 L'interface homme-machine

L'interface entre l'homme et le cyberespace s'apprête à franchir une nouvelle étape de développement révolutionnaire: la transformation de pensées en données de pilotage (interface cerveau-machine ou neuronale directe) constitue le niveau ultime d'une convivialité parfaitement efficiente. Avec elle, la mise en réseau de tout finit par inclure l'homme lui-même. D'ores et déjà au service de personnes handicapées, elle pourrait très bientôt révolutionner l'interface homme-machine après le clavier, la souris et l'écran tactile. Des systèmes de stimulation des tissus nerveux ou cérébraux à des fins thérapeutiques tels que les implants cochléaires ou du tronc cérébral, qui transmettent

des signaux sonores en cas de surdité, existent depuis longtemps. Dans quelle mesure ces technologies sont-elles adaptées à la transmission directe d'informations entre l'ordinateur et le cerveau? Il est trop tôt pour le dire.

La prochaine étape, qui est la connexion (interface) de l'homme à Internet, n'en est encore qu'à ses débuts mais progresse à grands pas, ce qui a inspiré à certains experts le terme d'Internet «de tout». Les risques à long terme de cette évolution sont évidents: ce genre d'interface pourrait un jour menacer la confidentialité de pensées n'ayant même jamais été verbalisées ni couchées sur le papier. Transformées en données, elles seraient exposées sur le web aux mêmes risques que n'importe quelle autre donnée. La technologie pourrait aussi priver de son fondement la conviction que les pensées sont le dernier bastion de la sphère privée et de l'autodétermination en matière d'information. Ce risque est encore purement théorique, mais l'évolution de la technologie ne permet plus de l'exclure absolument.

3.1.2.2 L'ordinateur quantique

Les États-Unis, la Chine et l'Europe sont engagés dans une course que gagnera celui qui aura développé le premier ordinateur quantique pleinement opérationnel. Contrairement à un ordinateur courant, l'ordinateur quantique peut, grâce à ses unités de stockage d'informations appelées qubits, représenter simultanément un nombre considérable (exponentiel) d'états intermédiaires, ce qui lui confère une puissance énorme. Il est probable que cette puissance dépassera largement, dans les années à venir, celle des ordinateurs courants les plus performants, mais uniquement dans le domaine de certains problèmes mathématiques bien spécifiques.

Le développement des ordinateurs quantiques aura aussi des effets intéressants dans d'autres domaines, comme la chimie, lorsqu'il permettra par exemple de modéliser les réactions de molécules complexes, ce dont les ordinateurs courants sont aujourd'hui incapables. Par ailleurs, on disposera sans doute, dans dix à quinze ans, d'un ordinateur quantique polyvalent, qui sera par exemple en mesure de déchiffrer les techniques de chiffrement asymétrique aujourd'hui largement répandues, en particulier le chiffrement RSA. Des experts estiment à 50 % les chances de voir apparaître un ordinateur quantique de troisième génération dans les dix prochaines années. Cela aurait des conséquences considérables puisque toute la sécurité du web repose précisément sur ces principes de complexité mathématique que l'informatique quantique sait résoudre (cf. ch. 4.4.1).

3.1.2.3 L'Internet des nano-objets

Le numérique, sous la forme du mesurage et du pilotage au moyen de données, s'imposera demain dans tous les domaines de la vie et de l'économie, même ceux qui n'avaient jusqu'ici aucun lien avec lui. Il affectera toujours plus les objets et le monde du vivant (plantes, animaux, êtres humains), et ce par l'action des nanocapteurs (une technologie qui n'en est qu'à ses balbutiements), qui transformeront l'Internet des objets en un Internet des nano-objets. Ces instruments cyberphysiques à l'échelle nano ne feront pas qu'enregistrer des données, ils influeront sur le monde réel, que ce soit dans le domaine médical, dans le contrôle de la qualité ou dans l'autoréparation d'objets grâce à des matériaux innovants. On peut aussi imaginer l'utilisation de nanocapteurs en amont d'une chaîne de production alimentaire, chez les animaux de rente et

les plantes, pour contrôler la qualité des produits de bout en bout et donner l'alerte si nécessaire.

3.1.3 Effets du progrès technologique

3.1.3.1 De l'ordinateur à l'Internet des objets

Si les premiers réseaux étaient uniquement formés d'ordinateurs connectés entre eux, l'IdO englobe aujourd'hui, grâce à la miniaturisation et à la transmission de données sans fil, tous les objets depuis le réfrigérateur jusqu'aux drones en passant par les terminaux numériques portables et les capteurs corporels (ce qu'on appelle la technologie portable ou mettable). Les systèmes cyberphysiques jouent un rôle déterminant dans cette évolution: il s'agit d'éléments mécaniques ou analogiques qui fusionnent avec des éléments d'information numériques pour collecter des données, les traiter puis agir sur l'environnement.

Ces objets et applications de l'IdO sont suffisamment intelligents pour percevoir et mesurer leur environnement, et pour répondre à des injonctions. Cette intelligence se limite toutefois à la création de données et à l'exécution d'ordres émis par des données. En effet, ces appareils, même les smartphones, ne disposent ni de la puissance de calcul ni de la capacité de stockage nécessaires pour un pilotage par la voix, par exemple. Leur intelligence leur vient de leur connexion à un traitement de données central situé dans un nuage.

L'IdO nous donne une idée de la réalité à venir. Selon certaines prévisions, dans deux ans, 1 milliard de PC, 5 milliards de smartphones et de 25 à 30 milliards d'objets connectés collecteront des données et les échangeront entre eux. En 2016, les utilisateurs d'Internet étaient 3,5 milliards. En mai 2018, ils étaient près de 4 milliards, c'est-à-dire que pour la première fois de l'histoire, plus de la moitié de la population mondiale était connectée.

Alors que le terme d'IdO s'utilise plutôt dans le contexte de la consommation et des services, celui d'«industrie 4.0» désigne le même phénomène d'interconnexion dans le domaine de la production. L'industrie 4.0 se caractérise par l'application, du début à la fin du processus d'organisation et de production, d'une communication et d'un pilotage fondés sur des données. Cela permet par exemple d'adapter la fonctionnalité de lignes de production en temps réel et avec une grande souplesse. Dans l'idéal, le produit communique avec son environnement pendant tout son cycle de vie (mise en service, contrôle du fonctionnement, maintenance, développement des fonctions, etc.). Pour cela, il faut que les machines puissent communiquer entre elles (M2M pour *machine to machine*), et même se piloter elles-mêmes, et que l'ensemble du processus de production soit «intelligent». Il faut donc connecter le contrôle et la surveillance des appareils et des processus à l'infrastructure d'information et de communication, ce qui ouvre de nouvelles perspectives, notamment dans la distribution: les fournisseurs peuvent faire évoluer leur offre de produits statiques vers des prestations de services dynamiques, adaptées aux besoins des clients. Cette approche est encore un projet d'avenir pour bon nombre de secteurs économiques.

La mise en réseau intelligente de systèmes cyberphysiques permet aussi de piloter des systèmes de plus grande envergure tels que des flux de circulation, des infrastructures énergétiques ou des infrastructures logistiques à l'échelle d'un pays. Elle s'impose chaque fois que le contrôle de systèmes au moyen d'installations de pilotage

en réseau présentant de nombreux nœuds de connexion devient de plus en plus complexe et que le traitement des données sortantes doit, si possible, avoir lieu en temps réel. Mais elle aussi n'en est encore qu'à ses débuts.

Le développement de l'IdO dans tous les domaines de la vie fait apparaître avec une force inédite la nécessité de réglementer l'interaction de tous les acteurs concernés, et ce dans des domaines aussi variés que les normes techniques et de sécurité, le droit de la protection des données, la responsabilité, la protection des consommateurs et la concurrence.

3.1.3.2 L'informatique en nuage

L'externalisation du stockage et du traitement des données dans le nuage grâce à des connexions rapides à large bande a apporté la flexibilité des ressources, l'efficience, les économies d'échelle et la spécialisation nécessaires pour permettre la gestion de volumes de données toujours plus importants. Les utilisateurs de services en nuage peuvent adapter leur puissance de calcul et leurs capacités de stockage à leurs besoins spécifiques et variables. En 2017, le nombre des serveurs en nuage a dépassé celui des serveurs d'entreprise. Sans cette technologie, qui permet aux utilisateurs de ne se soucier ni de l'infrastructure ni de la plateforme ni de l'application ni des données, l'univers des applications ne pourrait pas exister. La condition de son fonctionnement, ce sont des connexions à large bande stables, performantes et hautement disponibles, tant sur le réseau fixe que sur le réseau mobile.

L'informatique en nuage a aussi ses inconvénients: elle renforce la dépendance à l'égard du fournisseur (effet de verrouillage) et cause des inquiétudes concernant la sécurité. En effet, l'externalisation de données sensibles ou dont le traitement est soumis à des dispositions légales (données personnelles, par ex.) constitue un risque: lorsque le fournisseur de nuage est dépendant d'un système juridique étranger (ces systèmes ayant souvent une portée extraterritoriale; cf. ch. 8.2.7), ou contraint, pour d'autres raisons, de communiquer les données de ses clients à des autorités étrangères, la confidentialité est menacée.

3.1.3.3 L'avènement des données non structurées: les *big data*

Les données peuvent être générées directement par des activités humaines telles que recherches, transactions commerciales en ligne, interactions sociales sur les plateformes, ou simplement création de documents, de courriels ou de SMS. Mais une masse autrement plus importante de données provient d'ores et déjà de systèmes techniques de pilotage et de contrôle liés à la production ou à la technique des bâtiments. L'interconnexion de ces appareils grâce à la toile revêt une importance décisive: plus besoin de la main de l'homme pour saisir les données recueillies dans les infrastructures numériques; leur transmission et leur archivage se font automatiquement.

Avec la multiplication des capteurs, le monde réel est l'objet de mesurages et d'enregistrements de plus en plus étendus et précis, ce qui permet de le représenter par des données en temps réel. Les données secondaires qui documentent l'utilisation d'appareils électroniques tels que les téléphones mobiles en font partie. Ces données anticipent généralement les activités humaines, et s'il s'agit à première vue de données techniques, elles peuvent contenir de très nombreuses informations indirectes sur les personnes. La distinction, jusqu'ici statique, entre données personnelles et données

techniques perd ainsi de son acuité, ce qui soulève des questions épineuses, en particulier sous l'angle de la protection des données.

L'importance des données se trouve encore renforcée par les facteurs suivants:

- Il est aujourd'hui possible de copier des données, de les envoyer, de les modifier, de les enregistrer et de les mettre à la disposition de tous dans des proportions impensables il y a encore peu de temps, pour un coût marginal proche de zéro.

- La technologie et l'économie mettent à la disposition des utilisateurs de services informatiques des appareils et des terminaux numériques toujours plus conviviaux, à des prix toujours plus bas. Aujourd'hui, tout le monde ou presque a accès au cyberespace. Dans le monde développé, cet accès n'est pas loin d'être permanent pour quasiment 100 % de la population, grâce à des appareils numériques mobiles.

La donnée en tant que plus petite unité d'information est devenue l'unité de base de la transformation numérique. Le volume de données connaît une augmentation impressionnante: il double chaque année, et le rythme tend à s'accélérer. En 2020, il devrait franchir la barre des 40 zettaoctets (1 zettaoctet = 10^{21} octets)[1]. Internet voit transiter chaque jour quelque 4000 pétaoctets (1 pétaoctet = 10^{15} octets). L'ensemble des textes jamais écrits par l'humanité correspond à une centaine de pétaoctets. Selon certaines estimations, en 2018, on dénombre en une journée 280 milliards de courriels échangés et 3,5 milliards de recherches sur Google[2].

«*Big data*» s'est imposé comme terme générique pour désigner ce flot de données. Il désigne un phénomène qui se caractérise par les éléments suivants: la vitesse à laquelle les données sont collectées, générées et transférées, le volume des données, leur véracité ou leur qualité, et leur variété. Le terme variété se réfère à la nature des données: données courantes mais aussi photos, vidéos, enregistrements vocaux ou courriels. Les *big data* sont hétérogènes par leur nature et par leur format. Leur contenu n'est pas structuré et ne permet pas de les classer selon les critères d'une base de données relationnelle courante.

Selon certaines estimations, cela concerne bien plus de 90 % des données existantes. Les outils d'analyse des *big data* (cf. chiffre suivant) permettent de traiter et d'évaluer des volumes importants de données non structurées. Cependant, force est de constater que le stockage des données progresse beaucoup plus rapidement que leur évaluation. Plusieurs explications à cela: le manque d'outils d'analyse à un coût abordable, le manque d'expertise et l'évolution disparate de la vitesse de calcul d'une part et de la capacité de stockage d'autre part.

Les données sont communément considérées comme le pétrole du XXI^{e} siècle. Malgré leur marchandisation, leur valeur est presque impossible à déterminer. Les calculs et les estimations tendant à déterminer la valeur d'un lot de données concernant une personne sont très contrastés et reposent sur des informations indirectes. Chez

[1] Data Age 2015, The Evolution of Data to Life-Critical: https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf (état au 7.6.2018)

[2] http://www.internetlivestats.com (état en avril 2018); The Radicati Group, Inc. Email Statistic Report, 2017-2021, 2017: https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf

Google, qui réalise un chiffre d'affaires de 80 milliards de dollars avec près de 2 milliards d'utilisateurs, cette valeur devrait être d'une quarantaine de dollars par utilisateur. Mais elle dépend aussi du rachat d'entreprises qui travaillent sur des données. En 2014, Facebook a déboursé 19 milliards de dollars pour racheter WhatsApp, qui comptait alors 600 millions d'utilisateurs, ce qui donne une valeur de 32 dollars par utilisateur. IBM a payé 12 dollars par utilisateur lors du rachat de Truven Health Analytics, mais Microsoft 58 dollars par utilisateur pour le rachat de LinkedIn. Malgré leur caractère aléatoire, ces chiffres montrent clairement que les entreprises sont prêtes à investir des montants importants dans les données personnelles.

3.1.3.4 L'analyse de masses de données (*big data analytics*)

Techniquement parlant, l'analyse des *big data* permet d'évaluer d'importants volumes de données non structurées. Elle consiste souvent non pas à vérifier une thèse à partir de données recueillies, mais à détecter, par l'analyse statistique de données de masse, des corrélations et des interactions révélatrices de certains modèles de comportement ou d'événement, y compris en temps réel. Les résultats obtenus doivent contribuer à améliorer les processus de production, d'exploitation, de distribution et de gestion de toute nature, à réduire les risques, à accélérer le temps de réaction en cas d'imprévu, à mieux anticiper les comportements et les événements et à fournir des réponses appropriées. L'énorme potentiel de développement de ces outils est évident, tant pour l'économie que pour l'administration et pour le bien commun.

Tout cela fait des données une nouvelle source de création de valeur, puisqu'elles permettent de tirer des conclusions n'ayant parfois aucun rapport avec le but premier de leur collecte. D'où la notion de recyclage de données. L'analyse des *big data* modifie ainsi le cycle de vie jusqu'ici statique des données structurées. Lorsqu'un lot de données a été disloqué, des corrélations permettent soit de le recomposer à neuf, soit de le restaurer à l'identique. Ces manipulations ont des conséquences sur le traitement des données personnelles, sur les possibilités et les limites de l'anonymisation et, partant, sur la protection des données (cf. ch. 5.3.1.6).

Comme toute technologie, celle-ci recèle des possibilités (amélioration de la gestion des risques, fonctionnalité optimisée) et des risques (prévisibilité des actions humaines avec risque de discrimination et de manipulation) séparés par une fine frontière. La police prédictive (*predictive policing*) permet aujourd'hui de piloter l'affectation des forces de l'ordre par la reconnaissance du schéma d'infractions passées. En vertu de ce principe, un individu pourrait devenir préventivement suspect car une analyse des *big data* révèle qu'il risque de commettre un crime demain.

Les données personnelles ne sont pas les seules à générer des défis de taille. La production et les processus opérationnels génèrent eux aussi des masses de données. Ces données sont certes mesurées et enregistrées par les infrastructures de production, mais leur évaluation constructive est insuffisante, voire inexistante, faute d'outils d'analyse et de l'expertise nécessaire.

L'analyse des *big data* présente principalement deux risques:

- La méthode employée et l'ampleur des données computées tendent à faire considérer les résultats comme objectifs. Ce serait une erreur: l'analyse des *big data* ne fournit pas de bases de décision rationnelles, juste un instrument fondé sur des calculs de probabilité, en vue d'optimiser la prise de décisions.

- Elle repose sur des algorithmes (auto-apprenants pour certains) dont l'utilisation présente un potentiel d'erreur considérable.

3.1.4 Les algorithmes

3.1.4.1 Introduction

Les algorithmes sont des modes d'emploi (des programmes) indiquant pas à pas aux ordinateurs la marche à suivre pour résoudre un problème. Ils consistent en un nombre fini d'étapes clairement définies qui ont généralement été traduites, par un programme appelé compilateur, d'un langage de programmation supérieur plus facile à comprendre pour l'homme (code source) en instructions individuelles pouvant être interprétées par le matériel informatique (langage machine). Dans un algorithme, les données à traiter empruntent, selon leur nature, des parcours différents dans des arbres de décision prédéfinis. Dans un algorithme déterministe traditionnel, une entrée donnée produira toujours le même résultat, car le processus de décision ne change pas.

L'intelligence artificielle recourt fréquemment à des algorithmes dits auto-apprenants, que l'on a entraînés à traiter certains types de données et dont le fonctionnement n'est plus déterministe mais fonction des données avec lesquelles ils ont été entraînés. Cela ne veut pas dire que ces algorithmes se modifient eux-mêmes, mais qu'ils modifient leurs processus de décision de manière autonome. Ils nécessitent une programmation préalable et sont ensuite utilisés sous forme de réseaux d'apprentissage profond (DNN pour *Deep Neural Networks*). Les DNN servent par exemple à la reconnaissance d'images ou à la reconnaissance vocale. Il s'agit là d'une qualité nouvelle des algorithmes, car selon les données avec lesquelles il a été entraîné, l'algorithme pourra aboutir, pour une même entrée, à des décisions ou des résultats différents.

3.1.4.2 L'intelligence artificielle

Cette percée technologique a été rendue possible grâce à la forte augmentation de la puissance de calcul au cours des quinze dernières années, et à la disponibilité relativement grande de données d'entraînement pour les algorithmes auto-apprenants.

En 2015, on pensait encore qu'il faudrait au moins cinq ans pour qu'un ordinateur parvienne à battre les meilleurs joueurs de go du monde. Mais dès mars 2016, AlphaGo de Google battait le champion du monde dans quatre parties sur cinq. Une étape supplémentaire était ainsi franchie sur le chemin qui mène, peu à peu, aux systèmes pensant par eux-mêmes.

La variété des applications est infinie: l'intelligence artificielle peut assumer des tâches complexes avec une qualité constante, d'une manière rapide et économique, et sans se fatiguer. Cette forme de délégation est aussi particulièrement indiquée dans les situations où la machine offre un anonymat accru, pour des tâches de contrôle et de vérification, par exemple. Il n'est donc pas étonnant de voir l'économie investir massivement dans ce domaine.

3.1.4.3 Défis posés par les algorithmes

Les algorithmes sont la base du traitement de données. Étant donné que les nouveaux algorithmes dans les domaines de l'analyse des *big data* et surtout de l'intelligence

artificielle sont encore l'objet d'une recherche intensive, il faut aussi accorder une attention particulière aux risques.

La disponibilité et la qualité des données sont déterminantes pour les algorithmes auto-apprenants: ces données peuvent être erronées, incomplètes, obsolètes ou trop brutes. Les systèmes d'apprentissage profond sont particulièrement sujets aux préjugés historiques qui ressurgissent dans le matériel d'entraînement pour algorithmes (données provenant du web, par ex.). Google et Flickr ont fait parler d'eux lorsque leur système de reconnaissance faciale a confondu des personnes noires avec des gorilles. Des préjugés peuvent ainsi, en passant par les coulisses d'un traitement de données censément objectif, se transformer en faits objectifs et exercer une influence considérable sur la prise de décisions. En utilisant les données de masse, en partie non contrôlées, d'une société convertie au numérique, les algorithmes auto-apprenants restituent ce que cette société leur a appris.

Des erreurs peuvent se faufiler dans la construction du système de décision et dans son évaluation. Même des algorithmes corrects, une opérationnalisation adéquate et une quantité et une qualité de données appropriées ne peuvent éviter la survenue d'erreurs dans un processus de décision dans lequel la pondération des différentes données de mesure et des rétroactions erronées produisent des résultats faux ou déformés. Le développement de systèmes auto-apprenants finira par mettre les utilisateurs au défi de comprendre le mode de fonctionnement «caméléon» de leurs machines intelligentes (variation des variables et des pondérations). L'état actuel de la technique produit d'ores et déjà des situations dans lesquelles les exploitants ne parviennent plus à retracer le chemin emprunté par un système d'apprentissage profond pour trouver une solution.

L'élaboration de processus de décision avec des algorithmes nécessite une coopération interdisciplinaire de haut niveau entre analystes de données, programmeurs, experts en algorithmes et spécialistes du secteur concerné (politique, publicité, psychologie, sociologie, communication, installations de production, etc.). Cette coopération suppose des connaissances techniques transversales et une compréhension mutuelle, des conditions qui sont rarement réunies.

L'utilisation d'algorithmes, et en particulier d'algorithmes auto-apprenants, va se développer et aura des effets sur la société. Le traitement de données de communautés et de personnes morales et surtout physiques pourra entraîner un manque d'équité et des discriminations systémiques pouvant aller jusqu'à des infractions à des dispositions légales.

3.1.4.4 Réduction des risques liés aux algorithmes

Pour réduire les risques liés aux algorithmes, on peut agir à trois niveaux: le niveau juridique, celui des bonnes pratiques et celui des réflexions en matière d'éthique.

Les algorithmes dans le cadre des dispositions légales
Le débat qui commence porte sur les défis que représentent les algorithmes, en particulier dans le contexte de la protection des données. Lorsqu'on travaille avec des algorithmes, il faut évidemment respecter les principes de la transparence et de la finalité. Ce respect ne peut cependant pas se limiter à l'ingestion et à la production de données par les algorithmes, car l'utilisateur d'un système auto-apprenant n'est pas capable de retracer les processus de décision qui s'enchaînent, ce qui est contraire aux deux principes.

De plus, dans un tel contexte, le responsable du traitement des données ne peut plus établir d'analyse d'impact des risques du point de vue de la protection des données, telle qu'elle est prévue dans le règlement général de l'Union européenne (UE) du 27 avril 2016 sur la protection des données (RGPD) ou dans le message concernant le P-LPD. La protection des données précise certes ce qu'un algorithme doit ou peut fournir lors du traitement des données, mais elle n'a pas pour but de définir techniquement les moyens détaillés d'y parvenir. Par ailleurs, le développement de la protection des données dans le RGPD et dans le P-LPD prend en compte de nouvelles réglementations techniques telles que la protection de la vie privée dès la conception (*privacy by design*). Hormis quelques principes génériques (réduction des données au strict minimum, pseudonymisation, anonymisation et protection des données selon les derniers développements de la technique), les principes de la protection de la vie privée dès la conception ne sont pas exposés en détail et font l'objet d'un débat intense depuis quelque temps déjà. Il reste à préciser quelles exigences techniques détaillées ne font en fin de compte que refléter l'état des bonnes pratiques, et lesquelles sont censées déjà définir une norme de facto dans une perspective juridique. Ce débat ne s'est cependant jamais focalisé sur les algorithmes eux-mêmes, comme base du traitement de données moderne, mais sur des considérations générales relatives à un aménagement des techniques respectueux de la protection des données, autrement dit aux défis posés par l'analyse des *big data*.

Le principe de la transparence des algorithmes pose des problèmes spécifiques en matière de protection des données puisque les algorithmes peuvent contenir des secrets d'affaires et doivent être protégés à titre d'investissement. Ainsi, en cas de décision individuelle automatisée, le responsable du traitement doit divulguer les hypothèses de base de l'algorithme, mais non l'algorithme lui-même ni la structure fondamentale des processus de décision (art. 23, al. 2, let. f, P-LPD). L'étendue d'une telle divulgation n'a pas encore été fixée. On peut imaginer deux hypothèses.

Selon une interprétation large du devoir de divulgation en faveur des responsables du traitement, il faudrait ne révéler que les hypothèses de base qui, dans le descriptif du système algorithmique, présentent un rapport avec les dispositions légales et les principes déterminants dans un champ d'application spécifique. Les domaines spécifiquement réglementés sont, par exemple, la santé, la protection des consommateurs ou le droit fiscal.

Selon une interprétation plus restrictive, telle celle du groupe de travail «Article 29» de l'UE sur la protection des données[3], il faudrait divulguer les hypothèses de base, mais aussi le cheminement (dans ce cas précis, le processus de décision), les facteurs clés déterminant la décision et la pondération de ceux-ci. Cette hypothèse est cependant contraire au consid. 63 du RGPD, qui donne la priorité aux droits et aux libertés d'autrui, y compris le secret des affaires et la propriété intellectuelle. La pratique, la jurisprudence et les lignes directrices des autorités de surveillance clarifieront sans doute ces aspects. Mais le progrès technologique en matière d'algorithmes réduira la possibilité d'apprécier des cas particuliers à la lumière de précédents de portée générale.

Depuis quelque temps, les défis posés par les algorithmes font également parler d'eux dans le cadre de la loi sur les cartels. Les algorithmes tendent en effet à favoriser les

[3] Groupe de travail «Article 29», Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

«pratiques concertées» anticoncurrentielles au sens d'entente horizontale entre concurrents, sous réserve d'un comportement régulier. On parle alors d'«entente tacite» (cf. ch. 6.3.3).

Bonnes pratiques et aspects éthiques

L'adoption volontaire, par les utilisateurs, de mesures de bonne pratique pour la conception des algorithmes pourrait aussi contribuer à accroître la sécurité et la confiance. Ce pourrait être le cas si développeurs et utilisateurs s'engagent, par exemple, à:

- divulguer hypothèses de base, mode de fonctionnement des algorithmes et processus de décision;
- vérifier davantage la plausibilité des résultats lors de la mise en œuvre et de l'évaluation de systèmes auto-apprenants;
- mieux sensibiliser les utilisateurs aux risques, en leur indiquant les conséquences négatives potentielles du traitement algorithmique de leurs données;
- veiller à ce que les données d'entraînement soient correctes, complètes et dans un état d'agrégation maximal par rapport au but visé;
- mettre en œuvre un programme de contrôle automatisé dans la structure de base de la machine auto-apprenante;
- soumettre les systèmes, et en particulier les systèmes récursifs, s'améliorant eux-mêmes, à un contrôle renforcé confié à des tiers.

Les algorithmes auto-apprenants rendent nécessaire un système technique, juridique et équitable qui mette constamment en évidence, sur la base de modèles prédéfinis, les traitements non intentionnels, illicites et «injustes» infligés aux utilisateurs et qui assiste les personnes physiques dans leurs activités de contrôle. Ce système devrait opérer dès la saisie des données, savoir faire la distinction entre attributs sensibles (race, sexe), contextuels et autres (nécessaires, utiles ou discriminatoires), et identifier leur application dans le processus de décision. Il devrait en outre procéder à l'analyse statistique de la qualité des liens entre le résultat du processus de décision et les attributs. Les résultats fourniront les éléments de base qui permettront de comprendre le mode de fonctionnement de l'algorithme et d'identifier les effets négatifs systémiques sur certains groupes d'utilisateurs. Le développement de tels programmes de test est à l'étude, mais ces travaux doivent s'intensifier pour qu'on dispose le plus rapidement possible de systèmes commercialisables.

Il faudrait par ailleurs élaborer et examiner des mesures techniques et organisationnelles supplémentaires. On pourrait aussi concevoir des principes éthiques pour le développement d'algorithmes, et même une éthique professionnelle pour l'analyse des données. Cette éthique impliquerait notamment la compatibilité avec les idéaux de la diversité culturelle, de la liberté, des droits de l'homme et de la dignité (cf. ch. 11).

3.2 Facteurs d'attraction

3.2.1 L'économie

L'économie est l'un des facteurs d'attraction fondamentaux de la transformation numérique en ce qu'elle développe de nouveaux modèles d'affaires, en particulier des prestations de services et d'information par Internet, une meilleure gestion des risques et des bases de décision améliorées. Le numérique offre de nouveaux moyens de développer sa compétitivité: grâce à l'automatisation et à des chaînes de production flexibles et optimisées, l'efficience et la productivité augmentent. La possibilité d'offrir, en masse, des biens et services sur mesure est révolutionnaire. Elle implique une nouvelle proximité avec le client par l'emploi de voies de distribution et de plateformes numériques, de même qu'un profilage sophistiqué qui transforme le client de masse en individu, améliorant du même coup la fidélité de ce client. Dans le B2C, cette tendance est déjà pleinement établie; dans le B2B, elle se développe lentement mais sûrement.

La dématérialisation des processus entre les clients et les fournisseurs d'une part, et entre ces fournisseurs et leurs propres fournisseurs d'autre part, permet de redéfinir les chaînes de création de valeur existantes et de supprimer les intermédiaires. La collecte en amont de données concernant le client constitue à cet égard un facteur d'attraction décisif. L'évaluation des données et l'utilisation de moyens de communication numériques ont pour but d'optimiser la distribution et de développer le modèle d'affaires de telle manière que l'offre de produits et de biens se transforme en une offre de prestations globales.

Dans le domaine de l'exploitation, le numérique offre de nouvelles possibilités: capteurs, saisie et évaluation de données permettent une surveillance améliorée des systèmes en temps réel et une gestion plus rigoureuse de la qualité (dans l'idéal, sur l'ensemble du cycle de vie du produit et en tenant compte de prestations de soutien et de maintenance développées chez le client). Les données collectées permettent de réduire les risques opérationnels et commerciaux et d'améliorer les bases de décision.

3.2.2 La recherche

La recherche aussi est un moteur de la transformation numérique et du traitement de données, et plus particulièrement les nouvelles méthodes de recherche qui émergent grâce à la quantité, au raffinement, à la disponibilité, à la provenance internationale, à l'actualité et à l'analysabilité des données.

3.2.3 Les consommateurs et les utilisateurs de plateformes et de services numériques

Les consommateurs et les utilisateurs sont un facteur d'attraction décisif: les plateformes et les services numériques leur offrent un accès illimité dans le temps comme dans l'espace à des informations, des prestations, des biens, des divertissements et des réseaux sociaux. Des plateformes universelles combinent aujourd'hui différentes prestations telles que recherche d'informations, «shopping» et lieux virtuels de rencontre ou d'exposition.

Consommateurs et utilisateurs se sont habitués à la gratuité de nombreux services, informations et produits dans le cadre du modèle d'affaires «freemium», ce qui pose

la question suivante sous l'angle de la protection des données: l'abandon de la sphère privée et de l'autodétermination en matière d'information est-il foncièrement contraire au cadre juridique ou acceptable comme monnaie d'échange à certaines conditions (cf. ch. 7.2.4)? Face à une telle monétisation des données personnelles, tous les participants de ce réseau économique doivent se demander comment organiser l'échange entre sphère privée et prestation.

Consommateurs et utilisateurs ont internalisé l'étendue, la qualité et surtout le confort de toutes ces prestations et de ces écosystèmes intégraux comme un élément désormais incontournable de leur univers. Les prestations numériques leur apportent au quotidien une baisse des frais de transaction, un gain de temps et une indépendance temporelle dont ils ne veulent plus se passer. Dans bien des domaines, le consommateur ne peut ni ne veut plus accepter l'asymétrie des savoirs qui le séparait jadis du fournisseur. Un simple clic lui permet de comparer des prix, des services et des biens de consommation à l'échelle de la planète pour tirer le meilleur parti d'une concurrence mondialisée. Participer aux réseaux sociaux est devenu pour beaucoup une évidence et un véritable marqueur culturel.

3.2.4 L'État

La recherche militaire a joué un rôle majeur dans le développement de la capacité de calcul et des premiers réseaux informatiques. Son rôle reste déterminant, en particulier dans le domaine de la sécurité de l'information et comme incubateur de la recherche fondamentale, en robotique, par exemple. Le complexe militaro-industriel a cependant perdu de son importance comme chef d'orchestre technologique du traitement de données.

Du côté des utilisateurs, l'importance de l'État comme moteur de la transformation numérique augmente avec le déploiement systématique de la cyberadministration à l'échelle nationale, assorti de la mise à disposition des infrastructures nécessaires telles que connexion haut débit, réseaux mobiles ou signature électronique. Il ne faut pas pour autant perdre de vue le fait qu'avec le traitement de données, les infrastructures numériques offrent à l'État de nouveaux moyens de surveillance, voire de subordination sociale et de sanction, dont les instances de l'État de droit doivent impérativement pouvoir garantir le contrôle par des mesures appropriées. L'État collecte en effet de grandes quantités de données, ce qui fait de lui l'égal des géants du web et des plus gros courtiers de données, d'où la nécessité d'une protection appropriée des données et d'une politique OGD.

4 Champ d'analyse sécurité de l'information

4.1 Situation actuelle et évolution

Les statistiques relatives à la sécurité des infrastructures numériques en général et de l'«écosystème des interconnexions Internet»[4] en particulier doivent être considérées avec précaution. Mais elles indiquent à quel ordre de grandeur on a affaire et dans quelle direction on avance: en 2017, jusqu'à 65 000 sites Internet ont été piratés en une journée. Les systèmes d'analyse ont enregistré une nouvelle signature de maliciel toutes les 4,2 secondes. Le nombre de points faibles inconnus que l'on partage sur le réseau et pour lesquels il n'existe pas encore de correctif (exploits zero-day) augmente[5]. En 2017, le nombre des faiblesses de logiciel découvertes et leur degré de gravité ont atteint un sommet. Elles augmentent en particulier au niveau des processeurs. Encore rares il y a quelques années, elles se comptent aujourd'hui par dizaines. Ce type de vulnérabilité, comme on en a vu des exemples au début de l'année (Meltdown, Spectre), signifie ni plus ni moins que le système d'exploitation et les applications de l'infrastructure de base de l'ordinateur ne peuvent plus faire confiance au processeur. On a affaire ici à une menace d'un nouveau genre. Il est à craindre que les premières cyberattaques exploitant précisément ces points faibles se produisent tôt ou tard.

En 2017, la cybercriminalité devrait pour la première fois avoir généré plus d'argent que le trafic de stupéfiants: des estimations tablent sur 500 milliards de dollars. Les grandes entreprises telles que les banques et les administrations enregistrent chaque jour plus d'un millier de tentatives d'attaque. 90 % d'Internet sont inaccessibles avec les moteurs de recherche courants et échappent ainsi à toute possibilité de recherche structurée. C'est ce qu'on appelle le *deepnet* ou *darknet* (les réseaux Tor, Freenet ou I2P, entre autres). Celui-ci est quasiment impossible à surveiller. Les acteurs malveillants disposant des connaissances et des moyens d'accès nécessaires y évoluent au mépris de l'ordre et des lois.

On voit aussi se multiplier les pannes de services numériques dues à des erreurs de manipulation ou à des problèmes de logiciel ou de matériel. Les attentes en matière de continuité de l'exploitation des infrastructures numériques sont plus élevées que ce que les exploitants sont en mesure de fournir. En cause: la complexité et l'interconnexion croissantes des systèmes.

L'idée selon laquelle le recours aux infrastructures numériques n'est pas uniquement synonyme de gains d'efficience, de confort et de fonctionnalité mais aussi de frais supplémentaires en raison des exigences de sécurité et de stabilité peine à s'imposer. Les trois impératifs que sont la sécurité ou la stabilité de fonctionnement, le confort et la fonctionnalité sont de plus en plus inconciliables, tant dans les entreprises que chez les particuliers. Ces divergences ont des conséquences lourdes pour le traitement de données, qui est indissociable des infrastructures numériques.

Cela dit, on constate aussi des tendances positives: le compte rendu journalier des pertes de données, des pannes et autres interruptions de service a généré une prise de conscience en matière de sécurité informatique et de sécurité de l'information. Ce

[4] Terminologie de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

[5] http://www.internetlivestats.com/ (état en décembre 2017)

sujet préoccupe désormais tout le monde, et la nécessité d'agir fait l'objet d'un large consensus. Les frais supplémentaires liés à la sécurité informatique ne sont plus considérés uniquement comme le coût, dont on aimerait se débarrasser, d'un risque résiduel censément supportable, mais comme un investissement nécessaire. L'idée selon laquelle une transformation numérique sans sécurité ni confiance dans la sécurité de l'information est vouée à l'échec s'est imposée.

4.2 Risques affectant la sécurité de l'information: dangers et menaces

Les risques affectant la sécurité de l'information résultent de différents facteurs, dont le développement de la surface d'agression, l'accroissement des dégâts potentiels et l'augmentation des dangers et des menaces. Il convient à cet égard de bien distinguer les cyberattaques intentionnelles (menaces) et les incidents résultant d'erreurs (dangers).

4.2.1 Dangers

4.2.1.1 L'écosystème Internet

Les pères fondateurs d'Internet cherchaient, dans les années 1970 et 1980, une solution technique qui permette de connecter des ordinateurs de manière simple et efficiente. Ils ont défini comme éléments de base un réseau décentralisé et des protocoles de transport qui pouvaient envoyer tous les paquets de données d'un point du réseau à un autre, sans poste de coordination central. La structure fondamentale d'Internet allie une ouverture sans restrictions ni contrôles et une disponibilité totale. Tout le monde peut y participer. Trente ans plus tard, ces éléments de base restent les ingrédients de la réussite du web mais constituent en même temps sa plus grande faiblesse: le flux de données est incontrôlable, la sécurité des données menacée et les différents acteurs (entités telles que personnes physiques ou morales et infrastructures techniques) difficiles à identifier en raison des distances.

Bon nombre d'États ont réagi et édictent des lois visant à bloquer la libre circulation des données, que ce soit pour protéger la sphère privée, pour améliorer le contrôle des contenus (par ex. loi allemande de mise en œuvre du droit sur les réseaux sociaux [*Netzwerkdurchsuchungsgesetz*]), par mesure de sécurité, à des fins de censure ou pour des raisons commerciales. Il n'en résulte pas une sécurité accrue, mais le risque de disloquer Internet en plusieurs îlots distincts et de lui faire perdre la qualité qui a fait son succès. Dans ces conditions, comment rendre l'écosystème Internet plus sûr sans le détruire (cf. ch. 4.4.3)?

4.2.1.2 Pas de remède miracle contre les cyberrisques

Les mesures de protection individuelles (pare-feu ou périmètre de sécurité, par ex.) ne sont plus suffisantes aujourd'hui face aux cyberrisques, même correctement développées et mises en œuvre de façon cohérente. Pour s'en convaincre, il suffit de considérer l'expansion irrépressible de l'arsenal de munitions (menaces combinées ou *blended threats*) et l'obstination des attaquants.

La nécessité de mettre en place un système de défense en profondeur, qui prévoit plusieurs niveaux de risque, a longtemps été ignorée. Un tel système consiste à superposer plusieurs moyens de défense techniques (pare-feu, antivirus, analyse des vulnérabilités) en les associant à des mesures organisationnelles. Dans un système complexe, on peut aussi cumuler les types de défense similaires de différents fournisseurs. Il faut cependant partir du principe que l'agresseur finira par arriver à ses fins. De ce point de vue, il faut donc compléter les éléments de protection préventifs, qui réduisent la probabilité d'une agression, par des mesures réactives, c'est-à-dire la capacité d'identifier l'agression et de restaurer le système.

C'est pourquoi le facteur «résilience» gagne en importance: il s'agit de la capacité de maintenir l'activité informatique au minimum en cas d'attaque et de réduire autant que possible la perte de données.

4.2.1.3 Complexité due à la quantité et à l'interconnexion des infrastructures et des données

La transformation numérique pousse les organisations à construire toujours plus d'infrastructures numériques qu'elles connectent entre elles afin de permettre le déroulement de processus de traitement complexes sans rupture de média et une utilisation commune des données. Cette évolution est rapide et rend difficile toute vue d'ensemble des processus, des systèmes, des interfaces et des volumes de données. Les entreprises génèrent des volumes de données toujours plus importants et toujours plus déstructurés dont elles ne peuvent exploiter et archiver rigoureusement qu'une infime partie (le reste formant les *dark data*). Ainsi augmente le risque de ne plus savoir quels processus et données sont sensibles et nécessitent une protection. Bien souvent, l'examen des risques concernant les données individuelles ne suffit pas puisque c'est en combinaison avec d'autres que certaines d'entre elles deviennent sensibles (effet de regroupement).

Il est par conséquent de plus en plus difficile de fixer des priorités, la logique voulant que les organisations protègent tout. Faute de solutions bon marché et de ressources à affecter à la sécurité de l'information, la vulnérabilité et les risques augmentent. La mise en œuvre du RGPD illustre bien cette tendance. Les entreprises doivent savoir à quel endroit elles ont archivé quelles données, sans quoi il ne vaut même pas la peine qu'elles essayent de se mettre en conformité.

4.2.1.4 Absence d'industrialisation des systèmes de sécurité

Au cours des vingt dernières années, le développement des infrastructures numériques (du simple ordinateur aux systèmes complexes) a connu une industrialisation remarquable. Comme dans les industries traditionnelles (l'automobile, par ex.), la normalisation et l'automatisation ont grandement amélioré la fonctionnalité, la banalisation, l'externalisation dans le nuage et la convivialité tout en faisant baisser les frais d'acquisition. Elles ont aussi favorisé la sécurité dès le stade de la conception, mais uniquement pour certains composants et services. Malgré la connexion des systèmes à des infrastructures numériques, l'industrialisation n'offre pas encore de solutions de sécurité normalisées. On ne dispose à cet égard que de systèmes fragmentés, sans conception d'ensemble, qui menacent la stabilité des systèmes et n'offrent pas de protection globale. Des solutions spécifiques «cousues main» existent, bien sûr, mais elles mobilisent des ressources humaines et financières importantes car elles sont

élaborées par des experts en sécurité. Et n'étant pas automatisées, elles nécessitent une mise à niveau fastidieuse à chaque nouvelle version ou extension du système.

La maturation des systèmes de sécurité n'a pas suivi le rythme fulgurant du développement technique et économique. Le fossé se creuse entre la banalisation à bas coût (les infrastructures numériques promettent efficience et convivialité) et la nécessaire sécurité.

4.2.1.5 Croissance organique des systèmes

Dans de nombreuses organisations, les infrastructures numériques ont connu une croissance organique, ce qui fait qu'un bon nombre d'applications et de systèmes datant des débuts de l'informatique sont toujours en service. On hésite à les remplacer ou à les faire migrer dans un environnement moderne plus sûr par crainte des frais élevés et des pannes de disponibilité qu'une telle opération risque de générer à court et moyen termes. La maintenance de ces systèmes pose déjà des difficultés, et c'est encore plus vrai pour le transfert des données et des processus dans un système entièrement nouveau. En règle générale, on attend du numérique qu'il réduise les coûts en apportant un supplément d'utilité, et non le contraire. Le principe qui veut que «tant que ça fonctionne, on n'y touche pas» a la vie dure. En empêchant l'industrialisation de la sécurité, il créera tôt ou tard des problèmes de sécurité. Les systèmes numériques issus d'une croissance organique se reconnaissent à leur structure: au lieu de s'articuler autour d'un principe de sécurité fondé sur une interconnexion efficiente entre processus informatiques et processus d'affaires en fonction de la gestion des risques, ils présentent toujours des responsabilités et des postes de décision non coordonnés.

4.2.1.6 Sécurité inconditionnelle et sécurité fondée sur la complexité

En cryptologie, la sécurité inconditionnelle (*information-theoretic security*) fait que l'agresseur dispose de trop peu d'informations pour déchiffrer un code, même si ses ressources de calcul informatiques sont illimitées. Ces mécanismes de chiffrement sûrs du point de vue mathématique comprennent notamment la cryptographie quantique et, dans certains cas, la cryptographie symétrique. Leur utilisation, qui mobilise des ressources importantes, est trop fastidieuse au quotidien.

Dans le cas de la sécurité fondée sur la complexité, le chiffrement repose sur des problèmes mathématiques. Ces applications se sont imposées et ont fait leurs preuves. Mais tôt ou tard, les progrès de la puissance de calcul ou de nouvelles découvertes mathématiques rendront insuffisante la protection qu'elles offrent (cf. ch. 4.4.1).

4.2.1.7 Dilemme entre sécurité et confort

Les deux approches en matière de cryptographie illustrent à merveille le dilemme entre sécurité et confort, la priorité étant généralement accordée au second. L'expérience acquise dans le domaine économique le montre: lorsque les moyens financiers alloués à l'informatique diminuent, du fait de mesures d'économie, par exemple, et que les prestations sont de toute façon restreintes, la direction commerciale est rarement prête à réduire davantage la fonctionnalité pour améliorer la sécurité. Il en va de même dans

le privé. Quand l'infrastructure numérique, qu'il s'agisse d'une application ou d'un élément de l'IdO (téléviseur, par ex.), fonctionne en réseau sans difficulté particulière, plus personne ne s'intéresse aux questions de sécurité.

4.2.1.8 Le facteur humain

Les utilisateurs, professionnels comme particuliers, s'attendent à ce qu'on leur propose toujours plus de confort et d'objets numériques séduisants. La fascination pour le possible ne connaît pas le moindre essoufflement. Mais la sécurité numérique, qui est pourtant évoquée dans les médias tous les jours, reste cantonnée au second plan, comme le montrent par exemple différentes analyses des choix de mots de passe: les gens ont tendance à utiliser toujours les mêmes. Le grand bouleversement numérique permanent n'a pas vraiment augmenté la volonté de s'instruire. Les dangers contre lesquels les experts en sécurité ont mis en garde lors de la révolution de l'IdO se sont concrétisés depuis longtemps. On refait les mêmes erreurs, les mêmes fautes d'inattention que lors de la mise en réseau des ordinateurs il y a plus de vingt ans. La prise de conscience gagne du terrain, mais avec un résultat à double tranchant: d'un côté, les utilisateurs sont plus autonomes et plus responsables, de l'autre, ils sont dépassés par les événements, d'où une certaine impuissance et une forme de désintérêt. Nous risquons par conséquent, lors du passage à l'IdT, prochaine étape de la transformation numérique (qui englobe la mise en réseau des humains au moyen d'implants tels que stimulateurs cardiaques, capteurs, interfaces homme-machine inédites, etc.), de reproduire les mêmes erreurs pour les mêmes raisons, alors que le risque sera beaucoup plus élevé. Le sens de la sécurité et des responsabilités semble avoir atteint ses limites. Il est d'autant plus important de développer les capacités de la population et la responsabilité des producteurs et des fournisseurs de produits et de services numériques.

4.2.1.9 Le facteur économique

La révolution numérique n'épargne aucun secteur: même les entreprises n'ayant aucun rapport avec l'informatique sont obligées de mettre en place un écosystème numérique dans la distribution et dans l'exploitation. Une étude sur le passage au numérique des PME suisses révèle que près de trois quarts des entreprises interrogées ont déjà lancé des projets dans ce domaine. Elle indique aussi la nature des risques qui pèsent sur l'avenir: la grande majorité des entreprises s'inquiètent avant tout de leur manque de savoir-faire et des gros investissements qui sont nécessaires. Les PME sont particulièrement pénalisées par le fait qu'elles ne disposent pas de service informatique dédié, et que leurs marges bénéficiaires ne leur permettent pas de s'offrir les services coûteux d'experts en cybersécurité. Cet aspect mérite la plus grande attention car elles constituent l'épine dorsale de l'économie suisse: plus de 99 % des entreprises sont des PME (de 1 à 250 collaborateurs), qui fournissent les deux tiers des emplois et qui génèrent une part non négligeable du PIB.

Par ailleurs, les développeurs et les utilisateurs subissent une pression permanente: il faut constamment être les premiers sur le marché et tenir un rythme de renouvellement élevé. Ces deux aspects leur importent bien plus que de fournir de la «sécurité». Les petites entreprises n'ont pas le temps, les grandes non plus d'ailleurs, de procéder à des analyses de code ni à des tests de vulnérabilité. De plus, sur le marché de l'IdO, les marges bénéficiaires sur les produits de masse soumis à une concurrence mondiale sont trop faibles pour amortir ces frais supplémentaires. Le facteur humain joue

ici un rôle déterminant: comme on a du mal à imaginer ce que recouvre la notion de sécurité de l'information s'agissant des appareils numériques, on ne voit pas en elle une qualité. Là aussi, l'État doit veiller à accroître la sécurité, en collaboration avec les producteurs et les fournisseurs. Il est aussi nécessaire de lancer des campagnes de sensibilisation à l'intention des utilisateurs que de débattre de nouvelles dispositions en matière de responsabilité, des directives de certification des produits et services, et des normes de gestion.

4.2.2 Extension de la surface vulnérable

Les domaines qui s'appuient sur des infrastructures numériques sont de plus en plus nombreux. On appelle informatique ubiquitaire cette omniprésence des ordinateurs et des réseaux. La vulnérabilité de ces infrastructures rend vulnérables tous les domaines concernés par la transformation numérique. Dans les années 1990, les seuls appareils en réseau étaient des ordinateurs. Ils furent rejoints au début des années 2000 par des appareils mobiles tels qu'ordinateurs portables, smartphones et tablettes, et nous en sommes désormais à l'IdO: depuis les îlots de production complexes des entreprises jusqu'aux brosses à dents, tous les objets sont aujourd'hui connectés car Internet améliore le confort d'utilisation, l'automatisation, le contrôle, la maintenance et l'efficience. En 2017, des alertes de sécurité mettant en garde contre des cyberattaques dirigées contre des appareillages médicaux connectés tels que défibrillateurs, stimulateurs cardiaques, pompes à insuline, etc. ont défrayé la chronique. L'IdT ne s'arrête pas devant l'humain. La surface exposée aux attaques s'étend inexorablement tandis que les flux de données entre «objets» sont de plus en plus incontrôlables et vulnérables. Si le risque était jadis limité au monde virtuel, il affecte aujourd'hui également le monde réel.

4.2.3 Accroissement du potentiel de nuisance

Les infrastructures numériques sont de plus en plus chargées de tâches impliquant des données sensibles. Qu'il s'agisse de stimulateurs cardiaques ou de secteurs critiques tels que la santé, les finances, l'énergie ou les services de sécurité, un incident peut aujourd'hui devenir une question de vie ou de mort. Les cybercriminels n'hésitent plus à attaquer des hôpitaux. On imagine très bien la catastrophe écologique que pourrait déclencher une agression dirigée contre une entreprise de produits chimiques, par exemple.

L'attaque dont fut victime le réseau de communication interbancaire Swift en 2016 a montré les dégâts que peut causer une cyberattaque professionnelle, même sur des systèmes centralisés ultra-protégés. Dans l'IdT, tout est vulnérable, depuis l'ordinateur jusqu'à l'homme. Le développement de l'interconnexion devrait faire augmenter à l'avenir le nombre de cas et les dommages correspondants.

Le potentiel de nuisance ravageur des attaques dites systémiques, qui paralysent des infrastructures numériques de grande envergure, a fait de plus en plus parler de lui ces derniers temps. Il faut dire que l'effondrement de pans entiers ou de parties vitales de l'infrastructure numérique par suite d'une telle attaque équivaudrait à un «cybergeddon» avec des conséquences dévastatrices pour l'ensemble de la société et de l'économie mondiale. Pourtant, la plus grosse cyberattaque à effet systémique de ces dernières années, WannaCry, qui a touché plus de 400 000 systèmes dans plus de 150 pays, a montré les limites du potentiel de nuisance. Quoique dévastatrice sur le moment, elle s'est révélée insignifiante au point de vue systémique. Même dans le cas

de matériels et de logiciels largement répandus tels que SAP, Windows ou les processeurs Intel, la multiplicité des versions et des paramétrages contextuels spécifiques à tel ou tel utilisateur fait qu'on n'a pas affaire à une monoculture sur laquelle un ravageur pourrait causer des dommages systémiques. Bien que la révolution technique ne permette d'exclure aucune hypothèse, l'appréciation des risques ne devrait pas changer, même à moyen terme. L'état actuel d'industrialisation ou de normalisation du matériel informatique et surtout des logiciels, encore immature, présente certes des inconvénients (cf. «Menaces», ci-après), mais protège aussi contre de telles attaques du fait de sa diversité. À terme, la normalisation et la centralisation des infrastructures numériques devraient à la fois ouvrir la voie à de nouvelles formes d'attaque et améliorer notablement la protection et la maintenance de ces systèmes.

L'infrastructure «Internet» constitue un cas à part. Certains États disposent en effet d'un bouton d'arrêt d'urgence (*Internet kill switch*) qui leur permet de paralyser tout le réseau, du moins sur leur territoire (cf. ch. 4.4.3). On peut imaginer la mise en place d'interrupteurs d'une portée plus vaste, mais cette solution serait techniquement complexe et coûteuse en ressources, et sans doute réservée à des acteurs gouvernementaux.

4.2.4 Menaces

Dans le cybermonde, c'est l'agresseur qui a l'avantage. Libre d'attaquer à tout moment, il ne s'expose à aucun risque direct grâce à l'accès à distance et peut tester ses schémas d'agression jusqu'à ce que l'un d'eux aboutisse. Il en va tout autrement pour les responsables de la sécurité informatique: ils ont beau désamorcer des milliers d'attaques chaque jour, une simple erreur peut avoir des conséquences désastreuses.

Les agresseurs ont tendance à se professionnaliser. Ils pratiquent la répartition des tâches, ce qui fait qu'il ne faut plus être un expert pour passer à l'acte. Les cyberattaques «à la demande» (*cyberattack as a service* ou *cybercrime as a service*) offrent des prestations sur mesure à n'importe quel acteur du darknet prêt à payer. Les instruments d'agression sont de plus en plus sophistiqués tandis qu'on assiste à une chute des prix, notamment dans le cas des attaques par déni de service distribué (DDoS pour *distributed denial of service*). On peut les louer sur le web à bon marché. Les obstacles techniques à la criminalité ont nettement diminué dans l'ensemble. Les chiffres, pour autant qu'ils soient fiables, sont clairs: la criminalité et l'espionnage sont devenus la motivation principale dans beaucoup plus des trois quarts des cyberattaques. Les agressions criminelles ont explosé depuis 2015.

Avec les cyberattaques à la demande, on voit se multiplier les agressions multicouches. Les DDoS servent, par exemple, à distraire les utilisateurs de la corruption d'autres systèmes afin d'exfiltrer des données, pendant que les vulnérabilités détectées font l'objet de menaces combinées (virus, chevaux de Troie, ingénierie sociale, exploitation des failles, etc.).

Les services de renseignement ont eux aussi découvert les avantages du monde virtuel et investissent des moyens considérables dans les outils d'agression. L'espionnage technologique encouragé et soutenu par les États se développe. Il y a quelques années encore, les menaces persistantes avancées (*advanced persistent threats*) dirigées contre des objectifs spécifiques (tous les types de maliciels) et surtout les exploits zero-day étaient le fait d'acteurs gouvernementaux. Près de 90 % des maliciels nouvellement identifiés ne sont utilisés qu'une seule fois pour une attaque spécifique, ce qui complique l'identification.

Autrefois jalousement gardés par les services de renseignement et l'armée, ces cyberarmes complexes ont fuité ces deux dernières années, finissant par arriver sur le darknet. Dans certains États, elles atterrissent dans les mains de cyberacteurs qui travaillent pour l'État tout en employant leur savoir-faire à des fins criminelles. Il est donc de plus en plus difficile de distinguer les acteurs gouvernementaux des acteurs para-gouvernementaux.

Bien que l'on parle beaucoup du risque de rançongiciel ou d'attaque généralisée contre les opérations de paiement, le commerce de données volées (informations technologiques, secrets d'affaires, données relatives à la santé, secrets d'État, etc.) devrait encore augmenter.

Non seulement les véhicules d'agression mais aussi les possibilités de profit se sont fortement développés: la chaîne de création de valeur cybercriminelle s'est mondialisée et professionnalisée. Outre les services du darknet que nous avons évoqués, des marchés de données organisés facilitent la marchandisation des différents modèles d'affaires sur le darknet. Il n'y a donc rien d'étonnant à ce que le crime organisé exploite le potentiel du cyberespace en profitant du fait que les mesures de sécurité n'y ont pas encore atteint le niveau de celles du monde physique.

Bien entendu, les agressions contre la disponibilité d'infrastructures et de données numériques se remarquent très rapidement. Dans ce domaine, tout est possible et on a déjà tout vu: cryptage hostile de données par un rançongiciel, voire perturbation ou même destruction d'installations industrielles complètes, comme celle d'un haut-fourneau en Allemagne. Il est en revanche beaucoup plus difficile d'évaluer l'ampleur du risque que représente la perte involontaire de données, qui peut toucher des données de clients, des données d'affaires importantes, la propriété intellectuelle ou encore des données de connexion d'utilisateurs. Lorsqu'une attaque réussit, la période entre infection et détection devient de plus en plus longue et dépasse actuellement les 270 jours selon les estimations d'experts. De plus, la plupart des victimes sont alertées par un partenaire extérieur. Les attaques contre la confidentialité des données devraient encore augmenter nettement à l'avenir. Leurs avantages sont évidents: l'agresseur pénètre dans un système, si possible sans laisser de trace, copie les données puis disparaît. Difficile, ensuite, de retrouver l'auteur, de le poursuivre et de le condamner.

Si l'on part du principe que des experts disposant des ressources nécessaires sont capables, avec les mesures de sécurité actuelles, de corrompre la structure de base des systèmes et qu'il n'est pas possible de prévenir l'exfiltration de données, la résilience en matière de moyens de détection et de contrôle devient de plus en plus importante. L'État avant tout mais aussi la recherche et l'économie dans le domaine de la haute technologie doivent intégrer le fait que leurs systèmes sont déjà corrompus ou le seront tôt ou tard, et qu'une perte de données est possible.

La sécurité de l'information a accompli de gros progrès ces dernières années. Le risque global a néanmoins augmenté compte tenu des processus et des données sensibles concernées et de la hausse de la menace. Il a fallu des siècles pour hisser la sécurité physique à son niveau actuel. La société moderne ne dispose pas d'autant de temps. Les experts ne peuvent pas prendre plusieurs décennies pour régler les problèmes.

4.3 Formation, compétence, organisation

4.3.1 L'«autisme» des informaticiens

La sécurité de l'information est un domaine complexe et désormais hautement interdisciplinaire, qui oblige les informaticiens à collaborer avec des juristes ou des analystes des processus d'affaires, notamment. La protection des données montre de manière exemplaire que seule la multidisciplinarité peut mener à l'objectif. En effet, l'incapacité des experts en informatique, en conformité, en risques et en droit à trouver un langage commun et à développer une compréhension commune des problèmes pèse au moins autant dans la balance que les carences des paramètres de sécurité de base.

L'IdO aussi nécessite la collaboration des informaticiens, des spécialistes de la sécurité informatique, des experts en affaires et des ingénieurs. L'absence de communication entre familles d'experts constitue une faiblesse. Pourtant, du côté de la formation, on continue de considérer que les informaticiens ont pour mission de rechercher, en vase clos, des solutions numériques aux problèmes numériques, et qu'ils n'ont pas besoin d'échanges avec l'extérieur. À l'heure de l'IdT, cet «autisme» des informaticiens est un vrai danger. Il faut par conséquent compléter les cursus par des cours de communication écrite et orale pour permettre aux informaticiens d'exercer leurs compétences de créateurs en collaboration avec tous les autres acteurs concernés (cf. ch. 10.3).

4.3.2 Pénurie d'experts en sécurité de l'information

Il y a d'ores et déjà pénurie d'experts en sécurité de l'information en tous genres, des programmeurs sensibilisés aux questions de sécurité aux responsables de la sécurité des systèmes d'information (RSSI; en anglais *chief information security officer* [CISO]), en passant par les préposés à la protection des données avec les qualifications juridiques et surtout techniques requises. Cette pénurie ne peut que s'accentuer au fil de la transformation numérique.

Cette situation a de nombreuses causes: les écoles polytechniques fédérales, les universités et les hautes écoles spécialisées manquent de sections consacrées à la sécurité de l'information. Il n'existe pas non plus d'ensemble reconnu de contenus didactiques définissant une formation sanctionnée par un diplôme en sécurité de l'information (en «confiance numérique», par ex.) comparable au master en sciences des données (*data science*). Les écoles polytechniques fédérales (EPF) de Lausanne et de Zurich et la haute école spécialisée de Lucerne viennent à peine de lancer des projets dans ce sens. Les établissements de formation doivent intensifier leurs efforts dans ce domaine et développer une compréhension commune des contenus didactiques nécessaires. Faute de sections d'enseignement, d'enseignants spécialisés et d'un profil de formation clairement défini, les étudiants ne se sentent pas concernés.

4.3.3 Intégrer la sécurité de l'information à la formation de base

Les non-informaticiens aussi manquent de connaissances pour comprendre le développement numérique et les questions de sécurité. Il faut intégrer ces connaissances aux études de base des juristes, des médecins, des ingénieurs et des sociologues,

notamment, de même qu'à la formation professionnelle (de la même façon que le MBA est censé initier tous les non-économistes au monde de l'économie).

Il ne s'agit pas de transmettre uniquement des notions de programmation, mais aussi des bases telles que la pensée computationnelle, l'alphabétisme informatique et une compréhension minimale des interactions entre des éléments fondamentaux tels que réseaux, systèmes d'exploitation et applications, ainsi que les bases de la stochastique (cf. chap. 10).

4.3.4 Sensibilisation aux menaces: intégrer la sécurité de l'information à la culture générale

Dans l'écosystème numérique, la sécurité ne peut pas être meilleure que le maillon le plus faible de la chaîne, c'est-à-dire l'individu. Quiconque omet de se protéger met en danger autrui. Il faut des campagnes de sensibilisation et des programmes de formation pour tous les membres de la société; on y a trop peu recouru jusqu'ici.

1. Recommandation:

La Confédération veille à ce 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.

4.4 Sujets à approfondir

4.4.1 Avenir de la cryptographie

Dans l'écosystème Internet, des instruments de sécurité importants reposent sur des techniques de chiffrement elles-mêmes fondées sur la complexité mathématique. Ils permettent de sécuriser les connexions réseau, notamment entre le navigateur et une page Internet, d'authentifier des entités physiques (identité électronique [e-ID], entre autres), morales et techniques, d'enregistrer des signatures numériques ou encore de chiffrer des messages. Ils sont les piliers de la confiance et de l'intégrité sur le net.

Le chiffrement asymétrique revêt une importance particulière en matière de signature et de chiffrement numériques, car contrairement au chiffrement symétrique, il permet une gestion simple et sûre des clés. Le chiffrement symétrique oblige les utilisateurs à se transmettre la clé directement, par un canal différent. Il faut donc retransmettre la clé à chaque modification du cercle des destinataires. Plus les utilisateurs au sein d'un même système sont nombreux, plus la confidentialité de la clé est menacée.

Le chiffrement asymétrique supprime ces problèmes grâce à une infrastructure à clés publiques (PKI pour *public key infrastructur*e), qui ne permet d'établir aucun lien entre la clé publique utilisée pour le chiffrement et pour la vérification de signatures numériques, et la clé privée servant au déchiffrement ou à la signature. La communication

de la clé publique est donc l'une des caractéristiques principales de la cryptographie asymétrique.

Prenons un exemple: la clé publique d'un serveur web est connue. Dès que le navigateur d'un utilisateur établit une relation avec ce serveur, il vérifie l'identité de celui-ci au moyen d'un certificat établi par un tiers de confiance et lui propose une clé symétrique qu'il crypte à l'aide de la clé publique du serveur (en passant, par ex., par le système RSA). Cette procédure complètement automatisée se reproduit en arrière-plan des milliards de fois à chaque établissement d'une relation sûre, dite «https».

Les algorithmes de hachage font également partie des procédés cryptographiques. Ils convertissent une donnée d'entrée (message, texte ou mot de passe, par ex.) en une somme de contrôle, d'une longueur fixe, appelée valeur de hachage. Ils ont ceci de particulier que la somme de contrôle ne permet pas de recalculer la donnée d'entrée, et qu'il est pratiquement impossible de trouver deux données d'entrée produisant la même valeur de hachage.

Le chiffrement asymétrique et les valeurs de hachage ne protègent pas qu'Internet mais aussi d'autres infrastructures numériques telles que les blockchains, lesquelles sont une juxtaposition de transactions signées qui ont été hachées (cf. ch. 9.1.4).

Lors de l'instauration des systèmes asymétriques les plus courants tels que le système RSA, dans les années 1970, on envisageait un horizon de sécurité de plusieurs siècles. Compte tenu de l'évolution des ordinateurs quantiques et des avancées possibles en mathématiques, il est évident aujourd'hui que les systèmes de sécurité fondés sur la complexité mathématique ne sont pas adaptés à cet horizon. Une menace pèse, à terme, non seulement sur la confidentialité et l'intégrité du traitement actuel des données, mais sur toutes les données chiffrées jusque-là. Autrement dit, les systèmes de sécurité actuels fondés sur le chiffrement asymétrique constituent une véritable bombe à retardement. S'agissant des algorithmes de chiffrement symétrique tels qu'*advanced encryption standard* (AES, «norme de chiffrement avancé»), il suffit d'allonger la taille des blocs pour les protéger des attaques d'ordinateurs quantiques.

D'autres solutions technologiques existent déjà, mais elles ne sont pas près d'être mises en pratique au quotidien. D'autant moins qu'il faut beaucoup de temps pour apporter une modification fondamentale à l'écosystème Internet. À titre d'exemple, on n'a toujours pas fini de remplacer l'algorithme de hachage MD5, sur lequel on avait découvert en 2004 des faiblesses importantes.

Parmi les autres solutions figurent les algorithmes dits post-quantiques, fondés sur des problèmes mathématiques, que les ordinateurs quantiques sont incapables de résoudre en l'état actuel des connaissances. Le système de McEliece ou NTRUEncrypt sont des approches prometteuses à cet égard. Quoi qu'il en soit, aucun ordinateur quantique n'est aujourd'hui capable de vérifier pratiquement leur sécurité ou leur absence de sécurité.

Comme il est probable que toutes les approches fondées sur la complexité mathématique seront attaquables un jour (les ordinateurs quantiques devraient être en mesure de décoder les chiffrements asymétriques en usage aujourd'hui d'ici à dix ou quinze ans), les défis à relever sont immenses: chaque fois qu'on change d'algorithme de chiffrement, toutes les données chiffrées jusque-là doivent être rechiffrées au moyen de ce nouveau système. Dans l'état actuel des techniques et de l'organisation, cette opération n'est réalisable qu'au prix d'un effort économique disproportionné. Le risque

que des données soient soustraites à tout contrôle selon le principe du «copions maintenant, décodons plus tard» pèse encore plus lourd. Le recryptage n'a de sens que si les données n'ont pas déjà été volées.

On décrit régulièrement comme le pire des cyberscénarios possibles celui d'un écosystème numérique sans solution pour la cryptographie post-quantique. On comprend mieux les dimensions temporelles et les exigences en matière de confidentialité et d'intégrité des données lorsqu'on voit, par exemple, que la loi fédérale du 26 juin 1998 sur l'archivage (LAr) prévoit, s'agissant de la consultation des archives de la Confédération, des délais de protection et de blocage de trente ans, voire de cinquante pour les données personnelles sensibles, et courant au moins jusqu'au décès de la personne concernée.

Seules des techniques de chiffrement sûres du point de vue de la théorie de l'information garantissent une sécurité pérenne pour un horizon de cent ans. En fait notamment partie la distribution physique de clés cryptographiques sur la base de l'échange de clé quantique. Différents États tels que les États-Unis et l'Allemagne, mais aussi l'UE, prennent la cryptographie post-quantique très au sérieux et affectent à son étude des organes et des groupes de travail. Compte tenu de la longueur de la période d'adaptation, il faut s'y prendre tôt pour identifier des solutions concrètes et prévoir leur mise en œuvre. La Suisse aussi doit s'attacher à relever ce défi sans tarder, car tout cela prendra du temps.

Au fond, la qualité d'un chiffrement dépend avant tout du choix du générateur de nombres aléatoires. Les générateurs de nombres aléatoires physiques, tels que les sauts quantiques, offrent une meilleure protection lors de la génération des clés et, partant, lors du chiffrement, que les générateurs de nombres pseudo-aléatoires avec support logiciel, lesquels sont d'ailleurs à éviter. L'expansion des marchés tend à faire baisser le prix de ces systèmes, qui répondent aux exigences de sécurité.

4.4.2 Sécurité du traitement de données

Le traitement de données connaît trois états: le repos (*data at rest*), le mouvement (*data in transit*) et la modification (*data in use*). Chacun de ces états nécessite des techniques cryptographiques de protection.

Données en mouvement
Le chiffrement des données offre la sécurité nécessaire à la transmission des données et implique un système de distribution des clés entre les parties communicantes. Les systèmes asymétriques courants n'étant pas fiables à long terme, il faut trouver d'autres solutions. Un système sûr du point de vue de la théorie de l'information, qui restera inattaquable à l'avenir, repose sur l'échange d'une clé quantique. De tels systèmes physiques sont déjà commercialisés en Suisse. Comme pour les systèmes de distribution de clés cryptographiques, le chiffrement proprement dit passe par un algorithme symétrique, par exemple AES-256, qui permet une transmission de message plus efficiente.

Les systèmes d'échange d'une clé quantique fonctionnent très bien sur la fibre optique standard des télécommunications, y compris en parallèle avec le reste de la communication de données. Mais pour des raisons pratiques, on utilise pour le signal quantique une fibre optique dédiée. Celle-ci n'a cependant pas besoin d'un câble distinct; on peut la poser avec les centaines de fibres optiques servant pour les autres modes de communication. Ce canal photonique quantique doit être d'une seule pièce, de bout

en bout. En l'état actuel de la technique, on dispose d'une portée d'une centaine de kilomètres avant l'affaiblissement du signal. C'est suffisant pour relier les villes en Suisse. Dans les grandes agglomérations, l'État mettrait en place des nœuds administrés qui assureraient la transmission sur des distances plus longues et qui permettraient aux autorités de surveiller la communication dans le cadre de la loi.

Données au repos
Le chiffrement symétrique des données fait partie des mesures de prévention efficaces, outre les mesures de protection informatique courantes telles qu'une gestion cohérente des clés (principe de restriction des droits d'accès) et la protection physique des serveurs. Pour améliorer la protection de l'intégrité des données, il faut munir les protocoles de type signature numérique d'une date d'expiration. En cas de progression imprévue de l'analyse de chiffrement, cette date peut être modifiée de manière à ce que les données nécessitent une nouvelle signature. Comme pour les données en mouvement, il y a un risque que les données soient volées afin d'être décodées ultérieurement.

Données en cours d'utilisation
La menace représentée par un système d'exploitation compromis, par des applications malveillantes ou par du matériel corrompu transforme la protection des données en cours d'utilisation en défi.

Pour le relever, on peut employer des processeurs spéciaux qui protègent contre les systèmes d'exploitation corrompus et les applications malveillantes en offrant un environnement sécurisé (enclave des processus Intel, par ex.). Cela suppose d'avoir confiance dans les fabricants de matériel, alors que cette confiance a été fortement ébranlée par les nombreuses failles constatées ces dernières années. Aussi la recherche planche-t-elle activement – mais encore insuffisamment en Suisse – sur les moyens permettant de détecter les vulnérabilités et les portes dérobées dans le matériel.

Autres possibilités: recourir au chiffrement homomorphe de données, qui rend possible le traitement des données sans décodage préalable, ou au calcul multipartite sécurisé (*secure multi-party computation*), qui permet à plusieurs parties d'utiliser le même processus de calcul sans que les données saisies ou les résultats intermédiaires perdent leur confidentialité vis-à-vis des autres utilisateurs. Ces deux techniques permettraient à l'utilisateur de données sensibles de profiter des avantages des services en nuage sans avoir à rechercher un fournisseur fiable à 100 %.

Les applications de chiffrement homomorphe présentent des inconvénients qui ont empêché jusqu'ici leur utilisation commerciale opérationnelle: les fonctionnalités disponibles sont limitées, elles nécessitent une capacité de calcul importante et les processus s'exécutent trop lentement.

En outre, le chiffrement homomorphe et le calcul multipartite sécurisé reposent sur des principes du chiffrement asymétrique, ce qui les fragilisera tôt ou tard face aux ordinateurs quantiques et aux nouvelles solutions mathématiques. Pour pouvoir profiter au moins minimalement des avantages du nuage malgré ces vulnérabilités, il reste le chiffrement symétrique des données, qui implique toutefois de retélécharger les données sur son propre système chaque fois qu'on veut les modifier. Cela n'a de sens que si les données ne sont traitées que sporadiquement, ce qui est contraire à la tendance

actuelle, qui est d'externaliser l'ensemble des données et des processus dans le nuage.

Recommandation:

2. La Confédération veille, en collaboration avec les cantons, à ce que la technique de chiffrement 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.

4.4.3 Doter la Suisse d'un réseau de communication hautement sécurisé

Lorsque le chemin de fer a conquis la Suisse, il a fallu mettre en place une infrastructure sûre à l'échelle nationale. Un siècle plus tard, ce fut au tour de l'automobile. Ces infrastructures n'auraient jamais vu le jour sans un engagement national. Aujourd'hui, Internet relie des milliards de personnes et d'appareils à travers le monde. Un nombre croissant de services et de processus industriels dépendent de la cybercommunication. Les conséquences d'une défaillance d'Internet donnent une idée de l'ampleur de cette dépendance.

Il faut par conséquent doter la Suisse d'un réseau de communication national hautement sécurisé, qui garantisse la poursuite des échanges même en cas d'attaque. Ce réseau doit protéger le contenu des informations et les identités des expéditeurs et des destinataires, et surtout garantir une disponibilité élevée. Il servira à assurer la communication entre tous les échelons des autorités et les infrastructures critiques, y compris en cas de crise, et offrira par ailleurs à la société tout entière (autorités, entreprises, organisations et particuliers) les moyens d'une communication en réseau sûre, en fonction des besoins en sécurité et des ressources de chacun. Nul doute que l'insécurité croissante de l'écosystème Internet ouvert fera croître la nécessité d'une telle infrastructure nationale. Une fois en place, celle-ci devrait favoriser durablement la transformation numérique du pays.

La souveraineté sur Internet est un aspect important. Le web actuel et même les cyberprotocoles promettant une communication sûre sont dotés de dispositifs d'arrêt d'urgence qui permettent aux grandes puissances de couper le réseau dans une région donnée. Ces dispositifs comprennent notamment les attaques DDoS, qui rendent impossible toute communication, et les détournements de route, qui empêchent les paquets de données d'atteindre leur destinataire.

Comme expliqué dans le chapitre sur la cryptographie (cf. ch. 4.4.1), les instruments de sécurité couramment utilisés aujourd'hui sur le web (authentification, signature, sécurité des transports) reposent sur des techniques de chiffrement asymétriques dont la sécurité n'est pas garantie à long terme. Il convient donc d'examiner les moyens de mettre en place un réseau de communication national offrant une sécurité durable. Ce réseau devra être aussi compatible que possible avec les processus de communication actuels et il devra être accessible à toutes les personnes intéressées.

Selon une approche traditionnelle, on pourrait établir ce réseau suisse ultra-sécurisé sur des lignes de communication dédiées (lignes louées) telles que MPLS, SDN ou SD-WAN. Mais on obtiendrait ainsi un réseau rigide, difficile à gérer, à élargir et à redimensionner pour plusieurs fournisseurs. L'EPF de Zurich a développé une autre

approche: une nouvelle architecture réseau appelée SCION, qui garantit la souveraineté numérique et le maintien des communications, même en cas d'attaque. De plus, SCION est déjà largement compatible avec les processus de communication actuels et ne nécessite guère d'adaptation des réseaux existants.

Recommandation:

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.

4.4.4 Normes et certifications de produits

4.4.4.1 Introduction

La certification est un instrument délivré par un tiers indépendant, qui atteste qu'un produit, une prestation ou une organisation respecte des exigences bien définies (normes).

Les logiciels et en particulier les appareils cyberphysiques présentent depuis toujours des failles de sécurité inquiétantes. Ils manquent souvent des défenses nécessaires pour résister aux agressions. Les principales défenses sont les suivantes: la possibilité de personnaliser les paramètres par défaut au moyen de l'identifiant et du mot de passe de l'utilisateur, un système de mise à jour si possible automatisé et sous licence du logiciel intégré (apport de correctifs), des solutions de chiffrement sûres pour la téléphonie IP, un antivirus et un dispositif d'arrêt d'urgence intégré. Ce dispositif permet au producteur ou à une autorité de surveillance d'éteindre l'appareil en l'absence de mises à jour, lorsque l'appareil devient un danger non seulement pour son utilisateur mais aussi pour des tiers, par exemple s'il est utilisé comme élément d'un botnet (ou réseau zombie) en vue d'une attaque DDoS sur l'IdO.

En Suisse, les normes et les certifications ou évaluations de conformité concernant les logiciels se sont imposées dans différents secteurs comme une condition de l'autorisation de mise sur le marché ou de la mise en circulation de certains produits (médicaux et de télécommunication, par ex.). À cet égard, il convient de citer la norme d'audit suisse «Audit de progiciels» (NAS 870) de la Chambre fiduciaire et la prise de position «Principes de régularité de la comptabilité lors de l'utilisation de technologies de l'information» (PP 10), qui la concrétise.

Les normes d'audit des logiciels et des appareils cyberphysiques ne sont pas sans poser des difficultés. La fonctionnalité numérique se caractérise par une flexibilité, une multifonctionnalité et une adaptabilité au client élevées. Par ailleurs, la sécurité des logiciels et des appareils cyberphysiques dépend largement du contexte des infrastructures numériques dans lesquelles l'utilisateur les a installés et des paramètres spécifiques qu'il a définis à cette occasion. Il faudrait que les exigences en matière de conformité couvrent un vaste éventail de paramètres car chaque modification constitue un risque potentiel. La mise en œuvre d'un principe de certification, statique par définition, dans l'environnement dynamique des logiciels représente un défi particulier.

Les «critères communs» (CC) sont probablement la norme d'évaluation de la sécurité des technologies de l'information la plus répandue dans le monde et la plus reconnue. Mais le processus d'évaluation étant long et coûteux, il n'est utilisé que pour des produits hautement sensibles, par exemple dans la navigation spatiale. Le processus des

CC montre bien que l'évaluation de conformité fondée sur des normes atteint rapidement ses limites et devient disproportionnée dans la mesure où il faudrait la refaire intégralement à chaque mise à jour d'un appareil, par exemple un éclairage bon marché compatible réseau. L'écart entre la banalisation des produits informatiques et l'absence, dans le B2C comme dans le B2B, d'une norme imposant la sécurité dès le stade de la conception apparaît ici dans toute son ampleur. En fin de compte, un utilisateur de produits informatiques dans l'environnement économique ne peut se fier qu'à lui-même pour vérifier la sécurité informatique de sa chaîne de production.

Il n'y a donc rien d'étonnant à ce que l'UE, par exemple, ait imposé un sigle de conformité pour une grande variété de produits avec son label CE, qui garantit à l'utilisateur un niveau de protection harmonisé en matière de sécurité et de santé. Il manque un tel sigle pour les logiciels et les produits cyberphysiques.

4.4.4.2 Importance des certifications et des normes en matière de responsabilité

La question non réglée de la pertinence des normes et des certifications de produits complique aussi la délimitation des domaines de responsabilité entre utilisateurs, fabricants et intermédiaires et, partant, les questions de responsabilité délictuelle et contractuelle (cf. ch. 7.3). Du point de vue juridique, les normes et les certifications ont un sens lorsque leur observation correspond à une pratique largement répandue, du moins dans les milieux concernés (secteur), ou qu'elle est imposée par la loi. Le non-respect de normes reconnues équivaut, selon les principes généraux de la législation en matière de responsabilité, à une négligence coupable qui entraîne la responsabilité des dommages résultant de ce non-respect, sous réserve que les autres conditions de la responsabilité soient remplies (lien de causalité adéquat, illicéité ou violation d'une obligation contractuelle). Le lien de causalité n'est pas forcément évident à établir s'il n'est pas certain, dès le départ, que l'observation de la norme aurait permis d'éviter le dommage.

Sous l'angle de la responsabilité de l'employeur (art. 55 du code des obligations [CO]), le non-respect de normes reconnues équivaut à un défaut d'organisation entraînant la responsabilité du dommage survenu de ce fait de manière illicite et causale. En matière de responsabilité du fait des produits, le non-respect de normes reconnues peut constituer un défaut de produit engageant la responsabilité.

Lorsque la loi impose le respect d'une certaine norme ou un certain type de certification, le non-respect de cette obligation peut être considéré comme illicite.

C'est le cas lorsque la disposition légale en question doit être considérée comme une norme de protection, c'est-à-dire qu'elle a pour but de protéger des victimes potentielles contre les dommages susceptibles de résulter de son non-respect. Dans la mesure où c'est la responsabilité délictuelle qui est engagée ici (c'est-à-dire que le dommage n'est pas survenu entre deux partenaires contractuels), elle porte aussi sur les éventuels dommages ne résultant pas d'une atteinte à un bien juridique absolu (vie, intégrité corporelle, personnalité, propriété), car l'illicéité ne résulte pas dans ces cas d'une atteinte à de tels biens, mais d'une violation de la norme de protection légale.

4.4.4.3 Responsabilité des fournisseurs de services de certification

La question de la responsabilité des fournisseurs de services de certification en cas de dommage subi par un tiers pour cause de non-conformité de la procédure de certification mérite une attention particulière. En l'absence de règles de responsabilité spécifiques (telles celles prévues, par ex., pour les fournisseurs de services de certification et pour les organismes de reconnaissance de ces fournisseurs dans la loi du 18 mars 2016 sur la signature électronique [SCSE]), les principes généraux de la responsabilité délictuelle s'appliquent (violation du devoir de diligence à observer lors de la certification ou violation de normes de protection telles que des conditions de certification définies par la loi). On peut aussi envisager une responsabilité fondée sur la confiance (comme la responsabilité liée à des renseignements ou des expertises, par ex.), quand l'acquéreur d'un produit a confiance dans une certification et que le fournisseur de celle-ci doit tabler sur cette confiance, ce qui est sans doute régulièrement le cas.

4.4.4.4 Conclusions

Les chaînes de production de produits informatiques sont mondialisées et dominées par des acteurs non européens. Il serait donc absurde pour la Suisse d'élaborer en cavalier seul des normes de sécurité assorties, le cas échéant, d'une autorisation de mise sur le marché. Elle doit par contre examiner des modèles possibles et les approfondir en concertation avec l'UE ou au sein des organismes internationaux. Les autorités pourraient en outre publier, sur le modèle des conseils aux voyageurs du DFAE, une liste de logiciels et d'appareils cyberphysiques dangereux, afin d'élargir les moyens d'information (cf. ch. 5.3.1.12).

Recommandation:

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.

4.4.5 Bonnes pratiques et normes

Le développement des normes de sécurité de l'information et de sécurité informatique courantes et éprouvées est principalement le fait de grandes entreprises. Il existe différents cadres:

- la famille ISO 27000;
- l'Information Risk Assessment Methodology 2 (IRAM2), mise au point par l'Information Security Forum;
- le cadre de cybersécurité (CSF pour *cybersecurity framework*) et le référentiel SP 800-53 de l'institut national américain des normes et de la technologie (NIST pour *National Institute of Standards and Technology*), conçus pour les infrastructures critiques;
- les «Grundschutzkataloge» mis à disposition par l'office fédéral allemand de la sécurité informatique (BSI pour *Bundesamt für Sicherheit in der Informationstechnik*) et mis à jour en février 2018 et remplacés par les «BSI-Standards» et le «IT-Grundschutz-Kompendium».

Ces cadres reposent sur une approche systémique intégrale et sont souvent couplés avec la mise en place d'une gestion des risques détaillée. D'autres normes ou guides plus courts, comme le guide de la cybersécurité à l'intention des entreprises de la Chambre de commerce internationale, ne conviennent que pour l'initiation des dirigeants ou sont tellement succincts qu'ils se contentent de proposer une liste de vérification très simple (InfoSurance, ou l'aide-mémoire pour les PME de MELANI[6]), sans entrer dans le vif du sujet. Ce qui manque aujourd'hui, c'est un guide bref et concis qui montre aux PME mais aussi aux entreprises plus grandes comment accéder pas à pas à une sécurité accrue[7]. Un tel guide doit satisfaire aux critères qui suivent.

Ce guide doit initier les utilisateurs aux faiblesses des infrastructures numériques en tenant compte d'aspects généraux relevant des techniques de sécurité et de l'organisation de même que de questions de conformité avec la réglementation, mais en traitant aussi en détail des services importants tels que le courrier électronique ou le web. Il doit proposer trois niveaux de maturité et aider les utilisateurs à déterminer leur niveau de sécurité au moyen de questions de vérification. À chaque niveau correspondent des mesures de sécurité que le guide expose en détail dans la mesure du possible. Le principe de neutralité technologique souvent employé se justifie du fait de l'évolution rapide des techniques, mais il complique la définition claire de niveaux de sécurité. Le guide doit donc privilégier les critères et les recommandations concrets, ce qui implique sa mise à jour régulière par un service responsable. Un bref catalogue de critères doit aider l'utilisateur à décider où il y a lieu d'envisager une externalisation ou une infogérance (*managed services*). Le guide n'a pas vocation à fournir une introduction technique à la sécurité informatique (il n'explique pas comment configurer un pare-feu réseau, par ex.). Mais il doit être auditable et permettre une (auto-)certification.

Le guide doit donner aux utilisateurs, tant à la direction qu'aux administrateurs informatiques, les moyens de déterminer un niveau de maturité et de l'exiger des fournisseurs informatiques. Au niveau de la société en général, il sert de référentiel par rapport à des bonnes pratiques largement reconnues, et même de norme si cela paraît judicieux pour les infrastructures critiques, par exemple. Un tel guide, solidement étayé, reconnu et mis en œuvre, contribuera à créer une compréhension commune et fournira un ordre de grandeur du niveau de sécurité qui paraît raisonnable dans le cybercontexte. La possibilité d'une (auto-)certification contribuera quant à elle notablement à établir, par la transparence et la vérifiabilité, un réseau de confiance dans le B2B comme dans le B2C.

4.4.6 Identités numériques

Outre l'infrastructure de chiffrement asymétrique, la sécurité repose sur des entités numériques vérifiables. Ces entités peuvent être des personnes physiques ou morales ou des infrastructures numériques. Les identités vérifiables sont établies par une autorité de certification (AC ou CA pour *certificate authority*), qui gère une infrastructure à clé publique et délivre des certificats. Ces certificats contiennent, selon leur configura-

[6] https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html (état au 10.5.2018); «De la pratique – pour la pratique» Cahiers des PME, Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME), Une protection accrue grâce au programme en 10 points élargi, 2016

[7] Exposé en détail dans l'étude de l'ENISA «Information Security and Privacy Standards for SMEs», 2015

tion, différents couples de clés publique/privée. Ils sont signés par l'émetteur et rattachent une entité à la clé publique. Un acteur désirant prendre contact peut vérifier une identité à l'aide de la clé publique contenue dans le certificat, par exemple lors de la vérification d'un site web. Les signatures numériques servent à vérifier la fiabilité d'une information. Dans une infrastructure à clé publique, la vérifiabilité des émetteurs de certificat au moyen de certificats racines constitue le premier maillon de la chaîne de confiance.

Dans bon nombre de scénarios, des mécanismes de sécurité fondés sur des certificats jouent un rôle décisif en permettant:

- à un destinataire de vérifier les courriels provenant d'une compagnie d'assurance, et faire ainsi barrage au hameçonnage;
- de renforcer la sécurité de la connexion Internet entre le navigateur d'un utilisateur et l'identifiant de sa relation bancaire;
- de vérifier des messages d'utilisateurs au moyen de l'identité numérique;
- d'effectuer de nombreuses démarches administratives (déclaration d'impôt, etc.) par voie électronique, sous son identité numérique;
- d'authentifier, de signer et de chiffrer au moyen de l'identité numérique des prestations de santé et des paiements (par ex., envoi de résultats de laboratoire cryptés à un patient, qui pourra en authentifier l'origine).

Vu l'importance de la confiance et de la sécurité sur le web, les certificats figurent d'ores et déjà parmi les principales cibles des cybercriminels. Les certificats volés jouent un rôle décisif dans de nombreux schémas d'agression. Lors de la fameuse attaque Stuxnet contre les centrifugeuses iraniennes d'enrichissement d'uranium, des certificats numériques corrompus ont été des instruments clés de l'anéantissement des mécanismes de sécurité.

Les certificats vont être l'objet d'attaques de plus en plus nombreuses, car ils constituent aussi un élément de base de la confiance dans l'IdO. Dans la communication entre l'homme et la machine comme dans la communication entre machines (M2M), il faut que l'identité soit vérifiable. Le problème, c'est que la durée de vie des certificats numériques (généralement deux ans) est nettement plus courte que celle des appareils de l'IdO, en particulier dans le B2B (plus de dix ans). La gestion des identités et des accès (GIA ou IAM, pour *identity and access management*) dans le M2M ne reçoit pas encore l'attention qu'elle mérite.

Dans toute organisation comptant potentiellement des milliers de droits d'accès pour des personnes et des appareils connectés, la fiabilité de la GIA dépend de l'existence d'un système d'authentification et de validation des informations fondamentalement fiable qui repose, dans un système sûr, sur des certificats.

Il faut élaborer un réseau avec des AC fiables, en veillant à une grande compatibilité entre navigateurs et systèmes d'exploitation:

- Il faut faire en sorte qu'en Suisse, les personnes physiques et morales de même que les autorités puissent obtenir un certificat d'une AC suisse digne de confiance.

- Toutes les entités sensibles (telles que serveur web, notamment) des exploitants d'infrastructures critiques et de fournisseurs d'identité au sens de la future loi e-ID doivent s'appuyer sur une infrastructure à clé publique élaborée et vérifiée ou vérifiable en Suisse, et ne pas utiliser de certificats numériques étrangers.
- Les particuliers doivent obtenir par des moyens sûrs une identité numérique protégée contre les maliciels sur leur ordinateur privé. Il faut prévoir des mécanismes de restauration en cas de perte et pour les mises à jour. La restauration nécessite l'identification de la personne sur place (dans un bureau de poste, une gare ou une banque, par ex.).
- Il faut prévoir des mécanismes efficaces de révocation et de recertification à tous les échelons en cas de perte, de détérioration ou de vol d'une clé privée, et les intégrer dans l'écosystème existant avec le système d'exploitation (Mac OS, Windows, Unix, Android, etc.) et les applications (navigateur, client de messagerie, etc.).

Les accréditations anonymes sont des jetons d'authentification qui permettent à un utilisateur de conserver l'anonymat dans ses relations avec des organisations publiques et privées. Le système repose sur des algorithmes cryptographiques. Cette approche est plus favorable à la protection des données que la gestion centralisée courante de gros volumes de données d'utilisateurs.

Dans le monde analogique, les accréditations personnalisées et non anonymes comprennent les passeports, les permis de conduire, les cartes de crédit, les cartes d'assurance-maladie, les cartes de membre d'un club, etc. Elles indiquent le nom de leur propriétaire et comprennent des éléments d'authentification tels que signature, code PIN ou photo afin d'éviter toute utilisation illicite. Les données d'accès anonymes sont, par exemple, l'argent liquide, les billets de bus ou de train, et les jetons de jeux d'arcade. Elles ne contiennent aucune information d'identification et peuvent donc s'échanger entre utilisateurs sans que leur émetteur ou les tiers de confiance le sachent. Les justificatifs d'identité et les accréditations sont émis par des organisations qui vérifient l'authenticité des informations et peuvent la communiquer aux organes de vérification qui en feraient la demande.

Dans une procédure d'enregistrement numérique, une accréditation anonyme fournit suffisamment d'informations sur le propriétaire pour satisfaire à un critère spécifique et permettre l'octroi de l'autorisation, sans révéler toute son identité. Cette solution est avantageuse dans certaines situations et renforce la protection des données, par exemple lorsqu'il s'agit de déterminer l'âge de la personne, l'existence d'un permis de conduire, bien souvent la nationalité, ou encore de savoir si le demandeur a des dettes auprès d'une certaine organisation.

IBM Research a étudié ce principe technique en détail dans le cadre de projets européens tels que Prime, PrimeLife ou ABC4Trust. Les accréditations anonymes n'ont longtemps offert qu'une utilité pratique réduite, mais leur degré de maturité est aujourd'hui suffisant pour permettre une mise en œuvre concrète. Une fondation d'intérêt public, la Privacy by Design Foundation[8], a développé le concept et en propose désormais une version utilisable.

[8] https://privacybydesign.foundation (état en juillet 2018)

Recommandations:

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

4.5 Des pistes pour avancer

4.5.1 Comment mesurer la sécurité de l'information?

La recherche de solutions potentielles implique de déterminer des moyens de mesurer la sécurité de l'information. Sur le fond, on dispose de critères clairs: la fiabilité, la disponibilité, l'intégrité et la traçabilité. Par ailleurs, une multitude de normes, de guides et autres manuels de sécurité informatique et de sécurité de l'information ont vu le jour ces vingt dernières années. Bon nombre d'entre eux se sont imposés au fil du temps et ont contribué à améliorer la sécurité en imposant des contrôles systématiques. Mais l'évolution rapide de l'environnement technique ne permet pas de déterminer, par l'expérience, la correspondance entre une mesure de protection donnée et un niveau de sécurité ou de vulnérabilité. Comme la menace évolue chaque jour, restant insaisissable et réduisant d'autant l'efficacité des mesures de protection, il est impossible de déduire des niveaux de référence des mesures de protection et de la menace. On manque d'ailleurs d'éléments de comparaison.

Faute d'un barème fiable, il est difficile de déterminer le niveau de sécurité raisonnable pour une organisation dans son contexte spécifique, et les mesures de protection concrètes apportant la plus grande sécurité dans un contexte donné. Or une société moderne en pleine transformation numérique a besoin d'éléments de comparaison, ou du moins de valeurs indicatives, pour mieux gérer les risques. L'absence de ces valeurs et d'un historique des événements rend par ailleurs ces risques plus difficiles à assurer.

4.5.2 Un réseau national de promotion de la sécurité de l'information

En Suisse, le monde de l'économie, de la recherche et de la formation porte l'empreinte de la technologie, de l'innovation et de l'esprit de service. Un grand nombre d'acteurs se préoccupent activement des questions de sécurité de l'information, ou du moins s'y intéressent: dans les secteurs de la finance et de l'assurance, dans les domaines de la santé, de l'industrie pharmaceutique, des transports, de l'énergie, des technologies de l'information et de la communication, et dans bon nombre d'institutions académiques. Pourtant, il n'y a entre eux quasiment aucune coordination ni aucun échange d'informations (en particulier concernant les incidents).

À l'heure actuelle, le Fonds national suisse (FNS) ne consacre à la sécurité de l'information que de rares projets déconnectés les uns des autres. Plusieurs de ces projets s'inscrivent dans le Programme national de recherche 75 «*Big data*» (PNR 75). Il y a certes transfert de technologie de la science vers l'économie, mais uniquement sous

la forme de projets individuels, sans aucune structuration. Des start-up et des développements en matière de sécurité tels que ID Quantique, ProtonMail, Threema et Ethereum sont nés en Suisse et donnent une idée de ce qu'il serait possible de réaliser, mais une grande partie du potentiel est laissée en jachère ou exploitée à l'étranger.

Ce qui manque, c'est un écosystème structuré, un pôle national au sein duquel des partenaires économiques, scientifiques et gouvernementaux puissent construire une collaboration durable. Ce pôle devrait être financé par des fonds publics et privés, pourquoi pas dans le cadre d'un vaste programme Innosuisse. Cela pourrait commencer par la constitution d'un réseau national dans lequel entreprises, établissements de recherche, universités, hautes écoles spécialisées et start-up travailleraient main dans la main en réunissant leurs connaissances et leurs ressources. La construction d'un ou deux pôles de recherche nationaux (PRN) viendrait appuyer ce processus.

Conscients de la nécessité d'agir pour la sécurité de l'information, de nombreux États sont en train de consacrer des moyens importants au développement d'établissements de recherche (Helmholtz Institut ou Max-Plank-Gesellschaft en Allemagne, par ex.). L'UE a créé l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). De telles mesures auront des effets, mais leur efficacité soulève un certain nombre de questions.

L'exemple d'Israël montre que la constitution d'un réseau appuyé par un programme gouvernemental (*National Cyber Bureau*), par l'implication de tous les acteurs concernés dans un «CyberSpark» et par l'élaboration d'un «Cyberhub» (Université Ben Gourion) a produit un écosystème unique, au succès international. En Suisse, un tel écosystème encouragerait durablement la recherche et le développement dans les domaines du numérique et de la sécurité de l'information. Il aurait aussi pour effet d'attirer de nouveaux étudiants et de nouveaux talents.

Recommandation:

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.

4.5.3 Absence de vue d'ensemble et de partage des connaissances

Dans le monde physique, la police, les services de renseignement et l'armée tiennent à jour un «tableau» des événements et des risques potentiels. Ce tableau n'existe pas pour le monde virtuel, en partie à cause de la globalité des cybermenaces, qui ne respectent aucune frontière territoriale, en partie parce que la majorité des acteurs concernés omettent de signaler les incidents de sécurité, ce qui empêche la transmission de connaissances importantes. En Europe surtout, le principe de restriction au «besoin d'en connaître» est prépondérant: pas de transmission sauf contrainte ou impossibilité de faire autrement.

Alors que le parti des agresseurs a bien compris que le partage de connaissances et la répartition des tâches sont déterminants pour réussir, celui de la défense tarde à le reconnaître. Les centres privés et gouvernementaux de réaction aux urgences informatiques (CERT pour *computer emergency response team*), les entreprises spécialisées dans la sécurité de l'information, mais aussi et surtout les nombreuses entreprises concernées collectent en permanence des données sur les attaques ou des

signalements de tiers, mais ils ne collaborent et ne partagent pas suffisamment leurs connaissances pour obtenir une vue d'ensemble de la situation qui ne soit pas fragmentée. Un partage intensif des connaissances contribuerait à une meilleure gestion des incidents (cf. ch. 4.5.4). Les programmes de sécurité, voire la réglementation, doivent exploiter cette possibilité de coopérer. Dans le cadre du G2Ci/B, les acteurs concernés approfondissent les instruments nécessaires et formulent des recommandations (cf. ch. 8.2.5).

4.5.4 Gestion des incidents

Étant donné qu'il n'existe pas de protection intégrale et définitive contre les cyberincidents mais qu'il faut s'attendre à une multiplication des attaques ciblées, la mise sur pied et l'exploitation d'une organisation nationale et centrale de gestion des incidents constituent un élément clé de la lutte contre les cyberrisques. La gestion des incidents implique de détecter les incidents le plus tôt possible, d'identifier et d'appliquer les mesures qui conviennent, et d'analyser les incidents survenus pour en tirer des enseignements qui permettent d'améliorer la prévention. Pour assumer ces tâches, il faut des compétences techniques, des instruments d'analyse, une organisation qui fonctionne et une collaboration étroite entre tous les services concernés. L'échange d'informations fondé sur la confiance mutuelle des partenaires joue un rôle décisif, d'autant qu'une attaque vise souvent plusieurs cibles à la fois et qu'elle se surmonte plus rapidement et plus efficacement à plusieurs.

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI soutient depuis 2004 un cercle restreint d'exploitants d'infrastructures critiques dans la détection, la gestion et l'analyse des cyberincidents. MELANI fonctionne comme un guichet unique au niveau de l'État et apporte son aide pour l'analyse des incidents, aussi bien sous l'angle technique que sous celui du renseignement, notamment sous la forme d'une plateforme d'échange d'informations. Le besoin d'une organisation nationale et centrale et la dimension sociétale du sujet offrent la possibilité d'élargir le groupe cible de MELANI (cf. ch. 8.2.5).

4.5.5 Sécurité de l'information et réglementation

On entend souvent affirmer que chacun devrait être libre de choisir ses mesures de sécurité de l'information, voire de ne pas en appliquer, au motif que les mécanismes du marché finiront bien par générer une gestion des risques équilibrée: l'entreprise qui investit trop peu dans la sécurité informatique disparaîtra de la même façon que celle qui investit trop au détriment du développement de l'innovation. Cette conception de l'autorégulation du marché est peut-être juste du point de vue économique, mais dans le cybermonde elle repose sur des bases erronées car en négligeant de se protéger convenablement, on fait aussi augmenter les risques pour autrui. Les agresseurs se servent des infrastructures non protégées comme botnets pour des campagnes de spam, pour des attaques DDoS, pour leur infrastructure de commande et de contrôle (CC) ou pour masquer celles-ci. Et les attaques par rançongiciel qui réussissent de même que la commercialisation des données volées génèrent des ressources supplémentaires pour leur arsenal. Il se peut que cette approche réactive libertaire aboutisse, après de nombreux dommages et contre-mesures, à un équilibre entre niveau de protection et potentiel d'agression, mais à un coût nettement plus élevé et en exposant la société à une grande insécurité.

Il est donc urgent de débattre du niveau raisonnable de sécurité de l'information, de faire le point sur les contraintes techniques et organisationnelles nécessaires en tenant compte des bases légales, de déterminer les responsables de la mise en œuvre et d'identifier les mesures réglementaires qui s'imposent secteur par secteur.

Contrairement à l'UE ou aux États-Unis, la Suisse n'a pas encore réellement affronté ce débat. Quel est le niveau de sécurité nécessaire et raisonnable? Il faut tenir compte du fait que la société a de plus en plus de mal à gérer l'insécurité et à accepter un niveau de risque indéterminé. Faute de réponse à cette question, le risque «absence de sécurité de l'information» atteindra un niveau insupportable aux yeux de la société, pour qui tout risque, même ceux du cyberespace, doit être maîtrisable et s'inscrire dans des statistiques. Le groupe d'experts reconnaît qu'il est important, pour la société comme pour l'économie, de pouvoir assurer les cyberrisques, mais n'a pas approfondi ce sujet dans le présent rapport.

Ce débat a notamment pour éléments les normes et la certification des produits et des services, de même que l'obligation de notifier les cyberincidents ainsi que le besoin et la réglementation en matière de mesures de protection dans le domaine de la sécurité de l'information.

4.5.6 Nouvelles technologies: l'intelligence artificielle au secours des mécanismes de défense

Aujourd'hui, les mesures de sécurité techniques telles qu'antivirus, pare-feu ou contrôles d'interfaces et d'applications fonctionnent essentiellement selon des règles prédéfinies. Ce principe se heurte de plus en plus à ses limites: d'une part, on assiste à une multiplication des variantes de souches de maliciels, toujours les mêmes, dont les systèmes courants ne peuvent pas garantir la détection; d'autre part, la complexité et l'interconnexion des infrastructures numériques croissent sans cesse, ce qui fait qu'il devient tout simplement impossible de gérer le paramétrage de centaines ou de milliers de règles (pare-feu, par ex.), car cette gestion, il faut non seulement la mettre en place, mais aussi l'ajuster manuellement en permanence, avec l'aide d'experts.

Aussi les systèmes auto-apprenants (apprentissage profond) suscitent-ils de grands espoirs. Ils sont en effet capables d'interpréter le paramétrage initial d'un pare-feu au moyen des données reçues et de l'adapter d'une manière souple et automatique aux modifications du système (extension ou mise à jour). Ils peuvent aussi, lorsqu'ils surveillent des applications, détecter des routines (communication avec d'autres systèmes, dérogations relatives à la bande passante, aux ports et aux protocoles de transport, par ex.) et bloquer des fonctions non autorisées parce qu'elles s'écartent du comportement standard ou qu'elles révèlent des faiblesses de programmation. Tout repose ici sur la reconnaissance de modèles (que fait une application? Est-elle le point de départ d'anomalies affectant les échanges de données?). Cette approche est déjà largement employée. Les différentes démarches qui visent à pallier une industrialisation à la traîne par une sécurité automatisée et intelligente ont beau être prometteuses, leur intérêt reste limité. En effet, les systèmes auto-apprenants doivent, pour être efficaces, pouvoir s'entraîner sur des données de qualité. Un système en place peut avoir été corrompu et refléter une image fausse de l'état de sécurité «normal», tandis qu'un système neuf non encore connecté ne peut pas fournir une image de l'exploitation réelle. Conséquence: multiplication des fausses alertes contraignant les experts en sécurité à procéder à des vérifications manuelles, et impossibilité pour le système, trompé par du matériel d'entraînement corrompu, de détecter les problèmes véritables.

En outre, il est théoriquement possible pour un agresseur d'influencer la phase d'entraînement des systèmes auto-apprenants de manière à ce qu'ils assimilent un comportement incorrect ou qu'ils considèrent comme suspect un comportement correct, afin d'augmenter encore le nombre de fausses alertes.

Il est à craindre que les agresseurs se mettent eux aussi à utiliser des systèmes auto-apprenants, toujours plus accessibles et plus simples, et ce à tous les niveaux (criminels, acteurs proches de l'État, services de renseignement, armée et police). Ils se servent déjà de la technologie pour analyser les modèles de comportement courants d'un réseau dans une organisation afin de concevoir des modèles d'attaque qui seront pris à tort pour un comportement normal. Ils sont aussi capables de lancer des attaques personnalisées par hameçonnage. Nul doute que la «course aux armements» entre agresseurs et défenseurs s'accentuera aussi dans ce domaine, avec des effets certains sur la cybersécurité. Il est d'autant plus important d'intensifier la recherche afin d'armer au mieux l'État, les infrastructures critiques, les établissements de recherche et, bien sûr, l'industrie sensible (cf. aussi ch. 8.2.6 s.).

5 Champ d'analyse relations entre les entreprises et les consommateurs (B2C)

5.1 Situation actuelle et évolution

Le numérique a généré à l'intention des utilisateurs et des consommateurs une multitude d'offres abordables de biens et services, essentiellement électroniques jusqu'ici. Les services sont personnalisables, adaptés aux besoins du client et disponibles partout dans le monde, vingt-quatre heures sur vingt-quatre. La diversité des offres va sans doute continuer d'augmenter. Et dans ce domaine aussi, la frontière qui sépare le monde virtuel numérique du monde physique s'efface à vue d'œil. Le secrétaire virtuel qui commande un nouveau parapluie livrable par drone parce qu'il a vu, par surveillance vidéo, que son patron avait perdu le sien en se rendant au travail est bien plus proche de nous que d'un récit de science-fiction.

Les actuels géants du web (Google, Apple, Facebook, Amazon, Alipay/Alibaba, etc.) ont le pouvoir de contrôler les accès à la partie visible de l'écosystème Internet. Ce pouvoir leur confère un quasi-monopole sur les moteurs de recherche, les réseaux sociaux et le shopping en ligne, et dans une moindre mesure pour l'instant sur les services en nuage. Bon nombre de distributeurs ont dû, pour le commerce en ligne, céder leur place dans la chaîne de création de valeur en direction du consommateur ou sont obligés de coopérer avec les géants pour réussir. Dans la lutte pour le contrôle de l'interface entre les services numériques et l'homme, la commande vocale pourrait jouer un rôle majeur et accentuer le mouvement de centralisation. En effet, pourquoi un futur utilisateur recourrait-il à différentes interfaces à commande vocale s'il peut tout gérer à l'aide d'un secrétaire numérique unique? Il n'y a donc rien d'étonnant à ce que les grandes enseignes du cybermonde aient toutes lancé leur assistant vocal (Alexa chez Amazon, Google Now chez Google, Siri chez Apple et Cortana chez Microsoft).

Les fournisseurs intègrent de plus en plus d'intelligence artificielle dans leurs services numériques. On peut donc imaginer qu'à l'avenir, les clients auront à leur disposition des applications hyper-puissantes dotées de capacités comparables à celles de l'actuel Watson d'IBM. Les assistants vocaux ne sont que la première étape d'une anthropomorphisation de ces applications. Comme dans le monde analogique, la valeur de ces applications personnalisées augmente au fur et à mesure qu'elles connaissent mieux leur employeur et ses habitudes, ses préférences et son passé.

Quant aux internautes, ils ont une attitude contradictoire, en particulier sur les réseaux sociaux: en principe très attachés à la protection de leur sphère privée, ils publient sur le web une quantité croissante de données personnelles (nom, photos, numéro de portable, ou même croyances religieuses). La majorité d'entre eux semblent ainsi donner la priorité à leur cybervie sociale. Étant donné que les réseaux sociaux sont précisément fondés sur la révélation de données personnelles, le comportement des utilisateurs et le modèle d'affaires des fournisseurs constituent un véritable dilemme pour la protection des consommateurs et des données.

Dans le B2C, la transformation numérique bouleverse complètement le rapport entre fournisseurs et utilisateurs. Outre les spécificités courantes du numérique (disponibilité permanente des données, par ex.), elle s'y caractérise par l'analyse des *big data* (systèmes auto-apprenants), les modèles d'affaires fondés sur les données (en particulier

l'échange de données personnelles contre des services «gratuits») et les marchés bi-faces. Bien que bon nombre des services numériques B2C présentent deux de ces éléments, voire les trois, les effets de ceux-ci doivent être examinés à part.

5.2 Possibilités et risques

L'analyse des *big data* est déterminante lorsque le fournisseur se sert du suivi des clients et de l'analyse de données pour établir des profils de personnalité (profilage) et des évaluations (*scoring*) d'utilisateurs ou de groupes d'utilisateurs. Le scoring consiste à condenser les données personnelles en une seule valeur (score) afin de faciliter les comparaisons entre individus. Le profilage, lui, vise à répondre à un maximum de questions concernant une personne identifiable grâce à l'exploitation automatisée de ses données, afin d'obtenir un niveau de personnalisation élevé. Les fournisseurs de produits et de services n'ont jamais disposé d'autant de renseignements sur chaque utilisateur (situation économique, santé, préférences, comportement, lieu de villégiature, etc.).

Cette densité d'informations permet d'offrir des services particulièrement conviviaux et adaptés. Elle peut aussi entraîner des discriminations à l'encontre de certaines personnes ou groupes de personnes. Le profilage et le scoring peuvent avoir des conséquences négatives pour l'utilisateur, en particulier en matière de solvabilité, de prestations d'assurance, de recrutement, de transmission d'informations, d'évaluation professionnelle et (dans une moindre mesure pour l'instant) d'accès à des possibilités de formation: indisponibilité d'un produit, ou alors prix excessifs sans aucune transparence, exclusion d'une procédure de recrutement sans explication, etc. Il est même possible qu'à l'avenir, les réseaux sociaux excluent certains utilisateurs sur la base de leur score.

Le profilage permet aussi la création de «bulles de filtres» positives, c'est-à-dire que l'assistant de recherche donne effectivement la priorité aux informations les plus pertinentes pour l'utilisateur selon lui. Il serait souhaitable que la crédibilité des informations affichées puisse être vérifiée, mais dans l'état actuel de la technique, il s'agit là d'un objectif à long terme. Quoique les bulles de filtres positives s'éloignent de l'idéal d'un résultat de recherche neutre, l'utilisateur y gagne car elles réduisent le flux d'informations qui lui parvient.

On a davantage entendu parler ces derniers temps des bulles de filtres négatives, qui fournissent à l'utilisateur des résultats correspondant à son niveau de connaissance et à ses préférences, sans lui permettre d'aller plus loin. Personnalisés, ces filtres permettent de manipuler l'utilisateur en lui cachant certaines informations ou en lui en donnant d'autres, qui excèdent la pondération normale des résultats. Il peut donc arriver qu'un utilisateur n'ait pas accès à des éléments de comparaison importants ou à d'autres informations, ou alors difficilement (nouvelle recherche, long défilement vers le bas, autres moteurs de recherche, recherche plus approfondie). L'absence d'informations complémentaires et de substitution peut nuire à l'utilisateur. Le manque de transparence qui conduit le système au résultat est un élément important. Si l'on peut s'attendre à ce que les sites de médias et les réseaux sociaux personnalisent les résultats de recherche, les moteurs de recherche ne semblent appliquer pour l'instant que des bulles de filtres positives, quoi qu'en disent les rumeurs.

Le modèle d'affaires «service contre données personnelles» des moteurs de recherche, des réseaux sociaux, des services de santé (dispositifs d'auto-mesure ou

trackers) ou des solutions de stockage de masse dans le nuage a continué de s'imposer et suscite un débat sur la gestion future de la valeur des données (cf. ch. 7.2).

Sur les marchés bifaces, les effets de réseau directs et indirects jouent un rôle important. Plus les fournisseurs et les clients potentiels disposent d'informations les uns sur les autres, plus la transmission de services et de produits est efficace: amélioration des prix, du choix et du confort pour les utilisateurs, hausse du chiffre d'affaires des fournisseurs. Mais les risques aussi augmentent: les données personnelles recueillies par les exploitants peuvent entraîner des violations de la sphère privée ou de la législation sur la protection des consommateurs.

Prenons l'exemple de la différenciation des prix: le succès des plateformes de shopping en ligne, le suivi des clients, l'analyse des profils de clients et l'automatisation des processus de plateforme favorisent la souplesse des mécanismes de formation des prix, lesquels ne se contentent pas de suivre l'évolution de la demande au sens large et de l'offre ou le pouvoir d'achat ou le comportement d'achat d'un groupe de clients (par ex. des étudiants, à qui on va proposer des prix homogènes). Les méthodes modernes de traitement des données et la densité des données permettent une différenciation des prix parfaite du point de vue économique.

L'exemple classique, c'est celui du billet d'avion dont le prix augmente à chaque visite du consommateur sur le site de vente, alors que l'évolution de la demande ne justifie nullement cette augmentation. La différenciation des prix parfaite peut dans certains cas avantager autant les clients que le fournisseur, par exemple lorsque le profilage permet d'adapter le prix à ce que client est prêt à payer, en fonction du rapport offre / quantités et des frais de production. Son effet est négatif lorsque les différences de prix sont trop importantes, qu'elles évoluent rapidement, que les clients ne les comprennent pas car elles manquent de transparence, qu'il devient impossible de comparer les prix et que le monopole de l'offre ne laisse au client aucune solution de rechange.

Ceux qui critiquent la transformation numérique dans le B2C constatent fréquemment une asymétrie des connaissances en faveur du fournisseur. Ce n'est pas tout à fait exact. Le numérique présente aussi des avantages pour les consommateurs. Les portails d'évaluation et de comparaison de prix mettent en évidence la diversité de l'offre et des tarifs. Cela force les fournisseurs à pratiquer plus de transparence, sauf dans certains secteurs particulièrement complexes tels que les services, et notamment les prestations d'assurance. Par ailleurs, les nouvelles technologies permettent aujourd'hui au consommateur de jouer lui-même un rôle de fournisseur, en devenant un «prosommateur». Les plateformes d'hébergement illustrent bien ce principe: certes, le locataire est un consommateur «plus faible» que son bailleur, mais il a la possibilité de sous-louer son appartement à des touristes.

Conclusion

Il ne faut pas négliger les risques qui pèsent sur la protection de la sphère privée, de l'autodétermination en matière d'information et des consommateurs. Le débat sur le cadre juridique et sur les mesures à prendre doit donner toute leur place au droit de la protection des données et à certains aspects de la protection des consommateurs. Certains points d'éthique sont traités plus en détail au chapitre 11.

Les risques liés à la protection des données méritent une attention particulière:

- quand le suivi numérique des utilisateurs et le traitement mécanique des données ou les algorithmes utilisés contreviennent au principe de transparence (le traitement des données porte atteinte, à leur insu, à la sphère privée et à l'autodétermination en matière d'information des personnes concernées, exposant celles-ci à des dommages supplémentaires en aval, comme clients ou comme utilisateurs);
- quand le traitement des données sous-jacent des offres en ligne manque de transparence au point de rendre plus difficilement praticables toutes les autres voies de recours telles que le droit du consentement, le droit d'accès ou le droit d'opposition;
- en l'absence de choix véritable ou d'offres de substitution, en particulier dans les situations de monopole (par ex. lorsque l'utilisateur d'un réseau social est lié à la plateforme à cause de son cercle d'amis en ligne).

S'agissant de la protection des consommateurs, les principaux risques sont les suivants:

- diminution de la transparence et de l'applicabilité des droits et devoirs contractuels au détriment des consommateurs, du fait des nouvelles formes d'accords et de contrats favorisées par le numérique (cf. ch. 5.3.2.2 à 5.3.2.4);
- lésion découlant d'abus de position dominante et du profilage (cf. ch. 5.3.2.5);
- impossibilité de régler correctement les questions de responsabilité (notamment du fait des produits) faute d'une définition précise des prestations numériques et en raison de la complexité des chaînes de production (cf. ch. 7.3).

5.3 Cadre juridique et mesures à prendre

Dans le champ d'analyse B2C, deux champs juridiques méritent une attention particulière: la protection des données et la protection des consommateurs.

5.3.1 Protection de la sphère privée et de l'autodétermination en matière d'information

5.3.1.1 Introduction

Dans le B2C, la protection des données joue un rôle majeur, car elle vise à protéger la sphère privée et l'autodétermination en matière d'information de l'individu vis-à-vis de l'économie. L'individu doit pouvoir limiter la révélation par l'économie des données le concernant en déterminant lui-même les modalités de leur collecte, de leur stockage et de leur transmission. Les avantages et les inconvénients de la propriété des données et la question de l'accès à ses propres données (portabilité), thèmes transversaux entre B2B et B2C, sont traités à part (cf. chap. 7).

5.3.1.2 Comportement des utilisateurs

L'avenir de la protection des données ne dépend pas uniquement des prescriptions techniques et politiques propres à ce domaine mais aussi de la volonté du consomma-

teur ou de l'utilisateur européen de consacrer au quotidien le temps et l'énergie nécessaires à l'exercice de son autodétermination en matière d'information. Des sondages révèlent que la société, quoique très attachée à la protection des données, ne donne pas toujours la priorité à la sphère privée en raison du «paradoxe de la vie privée» et faute d'autres solutions. En fin de compte, les autorités de surveillance ont besoin, pour détecter et sanctionner les atteintes à la protection des données, de la coopération d'une population sensibilisée à cette question.

5.3.1.3 Protection des données: manque d'harmonisation du droit à l'échelle internationale et difficultés de l'Europe à imposer son point de vue

En matière de protection des données, les conceptions varient d'une région du monde à l'autre: l'accord «Safe Harbor» noué entre l'UE et les États-Unis a été invalidé par la Cour de justice de l'UE, son successeur, le «Privacy Shield», donne lieu à un incessant bras de fer entre les deux partenaires, et les procès se multiplient en Europe à l'encontre des géants américains du numérique, qui entendent mener la danse.

On constate néanmoins un véritable effort d'harmonisation du droit à l'échelle internationale. Par exemple, la convention du Conseil de l'Europe du 28 janvier 1981 sur la protection des données (Convention 108) a été ratifiée non seulement par 47 États membres du Conseil de l'Europe mais aussi par l'Uruguay, la Tunisie, Maurice et le Sénégal. D'autres États extra-européens dont le Maroc, le Cap-Vert, le Burkina Faso, l'Argentine et le Mexique s'apprêtent à les imiter, et ils pourraient devenir encore plus nombreux car l'UE considère cette démarche comme un critère important de ses décisions constatant le caractère adéquat du niveau de protection (et donc pour autoriser les échanges de données transfrontaliers sans précautions supplémentaires). Outre la Suisse, font actuellement l'objet d'une telle décision (c'est-à-dire que l'UE considère que le pays a un niveau de protection des données équivalent au sien) Andorre, l'Argentine, les Îles Féroé, Guernesey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande et l'Uruguay. D'autres États (le Japon et la Corée du Sud, par ex.) tentent actuellement de l'obtenir.

Il s'agit incontestablement d'une évolution positive, mais compte tenu de la suprématie de pays extra-européens dans le domaine du numérique (huit des dix plus grosses entreprises du monde sont des géants du web et ont leur siège aux États-Unis ou en Chine), l'Europe parviendra-t-elle à imposer ses principes en matière de protection des données?

5.3.1.4 Révision en cours de la législation sur la protection des données

Le 15 septembre 2017, le Conseil fédéral a adopté son projet de révision totale de la LPD (P-LPD) et l'a soumis au Parlement. Le but de ce projet est de renforcer la protection des données en l'adaptant à la réalité du traitement des données numériques. Le Conseil fédéral entend en outre doter la Suisse d'une norme internationalement reconnue qui tienne compte des derniers développements survenus en Europe (RGPD, révision de la Convention 108).

En plus de consolider les principes existants tels que la légalité, la proportionnalité, la finalité, l'identification et l'exactitude du traitement, et de les préciser par rapport au numérique, le P-LPD prévoit aussi de nouvelles mesures visant à adapter la législation au progrès technologique, en particulier:

- une augmentation de la transparence par l'extension du devoir d'informer lors de la collecte de données personnelles et par l'instauration d'un devoir de notifier l'autorité de surveillance de la protection des données en cas d'atteinte à la sécurité de l'information;
- la protection de la vie privée dès la conception et par défaut: ces concepts, qui reposent sur l'idée selon laquelle des précautions techniques et organisationnelles peuvent réduire significativement les risques de violation du droit de la protection des données, obligent les responsables du traitement à prendre ces précautions d'emblée (respect des prescriptions en matière de protection des données dès la conception de leurs systèmes et limitation des volumes de données à traiter au strict minimum) et à opter pour un paramétrage par défaut aussi respectueux que possible de la protection des données;
- l'analyse d'impact relative à la protection des données: cet instrument qui a fait ses preuves oblige les responsables du traitement à documenter en amont les risques élevés liés au traitement, à prendre, le cas échéant, les mesures qui s'imposent et, selon le résultat, à consulter le préposé fédéral à la protection des données et à la transparence (PFPDT), qui pourra proposer des mesures supplémentaires pour atténuer les risques constatés;
- de nouvelles prescriptions concernant le profilage et les décisions individuelles automatisées: ces deux formes de traitement ont gagné en importance à l'ère des *big data* et sont autorisées, mais soumises à des exigences plus strictes que d'autres formes en raison du risque qu'elles représentent pour les droits de la personnalité;
- le renforcement de la surveillance: le PFPDT pourra non seulement formuler des recommandations mais aussi prendre des décisions;
- le durcissement des dispositions pénales: le Conseil fédéral a allongé la liste des infractions prévues par la LPD et porté de 10 000 à 250 000 francs l'amende maximale encourue.

L'ensemble des nouvelles mesures contenues dans le P-LPD vise notamment à rapprocher la législation suisse en matière de protection des données du RGPD et à la rendre compatible avec la Convention 108 révisée, qui a été adoptée fin mai 2018. Mais contrairement au RGPD, le P-LPD ne prévoit pas de droit à la portabilité des données. Le système de sanction proposé diffère aussi sensiblement de celui du RGPD: les amendes sont nettement moins élevées, et le P-LPD ne prévoit pas de sanctions administratives. Le Conseil fédéral donne la préférence au système existant, ce qui fait que les tribunaux pénaux ordinaires restent compétents. Autre différence: le P-LPD n'interdit pas de lier la conclusion d'un contrat à un consentement au traitement de données non nécessaires à l'exécution du contrat. Le P-LPD est en cours d'examen au Parlement.

Bon nombre des mesures prévues par le P-LPD n'ont rien de foncièrement nouveau. L'analyse d'impact des risques ou le principe de la protection de la vie privée par défaut sont aujourd'hui appliqués dans tous les projets de traitement de données numériques d'envergure. De ce point de vue, la révision consiste à donner une forme légale à des éléments de bonne pratique et à combler des lacunes.

Il faut poursuivre et intensifier les mesures de bonne pratique. Les autorités de surveillance de la protection des données ont un rôle majeur à jouer à cet égard: elles tâchent de déterminer si les technologies favorables à la protection des données s'imposent

en pratique malgré l'absence d'harmonisation des législations au niveau international, et si oui comment, et œuvrent pour que les pratiques conviviales pour l'utilisateur, tel le fait de renvoyer par un lien à des éléments importants des conditions générales de vente (CGV), se généralisent en vue de constituer une norme.

En tant qu'autorité de surveillance au niveau fédéral, le PFPDT doit garantir l'accompagnement des grands projets numériques par une combinaison de conseil et de surveillance, afin de répondre aux besoins de la société et de l'économie. Malgré l'augmentation du nombre de ces projets et de la demande de prestations de conseil, il doit asseoir la crédibilité de sa compétence et assurer une densité de contrôle suffisante.

5.3.1.5 Enjeux de la révision de la LPD et de sa future mise en œuvre

Le P-LPD a notamment pour but de rapprocher autant que nécessaire le droit suisse de la protection des données du RGPD afin que l'UE maintienne à l'égard de la Suisse sa décision constatant le caractère adéquat du niveau de protection. Une révocation de cette décision aurait un impact très négatif pour la Suisse dans ses relations économiques avec l'UE, car elle interdirait la communication à la Suisse de données personnelles provenant de l'UE sauf garanties de protection supplémentaires ou dérogation spéciale.

L'entrée en vigueur du RGPD a établi des différences évidentes entre les compétences et les obligations administratives des autorités de contrôle (terme de l'UE pour «autorités de surveillance») de la protection des données des États membres de l'UE, qui ont été dotées de ressources humaines supplémentaires et de compétences décisionnelles, et celles des autorités de protection des données de la Suisse. Un principe du RGPD non applicable à la Suisse veut que pour les échanges de données transfrontaliers, les entreprises des États membres de l'UE aient pour unique interlocuteur l'autorité de surveillance de leur pays (principe du guichet unique). La Suisse doit établir la sécurité juridique sur ce point sans tarder, en menant à bien la révision totale de la LPD au plus vite et en entamant avec l'UE des négociations sur la délimitation des responsabilités territoriales et sur la coopération des autorités de surveillance de la protection des données.

Qu'est-ce qu'une mise en œuvre correcte ou suffisante au regard des nouveaux principes réglementés dans le P-LPD (finalité ou analyse d'impact des risques, par ex.)? La protection de la vie privée par défaut impose, par exemple, un paramétrage de base respectueux de la protection des données afin que la sphère privée de l'intéressé soit respectée. Seules les données indispensables au processus de traitement ou au fonctionnement du système peuvent être collectées, ce qui va dans le sens d'une limitation des données au strict minimum. Ce principe, qui paraît à première vue logique, simple et abstrait, est souvent difficile à mettre en pratique car la frontière entre les fonctions principales et accessoires d'un service n'est pas toujours claire, et bien souvent, la qualité et l'étendue d'une fonction dépendent directement de la densité des données concernant l'utilisateur. Par densité des données, on entend leur catégorie (sexe, âge, positionnement, etc.), leur durée de conservation et le caractère continu de leur saisie. S'il est facile de définir clairement les catégories de données absolument nécessaires pour une fonction spécifique (l'âge mais non le sexe, par ex.), définir le minimum de données nécessaire concernant la durée de conservation et l'exhaustivité de la saisie peut se révéler de plus en plus difficile. La qualité des dispositifs d'auto-mesure dans le domaine de la santé, par exemple, dépend de celle de la saisie des données. Il n'en faut pas moins garantir la transparence vis-à-vis de l'utilisateur. Vu la complexité du

sujet, il importe que l'élaboration des nouveaux modèles d'affaires numériques et de leurs infrastructures se fasse en concertation avec la protection des données au sein de l'entreprise.

Il faudra que les autorités de surveillance et la justice règlent un certain nombre de cas pour lever les ambiguïtés au fur et à mesure. Le recours à la justice est une pratique courante et efficace mais parfois fastidieuse. Tant qu'aucune décision n'est entrée en force, les entreprises concernées restent dans le flou quant à la pertinence de leur traitement de données. L'espace juridique européen offre à cet égard un exemple intéressant: le niveau de protection des données y est largement homogène car le RGPD ne laisse aux législateurs nationaux qu'une marge de manœuvre réduite.

Vu le manque de connaissances des personnes concernées et les faibles ressources de contrôle des autorités de protection des données, le groupe d'experts considère que la révision de la LPD a peu de chances de produire l'effet protecteur escompté et creusera au contraire un fossé entre les exigences en la matière et la réalité numérique. Par ailleurs, les lourdes sanctions prévues par le RGPD semblent inciter les responsables du traitement des données et les personnes concernées à prendre beaucoup plus au sérieux la protection des données.

5.3.1.6 Analyse des *big data*: défis en matière de protection des données

L'analyse des *big data* vise à cerner le comportement et l'état d'individus et de groupes d'utilisateurs. Le progrès technique permet l'exploitation rapide et différenciée de données non structurées telles que courriels, données audio et vidéo et documents numériques, mais il complique la classification juridique entre données personnelles et données non personnelles. Le traitement de données personnelles anonymisées et de données techniques qu'il est possible d'attribuer, de personnaliser ou de ré-identifier sans gros efforts fait des *big data* un défi grandissant en matière de protection des données.

Lorsqu'on parvient à rompre le lien entre données et personnes en recourant à l'anonymisation ou à une pseudonymisation suffisante aux yeux de la loi, on dispose de données techniques dont le traitement n'est pas soumis à la législation sur la protection des données tant que ce lien n'est pas restauré. L'anonymisation consiste à supprimer le lien entre informations différentielles et personnes par la randomisation ou la généralisation. Des travaux de recherche récents (sur le k-anonymat, la l-diversité ou la confidentialité différentielle) de même que l'expérience montrent cependant que l'anonymisation d'un lot de données n'est vraiment irréversible que si celles-ci sont largement vidées des informations qu'elles contiennent. Il faut donc s'attendre à ce que les techniques d'anonymisation actuelles perdent peu à peu leur fiabilité et qu'il faille définir de nouvelles normes techniques pour garantir la protection de la personnalité. Le recours croissant au k-anonymat, à la l-diversité ou à la confidentialité différentielle va de pair avec la perte d'informations spécifiques. S'agissant de la confidentialité différentielle, l'ajout de bruit rend impossible toute évaluation autre que statistique. Cette exigence de sécurité réduit fortement la possibilité d'effectuer des analyses créatrices de valeur dans le domaine du profilage.

Le progrès technique et la masse de données contextuelles disponible permettent une ré-identification lorsque l'anonymisation n'est pas irréversible. Mais comme il se peut qu'une anonymisation totale restreigne le potentiel de l'analyse des *big data*, le recours à cette analyse suppose d'accorder à l'analyse d'impact des risques toute l'importance qu'elle mérite.

La LPD ne s'applique pas aux données personnelles anonymisées. Mais le P-LPD (art. 17) oblige le responsable du traitement à informer la personne concernée s'il a collecté des données ré-identifiées, sauf si (art. 18, al. 2) l'information est impossible à donner (let. a) ou si elle nécessite des efforts disproportionnés (let. b), ce qui est le cas, par exemple, lorsqu'un très grand nombre de personnes sont concernées. Le message concernant le P-LPD précise toutefois que cette exception doit être interprétée de manière restrictive. Le responsable du traitement doit déployer tous les efforts qu'on est en droit d'attendre de lui dans le cas d'espèce pour remplir son devoir d'information. Cette obligation accroît sa tâche dans des proportions imprévisibles lorsque l'origine des informations et l'exploitabilité économique des données sont incertaines. Illustration: imaginons qu'un responsable du traitement récupère, en vue d'une nouvelle étude, des génomes décodés présentant une empreinte génétique claire mais que cette liste ne contienne aucune donnée permettant d'identifier ou de contacter les personnes concernées. Il aura du mal à remplir son devoir d'information vis-à-vis de ces personnes.

Par ailleurs, le principe de la finalité inscrit dans la LPD suppose de recueillir le consentement de la personne concernée lorsque le traitement des données dans le cadre de l'analyse des *big data* entraîne un changement de finalité (cas sans doute fréquent). Or il doit être difficile, pour le responsable du traitement, de définir clairement la finalité de celui-ci pour tout l'historique d'un ensemble de données. Le consentement de la personne concernée est pourtant obligatoire, sauf dans les cas (rares au demeurant) où le traitement des données (portant atteinte à la personnalité) se fonde sur d'autres motifs tels qu'une base légale ou un intérêt public ou privé prépondérant. L'analyste de *big data* devra donc soit prendre d'importantes mesures afin de réduire les risques au minimum, soit remettre en question le modèle d'affaires envisagé. L'anonymisation échoue quand le modèle d'affaires privilégie le profilage au détriment de l'exploitation statistique de données. Or le profilage va sans doute gagner en importance dans l'exploitation économique des données personnelles et para-personnelles.

Dans le contexte des *big data*, entre enrichissement d'informations, anonymisation et ré-identification, les données passant d'une plateforme de traitement à une autre peuvent alternativement acquérir et reperdre la qualité de «donnée personnelle» (parfois même particulièrement sensible). Là aussi, il n'y a pas d'autre solution que de prendre des mesures techniques (parfois très complexes) afin de garantir le respect des principes de la protection des données.

Le principe de la réduction des données au strict minimum peut aussi se retrouver en opposition avec les pratiques liées aux *big data*, qui visent à collecter et à analyser un maximum de données. Le caractère préventif du droit de la protection des données en vigueur implique que la collecte et la conservation de données personnelles sont des activités risquées qu'il convient de restreindre en conséquence. Ce principe a été intégré au P-LPD (protection de la vie privée dès la conception et par défaut) et fait dès lors partie intégrante des exigences techniques liées à la protection des données.

Certes, le droit de la protection des données prévoit, outre la finalité et le consentement, la possibilité pour l'individu de ne pas participer à la collecte de données. Mais l'exercice de ce droit peut exposer l'intéressé à des conséquences négatives s'agissant, par exemple, de l'évaluation de sa solvabilité, de l'examen de sa candidature à un poste ou du calcul de sa prime pour les prestations d'assurance-maladie complémentaires: un assuré refusant de porter un dispositif d'auto-mesure ne bénéficiera pas de certaines réductions, un candidat absent de tout réseau professionnel risque d'être considéré comme manquant de transparence et donc d'intérêt, un propriétaire qui

exige le floutage de sa maison sur Google Earth risque d'attirer l'attention de cambrioleurs potentiels.

On le voit: les nouveaux procédés de traitement des données, en particulier l'analyse des *big data*, peuvent être en contradiction avec les principes de protection des données. Seule une protection efficace permettra de renforcer la confiance des utilisateurs dans le monde numérique et de les inciter à partager leurs données. D'où cette question: la conception moderne de la protection des données permettra-t-elle de concilier respect du droit et conditions favorables à l'analyse des *big data* ou mènera-t-elle dans une impasse?

5.3.1.7 Évolution de la protection des données à moyen et long termes

Face à la révolution et à l'évolution technologiques, à la globalisation du traitement de données et, bien sûr, à la multiplicité des données non structurées, quel est l'avenir de la protection de la sphère privée et de l'autodétermination en matière d'information?

Les instruments de la protection moderne des données énoncés plus haut et qui figurent dans le P-LPD devraient se montrer efficaces, du moins à court et moyen termes, sous réserve que le PFPDT dispose des moyens nécessaires en matière de conseil, de contrôle et d'exécution. Deux paramètres seront décisifs à cet égard: la mise en œuvre rapide et sans retard de la révision de la LPD, et l'augmentation des ressources évoquée par le Conseil fédéral.

À moyen et long termes, différentes évolutions sont possibles, ce qui a incité le groupe d'experts à élaborer deux scénarios pour l'avenir de la protection des données.

Scénario I: les principes actuels de la protection des données sont adaptés à l'avenir

Le premier scénario suppose que les principes neutres au point de vue technologique de la LPD révisée resteront applicables à long terme et permettront d'atteindre les objectifs clés de la protection des données:

- Ces principes matériels ne seront pas remis en cause par la réalité des *big data* et de l'intelligence artificielle et permettront une mise en œuvre souple et efficace au quotidien.
- L'applicabilité et la réussite du droit de la protection des données reposent sur le modèle éprouvé d'une réglementation générale et abstraite suffisamment ouverte, dont la large marge de manœuvre renforce les atouts et les possibilités des *big data* au lieu de les restreindre, en tenant compte des besoins du consommateur et de l'utilisateur en matière de sécurité et de confiance.
- La recherche progressive de solutions et une jurisprudence constante résoudront au cours des années à venir les questions de mise en œuvre qui doivent l'être, concernant par exemple le principe de la protection de la vie privée dès la conception ou le «droit à l'oubli», et renforceront la sécurité juridique.

En résumé, selon ce scénario, la protection des données est compatible avec l'utilisation des *big data*. La protection des données et la jurisprudence produisent un rapport équilibré entre une protection efficace de la sphère privée et de l'autodétermination en matière d'information et les conditions générales d'un traitement de données moderne englobant les méthodes des *big data*.

Scénario II: les principes actuels de la protection des données ne sont pas totalement adaptés à l'avenir

Les risques qui pèsent sur le respect des principes actuels de la protection des données sont accentués par quatre facteurs:

- La mise en œuvre pratique des principes de base, neutres au point de vue technologique, de la protection des données se heurte à des difficultés non négligeables s'agissant des nouvelles techniques de traitement des données, en particulier l'analyse des *big data*.
- La mise en œuvre des nouveaux principes de la protection des données ne règle pas assez vite, du point de vue actuel, les incertitudes qui affectent les responsables du traitement des données et les personnes concernées, comme on l'a vu récemment avec l'exemple du RGPD.
- La majorité des utilisateurs, tout en soulignant l'importance de la sphère privée et de l'autodétermination en matière d'information, renoncent fréquemment au quotidien à assumer leurs responsabilités quant au respect de ces droits.
- Dans le B2C, le marché est actuellement dominé surtout par des entreprises qui développent leurs modèles d'affaires dans un système juridique où la protection des données n'a pas la même importance qu'en Europe, et où la protection de l'individu contre l'utilisation frauduleuse des données est assurée par d'autres moyens.

Conclusion des scénarios I et II

La révision de la LPD doit aboutir et passer au stade de la mise en œuvre au plus vite, car seules les adaptations à la réalité numérique qui sont proposées permettront de vérifier l'efficacité de l'approche traditionnelle en matière de protection des données dans le contexte du traitement de données moderne. Pour optimiste qu'il soit, le scénario I n'est pas exempt de difficultés: les nouvelles exigences techniques définies dans le P-LPD causeront des incertitudes chez les responsables du traitement des données, mais aussi chez les utilisateurs.

Les derniers incidents liés aux réseaux sociaux montrent que les risques évoqués dans le scénario II sont tout à fait réels et gagneront encore en gravité à l'avenir. Les défis techniques liés à la protection des données sont tiraillés entre le coût d'une mise en œuvre stricte de la LPD, les possibilités qu'offre le traitement de données moderne au moyen des *big data* et les effets négatifs d'une protection laxiste de la sphère privée. Les utilisateurs, eux, devront faire un choix entre la protection de leur sphère privée d'une part et le confort numérique, les fonctionnalités et la participation aux réseaux sociaux d'autre part.

Face à ce constat, le groupe d'experts a estimé nécessaire de formuler des mesures complémentaires de protection des données de même que d'autres solutions pour protéger la sphère privée et l'autodétermination en matière d'information, et de les soumettre au débat.

5.3.1.8 Mesures complémentaires de protection des données et autres solutions

La décision de l'UE constatant le caractère adéquat du niveau de protection, évoquée plus haut, influe aussi sur la marge de manœuvre de la Suisse s'agissant de la conception du droit futur de la protection des données. Ce qui ne doit pas empêcher la réflexion suivante: les pistes de solution telles que l'harmonisation de la protection des données à l'échelle de la Suisse, le principe de la responsabilité, l'approche *smart data*, le principe du partage des richesses et l'historique des flux de données s'inscrivent toutes dans le cadre traditionnel de la protection des données. Les autres mesures telles que l'assouplissement de la finalité ou les mécanismes juridiques situés en aval de la protection des données et visant à protéger la personne concernée du détournement de ses données vont au-delà de ce cadre.

Mesures complémentaires s'inscrivant dans le cadre traditionnel de la protection des données:

a) **Droits fondamentaux fonctionnels**

On peut d'ores et déjà affirmer que les principes constitutionnels relatifs à la sphère privée (art. 10 et 13 Cst.) ne doivent pas être considérés comme de simples droits de défense contre l'État mais comme des droits fondamentaux fonctionnels. La Cour constitutionnelle fédérale allemande (*Bundesverfassungsgericht*) a jugé en 2008 que les fournisseurs de systèmes et d'infrastructures doivent garantir la confidentialité des données personnelles, ce qui implique l'adoption de mesures techniques et de certains principes de traitement des données. Il n'y a pas lieu de modifier la Constitution pour l'instant, mais le groupe d'experts serait favorable à ce que la jurisprudence établisse peu à peu l'autodétermination en matière d'information comme un droit fondamental fonctionnel, comme c'est le cas en Allemagne.

b) Principe de la responsabilité

Le principe de la responsabilité, dont de nombreux éléments ont été intégrés au P-LPD, concerne au premier chef le responsable du traitement des données. Une entreprise assume ses responsabilités lorsqu'elle pratique un traitement transparent et qu'elle respecte en la matière une norme dont les éléments clés sont, outre la transparence, une démarche fondée sur les risques et des mesures de sécurité de l'information. L'entreprise doit aussi fournir aux intéressés une vue d'ensemble simple et claire des données les concernant. L'instauration de contrôles (par un PFPDT doté de moyens appropriés, par ex.) contribuerait largement à imposer une telle norme. Il faudrait par ailleurs envisager régulièrement d'autres mesures de bonnes pratiques telles que la soumission volontaire au principe des *smart data* (cf. Approche *smart data* ci-après). La norme de responsabilité pourrait fournir la base de la certification prévue dans le P-LPD, ce qui équivaudrait à décerner à une entreprise un label de qualité pour son traitement de données. Il faudrait aussi prévoir la possibilité, pour les entreprises, de procéder à une auto-certification, ce qui pourrait renforcer leur auto-régulation et leur sens des responsabilités. Quoi qu'il en soit, les principes d'une responsabilité élargie devront pouvoir s'appliquer tant à la régulation qu'au système de certification ou d'auto-certification.

c) Bac à sable (banc d'essai sûr)

Le recours à un bac à sable (*sandboxing*) a-t-il un sens pour le traitement de données non structurées dans le contexte de nouveaux modèles d'affaires? La question mérite qu'on l'approfondisse. Ce banc d'essai suivi étroitement par les autorités de surveillance à l'aide d'un outil spécifique permettrait, en limitant et en inventoriant le volume

des données, d'assouplir la finalité et de demander aux personnes concernées un consentement général. La complexité des *big data* s'en trouverait nettement réduite. Les formats admis et la provenance des données non structurées seraient contrôlés. Outre la structuration du pool de données, il faudrait piloter l'accès à ce pool (par un lien) du programme à examiner, et déterminer les paramètres que celui-ci recherche et utilise. Le banc d'essai permettrait aussi de voir de quelle manière et quand a lieu la ré-identification de données anonymisées.

Malgré un volume de données réduit et un groupe de personnes contrôlé, il n'est pas impossible que des personnes extérieures au banc d'essai soient soudain concernées. On peut par exemple imaginer que le fournisseur de données anonymisé d'un génome soit ré-identifié dans le bac à sable, que ce génome révèle une maladie héréditaire, et que les enfants adultes de l'intéressé soient intégrés à l'essai sans qu'on leur ait demandé leur consentement.

Compte tenu de ces éléments, le banc d'essai devrait répondre à deux impératifs: s'il faut mettre l'accent sur les évaluations statistiques, l'outil vérifierait si les statistiques élaborées et éventuellement destinées à être publiées permettent de retrouver des données personnelles (contrôle de divulgation statistique). Si tel est le cas, il procéderait à une analyse d'impact des risques nettement améliorée, ce qui irait dans le sens d'une protection des données fondée sur les risques.

Il faudrait de toute façon vérifier que ces outils sont compatibles avec la protection des données, le principe de la finalité risquant en particulier de poser problème. Ces outils sont par ailleurs si sensibles qu'il faudrait les inscrire dans un cadre détaillé. Ils pourraient être élaborés et mis à disposition par les autorités de surveillance de la protection des données, notamment, en collaboration avec la recherche et l'économie (partenariat public-privé).

d) Approche *smart data*

Certaines exigences du droit de la protection des données, en particulier la restriction des données au strict minimum, sont incompatibles avec l'analyse des *big data*, qui brasse des volumes importants de données personnelles. La solution réside peut-être dans l'approche *smart data*, qui vise à faire le maximum avec un minimum de données sélectionnées pour leur pertinence. Cela dit, le processus de recherche de corrélations propre à l'analyse des *big data* contredit précisément l'idée selon laquelle un résultat inconnu au départ pourra être obtenu au moyen d'un minimum de données, idée qui conduit plutôt au test de causalité et à la vérification des thèses avec un volume de données limité et des sondages.

e) Principe du partage des richesses

Le principe du partage des richesses s'intéresse à l'aspect économique de l'exploitation de données personnelles. Il satisfait le besoin de participation économique des utilisateurs et doit par conséquent être considéré comme une mesure de promotion de l'autodétermination en matière d'information. La portabilité des données étant essentielle à cet égard, le principe est exposé plus en détail au ch. 7.1.5.2.

f) Historique des données (cycle de vie)

L'un des grands défis que doit relever le droit de la protection des données réside dans l'absence de traçabilité des informations qui se composent d'au moins deux données (cycle de vie des données). Alors que jadis, une information était indissociable des données la concernant, les méthodes de traitement actuelles permettent une transformation dynamique des données, qu'elles soient techniques, personnelles, anonymisées ou ré-identifiées. Autrement dit, la catégorie juridique d'une donnée peut changer.

Par ailleurs, le traitement des données a de moins en moins lieu à l'endroit de leur obtention, ce qui ne semble pas, à première vue, affecter l'applicabilité de la protection des données. Juridiquement, la responsabilité incombe au responsable du traitement qui contrevient aux principes du droit de la protection des données en manipulant des données personnelles à un moment précis. Mais les historiques de données complexes nuisent à la transparence et rendent plus difficile le consentement, tout en relativisant le niveau d'application. C'est pourquoi il serait intéressant, techniquement, de joindre à chaque information figurant dans l'ensemble de données son historique. La traçabilité serait ainsi assurée et en cas d'utilisation frauduleuse de données (atteinte à la réputation, par ex.), on pourrait remonter jusqu'au responsable afin de lui faire rendre des comptes. Il ne s'agit pas là d'une initiative isolée mais d'un moyen supplémentaire de renforcer le principe de la responsabilité. Précisons que les concepts techniques correspondants n'en sont encore qu'au stade de la théorie et très éloignés d'une éventuelle mise en œuvre. Le moment venu, cela pourrait prendre la forme d'une blockchain haute performance.

g) Autres approches en dehors de la LPD

Compte tenu des réflexions qui précèdent, il convient d'envisager des modèles allant au-delà de l'acception courante de la protection des données (préservation de la sphère privée et protection contre l'usage frauduleux de données personnelles).

On devrait par exemple s'intéresser aux mécanismes juridiques situés en aval de la protection des données dans les situations où le traitement et l'utilisation des données entraînent abus et discrimination, ce qui peut être le cas dans les analyses de solvabilité, les assurances, la gestion du personnel, les procédures de recrutement ou encore l'octroi ou non de services ou d'informations. Les discriminations de ce genre sont particulièrement lourdes quand la puissance du fournisseur exclut toute solution de rechange, quand une marchandise ou un service sont proposés de manière confidentielle, quand il est question de produits ou de services se rapportant à des besoins courants, ou quand le fournisseur ne peut pas indiquer de motifs objectifs. Cette nouvelle manière de considérer les choses, en s'intéressant à l'utilisation des données plutôt qu'à leur collecte, offrirait aussi des solutions potentielles quand le devoir d'information ne peut être rempli en raison d'une décision individuelle automatisée.

La réglementation de la différenciation des prix dans la LCD et dans l'ordonnance du 11 décembre 1978 sur l'indication des prix (OIP, cf. ch. 5.3.2.5) va déjà dans ce sens en s'attaquant à la discrimination par les prix. Le problème se complique lorsque les données ont empêché «abusivement» l'octroi de services ou d'informations.

Dans ce cas, les effets sont particulièrement négatifs lorsque le service en question est une condition de l'obtention de certains droits, comme la conclusion d'une assurance-responsabilité civile pour véhicules automobiles pour la mise en circulation d'une voiture. L'obligation de contracter apporte une solution à ce problème, mais elle ne peut s'appliquer qu'avec une grande retenue, en particulier dans le domaine du droit privé: l'utilisateur ne doit avoir aucun autre moyen raisonnable à sa disposition.

Il faut par conséquent déterminer si de tels principes visant à limiter les abus peuvent porter leurs fruits, quels sont les domaines juridiques où leur application aurait un sens et quelles seraient les adaptations nécessaires.

Recommandation:

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.

5.3.1.9 Importance du scoring et du profilage dans les processus limitant la possibilité de libre consentement

En matière de recrutement, le droit du travail autorise l'employeur à traiter, concernant un candidat, uniquement les informations dont il a besoin pour s'assurer que celui-ci est apte à remplir son emploi (principe de la proportionnalité, art. 328*b* CO). Tout comme la vérification et la communication de références, le suivi, le profilage et le scoring doivent respecter le droit du travail et les règles de la bonne foi. Étant donné que ce type de traitement porte sur des traits de personnalité importants du candidat (profilage), il nécessite le consentement préalable et explicite de la personne concernée (art. 4, al. 5, LPD). Ce consentement est cependant soumis à caution dans le monde du travail, car les procédures de recrutement et les rapports de travail n'offrent généralement pas au candidat la possibilité d'exprimer sa volonté librement, alors qu'il s'agit là d'une condition de la validité du consentement.

Les candidatures à une place de formation ou de formation continue ne sont pas soumises au droit du travail mais elles posent néanmoins la question du consentement. Elles impliquent aussi le respect du droit de la protection des données, en particulier les principes de la proportionnalité, de la légalité et de la bonne foi.

Lors de la collecte de données sensibles, il faut informer la personne concernée en vertu de l'art. 14 LPD, y compris si la collecte est effectuée auprès d'un tiers, par exemple une agence de recrutement ou un gros service du personnel.

Dans ce domaine comme dans celui de la santé, il faut développer les lois spéciales correspondantes afin de les harmoniser avec le droit de la protection des données.

5.3.1.10 Enjeux de droit pénal

L'atout principal des applications pourrait bien devenir un risque incontrôlable, car il n'est plus possible de lier la discrétion et la confidentialité à une personne au sens de «collaborateur de confiance». Les questions techniques de protection des données et, dans une égale mesure, la protection des secrets, sont essentielles à cet égard. Vu les proportions que prennent l'éventail des tâches et la «responsabilité» de ces applications, on peut se demander si les dispositions correspondantes du droit pénal (en particulier les art. 162 et 321 du code pénal [CP]) représentent et définissent de manière adéquate la responsabilité des fournisseurs de ces services.

Recommandation:

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.).

5.3.1.11 Développement de la protection des données et de la sécurité informatique

Le délai de transition de deux ans concernant le RGPD a expiré le 25 mai 2018. Depuis cette date, non seulement les habitants de la Suisse peuvent faire valoir les droits de protection accrus que leur confère le RGPD vis-à-vis des responsables du traitement de données dans les États de l'UE, mais le RGPD s'applique aussi aux entreprises suisses qui pratiquent le traitement automatisé, à des fins de profilage, de données personnelles de personnes vivant dans l'UE. Ces entreprises doivent par conséquent prendre les mesures organisationnelles, techniques et juridiques qui s'imposent pour se mettre en conformité avec le RGPD. Compte tenu de l'importance que l'économie accorde à la protection des données, importance que l'instauration du RGPD, avec les possibilités de sanction considérables qu'il prévoit, et la révision de la législation suisse sur la protection des données n'ont fait qu'accroître, le PFPDT, unique autorité de surveillance compétente pour l'économie privée, a fort à faire: rien que la demande de prestations de conseil et d'accompagnement de projets en rapport avec le traitement de données numériques ne cesse d'augmenter. Bon nombre de mesures organisationnelles et techniques telles que l'analyse d'impact des risques, le droit à la suppression ou à la protection des données par la technologie et par un paramétrage par défaut respectueux des données ont été intégrées au RGPD, accédant ainsi à un statut légal formel qui a considérablement accru l'importance de ces instruments de la sécurité informatique. Les obligations en matière de prévention ont été fortement développées dans la foulée, notamment en ce qui concerne la documentation des activités de traitement des données, l'information des personnes concernées ou l'obligation de notifier les incidents de sécurité et ceux affectant la protection des données. Du fait de l'assujettissement de nombreuses entreprises suisses au RGPD, ces instruments font déjà partie de l'univers numérique de la Suisse et seront renforcés, au moins en partie, par la révision de la législation suisse sur la protection des données, qui les imposera aussi aux entreprises actives exclusivement sur le marché suisse, ce qui augmentera d'autant les activités de conseil et de surveillance du PFPDT.

Les possibilités offertes par le traitement de données moderne avec l'analyse des *big data*, l'intelligence artificielle et la cryptographie peuvent aussi présenter un risque d'origine technique pour la protection des données. Les disciplines telles que la gestion des risques informatiques, la sécurité fondée sur le matériel, l'anonymisation (en particulier la confidentialité différentielle), les solutions en nuage et la cryptographie (essentiellement les chiffrements homomorphes) imposeront de plus en plus aux autorités de surveillance un profil interdisciplinaire, seul moyen pour elles d'avoir une chance de relever les défis techniques et juridiques des grands chantiers du numérique.

Alors que le législateur fédéral n'en est encore qu'au stade de la révision de la LPD, qui date de 1993, les autorités de protection des données des États membres de l'UE, dotées de moyens supplémentaires et de pouvoirs de décision et de sanction, ont entrepris de regrouper leurs activités, y compris vis-à-vis d'entreprises de pays tiers. Les autorités de protection des données de la Confédération et des cantons doivent donc,

en attendant la nouvelle LPD, développer, avec des pouvoirs et des ressources modestes en comparaison, une activité de surveillance qui soit à la fois perceptible et crédible en Suisse comme à l'étranger. Il s'agit pour elles d'une période de transition difficile. Le PFPDT dispose, pour la protection des données, de 24 postes, un effectif inchangé depuis 2005, et certains de ses homologues cantonaux sont encore moins bien lotis proportionnellement.

La multitude des cas de perte de données, qui affectent aussi la réalité numérique en Suisse, a considérablement renforcé l'importance de la protection des données aux yeux de l'opinion[9]. Les autorités de surveillance fédérale et cantonales sont ainsi confrontées à des attentes auxquelles ni les bases légales ni leurs ressources, qui ont été définies au siècle dernier, ne leur permettent d'apporter des réponses crédibles. Pour accroître leur efficacité, il faut non seulement renforcer les effectifs et encourager la formation, mais aussi créer des formes de coopération efficientes (centres de compétence, par ex.).

Recommandations:

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.
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.).

5.3.1.12 Normalisation et certification dans la protection des données

Dans le domaine de la protection des données, les appareils cyberphysiques recèlent un potentiel de risque important pour la personnalité. C'est le cas des capteurs utilisés en informatique médicale (applications sur smartphone, mais aussi systèmes de contrôle industriels), des compteurs intelligents, des dispositifs de surveillance vidéo des bébés, des poupées connectées, bref de tous les appareils qui collectent et traitent des données pouvant se rapporter à des personnes. Dans le cadre de la LPD en vigueur, les produits ne font l'objet d'aucune certification, contrairement aux organisations et aux processus. La nouvelle LPD devra combler cette lacune en exigeant, sur le plan technique, que les produits intègrent la protection de la vie privée dès la conception et par défaut de même que la sécurité dès la conception.

Il convient d'envisager, sous l'angle de la protection des données et du RGPD, un principe de normalisation et de certification des produits qui intègre la protection de la vie privée et certains éléments de sécurité dès la conception. Par ailleurs, il faudrait créer les bases légales de l'autorisation de mise sur le marché correspondante. Ces exigences revêtent une importance particulière s'agissant des appareils de l'IdO, dont la diversité implique que la pertinence de leur certification et de leur éventuelle exclusion du marché fasse l'objet d'un examen approfondi.

[9] Cf. entre autres le rapport d'activités 2017/2018 du PFPDT, pp. 6 s.

Recommandation:

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.

5.3.2 Protection des consommateurs

5.3.2.1 Introduction

Les rapports entre acteurs du B2C mettent en évidence le rôle de consommateur de l'utilisateur, ce qui pose la question de la protection des consommateurs. Le B2C comprend des offres provenant tant du privé que d'entreprises liées à la Confédération (CFF, Poste, Swisscom). Abstraction faite de certaines réglementations commerciales et de prescriptions édictées par les cantons en matière de concessions, il n'existe aucune disposition réglementant la qualité en matière de protection des consommateurs. On part du principe que la concurrence assure le maintien du niveau de qualité requis. En Suisse, la protection des consommateurs repose en grande partie sur la transparence des prix et sur la protection contre les abus et la tromperie. Le groupe d'experts ne voit pas actuellement la nécessité d'un changement général de paradigme. Ces principes semblent aussi fonctionner dans la transformation numérique. Des modifications et une meilleure application du droit en vigueur s'imposent toutefois s'agissant des conditions générales de vente (ch. 5.3.2.2), du droit de révocation (ch. 5.3.2.3), du droit des contrats numériques (ch. 5.3.2.4), de la différenciation des prix (ch. 5.3.2.5) et du règlement en ligne des litiges (ch. 5.3.2.6).

Ce qui importe pour les consommateurs s'agissant de l'application du droit dans un marché mondialisé, c'est la question du for et l'instauration du principe du lieu où se tient le marché pour les fournisseurs non domiciliés en Suisse. Le choix d'un domicile de notification, que le Parlement a réclamé à de nombreuses reprises, mérite d'être envisagé sérieusement quoiqu'il paraisse difficile, à première vue, de l'imposer aux cyber-entreprises étrangères: exclure du marché, en guise de sanction, des réseaux sociaux qui le dominent risque surtout d'entraîner un large rejet de la part des utilisateurs concernés et donc de causer de sérieux dégâts plutôt que de produire le résultat escompté. Malgré toutes les critiques dont elle est l'objet, la loi allemande de mise en œuvre du droit sur les réseaux sociaux (*Netzwerkdurchsetzungsgesetz* du 30 juin 2017) a déjà montré que la simple mise en place d'un contexte faisant peser un risque sur la réputation produit déjà des effets. L'obligation légale, pour les réseaux sociaux, de nommer un interlocuteur de référence en Allemagne et à l'étranger donne aux personnes lésées la possibilité de poursuivre une entité concrète et identifiable.

5.3.2.2 Conditions de vente en ligne

Les conditions de vente en ligne sont des conditions générales de vente (CGV) qui ne font partie intégrante du contrat que si les deux parties (y compris, donc, l'acquéreur) les approuvent. Les CGV gagnant en importance dans les modèles d'affaires numériques, celles qui privilégient le fournisseur se révèlent problématiques.

La Suisse n'a pas repris à son compte la directive 93/13/CEE concernant les clauses abusives dans les contrats conclus avec les consommateurs, se contentant, face à

l'opposition des milieux économiques, de la prescription de contrôle relativement faible de l'art. 8 LCD. Elle ne prévoit même aucune règle contractuelle spéciale pour les CGV en ligne. La doctrine a développé un certain nombre de critères à respecter pour que les CGV en ligne puissent devenir un élément du contrat, notamment la lisibilité, la transparence et le caractère raisonnable, mais il n'existe aucune jurisprudence en la matière et ces critères sont peu respectés dans la réalité.

Le droit de la protection des données accorde pour sa part une grande importance à la clarté des CGV en ligne et à leur conformité avec ses dispositions. La surveillance de la protection des données exige le respect de cette exigence en vertu du principe de la transparence. Le problème tient moins à l'absence de règles juridiques qu'à l'application de ces règles, faute de moyens de conseil et de contrôle adéquats. Mais le nouveau RGPD, sans doute imité bientôt par la future LPD, durcit les exigences concernant l'adoption de CGV en ligne.

Recommandation:

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.

5.3.2.3 Droit de révocation en ligne

En Suisse, des dispositions particulières régissent le droit de révocation des consommateurs en matière de démarchage à domicile (art. 40*a* à 40*f* CO). Il est cependant communément admis que ces dispositions ne s'appliquent pas aux offres Internet ni à la conclusion de contrats électroniques en raison de la description restrictive des conditions et en particulier du fait que les parties au contrat ne sont pas physiquement présentes.

L'UE a instauré dès 2002, dans la directive 2002/65/CE concernant la commercialisation à distance de services financiers, un droit de rétractation (terme de l'UE pour «révocation») du consommateur, excepté pour les transactions irrévocables par nature. Elle entend, avec un nouveau projet de directive de décembre 2015 concernant certains aspects des contrats de ventes en ligne et de toute autre vente à distance de biens, consolider et développer les conditions générales régissant ces contrats, y compris le droit de rétractation. Cette directive devrait être adoptée au 2^{d} semestre 2018, les nouvelles propositions ne suscitant aucune opposition particulière.

En Suisse, un nouveau projet visant à instaurer un droit de révocation pour les opérations en ligne vient d'échouer. Il faudra cependant régler tôt ou tard la question des contenus numériques dans le droit des contrats.

Recommandation:

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

5.3.2.4 Droit des contrats numériques

Les nouveaux modèles d'affaires concernent le droit des contrats à bien des égards.

a) Conclusion de contrats par voie électronique

La possibilité créée par Internet, il y a plus de vingt ans déjà, de conclure des contrats par voie électronique a posé la question de la nécessité de légiférer sur ce point. Sur le plan international, la loi type de la Commission des Nations Unies pour le droit commercial international (CNUDCI) sur le commerce électronique (1996) a été complétée par la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005) que la Suisse n'a cependant pas ratifiée à ce jour. De son côté, l'UE a adopté la directive 2000/31/CE sur le commerce électronique, qui règle les principaux aspects des contrats électroniques et prévoit en particulier leur mise sur un pied d'égalité avec les contrats conventionnels de même que des dispositions de protection spécifiques concernant la conclusion des contrats. Cela a incité le DFJP à mettre en consultation, en 2001, un avant-projet de loi fédérale sur le commerce électronique contenant des dispositions analogues, mais une levée de boucliers des milieux concernés a abouti en 2005 à l'abandon définitif de ce projet.

L'expérience des vingt dernières années a montré que, hormis certaines particularités de la conclusion de contrats par voie électronique, les règles courantes du CO suffisaient à apporter des réponses appropriées, notamment aux questions de la déclaration de volonté sur le net (présence ou absence, durée de validité d'une offre, moment de la conclusion du contrat) et de la contestation des déclarations de volonté insuffisantes.

Seule la question de la forme écrite, lorsqu'elle est exigée par la loi (contrats individuels avec un consommateur ou cession, par ex.), nécessitait des mesures. Faisant suite à la directive de l'UE sur les signatures électroniques (1999/93/CE), le Conseil fédéral a adopté l'ordonnance sur les services de certification électronique, qui a ensuite été remplacée par l'ordonnance sur la signature électronique (OSCSE). Il n'y a cependant pas encore eu de reprise autonome du règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance (en vigueur depuis le 1er juillet 2016), qui a abrogé la directive 1999/93/CE. Certaines de ses dispositions pourraient cependant être adoptées en relation avec la création de l'identité électronique (e-ID).

b) Contrats et contenus numériques

Dans le domaine des contrats, l'importance du numérique s'est accrue ces dernières années, la focalisation se faisant sur les données ou les informations qui sont l'objet du contrat et représentent une certaine valeur, sans parler du recours aux nouvelles technologies telles que la blockchain.

c) Contrats intelligents

La technologie de la blockchain permet de fonder les relations contractuelles sur un algorithme connecté et auto-exécutable: au lieu de négocier le texte du contrat, on se réfère à des conventions antérieures dans un code source. On emploie souvent à cet égard le terme de contrat intelligent (*smart contract*).

Les contrats intelligents posent des problèmes juridiques que le droit des contrats traditionnel ne permet pas de régler facilement. Par exemple, l'exécution n'est possible qu'à l'intérieur de la blockchain, or un système transnational décentralisé pose la question de la compétence juridique. Certaines mesures de régulation s'imposent donc (cf. ch. 9.3.5).

d) Les données comme objets d'un contrat: contenus numériques

Les données sont l'objet de contrats depuis bien longtemps (achat d'informations, par ex.). Le numérique n'a donc pas fait naître ce type de contenu mais modifié sa qualité

et sa quantité. La transmission technique de l'objet du contrat suscite aussi des questions spécifiques (format, normalisation). Lorsque les données sont de plus en plus l'objet de contrats, le risque que la fourniture des données ne respecte pas les critères de qualité contractuels augmente, et avec lui celui que les recours pour livraison non conforme se multiplient. Le droit en vigueur est mal préparé à ces questions.

En décembre 2015, l'UE a présenté une proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique (COM[2015] 634 final). Le projet définit le terme «contenu numérique» comme l'ensemble des données produites et fournies sous forme numérique (vidéos, enregistrements audio, applications, jeux numériques et autres logiciels) et des services qui s'y rapportent. Le champ d'application de la future directive englobe par conséquent les transactions passant par les réseaux sociaux et les plateformes de commerce numériques. Malgré un certain nombre d'exceptions expressément mentionnées, la définition du contenu numérique reste très vaste.

e) Conformité des contenus numériques

Les dispositions traditionnelles du CO concernant les recours en cas d'exécution non conforme d'un contrat ne sont pas adaptées aux contenus numériques. La notion d'exécution non conforme, en particulier, ne convient que pour les prestations en nature et les services, le cas échéant. Le projet de directive de l'UE sur les contenus numériques prévoit de nouvelles dispositions concernant la conformité des contrats, et notamment un point essentiel en pratique: le contrat doit décrire précisément son contenu, ou plus exactement l'usage recherché par le client, car c'est sur ce descriptif que va se fonder l'évaluation de la conformité. Il faut donc que l'objet du contrat soit suffisamment clair pour que l'on puisse juger si son contenu numérique répond aux attentes du consommateur.

D'autres questions se posent s'agissant de l'intensité de l'«utilisation» des contenus numériques, cette utilisation n'affectant ni la qualité ni la quantité de ceux-ci (contrairement à l'utilisation de biens matériels), et du droit du client à transmettre des contenus numériques à des tiers. Où établir la limite par rapport au droit d'auteur, par exemple? Il se peut aussi que le droit de la protection des données entre en jeu lorsque les informations fournies englobent des données personnelles de tiers.

Une réglementation spécifique des recours est par ailleurs nécessaire. Si le contenu numérique est inutilisable et qu'il y a résiliation du contrat, les données doivent être restituées dans un format normalisé. Lorsque la qualité du contenu s'éloigne moins radicalement de celle annoncée dans le contrat, le client peut prétendre à une réduction du prix, mais la moindre valeur d'un contenu numérique est difficile à établir.

Au cours des derniers mois, non seulement les milieux concernés mais aussi les États membres ont vivement débattu des propositions de l'UE. Celles qui concernent la conformité des contrats et les recours suscitent des critiques car elles touchent à la compétence législative en matière de droit des contrats, qui est une prérogative des États membres. Nul ne sait par conséquent quelles propositions concrètes de la Commission européenne seront reprises dans la directive devant être approuvée au second semestre 2018.

La Suisse, nous l'avons dit, n'a adopté aucune disposition sur la conformité du contenu numérique des contrats ni sur les recours possibles. Selon l'issue des débats concernant la directive européenne, elle devra peut-être envisager de compléter le CO sur certains points.

Recommandation:

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.

5.3.2.5 Méthodes fallacieuses et dénigrantes: inutile de modifier la LCD

Le droit en vigueur dresse, à l'art. 3 LCD, une longue liste de méthodes fallacieuses et dénigrantes qui devrait suffire dans une large mesure à couvrir les nouveaux modèles d'affaires (concernant la reprise de résultats prêts à être mis sur le marché, cf. ch. 6.3.3).

5.3.2.6 Différenciation des prix: nécessité de modifier le droit de la concurrence et l'ordonnance sur l'indication des prix

Il faut examiner de plus près la question de la différenciation des prix fondée sur l'analyse de données et réfléchir à une éventuelle modification de l'ordonnance sur l'indication des prix (OIP), en particulier s'agissant de la transparence et de la publicité des mécanismes. La différenciation des prix personnalisée pose le problème de la discrimination (au regard des critères raciaux énoncés à l'art. 261bis CP, par ex.), sans compter qu'il faut respecter les principes fondamentaux du droit de la protection des données (limitation du profilage et des décisions automatisées, comme le veut le RGPD). Conformément aux art. 16 ss LCD et à l'OIP qui en découle, le prix à payer effectivement pour les marchandises offertes au consommateur doit être indiqué, et ce dans un double but: fixer clairement le prix de l'offre tous suppléments et taxes compris afin de permettre l'aboutissement correct du contrat (convergence des volontés sur les éléments clés) et permettre de comparer les prix (concurrence effective).

L'OIP suppose implicitement que les prix sont constants et identiques pour tous les clients, ce qui est de moins en moins le cas. La pratique de prix dynamiques ou personnalisés n'est pas nouvelle (prix de saison, réductions avant liquidation, rabais AVS ou étudiant, rabais de fidélité, par ex.) et correspond à la différenciation des prix selon ce que le client est prêt à payer. Du moment qu'elle ne repose pas sur une situation monopolistique, elle est le plus souvent génératrice de prospérité économique. Mais la saisie de données de plus en plus nombreuses se rapportant à des caractéristiques de plus en plus différenciées favorise le dynamisme et la personnalisation des prix à plus grande échelle, pour des offres de plus en plus nombreuses, tant en ligne qu'en magasin. De quoi contourner la fonction de l'OIP par rapport à la concurrence. Les analyses de données permettent aussi de comparer les prix plus facilement et d'une manière plus pertinente. Mieux vaut par conséquent attaquer ce problème non pas globalement dans le droit des contrats ou dans la LCD, mais au moyen de règles spécifiques en se limitant aux secteurs nécessitant une protection particulière tels que l'approvisionnement de base ou la protection sociale (facteurs pouvant être pris en compte pour calculer les primes de caisse-maladie, par ex.). L'analyse concrète des prix dynamiques soulève par ailleurs des questions relevant du droit des contrats et de la protection des données (cf. ch. 5.3.1.7).

Recommandation:

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.

5.3.2.7 Règlement en ligne des litiges

L'UE dispose depuis début 2016 d'une plateforme de règlement en ligne des litiges de consommation (RLL) qui fonctionne, mais qui n'a déployé jusqu'ici qu'une efficacité limitée. La Suisse serait bien inspirée d'adopter un principe analogue, ou en tout cas d'approfondir la question.

Le RLL n'est pas circonscrit à un domaine particulier du droit, mais c'est dans le contexte du droit des contrats (numériques) qu'il a la plus grande signification pratique. L'UE se préoccupe du règlement extrajudiciaire des litiges de consommation depuis plus de vingt ans. Les nouvelles formes de règlement des litiges sont particulièrement intéressantes quand la juridiction d'État ordinaire est trop lente ou trop coûteuse, ce qui peut très bien être le cas pour les transactions numériques d'une valeur limitée. En dehors des formes «physiques», les solutions en ligne suscitent un intérêt croissant.

L'UE a fixé le cadre de ces procédures dans le règlement (UE) nº 524/2013 relatif au règlement en ligne des litiges de consommation, qui est directement applicable dans ses États membres et que vient compléter le règlement d'exécution (UE) 2015/1051 définissant les modalités d'exercice des fonctions de la plateforme de règlement en ligne des litiges, les modalités du formulaire de plainte électronique et les modalités de la coopération entre différentes plateformes. La plateforme RLL de la Commission européenne a été mise en service en février 2016.

Cette plateforme propose une procédure en quatre étapes: introduction d'une plainte, choix par les parties d'un organisme de règlement des litiges, traitement de la plainte par l'organisme choisi, décision et issue du dossier. Les États membres sont tenus de créer des «points de contact» nationaux chargés d'aider les consommateurs à l'utiliser. La plateforme RLL n'a pas encore donné la mesure de son efficacité faute de temps, mais la Suisse ferait bien de réfléchir à l'instauration d'un tel système.

Recommandation:

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.

5.3.2.8 Géoblocage

Les fournisseurs utilisent le géoblocage pour interdire aux utilisateurs situés en dehors d'un périmètre défini l'accès à certains cyberservices. Par exemple, les consommateurs suisses sont exclus de certains magasins en ligne français ou renvoyés vers une version suisse du site. Cette pratique s'explique par différents motifs: différenciation des prix (discrimination géographique), souci d'éviter des contraintes administratives (dédouanement, par ex.), conditions d'autorisation, respect de droits de propriété intellectuelle ou de conditions de licence (les licences de droits d'auteur pour le cinéma sont souvent assorties de restrictions territoriales) ou encore dispositions légales (droits du consommateur tels que garanties ou restrictions applicables à la distribution de certains produits financiers).

L'UE a adopté un règlement visant à interdire le géoblocage en son sein, conformément au principe d'un marché européen unique. Quiconque propose des produits ou des services sur Internet dans un État membre doit normalement les proposer aussi aux internautes des autres États membres. Dans son état actuel, le règlement prévoit cependant des dérogations concernant, par exemple, le respect de droits d'auteur territoriaux, l'application des dispositions relatives aux consommateurs dans le pays d'origine plutôt que dans le pays de destination, ou l'obligation de livrer à l'étranger.

En Suisse, le géoblocage peut relever de la loi sur les cartels, par exemple en cas de position dominante (au sens de l'art. 7 LCart) ou de système de distribution vertical (au sens de l'art. 5, al. 4, LCart), quoiqu'il n'ait fait à cet égard l'objet d'aucune décision exécutoire. L'initiative populaire pour des prix équitables exige par ailleurs que la question soit réglée dans la LCD, sans pour autant concrétiser sa requête.

5.3.2.9 Blocage d'accès à Internet

En principe, Internet est un système ouvert dont la structure en réseau empêche le cloisonnement. Les données et les informations regroupées en paquets passent du fournisseur au destinataire en transitant par des nœuds appelés serveurs. Certains États souhaitent pouvoir empêcher l'accès à des contenus indésirables en bloquant, par des moyens techniques, les éléments d'adresse correspondants. En règle générale, ils demandent à l'opérateur concerné de bloquer l'accès à certains serveurs (sur le modèle du barrage routier). Mais des moyens techniques simples et en accès libre (anonymisation de serveurs ou réseaux privés virtuels [VPN pour *virtual private networks*]) permettent de contourner ces blocages. Différents pays recourent au blocage d'accès afin, par exemple, de protéger des droits (privés) de propriété intellectuelle (généralement des droits d'auteur), de bloquer des offres interdites sur le territoire (jeux d'argent, par ex.), de lutter contre la pédopornographie ou encore d'empêcher les activités menaçant l'État (terrorisme mais aussi informations subversives). En Suisse, il est pratiqué contre la pédopornographie sur la base de l'observation volontaire d'une liste de blocage établie par l'État. La nouvelle loi du 29 septembre 2017 sur les jeux d'argent (LJAr) permettra de bloquer l'accès à des jeux en ligne étrangers interdits en Suisse, mais la proposition visant à bloquer des accès Internet n'a pas été reprise dans la révision du droit d'auteur.

On s'est interrogé sur la constitutionnalité du blocage dans le domaine des jeux d'argent. Dans une expertise, l'Office fédéral de la justice (OFJ) part du principe que le blocage est conforme à la Constitution, du moins dans ce domaine[10]. Une expertise issue de la doctrine défend la position inverse[11]. L'Assemblée fédérale, suivant l'avis du Conseil fédéral, a décidé d'inscrire le blocage d'accès dans la LJAr.

Les politiques et la littérature spécialisée critiquent le fait que le blocage d'accès soit si facile à contourner. En pratique, il peut aussi conduire à des excès en entraînant le blocage de contenus légitimes (surblocage ou *overblocking*). Par ailleurs, la structure dynamique d'Internet fait que les blocages sont généralement décidés par des autorités administratives sans voies de recours, pratique compréhensible compte tenu de

[10] Cf. note de l'OFJ du 4 juillet 2017, «Le blocage de sites Internet et ses alternatives», qui contient de nombreux renvois (https://www.bj.admin.ch/dam/data/bj/wirtschaft/gesetzgebung/geldspielgesetz/notiz-internetsperre-f.pdf). Cet avis est partagé par Giovanni Biaggini, BV Kommentar, 2e édition, Zurich 2017, ch. m. 6 sur l'art. 106.

[11] Cf. expertise de Florent Thouvenin et Burkhard Stiller du 16 septembre 2016, publiée dans sic!, 2017, pp. 701 ss

l’urgence mais problématique du point de vue de l’État de droit. En dehors de la pédo-pornographie et des jeux d’argent, les blocages doivent donc rester tout à fait exceptionnels et être soumis à un examen critique minutieux de même qu’à une procédure judiciaire.

6 Champ d'analyse relations entre les entreprises (B2B)

6.1 Situation actuelle et évolution

Du point de vue macroéconomique, la transformation numérique stimule la croissance tout en provoquant une mutation structurelle sous l'effet, principalement, de deux facteurs: l'augmentation du capital physique et la hausse de la productivité (rapport du Conseil fédéral du 11 janvier 2017 sur les principales conditions-cadre pour l'économie numérique, pp. 18 ss). Elle réduit les frais de transaction, facilite les économies d'échelle et augmente le nombre d'acteurs potentiels sur le marché. On assiste à un phénomène de désintermédiation allié à l'importance croissante des effets de réseau. Cette mutation fulgurante a permis l'émergence de nouveaux modèles d'affaires et de nouvelles offres.

Les données restent des supports d'information mais sont aussi, et de plus en plus, des biens-valeurs. Leur importance économique croît en conséquence, et les données finissent par servir de monnaie d'échange. Faut-il intégrer cette nouvelle réalité au cadre juridique, et si oui sous quelle forme? Les principes fondamentaux d'un ordre économique social tel qu'il existe en Suisse, qui sont inscrits dans la Constitution (art. 94 Cst.), reposent sur l'initiative privée ou plutôt sur les incitations en faveur des entreprises et les interventions subsidiaires de l'État en cas de nécessité. La création de valeur et les emplois ne peuvent avoir sur la prospérité l'effet stimulant espéré que si le développement technologique et l'innovation ne sont pas entravés ou envoyés sur de fausses pistes par une réglementation excessive. Et une réglementation ouverte et libérale s'adapte plus facilement que les interventions gouvernementales strictes.

Le B2B se distingue par sa très forte interconnexion internationale, surtout compte tenu de la transformation numérique. Les infrastructures numériques sont aujourd'hui mondialisées, les données disponibles au téléchargement dans n'importe quel endroit du globe. En outre, les informations sont reproductibles à volonté, c'est-à-dire que, contrairement aux biens, elles ne se consomment pas une fois pour toutes, sauf mesures de protection spécifiques (droit d'auteur, par ex.).

Le caractère international des flux de données limite fortement la marge de manœuvre du législateur suisse, qui pourra de moins en moins adopter des solutions isolées dans le B2B numérique sans causer d'importants dommages collatéraux (blocage d'accès à Internet).

La transformation numérique exerce une forte influence sur le marché du travail, et ce à différents égards. Il faut s'attendre à des glissements importants entre groupes de professions, secteurs et types d'activité (indépendants / salariés). Les nouvelles formes de collaboration génèrent de la plus-value et des possibilités, mais elles mettent aussi employeurs et employés face à de nouveaux défis. Tout cela aura sans doute pour effet de modifier radicalement les exigences en matière de qualification (formation et profil professionnels). Il faudra réexaminer les normes de protection existantes dans un nouveau contexte. Indépendamment des changements structurels et de contenu, la transformation numérique permet aussi une souplesse accrue, en fait une quasi-simultanéité des formes et des rapports de travail, à tous points de vue:

géographique, temporel, opérationnel et organisationnel. Ces bouleversements font déjà l'objet d'interventions politiques concernant le droit du travail et plus particulièrement les prescriptions en matière d'horaires de travail, dont la forme actuelle ne tient pas suffisamment compte de ces développements.

La transformation numérique entraîne l'émergence de nouveaux modèles d'affaires susceptibles de rendre poreuse la frontière entre fournisseurs professionnels et privés de produits et de services (dans le contexte de plateformes d'hébergement, par ex.). On parle aujourd'hui d'économie collaborative, un terme qui désigne un écosystème complexe de services à la demande et d'utilisation temporaire de biens ou de services par l'intermédiaire de plateformes d'échange en ligne. L'importance économique de ce phénomène a beaucoup augmenté ces dernières années.

6.2 Possibilités et risques

Analyse SWOT

***Strengths* (atouts)**	***Weaknesses* (faiblesses)**
• Possibilité d'un développement rapide de nouveaux modèles d'affaires • Rayonnement au-delà des frontières avec un investissement (relativement) faible • Obstacles à l'accès au marché souvent réduits si le modèle d'affaires ne repose pas trop fortement sur des données • Suppression des frontières spatiales et temporelles • Accès à des ressources mondiales pour les services et les matières premières • Nouveaux débouchés • Disponibilité généralement grande d'informations générales et spécifiques (*big data*) • Multiplication des possibilités grâce à une mutation rapide	• Réglementation différente de celle des modèles d'affaires traditionnels • Positions commerciales plus vulnérables, notamment par rapport à l'étranger • Ruptures structurelles dans les chaînes d'approvisionnement et de distribution • Vulnérabilité par rapport aux attaques et aux abus (cyberdangers) • Obstacles au transfert de données dus à des réglementations nationales hétérogènes • Protection des investissements non garantie à l'échelle internationale • Risques de réputation liés à la transparence et à la quantité d'informations • Soumission simultanée à différentes réglementations (pour cause d'extraterritorialité) • «Demi-vie» courte de certaines connaissances (exigences éle-

	vées en matière de formation continue, de recherche et de développement)
***Opportunities* (possibilités)** • Possibilité d'assouplir les réglementations • Accès relativement facile (possibilités pour les start-up et les PME) • Avantage du pionnier • Exploitation des effets de réseau • Nouveaux débouchés • Possibilité de faire des offres sur mesure (petites séries), économies d'échelle et coûts irrécupérables relativement faibles • Approvisionnement à l'échelle mondiale (externalisation) • Formation continue et développement	***Threats* (menaces)** • Effets de bascule et risque de monopolisation dû aux effets de réseau («le gagnant rafle la mise»), en particulier sur les plateformes • Investissement initial élevé, notamment dans le marketing, en raison de l'orientation internationale des offres • Dépendance des plateformes en raison des économies d'échelle • Flou entourant la propriété et l'utilisation des données (politique en matière de données) • Risque de décrocher au niveau technique

Conclusion:

Compte tenu de la rapidité de l'évolution et des nouvelles structures de marché, l'État doit évaluer ses mesures de régulation et en envisager de nouvelles, en tenant compte du fait que dans le contexte numérique, les possibilités et les atouts évoqués sont très sensibles à ces mesures. Le but étant de conquérir de nouveaux secteurs économiques par essai et erreur, une réglementation précipitée et irréfléchie risque de couper les ailes des nouveaux modèles d'affaires avant qu'ils aient eu une chance de développer un profil et de prendre pied économiquement. Sur un même marché, il faut traiter les secteurs économiques analogiques et numériques sur un pied d'égalité et éviter les distorsions du marché.

6.3 Cadre réglementaire et mesures à prendre

6.3.1 Remarques préliminaires

Compte tenu de la transformation numérique, trois thèmes relevant du B2B méritent, dans l'ensemble, d'être débattus, d'autant qu'ils entrent dans le champ de réglementations futures.

Premier thème: la réglementation dans le domaine de l'économie collaborative. Le groupe d'experts s'est contenté de déterminer les besoins généraux en la matière (cf. ch. 6.3.2). La protection des données et des consommateurs a déjà été présentée dans le contexte du B2C (ch. 5.3.2). Le groupe d'experts n'a pas examiné en détail les

domaines juridiques spécifiques tels que droit du travail, droit fiscal, droit de bail, etc., faute d'une expertise suffisante en droit fiscal et des assurances sociales, notamment, mais aussi pour éviter les répétitions, sachant que le Conseil fédéral a chargé différents offices fédéraux (le SECO et l'OFROU, entre autres) d'effectuer des clarifications dans ce domaine.

Deuxième thème: les rapports des entreprises entre elles, avec des questions relevant du droit de la concurrence et du droit des cartels (cf. ch. 6.3.3).

Troisième thème, traité au ch. 6.3.4: les droits de protection liés au traitement des données et la réglementation des flux de données dans le B2B, avec un renvoi au chap. 7, qui traite de l'accès aux données et de la propriété des données en général.

Un certain nombre d'autres aspects transversaux concernent aussi le B2B. Afin d'éviter les répétitions, les sujets suivants sont traités dans d'autres chapitres:

- importance d'une identité électronique (e-ID) universellement valable pour l'économie et possibilités de mise en œuvre (cf. ch. 4.4.6 et 8.4.2);
- adaptation des prescriptions relatives aux formes exigées pour les contrats en raison de la trop grande complexité des exigences de la loi sur la signature électronique en vigueur (cf. ch. 5.3.2.3);
- nouvelles questions de responsabilité (cf. ch. 7.3);
- blockchain (cf. chap. 9).

Dans tous les champs d'action potentiels, il convient de garder à l'esprit la forte interconnexion internationale et le fait que, l'interconnexion touchant tous les domaines, notamment le droit de la concurrence et celui de la protection des données, les effets extraterritoriaux jouent un rôle croissant. Il convient en particulier de suivre les efforts de l'UE en matière de réglementation.

6.3.2 Réglementation et assouplissement des règles en fonction des nouveaux modèles d'affaires de l'économie collaborative

L'autorisation et la surveillance éventuelles des nouveaux modèles d'affaires numériques posent la double question de l'allègement de la réglementation existante et de l'adoption de nouvelles règles se révélant nécessaires. L'économie collaborative consiste, par exemple, en des plateformes d'intermédiation proposant de l'hébergement ou des services de mobilité pour les plus populaires d'entre elles. De nombreuses autres plateformes (de covoiturage ou de partage de places de stationnement, par ex.) offrent leurs services mais n'ont pas encore la même visibilité. Là aussi, des questions de réglementation se poseront tôt ou tard.

6.3.2.1 Plateformes d'hébergement

Les plateformes d'hébergement sont un modèle d'affaires important de l'économie collaborative, qui intéresse le monde politique. Airbnb et d'autres facilitent la recherche d'hébergements, font potentiellement baisser le prix d'utilisation des logements, diversifient l'offre et élargissent les possibilités du tourisme suisse grâce à la portée mondiale des offres en ligne. Le Conseil fédéral a examiné le phénomène de près dans son rapport du 11 janvier 2017 sur les principales conditions-cadre pour l'économie numérique. En réponse au postulat 16.3625 de la Commission de l'économie et des

redevances du Conseil des États («Développement de nouvelles formes d'hébergement. Examen du droit fédéral»), le Conseil fédéral a chargé le Département fédéral de l'économie, de la formation et de la recherche (DEFR) d'examiner, pour la fin 2017, si une adaptation du droit du bail s'avérait nécessaire, compte tenu du nombre croissant de sous-locations à court terme et répétées contractées via des plateformes d'hébergement, de vérifier que la protection des voisins et des copropriétaires prévue dans le droit privé était suffisante dans ce contexte, et de lui en faire rapport.

Le Conseil fédéral, s'appuyant sur l'étude «Regulierungen in der Beherbergungswirtschaft – Analyse der Deregulierungspotentiale auf Bundesebene aufgrund neuer internetbasierter Geschäftsmodelle» commandée à un prestataire externe, a publié le rapport «La réglementation dans le secteur de l'hébergement» le 15 novembre 2017. Cette analyse détaillée conclut globalement que la plupart des dispositions légales qui s'appliquent aux canaux de distribution traditionnels de services d'hébergement conviennent pour les plateformes Internet. Pour bon nombre de lois, en particulier celles sur l'aménagement du territoire (LAT), sur les résidences secondaires (LRS), sur l'acquisition d'immeubles par des personnes à l'étranger (LFAIE), sur l'égalité pour les handicapés, sur les étrangers (LEtr), sur les denrées alimentaires (LDAl), sur l'impôt fédéral direct (LIFD), sur la TVA (LTVA), sur la protection de l'environnement (LPE) et sur la radio et la télévision (LRTV), il n'y a pas lieu d'intervenir au-delà des modifications qui ont déjà été effectuées. S'agissant du droit du travail et de la législation sur les assurances sociales, le rapport renvoie aux travaux parallèles en cours dans l'administration fédérale. Les droits des voisins et des membres d'une copropriété semblent être suffisamment protégés par le code civil. Mais une révision du droit du bail est nécessaire pour préciser ce qu'il faut entendre par appartement de vacances, pour fixer les modalités de la demande de consentement des bailleurs et pour en définir les motifs de refus. Cette analyse est pertinente et conforme au principe selon lequel il ne faut légiférer qu'en vue de contrer des risques potentiels importants.

En dehors des questions d'aménagement du territoire (respect / application de l'initiative sur les résidences secondaires) et de politique du logement (hausse des loyers au détriment de la population locale), il faut néanmoins garder à l'œil deux autres points: les plateformes d'hébergement en ligne sont consultables de n'importe quel endroit du monde et permettent de conclure des contrats avec n'importe qui. Aussi les dispositions non contraignantes du droit du bail ne s'appliquent-elles pas, du moins aux baux commerciaux. Pour améliorer l'application du droit en vigueur, le rapport préconise la coopération avec les plateformes en ligne, une démarche qui paraît appropriée mais qui ne dispense pas d'accorder plus d'importance, à l'avenir, à la vérification du respect des dispositions légales.

6.3.2.2 Services de mobilité

La transformation numérique permet d'interconnecter les services de mobilité. Ce développement est favorisé par le regroupement qu'ont déjà opéré de nombreux prestataires de transports publics en Suisse. À l'avenir, les prestataires de services privés (taxis, loueurs de véhicules, etc.) et de l'économie collaborative (plateformes d'autopartage [*car sharing*], Uber, etc.) viendront compléter ces chaînes de transport existantes, et on verra sans doute apparaître sur le marché des acteurs entièrement nouveaux. Les avantages d'une approche globale sont évidents: un service de mobilité sur mesure et bon marché, et l'exploitation efficiente des moyens de transport publics et privés. Son développement suppose de disposer d'un réseau de données dense et

interconnecté, qui centralise les données de tous les acteurs du marché concernant les utilisateurs, la localisation, l'exploitation et les prix. Ce réseau n'existe pas encore.

Compte tenu de ces éléments, le groupe d'experts approuve le projet du Conseil fédéral de développer les services de mobilité et de garantir, à cet effet, la disponibilité de données de base.

Dans cet écosystème, la densité de données personnelles et techniques (concernant notamment l'exploitation et les prix) nécessaire représentera, pour les prestataires de services, un défi en matière de protection des données et d'équilibrage des flux de données entre libre accès et compartimentage. Le développement du projet consacré aux services de mobilité multimodaux et à l'organisation des données devra en tenir particulièrement compte. La qualité du service, y compris l'important service après-vente, est un autre aspect significatif, s'agissant de la protection des consommateurs, de ce système multimodal comportant une multitude de prestataires (privés).

6.3.3 Rapports des entreprises entre elles

Les entreprises sont concurrentes non seulement sur les marchés traditionnels mais aussi sur les nouveaux marchés numériques (en ligne, par ex.), dont certains sont encore en cours de constitution. Leurs activités sont plus particulièrement régies par les deux lois suivantes:

- la loi sur les cartels (LCart), qui réglemente le niveau de concurrence souhaité (et qui est évoquée plus en détail ci-après);
- la loi fédérale contre la concurrence déloyale (LCD), qui contient des dispositions sur la qualité de la concurrence; indépendamment des dispositions qui régissent le comportement des entreprises vis-à-vis des consommateurs (cf. ch. 5.3.2), l'une des normes qui importent s'agissant des rapports entre entreprises est celle qui concerne la reprise de résultats prêts à être mis sur le marché (art. 5, let. c, LCD), qui a pour fonction de protéger les investissements, d'où son examen dans le débat sur la propriété (cf. ch. 7.2).

Le Conseil fédéral s'est déjà penché, dans son rapport du 11 janvier 2017 sur les principales conditions-cadre pour l'économie numérique, sur la nécessité de modifier le droit des cartels et a chargé le SECO d'analyser de plus près la question de la révision de dispositions de la LCart, en particulier concernant le contrôle des fusions. Le SECO a associé la nécessité d'agir par suite du passage au numérique à des questions relevant du droit des fusions qui avaient déjà été traitées il y a quelques années dans le cadre d'une grande révision de la LCart, mais qui n'avaient pas abouti pour d'autres raisons (la structure organisationnelle de la Commission de la concurrence [COMCO], par ex.), alors qu'en fait personne ne s'y opposait. Le SECO a ensuite chargé Swiss Economics d'établir un rapport scientifique pour connaître l'avis d'experts sur la question.

Le 27 octobre 2017, Swiss Economics a remis un rapport intitulé «Einführung des SIEC-Tests» (instauration du test SIEC), qui traite essentiellement du contrôle des concentrations mais guère du numérique. Le test SIEC (pour *significant impediment to effective competition*, «atteinte significative à une concurrence effective») est déjà employé dans l'UE depuis longtemps et les experts du droit des cartels en recommandent l'adoption par la Suisse (sans «*Swiss finish*»). Dans son rapport, Swiss Economics

considère comme acceptables la légère augmentation du taux d'intervention des autorités et le surcroît de travail qui résulterait pour elles de l'instauration du test. Mais cette modification de la LCart affecterait autant les marchés traditionnels que les marchés numériques. Cette réflexion vaut aussi pour d'autres sujets abordés dans le rapport, comme la modification de l'art. 9, al. 4, LCart, qui oblige les entreprises occupant une position dominante à notifier les opérations de concentration à la COMCO indépendamment des critères d'intervention (seuils de chiffres d'affaires). Dans la perspective du numérique, il aurait fallu se demander si le test SIEC, qui est axé sur des variables liées aux prix, est bien adéquat car dans les modèles d'affaires numériques, le prix est souvent insignifiant.

Swiss Economics n'examine pas sérieusement dans son rapport les mesures rendues nécessaires par le passage au numérique. La recommandation qui vise à ne pas abaisser les seuils de chiffres d'affaires (critères d'intervention) peut se défendre en cas d'instauration du test SIEC, même si le rachat de petites entreprises par un gros concurrent restera de ce fait invisible. Ces considérations valent-elles également pour les marchés numériques? La question mérite d'être approfondie. Swiss Economics écarte aussi, après des explications relativement brèves, la possibilité de compléter, pour les marchés numériques, les critères d'intervention par des valeurs seuils pour les transactions, alors que la fusion de Facebook et WhatsApp (une transaction d'une valeur de 19 milliards de dollars) n'était pas soumise à notification dans la plupart des pays en raison du chiffre d'affaires modeste de WhatsApp. Entre-temps, l'Allemagne a instauré un seuil de 400 millions d'euros pour la valeur de la transaction, et l'UE réfléchit à un projet dans ce sens. En Suisse aussi, la plupart des experts du droit des cartels estiment qu'il existe une lacune dans le contrôle des concentrations sur les marchés numériques.

Le SECO doit soumettre au Conseil fédéral d'ici à la fin 2018 des propositions concrètes en vue d'une révision de la LCart. Que le test SIEC soit adopté ou non, il paraît opportun de repenser les critères d'intervention en vigueur dans cette loi en fonction de la valeur de la transaction, en tenant compte de l'évolution du droit sur le plan international eu égard à la portée mondiale des marchés numériques.

Ces derniers mois, un nouveau phénomène auquel les autorités fédérales n'ont pas encore eu le temps de s'intéresser, celui des distorsions de la concurrence au moyen d'algorithmes, fait de plus en plus parler de lui. Le comité de la concurrence de l'Organisation de coopération et de développement économiques (OCDE) s'est emparé du sujet et commence à sensibiliser les autorités de la concurrence des différents États. Selon le droit en vigueur, il n'y a «pratiques concertées» ou «convention» que si les concurrents agissent dans l'intention de fausser le marché. Mais si deux offres s'harmonisent sous l'effet d'algorithmes réagissant à leurs variations de prix, l'«intention» (humaine, dans l'esprit de la LCart) fait défaut et il y a «entente tacite», un cas non prévu par la LCart. Ce problème n'exige pas de mesure législative urgente car la formulation ouverte de la LCart permet d'englober des phénomènes nouveaux, mais il mérite d'être examiné dans la perspective de la révision de la LCart.

Recommandations:

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.

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.

6.3.4 Question de la propriété des données dans la mesure où celles-ci représentent une «valeur»

L'un des principaux aspects de cette thématique réside dans l'analyse des droits de la protection, qui découlent aujourd'hui des droits réels et du droit de la propriété intellectuelle, et des effets sur la transmissibilité des données ou des valeurs et sur la protection de l'investissement, en tenant compte des développements se profilant sur le plan international. La propriété et les valeurs revêtent une importance capitale en matière de traitement des données et de sécurité de l'information.

Outre la propriété légale, qui permet des contrôles, le contrôle exercé dans les faits par les entreprises qui accaparent les données joue un rôle de plus en plus important en pratique, ce qui pose la question de l'accès aux données et de la portabilité de celles-ci (cf. ch. 7.1).

6.3.5 Droit de la concurrence

Les normes générales d'intervention de la LCD suffisant à couvrir les comportements déloyaux susceptibles de survenir dans le contexte numérique, il n'y a pas lieu de modifier cette loi.

Le profilage et les données personnalisées contournent la fonction protectrice de l'OIP. Les prix dynamiques individuels réduisent la transparence et empêchent les comparaisons, privant ainsi le consommateur de tout moyen de réaction. Une réglementation générale (dans le droit des contrats ou dans la LCD) ne réglerait cependant pas le problème. Mieux vaut envisager l'instauration de mesures de protection spécifiques dans des secteurs particulièrement vulnérables (protection sociale, assurances / caisses-maladie, etc.).

6.3.6 Accès aux données

L'aspect «accès aux données» revêt une grande importance car les moyens offerts par le droit des cartels sont insuffisants en pratique. En Suisse, ce débat, qui devrait faire partie intégrante d'une politique d'envergure en matière de données (non seulement de la part du secteur public mais aussi de celle du privé), n'a pas encore eu lieu. La Commission européenne a une longueur d'avance en ce qu'elle entend non pas rebondir directement sur les droits de la propriété intellectuelle en vigueur, mais développer un «droit de l'accès» autonome sur le modèle de l'accès à l'information vis-à-vis du secteur public. Ces questions, qui relèvent à la fois du B2C et du B2B, sont traitées plus en détail au chapitre 7.

7 Thèmes communs aux champs d'analyse B2C et B2B: accès aux données, propriété des données et nouveaux enjeux liés à la responsabilité

Entre les deux extrêmes que sont le cloisonnement des données par leur propriétaire et une circulation libre et illimitée des données, l'éventail des possibilités est large. Le traitement des différents types de données fait face à un double défi de taille: d'une part, parvenir à un compromis équilibré entre une utilisation libre et une transmission limitée des données et, d'autre part, garantir une prise en compte appropriée des données dans la législation. Le ch. 7.1 traite de l'accès aux données et de leur portabilité. Le ch. 7.2 («Propriété des données») analyse les avantages et les inconvénients liés à l'introduction d'une propriété des données tout en proposant des solutions de remplacement. La transformation numérique soulève de nouvelles questions en matière de responsabilité. Ces questions sont examinées au ch. 7.3 («Nouveaux enjeux liés à la responsabilité»).

7.1 Accès aux données et portabilité

7.1.1 Remarques préliminaires

Le droit d'accès aux données concerne le domaine tant public que privé. Lorsque le propriétaire des données n'assure pas lui-même activement la transparence, on peut se demander s'il ne convient pas, dans certaines circonstances, de *faire en sorte* que l'accès aux données soit garanti, notamment quand la personne concernée le demande. Il faut en outre déterminer si les données auxquelles on donne accès peuvent être réutilisées.

Dans le domaine public, l'accès aux données est réglementé par des lois, notamment la loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans) et les lois cantonales *ad hoc*. Ces bases juridiques abordent à plusieurs endroits les conditions régissant l'accès aux données et la procédure à suivre à cet égard. Par contre, la question de l'utilisation des données n'est pas réglementée. Ces dernières années, des voix se sont élevées en faveur d'une plus grande transparence des données publiques. En effet, l'un des objectifs du projet dénommé *Open Government Data* (ODG) est de rendre les données officielles accessibles pour que le public puisse les consulter et les réutiliser.

Le thème de l'OGD a été analysé par un groupe de travail interdépartemental dirigé par les Archives fédérales suisses. Ce groupe a présenté un certain nombre d'approches possibles: adaptation des lois spécifiques par l'intermédiaire de projets législatifs menés par les services spécialisés compétents, réglementation transversale uniforme ou adaptation des actes spécifiques dans le cadre d'un projet législatif centralisé. Toutefois, à l'exception de la mise en place du portail OGD «opendata.swiss», les travaux à cet égard n'ont pas été poursuivis. Aussi l'OFCOM est-il désormais chargé, dans le cadre de son rapport sur la politique des données, de formuler également des propositions relatives au libre accès aux données produites par l'administration (voir aussi ch. 8.5).

Dans le domaine privé, les droits d'accès aux données sont également régis par des dispositions spéciales. Le droit de la protection des données (art. 8 LPD), le droit du

mandat (art. 400 CO), le droit de la société anonyme (art. 697 CO) et de nombreuses autres lois attribuent ainsi à la personne concernée des droits d'accès concrets. Le présent chapitre se penche uniquement sur les droits d'accès aux données dans le domaine privé et examine dans quelle mesure la création de tels droits est utile et pertinente.

7.1.2 Utilité et pertinence des droits d'accès

Tout comme dans le débat autour de la propriété des données, il convient de faire la différence, dans le cadre de l'examen des droits d'accès aux données, entre un contrôle juridiquement fondé et un contrôle effectif des données. S'il jouit d'un droit d'exclusivité, fondé par exemple sur un droit de propriété intellectuelle, un propriétaire de données peut en principe refuser que des tiers accèdent à ses données. Toutefois, même dans un tel cas de figure, il existe certaines limitations (par ex. exception d'«usage loyal» dans le droit d'auteur) qui restreignent, dans une certaine mesure, le droit d'exclusivité.

La restriction d'un contrôle effectif des données, opération souvent liée à un traitement spécifique des données, est plus importante encore dans une société de l'information. Par exemple, si une entreprise réalise d'importantes analyses de données massives (*big data*), elle aura tendance à conserver les résultats obtenus dans des «silos de données» et à éviter de les transmettre à des tiers. La restriction d'un accès aux données est rarement justifiée par des motifs techniques. C'est pourquoi il faut avant tout définir précisément le cadre technique régissant l'accès aux données personnelles et aux données techniques (deux types de données qu'il convient de distinguer). Les droits d'accès aux données doivent être examinés sous deux angles différents : l'accès à des données pour des raisons d'intérêt public et l'accès à des données d'un concurrent.

1. Les données d'intérêt public sont pertinentes, en particulier pour les instances publiques (par ex. pour les autorités). Le législateur doit ainsi fixer les conditions auxquelles un droit d'accès à ces données peut être obtenu. Il doit également déterminer s'il convient de rendre cet accès payant.
2. La question de l'accès à des données d'un concurrent est plus complexe. En effet, dans ce domaine, de nombreuses données sont protégées par le secret d'entreprise, et une transparence accrue va à l'encontre du principe de confidentialité. Toutefois, indépendamment des prescriptions concernant le maintien du secret, il convient de garder à l'esprit que l'accès aux données est parfois nécessaire, ne serait-ce que pour envisager une entrée sur le marché ou pour pouvoir intervenir sur un marché aval ou un marché amont. Le marché de l'automobile est un bon exemple à cet égard. En effet, s'il ne peut obtenir certaines données de la part du fabricant, un garagiste ne pourra pas forcément effectuer la réparation voulue. Dans un tel cas de figure, il faudra peser les intérêts en présence dans le cadre des prescriptions légales.

7.1.3 Instruments juridiques réglementant l'accès aux données

Le législateur peut, au moyen de normes spécifiques, inscrire différents droits d'accès dans la législation. Comme mentionné plus haut, le droit suisse prévoit une multitude

de droits d'accès. L'art. 8 LPD est central à cet égard, bien qu'il ne traite que des données personnelles. On relève d'une manière générale que la présence de règles éparses est un désavantage.

L'utilisation de données par un tiers peut être réglementée dans le cadre d'un contrat de licence (par ex. un contrat de savoir-faire). Souvent, le concédant octroie spontanément la licence, car il est intéressant pour lui qu'un tiers utilise ses données contre paiement.

Le législateur peut également introduire un régime de licences obligatoires avec pour objectif d'éviter que la personne ou l'entité qui effectue le contrôle effectif des données refuse d'octroyer spontanément une licence. Le législateur doit dès lors déterminer précisément les conditions auxquelles une licence obligatoire peut être obtenue.

En 1996, l'UE s'est dotée d'une directive sur la protection des bases de données, laquelle, d'après la Commission européenne elle-même, ne porte pas vraiment ses fruits. Forte de ce constat, la Commission propose de nouveaux instruments juridiques: elle reconnaît notamment un droit spécifique au producteur de base de données et développe un modèle de droits d'accès aux données. En janvier 2017, dans sa communication intitulée «Créer une économie européenne fondée sur les données», la Commission européenne a proposé d'envisager l'introduction d'un système de licences obligatoires, qu'elle considère également comme une alternative à l'introduction d'une propriété des données, qui ne fait pas l'unanimité. En Suisse, le concept des licences obligatoire n'a pas encore fait l'objet d'analyses approfondies.

La Commission européenne n'a pas encore donné de détails sur les conditions générales du régime des licences obligatoires. En règle générale, l'utilisation de ce type de licences ne se justifie qu'en présence de conditions spécifiques sur le marché. Il convient de réglementer avant tout les critères d'intervention concernant le contrôle effectif des données entraînant des conséquences juridiques. On trouve des recoupements dans la manière dont cette question est traitée notamment dans le droit de la concurrence. En effet, de nombreuses décisions de la Cour de justice de l'Union européenne (mais aussi un certain nombre de décisions des tribunaux suisses) fixent les conditions de l'accès aux «installations essentielles (*essential facility*). La jurisprudence a tout d'abord considéré que ce concept se référait aux installations physiques, avant d'admettre que des volumes de données pouvaient également être qualifiés d'«installation essentielle» (arrêts Magill, IMS Health et Microsoft).

Si l'on envisage l'introduction d'un système de licences obligatoires, le législateur devra déterminer s'il convient de procéder de manière horizontale en créant une réglementation générale sur les licences obligatoires ou s'il est plus avantageux d'adopter une approche verticale et de créer une réglementation par secteur. Les dispositions normatives étant par définition précises, il serait opportun d'envisager une réglementation par secteur. Si elle permet de prendre en compte des spécificités du marché, cette approche est toutefois plus chronophage et plus complexe au niveau administratif qu'une réglementation générale.

7.1.4 Cadre général applicable à un système de licences obligatoires

En présence d'un système de licences obligatoires, les conditions de l'accès aux données et de l'exploitation des données ne sont pas fixées dans le cadre d'un contrat. C'est pourquoi les principaux critères régissant ce système doivent être définis par le

législateur. Les dispositions réglementaires concernant le contenu des licences obligatoires doivent tenir compte des aspects suivants:

- Dispositions tarifaires: les données ont une valeur certaine, même s'il est souvent difficile de vérifier cette valeur. Comme le relève un rapport récent de l'OCDE, chiffrer une valeur est une opération extrêmement complexe. Ce constat ne doit toutefois pas nous faire renoncer à la tentative de chiffrer de manière raisonnable la redevance de licence. La personne qui jouit d'un droit d'accès à des données ne peut se prévaloir du droit d'utiliser ces données sans payer une redevance.
- Le volume des données auxquelles il est donné accès doit être défini soit librement sur la base d'un contrat, soit au moyen d'une disposition réglementaire. Un droit d'accès doit permettre d'accéder non pas à autant de données qu'on le souhaite, mais «seulement» aux données pertinentes pour la personne concernée.
- Le contrat de licence ou les dispositions réglementaires doivent établir si la personne qui dispose d'un droit d'accès jouit également du droit de réutiliser les données auxquelles elle a accès.
- Conformément aux prescriptions du droit de la concurrence, le droit d'accès à des données ne peut être subordonné à d'autres obligations de la personne qui jouit de ce droit.

La licence obligatoire est un instrument juridique qui existe déjà depuis de nombreuses années dans le droit de la propriété intellectuelle. Dans ce domaine également, on a établi que les conditions auxquelles une licence est délivrée doivent être acceptables et plus précisément équitables, raisonnables et non discriminatoires (conditions «FRAND», de l'anglais *fair, reasonable and non-discriminatory*). Les différentes interprétations relatives à la notion des conditions «FRAND» font déjà l'objet d'une vaste jurisprudence, qui peut également servir dans le contexte de l'accès aux données.

On relève d'une manière générale que la réglementation des droits d'accès pour le contrôle effectif des données peut constituer une alternative tout à fait viable à l'introduction d'une propriété des données. On ne peut certes ignorer le fait que l'élaboration d'une législation réglementant un système de licences obligatoires n'est, de loin, pas une tâche aisée. Néanmoins, bien que complexe, cette approche offre l'avantage d'éviter les problèmes qui se poseraient avec l'introduction d'une propriété des données.

Recommandation:

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

7.1.5 Portabilité des données personnelles et des données techniques

7.1.5.1 Portabilité des données personnelles

La portabilité est une question souvent examinée dans les débats sur la propriété des données et l'accès aux données. Il s'agit, en substance, de déterminer si la personne qui jouit d'un droit d'accès à des données peut exiger de l'entreprise qui réalise le

contrôle effectif de ces données qu'elle transfère ces informations à une autre entreprise. Cela présuppose que les données soient présentées dans un format couramment utilisé et lisible par machine.

Le Règlement européen sur la protection des données (RGPD) consacre un droit à la portabilité des données personnelles à son art. 20. La France a également introduit un droit à la portabilité des données au niveau national, qui est en vigueur parallèlement au RGPD depuis mai 2018. La loi française prévoit toutefois une réserve lorsque que la valeur des données a sensiblement augmenté dans le cadre des activités de la personne qui les a traitées. À notre connaissance, aucun pays autre que ceux qui appliquent le RGPD ne reconnaît un droit à la portabilité des données.

Dans ses explications sur l'avant-projet de révision totale de la loi fédérale sur la protection des données (AP-LPD), le Conseil fédéral a fait savoir que l'introduction d'un droit à la portabilité des données n'était pas prévue. Lors de la consultation, cette prise de position a été largement critiquée. Dans son message sur le P-LPD, le Conseil fédéral a néanmoins maintenu sa position, invoquant le fait que la portabilité des données visait davantage à renforcer la concurrence qu'à protéger les droits de la personnalité. Il a également mis en avant que l'exigence selon laquelle les données doivent être traitées dans un format structuré et lisible par machine entraînerait des coûts non négligeables, en particulier pour les petites entreprises.

La portabilité des données représente à plusieurs égards une véritable opportunité pour l'évolution du traitement des données personnelles. Ce droit permet aux personnes de faire sortir, de manière standardisée et automatisée, les données les concernant des «coffres-forts» des personnes qui traitent ces données, et de les gérer elles-mêmes. Ce processus étant complexe, des systèmes de gestion des informations personnelles (*Personal Information Management Systems [PIMS]*) ont été mis en place afin d'aider les personnes concernées dans leurs démarches. Aussi, l'«objet de données» peut désormais disposer de ses données en tant qu'utilisateur ou «sujet de données», jouir ainsi d'une autodétermination en matière d'information et monétariser des données. Cette évolution aura peut-être pour effet d'encourager la libre circulation des données personnelles et, à terme, de réglementer le marché des données personnelles, puisque leur prix sera désormais mieux chiffrable. Les utilisateurs des données, la recherche, l'économie et, au final, l'ensemble de la société profiteraient de cette évolution.

Dans ce contexte, le groupe d'experts estime qu'il faut encourager la libre circulation des données personnelles au nom de l'autodétermination en matière d'information et que le droit de la protection des données pourrait servir de point de départ pour l'introduction d'un droit à la portabilité. Le recours à d'autres instruments juridiques pour mettre en œuvre la portabilité des données, tels que la législation sur les cartels, serait certainement moins approprié. En effet, on se baserait dès lors sur l'argument de la concurrence, et la mise en œuvre des droits de la concurrence est longue et coûteuse. D'autres lois sont trop sectorielles, comme la loi sur le dossier électronique du patient, qui ne couvre en l'occurrence que les données du patient.

Contrairement à ce que prévoit le RGPD, c'est le droit d'accès tel qu'il est défini aujourd'hui dans la LPD qui doit servir de point de départ à l'introduction de la portabilité des données. Cette approche permettrait en effet de couvrir l'ensemble des données traitées (y compris les données observées) et pas uniquement les données directement transmises par l'utilisateur, comme c'est le cas dans le RGPD. Si l'on complète

le droit d'accès, il faudra également veiller à garantir et à concrétiser le droit de l'utilisateur d'obtenir des données dans un format standardisé et lisible par machine afin de permettre le transfert direct de ces données à des tiers (par ex. PIMS, voir ch. 7.1.5.2 pour plus de détails).

Un droit d'accès étendu donne lieu, dans la mesure où les données sont sauvegardées, à des conflits d'intérêts entre les personnes qui traitent les données, les personnes concernées et les tiers, notamment en matière de confidentialité. Il convient d'examiner ces conflits et de veiller à équilibrer la situation en en tenant compte dans le droit d'accès étendu. Des travaux préparatoires ont déjà été entamés dans ce domaine. Le 9 mai 2018, le Conseil fédéral a chargé l'Office fédéral de la justice d'analyser le besoin de réglementation pour introduire la portabilité des données personnelles selon le secteur ou la branche.

7.1.5.2 Principe du partage des richesses

Ce principe économique veut que non seulement les personnes qui traitent des données, mais aussi les personnes concernées par ces données bénéficient de la nouvelle valeur créée par ces dernières. Aussi, en vertu de ce principe, les personnes concernées seraient désormais considérées comme des partenaires égaux pouvant elles aussi apprécier la valeur ajoutée des données. Elles seraient aussi clairement informées de la manière dont leurs données sont collectées et utilisées, et ne seraient dès lors plus en situation d'infériorité en termes de connaissances relatives à leurs données. En 2016 déjà, le Contrôleur européen de la protection des données a reconnu que les PIMS permettaient aux utilisateurs de reprendre le contrôle de leurs données, même s'il considère que cette approche viendrait compléter plus que remplacer le RGPD et le principe de la portabilité.[12] Il faudrait également examiner comment les personnes qui traitent les données pourraient être incitées à renoncer au droit d'exclusivité dont elles se prévalent aujourd'hui concernant le contrôle du traitement des données. Ce partage donnerait inévitablement une valeur économique aux données et serait ainsi assorti tant d'avantages que d'inconvénients, tels que le problème non résolu des droits de propriété sur les données.

Recommandation:

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.

7.1.5.3 Portabilité des données techniques

La question de la portabilité concerne également les données techniques. Une entreprise qui stocke ses données dans un *cloud* (ou nuage informatique) peut vouloir changer de fournisseur pour le stockage de ses données. Dans le cas des entreprises, la portabilité des données est le plus souvent réglée dans le cadre d'un contrat contenant des dispositions relatives au transfert des données et à la résiliation.

La Commission européenne a examiné cette question dans le cadre de sa proposition de règlement concernant la libre circulation (transfrontière) des données techniques

[12] https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_fr (état au 30 avril 2018)

dans les pays de l'Union européenne, présentée le 13 septembre 2017 [COM (2017) 495 final]. La question du portage des données y est abordée à l'art. 6, dans lequel la Commission n'établit pas un droit impératif à la portabilité des données techniques, mais s'engage à encourager l'élaboration de codes de conduite au niveau de l'Union, afin de faciliter le changement de fournisseur d'accès à Internet. La proposition doit encore être débattue. La Suisse n'a à ce jour pas engagé d'action dans cette direction. Toute intervention en faveur d'une portabilité des données techniques doit tenir compte des évolutions observées sur le plan international à cet égard et éviter un «Swiss finish» (tendance à vouloir aller plus loin que les exigences internationales dans l'élaboration des normes).

Recommandation:

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

7.2 Propriété des données

La notion de «propriété des données» apparaît régulièrement au niveau tant juridique que politique. Elle ne désigne toutefois pas toujours la même chose et n'a pas encore été clairement définie. Par ailleurs, il n'est pas facile de délimiter sa portée sémantique du fait qu'une multitude de catégories de données et de formes de propriétés des données doivent être prises en considération.

7.2.1 Tour d'horizon sémantique

La notion de «propriété des données» englobe deux éléments, à savoir les «données» et la «propriété». Sans être clairement définis, les droits issus de la propriété sont consacrés dans la loi, qui se réfère explicitement à la propriété mobilière (art. 641 et 713 CC). Dans le contexte des données toutefois, la propriété au sens de «détention» ou de «possession» est essentielle.

La définition du terme de «donnée» est plus complexe. Il existe une dichotomie – essentielle au niveau juridique – entre les données personnelles et les données techniques. Les données personnelles sont liées au droit de la personnalité, qui, comme la propriété, confère des droits inaliénables et dont chacun peut se prévaloir à l'encontre d'autrui. Les données personnelles sont régulièrement abordées dans la législation sur la protection des données. Les données techniques sont quant à elles davantage régies par des aspects économiques. En effet, les données techniques sont attribuées à des personnes ou des entreprises qui peuvent ensuite les traiter et les exploiter.

Le concept de «donnée» doit être distingué de celui d'«information». Il possède en effet trois dimensions : une dimension syntaxique qui, dans le monde numérique, concerne la structure des données (successions de 0 et de 1); une dimension sémantique se référant au rapport qu'ont les différentes données entre elles et se traduisant en fin de compte par une information, c'est-à-dire le contenu qui se cache derrière les données; et, enfin, une dimension que l'on pourrait qualifier de «pragmatique», qui nous amène à nous poser la question suivante: les connaissances transmises par l'information ont-elles des répercussions ou poursuivent-elles un certain objectif ? Le fait d'être propriétaire de la structure syntaxique des données a des conséquences au niveau de leur infrastructure (mais pas au niveau de leur contenu). Le fait d'être propriétaire d'une

information peut être utile, mais cette propriété soulève une question importante, à savoir celle de la monopolisation de l'information.

Par ailleurs, il convient de différencier les «données volontaires» (que des personnes se transmettent volontairement entre elles), les «données observées» (que des tiers collectent, mais qui peuvent être échangées) et les «données inférées» (basées sur des analyses de données de grande envergure, comme les analyses de *big data*).

Enfin, on distingue également deux types de contrôle des données – et ce indépendamment du type de données –, à savoir le contrôle juridiquement fondé et le contrôle effectif des données. Le premier se base sur un titre juridique défini et confère des droits exclusifs sur des données, notamment quant à leur utilisation et à leur mise à disposition. Par «contrôle effectif des données», on entend la possibilité de contrôler l'accès aux données ou aux informations et de réguler ainsi leur mise à disposition. Ce type de contrôle peut conférer un pouvoir analogue à celui de la propriété.

7.2.2 Motifs justifiant la création d'un cadre pour la propriété des données

Le législateur peut créer un nouveau cadre juridique lorsque l'analyse de la situation juridique existante met en lumière la nécessité d'agir dans un domaine. Une action législative peut être appelée aussi bien par des exigences théoriques que par des besoins pratiques.

Une intervention au niveau de la réglementation se justifie le plus souvent en cas de défaillance du marché, une situation qui se présente lorsque le marché ne produit pas les biens ou services souhaités. Il faudrait donc que l'on se trouve dans une situation d'absence de création, de mise à disposition et d'utilisation de données, et ce malgré l'intérêt de la société pour ces processus. Autrement dit, il faudrait que même si les données peuvent être facilement dupliquées, l'économie des données souffre d'un manque d'incitations et qu'elle ne soit de ce fait pas stimulée. Mais la réalité est tout autre: l'augmentation exponentielle du volume de données laisse entendre que la société est fortement encouragée à créer et échanger des données.

Un autre argument en faveur d'une réglementation pourrait être les coûts de transaction, c'est-à-dire, dans le monde numérique, en particulier les frais liés aux recherches et aux négociations menées dans le contexte du traitement des données. Les études réalisées jusqu'ici ont toutefois montré que les coûts de transaction ne baisseraient très probablement pas de manière significative si le législateur introduisait une propriété des données. En outre, une standardisation a souvent lieu spontanément en raison de l'intérêt montré par les personnes concernées.

Toujours au niveau économique, une réglementation pourrait être justifiée par une affectation inappropriée des coûts et des avantages. À cet égard, on évoque parfois le fait que les propriétaires des données peuvent retirer des avantages économiques de la collecte de données, mais qu'ils ne sont pas obligés de dédommager les personnes concernées par ces données (on parle aussi d'«internalisation des bénéfices»). Néanmoins, les études montrent d'une manière générale que les personnes concernées auraient de la peine à en retirer un bénéfice réel et que le revenu annuel qu'elles pourraient réaliser dans ce contexte serait vraisemblablement minime (moins de 100 francs suisses par an).

Les valeurs éthiques comme la liberté, la dignité et l'autonomie de l'être humain, la non-discrimination, le droit à l'autodétermination en matière d'information ou encore la

possibilité de s'épanouir seront mieux encadrés par les droits fondamentaux ou des réglementations ayant des motifs non économiques que par l'introduction d'une propriété des données. Par ailleurs, il ne semble pas que le problème du flou juridique qui entoure le droit aux données soit aussi grave pour justifier l'introduction d'un nouveau cadre juridique. Cela étant, l'absence d'une propriété des données a donné lieu à un certain vide juridique auquel il conviendra d'accorder une attention particulière (voir ch. 7.2.6).

7.2.3 Fondements juridiques d'une propriété des données

Le terme de «propriété des données» rappelle celui de «propriété mobilière». Aux termes du code civil, la propriété a pour objet les choses et les forces naturelles (art. 641 et 713 CC). Les données n'ont toutefois aucun caractère physique et il est généralement admis qu'elles ne possèdent pas les caractéristiques nécessaires pour constituer l'objet d'une propriété mobilière. C'est pourquoi on ne peut approuver sans autres explications un droit subjectif d'exclusivité aux données. Le législateur devrait élargir la réglementation des droits réels, ce qu'il pourrait faire en adaptant légèrement la loi. À cet égard, la Commission européenne a présenté en janvier 2017 un document de réflexion sur la création d'une propriété des données. Toutefois, on ne peut exclure qu'une telle réglementation ne crée de nouveaux problèmes auxquels nous n'avions pas pensé (ch. 7.2.5).

Il en va de même pour la notion de «possession» (art. 919 CC). Comme pour la propriété, la possession se fonde sur des caractéristiques physiques (maîtrise effective d'une chose). Aussi, bien qu'on le rencontre souvent, le terme de «possession des données» n'a aucune assise juridique.

Depuis plus de 100 ans, la propriété intellectuelle est un élément important du droit. Contrairement à la propriété mobilière, le droit d'auteur et le droit des brevets, par exemple, n'exigent aucune caractéristique physique qui irait à l'encontre de la forme virtuelle d'une propriété des données. Le problème qui se pose en matière de propriété intellectuelle est le fait que les données ne présentent souvent ni le degré d'inventivité, ni la créativité intellectuelle nécessaires. On a certes tenté à plusieurs reprises de créer un droit de propriété intellectuelle *sui generis*, mais cette approche ne s'est pas encore imposée.

Parallèlement aux droits de propriété intellectuelle «classiques», des formes spéciales de statuts juridiques semblables à ces droits se sont développées ces dernières décennies, notamment le droit réglant les rapports de voisinage, appelé «droit du voisinage» (ou «droits voisins»), ou la protection *sui generis* des propriétaires de banques de données. La Suisse, mais aussi les États-Unis n'ont délibérément pas repris ce droit de protection inscrit dans le droit européen. L'idée de protection sous-jacente à ces statuts juridiques, qui visent des expressions artistiques «éphémères» et des recueils de données (et non des données mêmes), n'est pas comparable à la protection que viserait une propriété des données. En d'autres termes, une application par analogie du droit de la propriété intellectuelle ne serait pas appropriée.

Enfin, le contrat ou le délit peuvent également justifier l'introduction d'une propriété des données. Ces faits juridiques n'ont toutefois que des effets relatifs (relevant du droit des obligations), mais ils n'ont pas de conséquences absolues. Nous sommes en présence d'un acte considéré comme illicite sur la base de la responsabilité civile ou du droit de la concurrence en cas de violation du secret de fabrication ou du secret

commercial, ou en cas de violation de l'interdiction de reprendre une prestation d'autrui, par exemple. Le droit ne prévoit toutefois pas de protection étendue des données.

On constate donc qu'il n'est pas facile de définir – et de justifier – un cadre juridique régissant la propriété des données. Il serait donc plus judicieux d'identifier les véritables lacunes en matière de réglementation (ch. 7.2.6). Cependant, dans un souci d'exhaustivité, il convient d'abord de se demander si la création d'une propriété des données n'entraînerait pas de nouveaux problèmes (ch. 7.2.5).

7.2.4 Les données en tant que moyen de paiement

Un véritable changement de paradigme s'est récemment produit en lien avec les données, qui ne sont plus seulement vendues et achetées (contre paiement), mais qui peuvent désormais également être utilisées en tant que moyen de paiement de prestations en nature et de services. Cette possibilité d'utiliser les données pour rémunérer d'autres biens soulève de nouvelles questions juridiques auxquelles les lois existantes n'amènent pas toujours des réponses satisfaisantes.

La proposition de directive présentée par la Commission européenne sur les contrats de fourniture de contenu numérique (COM 2015 634 final) tient compte de ce changement de paradigme et réglemente les données (aussi) en tant que «monnaie de l'avenir». En pratique, les parties contractantes conviennent que le fournisseur de prestations en nature ou de services est «dédommagé» par la mise à disposition de données du client. Autrement dit, le client ne paie pas la prestation en nature ou le service qu'il achète par le moyen traditionnel qu'est l'argent, mais il permet au fournisseur d'utiliser ses données en contrepartie de la prestation en nature ou du service achetés. Par conséquent, il s'agit non pas d'une «transaction gratuite», mais d'un accord entre les deux parties qui partent du principe que les données du client ont une valeur économique pour le fournisseur correspondant à une contrepartie en espèces.

Une disposition spéciale s'est révélée nécessaire pour les cas où la validité du contrat est contestée pour de justes motifs (par ex. pour erreur sur les éléments nécessaires du contrat ou pour défauts matériels graves) et que, par conséquent, les prestations réciproques sont annulées à la suite de la résolution du contrat. Dans une telle situation, le prestataire est dans l'obligation de retransférer au client, dans un format technique courant et standardisé, les données que ce dernier avait mises à sa disposition, et ce sans les avoir préalablement copiées et sans les utiliser dans une autre forme. Cette réglementation se base sur le même concept de la portabilité des données prévu à l'art. 20 du RGPD. La formulation choisie n'est toutefois pas identique, ce qui n'est pas sans poser problème sur le plan juridique, mais la directive sera en principe adaptée en conséquence dans sa version finale.

Cette directive devrait être adoptée au cours du deuxième semestre de 2018. La Suisse ne dispose d'aucune base juridique correspondante. Il convient toutefois de se demander si une réglementation similaire ne devrait pas être envisagée eu égard aux questions qui se posent en matière de propriété des données et d'accès aux données.

7.2.5 Nouveaux problèmes occasionnés par l'introduction d'une propriété des données

Le législateur est en mesure de combler le vide juridique créé par des développements nouveaux dans un domaine. Toutefois, l'activité législative peut avoir des effets négatifs lorsqu'elle fait naître des problèmes jusque-là inexistants sur le plan juridique.

7.2.5.1 Facteurs d'incertitude

Comme nous avons pu le constater ces dernières années, notre environnement technologique évolue très rapidement. Des règles de droit généralisées et rigides risquent de faire obstacle au développement technologique. L'expérience a montré que l'élaboration de normes juridiques est un processus souvent si long que la technologie évolue entre-temps. Aussi, même si une propriété des données était introduite, des technologies nouvelles ou hautement spécialisées pourraient surgir dans un vide juridique.

D'après les études empiriques réalisées jusqu'ici, l'absence d'une propriété des données n'a vraisemblablement aucun impact négatif sur l'investissement et l'innovation. Il faudrait néanmoins s'assurer que l'introduction d'une propriété des données ne se solde pas par de nouvelles charges sur le plan économique, qui seraient plus graves que l'absence d'un droit absolu. L'établissement d'une propriété des données pourrait notamment engendrer l'émergence de coûts de transaction lors des «changements de propriétaire».

Les incertitudes à craindre sur le plan juridique concernent la portée d'un droit de propriété sur les données défini en termes généraux. Les tribunaux jouiraient dès lors d'une marge de manœuvre relativement importante dans l'exercice de leur pouvoir d'appréciation, ce qui pourrait déboucher sur des jugements contradictoires.

7.2.5.2 Problèmes de mise en œuvre

Les principales difficultés qui surgiraient en cas d'introduction d'une propriété des données seraient liées à la mise en œuvre d'un nouveau cadre juridique. La tenue d'un registre de la propriété des données – à l'instar du registre foncier ou du registre du commerce – ne serait sans doute pas la solution idéale en raison des coûts administratifs élevés qui pourraient en résulter. La technologie blockchain (chaîne de blocs) serait appropriée en tant qu'infrastructure à des fins d'enregistrement. Mais cette technologie est entre les mains de personnes privées et se trouve ainsi hors de contrôle (voir ch. 9.1.3). L'État n'est en principe pas impliqué dans cette infrastructure. C'est pourquoi l'application de droits sur la base de dispositions émanant des autorités est beaucoup plus compliquée en présence d'une telle infrastructure. La définition de la propriété reste toutefois une exigence primordiale si l'on veut faire en sorte que la réalisation de cette notion soit réalisable et efficace.

Comme on a pu le constater, les marchés des données sont exposés à un risque de monopolisation élevé. Les procédures intentées par l'UE à l'encontre de Google constituent un exemple très représentatif à cet égard: l'entreprise américaine avait été soupçonnée de pratiquer un monopole illicite et a finalement été condamnée à des amendes substantielles. L'introduction d'une propriété des données créerait d'autres droits absolus et pourrait, dès lors, encourager les tendances au monopole.

Il convient enfin de s'interroger sur une éventuelle durée de vie de la propriété des données et de déterminer ainsi si cette propriété devrait être éternelle ou avoir une «date d'expiration», sachant que les données ne sont en principe pas vouées à durer éternellement (elles le sont en tout cas dans une moindre mesure que les objets). Une date d'expiration est techniquement programmable, mais il n'est pas certain que le code en question contienne les signaux appropriés pour annuler la propriété des données.

7.2.6 Éventuelles mesures à prendre du fait de l'absence d'une propriété des données

La création d'une propriété des données serait justifiée dès lors que des lacunes en matière de réglementation pourraient créer une insécurité juridique et que l'adoption de normes pourrait contribuer à la sécurité du droit.

7.2.6.1 Éventuelles lacunes en matière de réglementation

Nous présentons ci-après un certain nombre d'éléments relevant de plusieurs domaines juridiques (à l'exception du droit fiscal, qui n'est pas abordé dans le présent rapport), dont la réglementation n'est pas considérée comme satisfaisante dans l'état actuel du droit.

- Questions relevant du droit des successions: concernant le transfert des objets de la succession entre les héritiers légitimes, le droit des successions part du principe que la masse successorale se compose de biens et de créances. Néanmoins, certaines questions restent ouvertes, notamment celle de savoir si les données de la personne décédée – par exemple les données figurant sur Facebook – peuvent être revendiquées. Cette problématique doit être abordée sur le plan législatif. Le P-LPD (art. 16) contient désormais une disposition qui, se référant aux données personnelles d'une personne décédée, précise expressément les conditions auxquelles les héritiers peuvent en demander la consultation ou la suppression.
- Portabilité des données: les données ayant souvent une valeur économique ou sociale, l'ayant droit doit être en mesure de transférer ses données d'un intermédiaire Internet à un autre intermédiaire. L'art. 20 du RGPD consacre désormais un droit à la portabilité des données personnelles. Le P-LPD ne contient pas de disposition prévoyant un droit à la portabilité des données (message du Conseil fédéral 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, ch. 1.7.4), mais cette problématique doit encore faire l'objet d'un examen détaillé.
- La portabilité des données a également son importance pour les données techniques. On peut envisager de la réglementer dans le contexte de l'accès aux données (voir ch. 7.1.3).
- Faillite: lorsqu'une entreprise qui stocke des données fait faillite, la personne concernée par ces données doit pouvoir faire valoir une revendication. Les dispositions légales sur l'administration de la faillite prévoient aujourd'hui la revendication de biens meubles et la cession de créance (art. 242 LP), mais les données virtuelles ne font pas l'objet d'une réglementation. Si l'on voulait que des données puissent également être revendiquées à la suite d'une faillite, la notion de possession devrait être comprise dans un sens très large concernant les données. Aussi, il semble plus adéquat d'adapter légèrement la loi en vigueur. Le groupe de travail sur les cryptomonnaies présentera une proposition de réglementation d'ici la fin 2018.
- Perte d'appareils/de données: la perte d'appareils tels qu'un iPhone ou un iPad représente une perte économique certaine, mais qui n'est aujourd'hui plus aussi conséquente qu'avant compte tenu du prix d'achat de ces appareils. Le droit suisse met à disposition les instruments juridiques nécessaires en cas de perte

de données suite à l'intervention d'un tiers: le vol, la dépossession et la divulgation sont couverts. Mais ces instruments sont difficiles à mettre en œuvre. Les données pouvant être reproduites à volonté, le plaignant aura des difficultés à exposer précisément les faits aux autorités de poursuite pénale en cas d'obtention illicite de données par un tiers non impliqué. La perte de données à caractère non personnel qui n'est pas due à l'intervention d'un tiers ne fait pas l'objet d'une réglementation en l'état actuel du droit. On ne peut se référer au droit pénal ou au droit de la concurrence déloyale à cet égard. On peut donc se demander si les détenteurs de données ne devraient pas être mieux protégés. L'idée n'est pas de créer impérativement une propriété générale des données, mais de déterminer quelle approche réglementaire il convient d'adopter pour remédier à ce problème.

- *Web (Screen) Scraping*: cette technique consistant à obtenir des informations en prélevant des données souhaitées à partir d'autres sites web (par ex. au moyen d'un *crawler* ou robot d'indexation) pose un problème qui n'a pas encore été suffisamment abordé. Cette question concerne toutefois davantage les comportements dans un environnement concurrentiel et moins le rattachement des données aux droits réels.

Certaines situations exigent ainsi l'intervention du législateur. Nous exposons dans les deux encadrés suivants comment les régimes juridiques existants peuvent être remplacés moyennant les compléments correspondants.

Aspects positifs du droit de propriété (droits de disposition)	**Données personnelles**	**Données techniques**
Possession de la chose	• Autodétermination en matière d'information (effet limité) • Droit des successions: norme spécifique dans le P-LPD • Droit des faillites: situation juridique à clarifier	• Droits de propriété intellectuelle, par ex. LBI et LDA, lorsque les conditions sont remplies (degré d'inventivité et créativité intellectuelle) • Protection du savoir-faire (plus forte dans l'UE qu'en CH) • Protection des détenteurs de banques de données (dans l'UE, bien que contestée; pas en CH, seulement art. 5, let. c, LCD) • Les idées et les informations *per se* ne sont pas protégées • Droit des faillites: situation juridique à clarifier
Utilisation de la chose	• Autodétermination en matière d'information	• Droits de propriété intellectuelle, par ex. LBI et LDA,

	(effet limité) • Droit de la possession (effet limité)	lorsque les conditions sont remplies (degré d'inventivité et créativité intellectuelle) • Protection du savoir-faire (plus forte dans l'UE qu'en CH) • Protection des détenteurs de banques de données (dans l'UE, bien que contestée; pas en CH) • Les idées et les informations *per se* ne sont pas protégées
Disposition de la chose	Transmission des données: • Contrat de vente ou de licence • Portabilité des données (art. 20 RGPD, pas dans le P-LPD) Perte des données: pas de réglementation	Transmission des données: • Contrat de vente ou de licence, si prévu dans le droit de la propriété intellectuelle • Portabilité des données conformément à l'art. 6 du règlement de l'UE (COM 2017 495 final) Perte des données: pas de réglementation

Aspects négatifs du droit de propriété (droits de défense)	**Données personnelles**	**Données techniques**
Revendication de la chose	Droit d'accès de la LPD	Droits d'accès aux données: prévus dans le projet de règlement de l'UE (10 janvier 2017, COM (2017) final, 9, 12 ss); question toujours ouverte en Suisse
Défense contre les atteintes	Protection de la personnalité prévue par le CC Protection de la personnalité prévue par le P-LPD	Protection prévue par la LCD (le cas échéant)

	Réserve: consentement (révocable) de la personne concernée	

Conclusion:

Comme nous l'avons exposé au ch. 7.2.6.1, si l'on renonce, comme escompté, à introduire une propriété des données, certaines lois devront être adaptées. Ces adaptations permettront de combler des lacunes spécifiques en matière de réglementation du traitement numérique des données et de garantir ainsi la sécurité du droit.

Concernant le traitement des données en cas de faillite, la LP doit prévoir une nouvelle norme autorisant la revendication de données (au même titre que d'autres biens matériels).

Le droit des héritiers d'une personne décédée d'obtenir les données de cette personne doit être réglementé dans le CC ou la LPD.

La portabilité des données est un concept qu'il convient d'introduire dans le contexte du droit d'accès, dans la mesure où elle se justifie. Les évolutions en la matière sur le plan international doivent être observées avant d'introduire de nouvelles normes dans le droit suisse.

7.2.6.2 Décision de principe concernant la réglementation

Les exemples susmentionnés montrent qu'en l'état, le fait qu'une propriété des données ne soit pas prévue dans le droit suisse engendre un certain vide juridique, car les institutions juridiques «traditionnelles» ne tiennent pas suffisamment compte du caractère virtuel des données. Ces exemples n'appellent toutefois pas la création conséquente d'une propriété des données en tant que nouveau cadre juridique. Dans certaines situations, des droits absolus pourraient offrir une plus grande sécurité juridique, sans toutefois remédier entièrement aux problèmes qui se posent.

Il importe plutôt d'examiner si, dans le sens des réflexions faites plus haut, des adaptations législatives ponctuelles et spécifiques suffiraient à créer la protection juridique souhaitée sans engendrer les conséquences indésirables évoquées. Le législateur dispose ici d'un très grand pouvoir discrétionnaire.

Recommandation:

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.

7.3 Nouveaux enjeux liés à la responsabilité

7.3.1 Enjeux numériques pour le droit de la responsabilité

L'Internet des objets (IdO) est un nouveau réseau établi sur Internet qui a été créé initialement pour les relations d'affaires, mais qui, de plus en plus, sert également des

intérêts privés. Il est très pratique dans le secteur de la santé, parce que les données sont non seulement très abondantes, mais aussi très sensibles. Or l'apparition d'un dysfonctionnement sur ce réseau (par ex. à la suite d'une erreur de conception, d'une erreur de fabrication ou d'une mauvaise manipulation) peut avoir deux conséquences (négatives):

- Des données peuvent être perdues ou illégalement divulguées. Au niveau juridique, la question du respect du droit à la protection et à la sécurité des données entre en ligne de compte.
- Des dommages physiques peuvent être causés, tels que l'explosion d'appareils interconnectés ou la détérioration de produits tiers (par ex. lorsque des aliments s'avarient dans un réfrigérateur hors service).

En raison de la multitude de personnes impliquées – notamment les acteurs du marché – dans les structures de l'IdO et de leurs interdépendances, il est souvent difficile de trouver le/la ou les responsable(s) du dysfonctionnement. Dans le cas d'un réfrigérateur qui explose, il peut s'agir du fabricant de l'appareil, de l'exploitant du réseau, du développeur du logiciel ou du client qui a fait une erreur de manipulation.

Systèmes autonomes

Les systèmes autonomes – par ex. les robots industriels, les robots utilisés dans le secteur médical, les voitures sans conducteur et les drones – engendrent des problèmes encore plus complexes en matière de responsabilité. Ce qui les distingue d'autres types de systèmes est leur capacité d'analyser et d'interpréter, de manière autonome, une chose ou une situation, et, en se basant sur les résultats de ces analyses et de ces interprétations, d'agir ou de réagir plus ou moins correctement.

Le droit de la responsabilité part du principe que l'homme peut exercer un contrôle, que ce soit sur son propre comportement, sur un produit qu'il a fabriqué ou qu'il propose ou sur le déploiement de certaines activités. Avec les systèmes autonomes, il est souvent difficile de déterminer à qui revient la traditionnelle «fonction de contrôle». Dans le cas d'une voiture sans conducteur, la responsabilité du dysfonctionnement pourrait revenir au fabricant, au fournisseur de pièces détachées ou au développeur de l'un des nombreux logiciels intégrés au système.

La plupart des systèmes juridiques reconnaissent ce que le droit suisse appelle la responsabilité à raison du risque: toute personne créant un état «dangereux» ou réalisant une opération «dangereuse» a la responsabilité de prendre les précautions qui s'imposent pour éviter des dommages. Contrairement à celle créée par une centrale nucléaire ou par un véhicule, la menace créée par les robots est plus difficile à évaluer.

Importance de la sécurité de l'information dans certains marchés

La sécurité de l'information est très importante non seulement dans le contexte de l'IdO et des systèmes autonomes, mais aussi, d'une manière générale, en lien avec le traitement et la transmission de données. Les exigences en matière de sécurité de l'information sont complexes à cet égard, car les produits et les services font intervenir des données à de nombreux niveaux, notamment à ceux de la collecte et du traitement des données, du développement de logiciels (qu'ils soient intégrés aux produits ou

pas), des applications (multitude d'applications Internet), et des capteurs et des actionneurs. L'imputation de la responsabilité est aujourd'hui déjà problématique dans certains domaines, par ex. dans le contexte de l'informatique en nuage (*cloud computing*) ou de l'externalisation (*outsourcing*). Par ailleurs, les bases juridiques régissant la sécurité de l'information ne sont pas fortement développées. Les exigences en la matière reposent davantage sur diverses autorégulations élaborées par des associations de branches professionnelles. Ces régulations sectorielles offrent l'avantage d'être orientées sur la technologie et d'être flexibles. Par contre, leur caractère contraignant et leur mise en œuvre ne sont pas toujours garantis (exemples: ISO IEC 27000f, abrégé sur la protection dans le domaine des technologies de l'information publiée par l'Office fédéral allemand pour la sécurité en matière de technologies de l'information [BSI], etc.).

7.3.2 Faiblesses du droit actuel de la responsabilité

La plupart des régimes de responsabilité appliqués dans les pays européens distinguent quatre types de responsabilité, à savoir la responsabilité contractuelle, la responsabilité délictuelle, la responsabilité à raison du risque et les responsabilités dites «spéciales».

7.3.3 Responsabilité contractuelle

La responsabilité contractuelle est régie par le droit des contrats. Les faiblesses législatives en la matière sont aujourd'hui partiellement reconnues, notamment pour ce qui est de définir la conformité des contenus numériques réglés par contrat. L'UE prévoit d'ailleurs de prendre des dispositions face à cette problématique.

Les «contrats intelligents» (de l'anglais *smart contracts*) soulèvent eux aussi de nouveaux défis en ce qui concerne l'organisation des voies de recours. En raison de l'absence d'intermédiaires sur la blockchain, le code de programmation (auto-exécutable) doit contenir une solution prédéfinie (par ex. un mécanisme de conflit) lorsque des dispositions contractuelles ne sont pas respectées. L'utilisation d'une interface technologique (généralement connue sous le nom d'«Oracle»), servant de point de contact entre la blockchain et le monde réel, devrait également permettre l'intervention d'une instance arbitrale en cas de conflit (voir ch. 9.3.5 let. a).

En raison de l'importance croissante du langage des contrats dans le code de programmation, les frontières entre la responsabilité contractuelle, la responsabilité délictuelle et la responsabilité du fait des produits ont tendance à s'estomper. L'utilisateur et le fournisseur d'un bien virtuel sont certes liés par une relation contractuelle, mais celle-ci ne s'étend pas à la personne qui a développé le code de programmation (selon l'arrangement contractuel). C'est pourquoi, en cas de dysfonctionnement, l'utilisateur ne peut faire valoir que des droits non contractuels.

7.3.4 Responsabilité délictuelle

La responsabilité délictuelle (art. 41 CO) régit les situations où une personne cause, d'une manière illicite, un dommage prévisible à autrui, soit intentionnellement, soit par négligence. Elle laisse généralement supposer qu'il y a eu violation du devoir (standardisé) de diligence.

Dans le domaine technologique, ce type de responsabilité est associé à une problématique importante. En effet, il est souvent difficile de savoir, pour le fournisseur d'un produit ou d'un service, quels tiers peuvent être lésés par un éventuel dysfonctionnement du produit ou du service fourni. Il devient dès lors très complexe d'évaluer la zone de risque sur la base du devoir de diligence tel que nous le connaissons habituellement. Les produits de l'IdO ainsi que les systèmes autonomes sont également concernés par cette problématique.

Par ailleurs, le fournisseur d'un produit de l'IdO ou d'un système autonome ne peut souvent pas déterminer l'impact qu'auront les différentes composantes du produit ou du système mises à disposition par un tiers sur le produit ou système livré à l'utilisateur. Or les contrats excluent souvent toute responsabilité pour les composantes fournies par des tiers. Par conséquent, l'utilisateur lésé ne pourra invoquer qu'une responsabilité non contractuelle et devra donc réunir lui-même toutes les preuves nécessaires pour faire valoir ses droits à réparation.

7.3.5 Responsabilité à raison du risque

7.3.5.1 Responsabilité du fait des produits

Les États membres de l'UE ont réglementé la responsabilité du fait des produits à la fin des années 80, sur la base de la directive 85/347/CEE. La Suisse leur a emboîté le pas en adoptant, le 18 juin 1993, la loi fédérale sur la responsabilité du fait des produits (LRFP). On parle ici de responsabilité indépendante de la faute (responsabilité causale).

L'application du droit de la responsabilité du fait des produits est problématique pour les produits et les services basés sur des données dans la mesure où ce droit ne prévoit en principe que des dommages causés par des biens physiques. Par produits, on entend toute chose mobilière ainsi que l'électricité (art. 3 LRFP). Les biens virtuels comme les données n'entrent donc pas dans le champ d'application du droit de la responsabilité du fait des produits. Les activités commerciales relevant de l'IdO impliquent le plus souvent des livraisons de biens physiques. Toutefois, ce ne sont généralement pas ces biens qui sont à l'origine des dommages, mais les logiciels utilisés dans la chaîne d'approvisionnement ou le traitement/la réutilisation des données de base. Or ces éléments ne sont pas physiques et ne constituent donc pas des produits. Il en va de même pour les systèmes autonomes, comme l'illustre l'exemple de la voiture sans conducteur: un accident se produisant avec ce type de véhicule sera plus probablement dû à une faille liée aux données ou à une erreur logicielle qu'à une erreur de construction.

En outre, la notion courante de «défaut» se concrétise difficilement dans le contexte des biens virtuels. Aux termes de l'art. 4 LRFP, un produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre compte tenu de toutes les circonstances. Outre le fait qu'en pratique, on ne peut rarement savoir précisément à quel niveau de sécurité l'utilisateur s'attend, il est également difficile de prouver le lien de causalité à l'origine du «défaut».

Au regard des récentes évolutions technologiques, l'UE a reconnu la nécessité d'adapter la responsabilité du fait des produits telle que nous la connaissons aujourd'hui. Aussi, le 25 avril 2018, la Commission européenne a publié les résultats détaillés de

la consultation sur l'adaptation de la directive 85/347. Le législateur suisse devrait adopter une approche similaire.

7.3.5.2 Responsabilité de la sécurité des produits

Quelques années après que l'UE a arrêté la directive 2001/95/UE relative à la sécurité générale des produits, la Suisse a elle aussi réglementé cette question en adoptant la loi fédérale du 12 juin 2009 sur la sécurité des produits (LSPro). Aux termes de l'art. 2 de la LSPro, est réputé produit au sens de cette loi tout bien meuble prêt à l'emploi. Les biens virtuels ne sont donc pas pris en considération, comme dans le contexte de la responsabilité du fait des produits.

Les dispositions du droit sur la sécurité des produits ne sont vraisemblablement plus tout à fait adaptées, en particulier suite à l'émergence des systèmes autonomes. Il faut donc se demander si l'on peut appliquer ces dispositions par analogie dans le contexte des nouvelles technologies et parvenir ainsi à des solutions satisfaisantes ou s'il convient plutôt d'envisager d'adapter la loi en vigueur.

7.3.5.3 Conclusion

Le droit réglementant la responsabilité du fait des produits et la responsabilité de la sécurité des produits n'est pas adapté au contexte des biens virtuels, et ce pour plusieurs raisons, notamment la nature virtuelle du produit (données), l'absence de normes définissant le «défaut» pour ce type de bien et la difficulté d'établir des liens de causalité. De plus, certains éléments de la responsabilité de la sécurité des produits semblent aujourd'hui également inadaptés au contexte de l'intelligence artificielle et des systèmes autonomes.

7.3.6 Responsabilités spéciales

7.3.6.1 Responsabilité des prestataires

La directive 2000/31/CE sur le commerce électronique contient des dispositions traitant spécifiquement de la responsabilité des fournisseurs Internet (art. 12 à 15). Le niveau de responsabilité des fournisseurs Internet dépend de leur niveau d'implication dans l'organisation du contenu des informations qu'ils mettent à disposition: plus ils se limitent au seul déroulement technique des communications électroniques, moins leur responsabilité est engagée.

La Suisse n'a pas de réglementation de ce type. Dans son rapport très détaillé du 11 décembre 2015 sur la responsabilité civile des fournisseurs de services Internet, le Conseil fédéral ne considère pas qu'il soit nécessaire d'intervenir immédiatement à cet égard, ce qui est pourtant jugé parfois différemment dans la doctrine. Il existe cependant déjà un certain nombre d'autorégulations spécifiques dans ce domaine.

7.3.6.2 Responsabilité de la protection des données

Les obligations qui incombent à chaque personne traitant des données sont considérablement plus nombreuses avec le nouveau RGPD et la révision de la LPD. Il s'agit pour la plupart d'obligations visant la protection des données pertinentes au regard du

droit de la surveillance. En cas de violation de ces obligations, il est possible de faire valoir des prétentions civiles, car les bases juridiques existent déjà à cet effet.

En l'occurrence, la responsabilité civile repose sur un contrat ou sur un délit. Le droit de surveillance présente l'avantage que l'aspect de l'illicéité est examiné dans le cadre d'une procédure officielle et qu'il peut ensuite servir de base à la revendication de droits dans le cadre d'une procédure civile. Il faut donc s'attendre à une augmentation du nombre de procédures de ce type. On ne prévoit pas qu'il soit nécessaire d'adopter de nouvelles mesures réglementaires dans ce domaine, hormis la loi révisée sur la protection des données.

7.3.6.3 Responsabilité de l'infrastructure numérique

L'UE a adopté en 2016 la directive 2016/1148/UE concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Cette directive prévoit que les États membres de l'UE prennent plusieurs mesures d'ici 2018 pour améliorer les infrastructures numériques, au niveau tant des perturbations que des attaques de tout type commises par des tiers (cybersécurité). Même si les prescriptions initiales de la Commission européenne ont été partiellement allégées dans le texte final, il ne fait pas de doute que la transposition de cette directive dans le droit national des États membres permettra d'améliorer le niveau de sécurité des infrastructures numériques.

En Suisse, les prescriptions de la législation sur les télécommunications vont beaucoup moins loin que celles de la directive 2016/1148/UE. Le législateur doit donc déterminer dans quelle mesure les règles en vigueur dans le droit suisse doivent être conçues de manière autonome (voir ch. 8.2.3.1).

7.3.7 Nouveaux concepts de responsabilité

Dans le cadre d'une communication et d'un document de travail circonstancié des services de la Commission publié en janvier 2017, l'UE propose d'examiner – et, le cas échéant, d'appliquer – de nouveaux concepts de responsabilité. Trois thèmes sont ainsi mis en avant, à savoir les obligations de diligence et l'attribution de la responsabilité, les modèles de gestion des risques et les solutions d'assurances facultatives ou obligatoires.

7.3.7.1 Obligations de diligence et attribution de la responsabilité

Eu égard aux défis posés par la responsabilité délictuelle en particulier, les entreprises ont aujourd'hui déjà l'obligation d'élaborer des stratégies et de mettre en œuvre des mesures pour réduire les risques liés à la sécurité de l'information dans leurs propres systèmes et dans leurs relations d'affaires avec des tiers. Les exigences en la matière sont déjà plus ou moins bien respectées par les entreprises. On parle souvent de «gestion du risque d'entreprise» (de l'anglais *enterprise risk management*). Dans ce contexte, la sensibilisation et la formation des collaborateurs prennent toujours plus d'importance pour soutenir l'adoption de mesures techniques de prévention.

Les entreprises prennent également des mesures d'autorégulation pour réduire les risques, par exemple concernant l'utilisation des outils électroniques (iPhone, iPad, etc.). Ces dispositions peuvent les aider à évaluer comment les risques sont répartis

en cas de sinistre. La mise en œuvre de mesures préventives aide ainsi les entreprises à réduire les risques.

7.3.7.2 Modèles de gestion des risques

Au-delà des obligations de diligence et de l'attribution de la responsabilité, l'UE propose d'introduire des mesures spécifiques concernant des modèles de gestion des risques : les fournisseurs de biens et de services doivent mettre en œuvre un certain nombre de mesures visant à écarter ou réduire les risques en fonction de l'ampleur du risque qu'ils créent pour la sécurité de l'information.

Pour ce qui est la répartition des tâches dans ce domaine, l'UE propose de reprendre le concept économique – créé il y a plusieurs décennies déjà – du *cheapest cost avoider*, qui désigne la personne ou l'entité qui peut réduire les frais au meilleur coût. Selon ce principe, celle qui sera tenue de prendre des mesures pour écarter les risques menaçant la sécurité de l'information sera celle pour qui ces mesures impliqueront le moins de coûts. Il peut également s'agir de l'utilisateur s'il peut contribuer facilement à la sécurité de l'information.

7.3.7.3 Solution d'assurance facultative ou obligatoire

Une autre option envisagée par l'UE consiste à introduire une solution d'assurance facultative ou obligatoire. Cette solution vise à dédommager la personne (en particulier le consommateur final d'un produit) qui a subi un (important) préjudice, sans qu'une indemnité ne soit versée par le responsable du préjudice, soit parce que ce dernier ne peut être désigné en raison de la complexité des relations économiques en jeu, soit parce que, compte tenu des circonstances, la personne lésée ne peut s'acquitter de la charge de la preuve. Il est actuellement difficile de savoir si cette solution trouvera un soutien suffisant dans le cadre de la consultation en cours. Quoi qu'il en soit, si cette approche était poursuivie, plusieurs questions devraient encore être examinées en détail, notamment aux niveaux technique et économique.

7.3.7.4 Perspectives

Le 25 avril 2018, la Commission européenne a publié une série de documents qui doivent servir de base au débat relatif à l'élaboration de dispositions juridiques réglementant la libre circulation des données et la responsabilité en matière d'intelligence artificielle. Elle n'a pas proposé de mesures concrètes, mais elle a souligné que les principes éthiques devaient être mieux respectés. On ignore en l'état quel concept de responsabilité, parmi ceux présentés plus haut, sera mis en œuvre.

Recommandation:

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.

8 Champ d'analyse relations entre l'État et les citoyens ou les entreprises (G2Ci/B)

8.1 Introduction

Tâches de protection de l'État

Depuis que les acteurs étatiques ont découvert le cyberespace comme nouvelle sphère d'opération, le traitement des données et la sécurité de l'information sont exposés à des risques de plus en plus importants.

Il faut partir de l'idée que les futurs conflits militaires seront de nature hybride et que des moyens numériques offensifs seront mis en œuvre à tous les niveaux, y compris sous la forme de campagnes de désinformation. Toutefois, par manque de temps et de ressources, le groupe d'experts a décidé de ne pas approfondir ce scénario particulier et renvoie à ce sujet au rapport 2017 sur la politique de sécurité de la Suisse ainsi qu'aux analyses de l'armée dans le domaine de la cyberdéfense.

Les activités étatiques dans le cyberespace (espionnage et sabotage) soulèvent des questions de plus en plus pressantes: comment, à partir de quel niveau d'escalade et dans quelle mesure l'État doit-il assumer des tâches de protection de la société, comme le prévoit notamment l'art. 2 de la Constitution? Citons ici l'espionnage pratiqué par des services de renseignement, l'instrumentalisation d'entreprises informatiques, ainsi que le dossier de l'accord *Safe Harbor*, remplacé aujourd'hui par l'accord *Privacy Shield*. Enfin, la cybercriminalité organisée met de plus en plus péril la transformation numérique, dans un contexte où il est chaque jour plus difficile de distinguer, parmi les cybercriminels, entre acteurs étatiques, paraétatiques et non étatiques.

Le cyberespace étant perçu comme une extension de l'espace public et privé traditionnel, on peut se demander comment l'État peut y remplir ses tâches (protection de la liberté et de la sécurité, égalité des chances, prospérité, ordre international juste et pacifique).

La conception des obligations de protection de l'État à l'égard de la société et de ses moyens d'action dans ce domaine, notamment la possibilité d'intervenir dans la sphère privée des individus, est un autre aspect clé des relations entre l'État et les citoyens. Durant l'élaboration du présent rapport, deux thèmes de première importance étaient en discussion dans le domaine de la sécurité de l'État en Suisse, à savoir la surveillance de la correspondance par poste et télécommunication et les activités de renseignement, objets respectivement de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et de la nouvelle loi fédérale du 25 septembre 2015 sur le renseignement (LRens). L'essentiel de la discussion portait sur la question centrale suivante: dans quelle mesure la sphère privée de l'individu peut-elle être restreinte dans l'intérêt de l'ensemble de la société? Toutefois, comme cette question n'est pas en rapport direct avec l'évolution technologique ni avec le traitement des données, mais relève plutôt de décisions à prendre dans le domaine de la politique de sécurité, le groupe d'experts a décidé de ne pas l'approfondir. Il souligne néanmoins le potentiel d'utilisation abusive que recèlent les technologies au service du pouvoir.

L'État en tant que prestataire de services (cyberadministration) et promoteur d'une culture du libre accès aux données publiques

L'État se doit de créer les conditions nécessaires pour que la société dispose d'un accès aux données sûr, performant et stable (par ex. au moyen d'un réseau à haut débit), sans lequel il ne peut y avoir de traitement moderne des données ni de société numérique. De plus, il s'agit également pour l'État, dans ses relations avec les citoyens, de fournir des prestations officielles sous forme numérique (cyberadministration), parmi lesquelles des services de base tels que l'identité électronique (e-ID).

D'énormes quantités de données sont collectées en permanence et de plus en plus centralisées. Or le contrôle de ces données est actuellement exercé non pas par des organismes de recherche publics ou par l'État lui-même, mais de plus en plus par des privés, en particulier par les portiers d'Internet: Google, Apple, Facebook et Amazon (appelés aussi les GAFA), ainsi qu'Alipay/Alibaba. Bien que le droit n'ait jusqu'ici pas clarifié uniformément les notions de propriété et de possession des données, celles-ci sont aujourd'hui traitées, dans la plupart des cas, comme un bien en propriété et stockées dans des silos appartenant aux entreprises qui les contrôlent. Il s'ensuit qu'elles ne sont pas à la disposition d'une recherche (publique) indépendante, ni par conséquent de la société, mais servent des groupes d'intérêts privés aux motivations purement économiques. Les entreprises concernées profitent ainsi d'avantages en matière à la fois de développement et de concurrence: elles gagnent en compétitivité et peuvent promettre une utilité et un confort accrus aux consommateurs et aux utilisateurs. Le débat en cours sur le développement numérique de l'économie a cependant montré que ces silos de données sont aussi de nature à entraver l'innovation.

Il est donc d'autant plus important de trouver un nouvel équilibre favorisant le libre accès aux données, fondé sur une juste pesée des intérêts de la société, de l'économie et des entreprises liées à la Confédération. Les questions de l'accès aux données et des flux de données ouverts en droit privé ont été examinées au ch. 7.1. L'accès aux données publiques et aux données des services liés à la Confédération est traité ci-après, dans le chapitre «Libre accès aux données publiques et données ouvertes» (cf. ch. 8.5). Enfin, le présent rapport examine également si l'actuelle LTrans permet à l'État de remplir ses obligations d'information vis-à-vis des citoyens.

État et démocratie 2.0

La transformation numérique modifie les flux de données et d'informations. Il en résulte certes des chances pour la démocratie, grâce aux possibilités de participation directe et de meilleure information des citoyens, mais aussi des risques: les technologies numériques permettent, comme jamais jusqu'ici, de manipuler les masses sur une base individuelle. Les citoyens sont exposés à un flot d'informations falsifiées, unilatérales, non vérifiées et non vérifiables, si bien qu'il est difficile pour eux de se former une opinion aussi fondée que possible et de prendre des décisions sans être sous influence. La situation des médias et leur avenir en tant que quatrième pouvoir sont appelés à jouer un rôle important dans ce domaine.

8.2 Tâches de protection de l'État

8.2.1 Situation actuelle, évolution, chances et risques

L'un des principaux éléments constitutifs de la souveraineté numérique est le droit de contrôler le cyberespace et d'y assurer, outre la sécurité et le respect du droit national, la protection des organes de l'État ainsi que celle de tous les membres de la société, y compris leur droit à l'autodétermination, leur dignité humaine et leurs valeurs. Or le fait qu'Internet n'a pas de structure territoriale et repose fondamentalement sur l'idée d'ouverture complique singulièrement l'application de ces principes régaliens. Il est certes relativement facile de bloquer la libre circulation des données sur Internet, et nombre d'États autoritaires se sont d'ailleurs donné les moyens d'y contrôler les échanges d'informations. Il est cependant nettement plus difficile de faire en sorte que les flux de données circulent dans des conditions de sécurité accrues, sans pour autant limiter les possibilités d'information et de développement des citoyens. Toute entrave préventive à ces flux – par ex. contrôle des maliciels ou prévention de l'exfiltration de données – remet en effet en question les principes fondamentaux régissant Internet, en particulier celui de la libre circulation des données.

Les cyberattaques qui ont visé l'Estonie ainsi que le réseau d'approvisionnement en électricité et les infrastructures numériques de l'Ukraine, fin 2015, ont mis en évidence l'existence de nouveaux cyberrisques. Les attaques étaient massives et ont causé des dommages considérables – en Ukraine, un quart de million de personnes ont été privées d'électricité pendant plusieurs heures –, mais il est impossible d'en désigner clairement les auteurs. Les indices portant vers des acteurs russes n'ont fait que renforcer le climat de menace qui règne dans la région, augmentant en outre par des moyens peu diplomatiques les pressions politiques exercées sur l'Ukraine. De nombreux experts considèrent que l'attaque contre le réseau électrique ukrainien était un test visant à étudier la possibilité de pirater les infrastructures critiques d'autres États, afin de les paralyser et de provoquer un sentiment d'insécurité au sein de la population.

Compte tenu de cette évolution et de la dépendance croissante des infrastructures critiques vis-à-vis des infrastructures numériques, l'État se doit de réexaminer ses dispositifs de défense, tant préventive que réactive. Il s'agit en particulier de réduire le risque de cyberattaques susceptibles d'impacter la société à l'échelle nationale, mais aussi, si une telle attaque survient malgré tout, d'en limiter les dommages grâce à des systèmes résilients et de garantir le maintien de la capacité d'agir de l'État.

L'attribution de la responsabilité des cyberattaques est d'autant plus difficile qu'il est chaque jour plus compliqué de distinguer parmi les cybercriminels, peu importe qu'ils agissent sur ordre ou se servent des ressources et du savoir-faire disponibles à leurs propres fins, entre acteurs étatiques, paraétatiques et privés. De plus, les arsenaux d'armes numériques des services secrets et des services de l'armée représentent une menace croissante, dans la mesure où ces services s'en servent en exploitant les failles du contrôle de l'État. Les milieux des services de renseignement civils et les milieux militaires se mélangent et ce sont les acteurs criminels qui en tirent profit. C'est ainsi que la cybercriminalité a augmenté de manière exponentielle ces trois dernières années.

Les limites fluctuantes entre groupes d'acteurs et l'absence d'adversaire identifiable rendent difficile, même en cas d'attaque précise contre des infrastructures critiques,

d'évaluer à partir de quand on a affaire à une situation particulière relevant du cyberespace. Il faut en outre se demander à partir de quels niveaux d'escalade les autorités civiles ou l'armée doivent fournir leur aide à titre principal ou à titre subsidiaire. À cet égard, les nouvelles compétences et les nouvelles ressources devront être mises en place de manière à ce qu'il ne soit pas nécessaire de modifier les principes qui ont déjà fait leurs preuves dans ce domaine.

Les révélations d'Edward Snowden et de WikiLeaks ont débouché sur une prise de conscience générale du fait que les services de renseignements et d'autres autorités étatiques se servent de la numérisation et des nouvelles possibilités techniques qui en découlent pour collecter des données à large échelle et les stocker. La menace d'un tel espionnage massif de particuliers et de services de l'État en Suisse constitue une grave violation de la souveraineté de notre pays. Ce risque s'est en outre accentué dans la mesure où certains pays peuvent demander – et demandent effectivement – à leur industrie informatique, par des voies légales ou d'une autre manière, de ne pas respecter leurs obligations de maintien du secret vis-à-vis de leurs clients, peu importe que ces obligations soient convenues contractuellement ou prescrites par la loi. Il s'ensuit que dans l'environnement déjà difficile de la cybersécurité, il n'est plus possible de faire entièrement confiance à ses partenaires de sécurité et à ses partenaires commerciaux du secteur informatique, pas même à ceux connus de longue date. La chaîne d'approvisionnement (de données) devient ainsi un facteur d'insécurité.

Il faut également partir du principe que dans certains pays, l'État ou des acteurs proches de l'État poussent sciemment l'industrie technologique nationale à s'approprier illégalement des contenus protégés par des droits de propriété intellectuelle ainsi que des données commerciales critiques d'entreprises étrangères, tout en participant activement à la défense de leurs propres entreprises et à la surveillance des fuites de données. Certes, les services de renseignement et les militaires de ces pays soutenaient déjà leur industrie nationale à l'ère analogique, mais aujourd'hui, à l'ère numérique, les actes d'espionnage se multiplient dans le cyberespace, en raison des avantages dont profitent leurs auteurs (attribution difficile, diversité des possibilités d'attaque, accès à distance). Lorsqu'il s'agit d'espionnage industriel, il peut même en résulter des distorsions de la concurrence.

Le nouvel accord *Privacy Shield* conclu entre l'UE et les États-Unis, qui a remplacé l'accord *Safe Harbour* après que la Cour de justice de l'UE l'a déclaré non valide, est un progrès. Grâce aux principes régissant le nouvel accord, les données transmises aux États-Unis sont techniquement mieux protégées dans les entreprises participantes. La Suisse est parvenue à négocier l'application d'un régime similaire avec les États-Unis. Cette nouvelle solution est certes très critiquée – elle n'apporterait aucun progrès de fond en relation avec la question très sensible de la surveillance de masse –, mais la marge de manœuvre dont dispose la Suisse pour exiger davantage de protection est limitée. Il est donc préférable qu'elle s'en tienne à l'approche suivie jusqu'ici, à savoir s'inspirer de la politique de l'UE, car cela lui garantit au moins un certain pouvoir de négociation.

L'État dispose de plusieurs possibilités et instruments pour améliorer la protection de la société contre les cyberrisques. Citons en particulier la définition et l'application de normes de sécurité, l'adoption d'obligations de notification, la création d'une organisation centralisée de soutien et d'information en cas d'incidents de sécurité, le soutien aux entreprises et aux organismes de recherche en matière de contrôle de la sécurité des chaînes de livraison et des fournisseurs en relation avec les infrastructures numériques et, enfin, le recours à l'armée. Les instruments et les objectifs à atteindre doivent

être opportunément adaptés aux divers groupes cibles, qui vont des infrastructures critiques ou hautement critiques aux institutions de recherche et à l'économie privée, en passant par les services en ligne importants. Depuis un an et demi, ces possibilités et instruments de l'État font l'objet de discussions controversées.

8.2.2 Évolution à l'étranger

La menace croissante inhérente au cyberespace et la forte dépendance d'équipements critiques vis-à-vis des infrastructures numériques ont poussé de nombreux pays à réglementer, à définir des normes, à adopter des obligations de notifier et à créer des organisations centralisées. En collaboration avec le DFAE, le groupe d'experts a réalisé une étude comparative incluant les pays voisins de la Suisse, l'UE, les États-Unis, la Chine ainsi que certains pays scandinaves et asiatiques (cf. synthèse de l'étude à l'annexe 4).

Au cours des trois dernières années, les pays à régime autoritaire ont adopté des réglementations très strictes, ce qui n'est guère surprenant. C'est ainsi que les infrastructures critiques et toutes les infrastructures numériques considérées comme importantes y sont soumises à des normes de sécurité de l'information et à des obligations de notifier. Aux États-Unis, avec le cadre de cybersécurité du *National Institute of Standards and Technology* (NIST), on a adopté une «quasi-norme» relativement détaillée applicable aux infrastructures critiques. Bien qu'elles n'aient pas explicitement force obligatoire, les propositions faites en matière de sécurité exercent une certaine pression, conjointement avec différentes lois fédérales et lois des États de l'Union, ce qui permet à l'administration d'imposer des règles aux exploitants privés.

En Europe, la norme déterminante est la directive NIS, qui est entrée en vigueur en août 2016. Elle vise à garantir un niveau élevé de sécurité des réseaux et des systèmes d'information au sein de l'UE. Chaque État membre est tenu de désigner un point de contact national unique, de disposer de centres de réponse aux urgences informatiques (*computer emergency response team*, CERT) et d'identifier les entreprises qui font partie des infrastructures numériques critiques. Ces entreprises doivent définir des mesures techniques de protection appropriées (normes de sécurité) et notifier tous les incidents de sécurité. Ces exigences s'appliquent aussi aux fournisseurs de services numériques importants (informatique en nuage, plateformes de recherche ou de commerce en ligne). En Allemagne, les associations professionnelles souhaitent que la nouvelle loi sur la sécurité informatique étende le champ d'application de la réglementation NIS à toutes les entreprises. La mise en œuvre de la directive NIS va se traduire par le développement à large échelle d'une véritable culture de la gestion des risques informatiques chez tous les exploitants d'infrastructures critiques et fournisseurs de services en ligne importants.

Quelles que soient les mesures adoptées, l'élargissement du cercle des destinataires du soutien de l'État et des assujettis à la réglementation joue un rôle décisif. En incluant les fournisseurs de services numériques (informatique en nuage, plateformes de recherche ou de commerce en ligne), la directive NIS tient compte de la transformation numérique et oblige de nouveaux acteurs de première importance à contribuer à la sécurité de l'approvisionnement. La directive visait précédemment surtout les gros prestataires que sont Google, Amazon, Facebook et Apple (GAFA). L'élargissement de son champ d'application entraîne désormais aussi une difficulté de délimitation: quelle doit être la marge de manœuvre en matière de définition des services numé-

riques? Des dérogations sont prévues pour les petites entreprises et les microentreprises. Malgré ces restrictions *de minimis*, sont assujetties les entreprises comptant plus de 50 collaborateurs et dont le chiffre d'affaires s'élève à au moins 50 millions d'euros. La directive s'applique donc aussi aux PME les plus importantes exploitant un portail en ligne pour clients B2B.

De nombreuses mesures relevant de la réglementation NIS ont d'ores et déjà contribué à améliorer la cybersécurité. Il s'agit cependant d'en évaluer plus précisément les avantages et les inconvénients, en particulier pour ce qui est de l'obligation de notifier. Dans quelques pays, le nombre de notifications a en effet notablement diminué. Les entreprises y font manifestement preuve de retenue, car elles craignent de nouvelles interventions réglementaires et une inutile déstabilisation du marché.

8.2.3 Normes de sécurité, standards et bonnes pratiques

8.2.3.1 Dans le domaine des infrastructures critiques

La stratégie nationale pour la protection des infrastructures critiques et la stratégie nationale de protection de la Suisse contre les cyberrisques ont déjà nettement amélioré la protection des infrastructures concernées en Suisse. Désormais, entre autres mesures, des analyses des vulnérabilités sont réalisées dans tous les secteurs critiques. La Suisse ne connaît cependant pas de dispositions générales de protection contre les cyberrisques, au sens de normes réglementaires contraignantes applicables aux infrastructures critiques. Il n'existe donc pas non plus de service centralisé disposant de compétences et de possibilités d'intervention intersectorielles, tout comme il n'existe pas d'autorité de régulation dans la plupart des secteurs.

Les éventuelles prescriptions et obligations sont réglées secteur par secteur, de manière spécifique. C'est ainsi que dans le trafic aérien et ferroviaire, où la protection et la sécurité sont prioritaires, des mesures techniques et organisationnelles sont imposées dans des prescriptions internes. Dans le secteur financier, sous la pression des cybermenaces, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a durci les prescriptions de cybersécurité arrêtées dans ses circulaires, qui ont force obligatoire. Des bases légales existent également dans le secteur des télécommunications, tandis que dans celui de l'énergie, les associations de la branche sont en train d'élaborer une solution sous la forme d'une norme. En outre, un premier inventaire des besoins en matière de normalisation et de réglementation dans les différents secteurs a été dressé, en collaboration avec les milieux économiques.

L'élaboration de normes de sécurité informatiques contraignantes et dont l'application puisse être auditée est indispensable dans tous les secteurs comportant des infrastructures critiques. Dans les autres secteurs et pour les exploitants de services en ligne importants, la nécessité de telles normes et, le cas échéant, leur niveau d'ambition doivent être soigneusement examinés.

Dans le détail, il s'agit d'accorder une plus grande attention aux points ci-dessous.

a) Il est impératif de prendre en considération les domaines suivants: énergie, transports, système financier, plateformes de négociation électroniques, système de

santé, fourniture et distribution d'eau potable, ainsi que services essentiels dans les domaines des technologies de l'information et des télécommunications[13].

b) Les exploitants d'un même secteur ne présentent pas tous le même niveau de criticité. Il s'agit donc de les différencier et d'élaborer des critères permettant de le faire.

c) Il faut examiner s'il y a lieu d'adopter une norme différente pour chaque secteur, du fait que le niveau de sécurité requis n'est pas partout le même.

d) Il faut déterminer quel service centralisé ou décentralisé peut remplir les tâches de coordination et veiller à ce que les normes soient également appliquées dans les secteurs où il n'existe pas d'autorité (de surveillance) compétente.

e) Il y a lieu de clarifier dans quelle mesure les exploitants de services numériques importants doivent être pris en considération et quelles règles *de minimis* doivent être adoptées.

f) Enfin, il s'agit d'examiner quelles bases légales sont nécessaires. Elles peuvent être propres à chaque secteur ou former un cadre légal général, comme en Allemagne et en France.

Ces travaux doivent être réalisés en collaboration entre les autorités, les associations et l'économie privée, et se fonder sur des cadres normatifs connus ainsi que sur les résultats des analyses des vulnérabilités. Dans les secteurs où il n'existe pas d'autorité de surveillance, les normes de sécurité informatiques nécessaires devraient être élaborées par les associations professionnelles concernées. La procédure de surveillance du respect des normes doit aussi être réglée à l'échelle du secteur. Enfin, la Confédération doit créer un centre de compétence en matière de cybersécurité, dont la mission sera d'accompagner ces travaux ainsi que de conseiller et d'assister les autorités de surveillance de la protection des données.

Recommandations

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.

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.

8.2.3.2 Dans le domaine de l'économie en général

Les infrastructures numériques en général doivent atteindre un niveau de maturité plus élevé que ce n'est le cas aujourd'hui. Cela vaut dans la même mesure pour les organisations et les organismes de recherche que pour l'économie privée, y compris pour les PME. Dans ce contexte, l'adoption – à titre de bonnes pratiques – de normes de sécurité informatique et de normes de sécurité de l'information garantissant une protection de fond ainsi que l'émission de recommandations sont de nature à nettement améliorer la situation. La Confédération doit donc lancer, en étroite collaboration avec les associations faîtières, les associations de branche, les associations de prestataires

[13] La directive NIS tient compte des points d'échange Internet (*Internet Exchange Point*, IXP), des fournisseurs de services DNS et des autorités de certification.

de services informatiques et les entreprises intéressées, un programme d'amélioration de la sécurité de l'information dans le monde des PME.

L'établissement d'une norme par l'État serait par contre en contradiction avec la notion de liberté économique telle qu'elle est comprise en Suisse. De plus, la diversité des branches concernées exige que les mesures de protection destinées à garantir une protection informatique de fond présentent une certaine flexibilité. La mesure dans laquelle il sera possible d'harmoniser cette protection de fond devra être déterminée en cours de travaux, conjointement avec tous les groupes d'intérêts concernés.

Recommandation

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.

8.2.4 Obligations de notifier

Disposer en permanence d'un tableau complet de la situation en matière de cyberattaques et s'échanger toutes les informations sur ces dernières aurait pour effets de sensibiliser de manière déterminante les acteurs concernés et de réduire les vulnérabilités. Cette approche repose nécessairement sur une obligation de notifier les cyberincidents applicable à tous les exploitants d'infrastructures critiques et fournisseurs de services numériques importants. Or la Suisse ne connaît actuellement pas d'obligation générale de notifier. Relevons toutefois que l'art. 22 P-LPD prévoit une obligation de notifier les violations de la sécurité des données. Sous le droit en vigueur, les obligations de notifier se limitent à certaines interruptions de la fourniture des services, par exemple dans le domaine des télécommunications, mais elles ne sont pas spécifiquement axées sur la notification des cybermenaces.

Aux fins de l'adoption d'une obligation de notifier, il y a lieu d'examiner en détail les questions suivantes:

- À qui devra s'appliquer l'obligation de notifier? Il convient de définir des critères permettant de déterminer si tous les secteurs et si tous les exploitants d'un même secteur devront être soumis à l'obligation de notifier.
- Faut-il prévoir une obligation de notifier générale ou limitée à des événements spécifiques (ne pas confondre avec la notion de gravité, cf. point suivant)? Dans le second cas, des critères de limitation devront être définis (par ex. mise en danger du public ou perte de données en relation avec la non-prolifération).
- À partir de quelle gravité devra-t-il y avoir obligation de notifier un événement? Ce seuil de gravité devra-t-il s'appliquer à tous les exploitants?
- À qui devront être notifiés les incidents de sécurité? L'obligation de notifier devra être remplie en priorité auprès des autorités (de surveillance) ou d'une centrale comme MELANI. Étant donné toutefois que les secteurs ayant une autorité de régulation sont peu nombreux, il y aura lieu de créer, pour ceux qui n'en ont pas, de nouveaux services ou un service centralisé *ad hoc*.
- Les fournisseurs de services numériques importants devront-ils aussi être soumis à l'obligation de notifier, et quels critères devront-ils s'appliquer pour eux?

- Quelles bases légales faudra-t-il créer? Elles pourront être propres à chaque secteur ou former un cadre légal général, comme en Allemagne et en France.

Contrairement à l'obligation de notifier, il n'y a pas lieu de prévoir un dispositif de culpabilisation du type *blame and shame*, comme le *Health Wall of Shame* aux États-Unis. Informer le public de tous les incidents de sécurité, même de ceux qui ne le concernent pas, uniquement pour exposer les «coupables» à la réprobation générale ne paraît pas nécessaire et n'est au demeurant pas dans les habitudes helvétiques. La dénonciation publique peut même être contre-productive, dans la mesure où elle peut pousser les entreprises à ne pas notifier les incidents et à les dissimuler, afin d'éviter d'être montrées du doigt.

Recommandation

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.

8.2.5 Organisation nationale centralisée de gestion des cyberincidents

Fonctionnant comme un guichet unique au niveau étatique, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) fournit son assistance dans l'analyse des incidents, tant sur le plan technique que sous l'angle du renseignement, et gère la plateforme d'échange d'informations nécessaire à cet effet.

En raison des ressources limitées à disposition, les exploitants d'infrastructures critiques ne font pas tous partie du cercle des clients de MELANI. Il y a donc lieu, aux fins de l'élargissement de ce cercle, d'examiner l'importance de chaque secteur du point de vue de la transformation numérique, puis d'évaluer et d'affecter les ressources nécessaires à son intégration. La priorité doit porter sur les prestataires de services des domaines suivants: énergie, transports, système bancaire, plateformes de négociation électroniques, système de santé, fourniture et distribution d'eau potable ainsi qu'infrastructures numériques. Il s'agira ensuite d'examiner, dans un second cycle d'élargissement du cercle des clients de MELANI, les fournisseurs de services en ligne importants.

L'étroite collaboration qui existe déjà avec les centres de compétence concernés (notamment les CERT) doit être intensifiée de manière ciblée, afin que les ressources spécialisées limitées disponibles en Suisse soient utilisées avec un maximum d'efficacité et d'efficience.

Compte tenu du tableau général des risques de sécurité, l'actuel groupe cible des infrastructures critiques doit être notablement élargi et inclure notamment les institutions de recherche et l'économie privée, en particulier dans les domaines sensibles où l'espionnage technologique et la protection des clients jouent un rôle important. Enfin, il y a également lieu d'y intégrer le monde des PME.

Les services fournis par MELANI, notamment l'assistance en cas d'incidents, les informations et les conseils préventifs et la plateforme d'échange d'informations, doivent être étendus en conséquence et rassemblés dans un véritable centre de compétence

de la Confédération en matière de cybersécurité. Déjà formulés dans la stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022, ces objectifs doivent être rapidement réalisés.

Même avec un cercle de clients fortement élargi, il s'agira de maintenir le niveau de qualité actuel, ainsi que le climat de confiance dans lequel les échanges d'informations avec les exploitants d'infrastructures critiques doivent se dérouler. Il faudra en outre définir clairement quels clients de quels secteurs auront droit à quels services et à quelles informations. On pourrait envisager un modèle en oignon, dans lequel MELANI développerait surtout des services de prévention et de gestion des incidents destinés aux clients à faible criticité des couches externes de l'oignon. Ce soutien serait en outre toujours subsidiaire aux offres de protection et de gestion des incidents proposées sur le marché. Avec ce développement, MELANI deviendra un organisme national de gestion des cybercrises, qu'il s'agira d'intégrer dans la structure des états-majors de crise de la Confédération et des cantons.

Aux fins de la création d'un tel centre national, il y a lieu d'examiner en détail les questions ci-dessous.

- Comment garantir la subsidiarité du nouveau centre national? Quels échelons définir dans le processus d'escalade nécessaire à cet effet? Les services correspondants de l'économie privée ne devront pas être inutilement concurrencés.
- La définition des échelons du processus d'escalade devra-t-elle tenir compte uniquement de la capacité d'agir de l'État et de l'intérêt public ou reposer également sur des considérations économiques?
- Quels services devront être proposés à quels clients (économie en général, PME, instituts de recherche) dans quelles situations?

Recommandation

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).

8.2.6 Procédure de sécurité relative aux entreprises pour les exploitants d'infrastructures critiques et les autres parties prenantes

Selon le message du Conseil fédéral concernant la loi sur la sécurité de l'information (LSI), le projet de loi prévoit qu'une procédure de sécurité relative aux entreprises s'appliquera également dans le domaine non militaire. Cette procédure permettra de vérifier la fiabilité des entreprises qui souhaitent obtenir des mandats des autorités. Il sera ainsi possible d'améliorer le contrôle de sécurité au moins des fournisseurs de services informatiques ayant un siège en Suisse, mais dont le siège principal est à l'étranger. Un contrôle de l'intégralité de la chaîne de livraison restera cependant irréaliste. Pour contrôler l'adéquation des sociétés en matière de sécurité, la procédure de sécurité relative aux entreprises reposera également sur les moyens du Service de renseignement de la Confédération. Rappelons qu'une procédure de sécurité obligatoire applicable aux exploitants d'infrastructures critiques et à leurs fournisseurs avait déjà été

envisagée en 2011, pour être finalement rejetée. Aujourd'hui, compte tenu des enseignements tirés de l'affaire Snowden et des événements en Ukraine, le groupe d'experts recommande d'appliquer plus largement la procédure de sécurité relative aux entreprises, en tant qu'instrument de sécurité.

Recommandation

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.

8.2.7 Limites des possibilités de défense de l'État

Le mécanisme de la dissuasion, tel qu'on le connaît notamment dans le domaine des armes nucléaires, semble s'imposer également dans le monde numérique: les grandes puissances se dotent toutes d'arsenaux tant offensifs que défensifs. En effet, étant donné qu'il n'est généralement pas possible de remonter la trace des attaques jusqu'à leur origine et qu'en raison du manque de preuves, une éventuelle escalade diplomatique n'a guère d'utilité, il est essentiel de prendre des mesures de défense appropriées et de faire savoir à la partie adverse que l'on dispose aussi de moyens d'attaque.

Pour ce qui est de la Suisse, sa marge de manœuvre est très étroite: d'une part, l'industrie informatique suisse, comme celle de la plupart des pays, n'est pas à même de mettre à disposition une chaîne logistique (*supply chain*) entièrement sécurisée; d'autre part, contrairement à celle des grandes puissances, elle ne s'est pas dotée de ressources défensives et offensives dans ce domaine. Ainsi, les moyens à la disposition de l'État pour soutenir les efforts de cyberdéfense des institutions de la recherche scientifique et des domaines sensibles de l'économie – dont font partie les infrastructures critiques et de nombreux autres secteurs industriels importants pour le pays – sont limités. En ce qui concerne le matériel informatique et en partie également les logiciels, l'Europe et la Suisse dépendent des États-Unis et de la Chine.

Il serait certes envisageable de créer un cybercentre disposant des moyens nécessaires pour étudier et développer des vecteurs d'attaque ainsi que des mesures de défense à tous les niveaux. Ce centre pourrait également proposer des formations appropriées aux exploitants des infrastructures critiques. Toutefois, en raison de l'absence d'industrie de la sécurité informatique en Suisse, la réalisation d'un tel projet se heurterait à d'énormes difficultés, sans compter que chaque acquisition de savoir-faire à l'étranger, que ce soit auprès de sources publiques ou privées, remettrait en question l'indépendance de notre pays.

S'ils doivent choisir entre respecter leurs obligations de confidentialité et de fourniture de prestations envers leurs clients à l'étranger ou obéir aux injonctions de leurs propres autorités (par ex. services de renseignements) et violer un contrat, la plupart des fournisseurs de services informatiques vont céder à la pression des autorités. Les conséquences en sont la transmission de données de leurs clients (violation de la confidentialité) ou l'interruption ou le report de la fourniture de leurs prestations (restrictions de

la disponibilité des services). Dans ce contexte, on ne peut plus guère considérer que les fournisseurs de services informatiques sont des partenaires sûrs à 100 %.

Afin de réduire la dépendance de la Suisse vis-à-vis de l'étranger, en particulier des entreprises étrangères, on pourrait envisager de créer des infrastructures numériques autarciques, par exemple un nuage informatique suisse. Il ne faut cependant pas sous-estimer les défis, les coûts et les risques que comporterait un tel projet: plus les exigences d'indépendance vis-à-vis de l'étranger sont élevées, plus celles relatives au contrôle des composants – matériel, logiciels, systèmes d'exploitation, puces – augmentent. Elles peuvent même aller jusqu'à la nécessité de développer ces composants soi-même, avec des coûts énormes, si l'on songe que le contrôle de quelques lignes à peine d'un code de programme coûte des dizaines de milliers de francs et que celui des puces est encore beaucoup plus onéreux. Il faudrait en outre disposer d'une infrastructure actuellement inexistante en Suisse. Enfin, il convient de souligner que le développement de logiciels et de matériel maison s'accompagne souvent de «maladies de jeunesse», qui peuvent, selon les circonstances, comporter de plus grands risques que la dépendance vis-à-vis de l'étranger évoquée plus haut. Il existe bien sûr aussi des solutions de compromis, consistant par exemple à adapter des logiciels à code source ouvert à ses propres besoins et à créer et exploiter un nuage informatique en Suisse en utilisant des composants matériels de divers fabricants. Au mieux, la dépendance vis-à-vis de certains fabricants étrangers diminuerait, mais pas la menace provenant des États, laquelle est pourtant à l'origine de ces efforts de protection. Les États pourraient en effet installer des portes dérobées (*back doors*) ou des interrupteurs de blocage (*kill switches*) directement sur les puces. Dans d'autres domaines, par exemple la construction d'un réseau de haute sécurité en Suisse, le gain de sécurité devrait en revanche être significatif, pour des coûts nettement moins élevés (voir aussi à ce sujet le ch. 4.4.3).

Le message concernant la LRens souligne que l'infiltration dans des systèmes et des réseaux informatiques à l'étranger peut être sensible du point de vue de la politique extérieure. L'éventuelle découverte de l'infiltration et de son origine peut en effet entraîner des mesures de rétorsion ou des contre-attaques portant atteinte à la confidentialité et à la disponibilité des infrastructures numériques et des données en Suisse. Force est donc de constater que la Suisse ne dispose actuellement pas de moyens suffisants pour garantir sa souveraineté numérique, et c'est pourquoi l'avenir du traitement des données et de la sécurité de l'information doit faire l'objet d'un débat de politique de sécurité, visant à déterminer comment remédier à cette situation. Il s'agit en l'occurrence de prendre en considération aussi bien la mise en place de moyens de défense propres, à très forte intensité de ressources, que l'établissement d'étroites coopérations avec d'autres États. Relevons toutefois qu'établir de telles coopérations sans développer des capacités propres pourrait déboucher sur une situation où la Suisse se placerait simplement sous le parapluie de protection de ces États partenaires, avec toute la dépendance qui en résulterait.

Recommandation

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.

8.2.8 Tâches de l'armée

Face à une menace de cyberattaque ou à une cyberattaque effective susceptible de porter ou portant gravement atteinte à la sécurité de la Suisse, la question se poserait si l'armée doit intervenir dans le cadre d'un cas de défense à proprement parler ou uniquement à titre subsidiaire (service d'appui destiné à soutenir les autorités civiles).

Il y a cas de défense lorsque l'intensité et l'étendue de la menace sont telles que l'intégrité territoriale, l'ensemble de la population ou l'exercice de la puissance étatique sont en danger, même si l'auteur de la menace n'est pas un État. Lors de cyberattaques lancées par des terroristes, des extrémistes ou des acteurs non clairement identifiables liés à la criminalité organisée ou à des milieux proches de l'État, l'adversaire peut atteindre ses objectifs en s'en prenant à des infrastructures critiques essentielles au bon fonctionnement de l'État, de l'économie et de la société. En cas de situations extraordinaires ou entraînant un état de nécessité, l'armée peut être appelée à intervenir dans le cadre de sa mission primaire de défense si les critères suivants sont remplis:

- l'intégrité territoriale, l'ensemble de la population ou l'exercice de la puissance étatique sont concrètement menacés,
- la menace perdure et dépasse le cadre d'une simple menace ponctuelle,
- la menace n'est pas simplement locale ou régionale mais pèse sur tout le pays, et
- la menace est d'une telle intensité (comparable à une attaque) que seuls des moyens militaires peuvent la combattre.

Ces critères sont cumulatifs, mais ne doivent pas être compris comme s'appliquant à la lettre, autrement dit comme déclenchant automatiquement la décision d'engager l'armée à titre primaire. Ils servent de points de repère au Conseil fédéral et au Parlement, auxquels il appartient de prendre ou non cette décision compte tenu de la situation globale.

Si la cybermenace n'atteint pas l'intensité ni l'étendue dont il est question ci-dessus, mais que les autorités civiles, en collaboration avec l'économie privée, ne sont pas en mesure de la contrôler, l'armée peut, à la demande des autorités civiles compétentes, fournir un service d'appui, notamment pour sécuriser les infrastructures critiques et leur apporter son soutien. Pour ce service d'appui également, les critères à remplir ne doivent pas être compris comme s'appliquant à la lettre. La décision d'y recourir appartient, selon la situation, au Conseil fédéral, au Département fédéral de la défense, de la protection de la population et des sports (DDPS) ou au Parlement.

L'armée doit conserver son rôle de réserve stratégique, même face aux nouvelles cybermenaces. De plus, la répartition des compétences entre la Confédération et les cantons fixée dans la Constitution fédérale ne doit pas être modifiée. Il y a cependant lieu d'adapter les moyens de défense civils de la Confédération et des cantons, de manière à ce qu'ils couvrent également les cybermenaces. De plus, il ne faut pas que, par manque de moyens, une cybermenace importante soit traitée au même titre qu'une situation extraordinaire, une surcharge extrême ou une catastrophe. Il s'agit donc de réfléchir aux critères à appliquer pour définir – comme dans le monde analogique – un niveau d'ambition qui, en ce qui concerne le service d'appui, tienne compte de l'obligation de proportionnalité visée à l'art. 67, al. 2, de la loi du 3 février 1995 sur l'armée (LAAM) et permette d'engager l'armée au titre de l'aide spontanée prévue à l'art. 52, al. 7, LAAM.

Enfin, il faut prendre les indispensables mesures propres à garantir une collaboration optimale entre les différentes forces d'intervention de l'État (armée, police, protection civile et de la population, approvisionnement du pays, etc.) en cas de menace.

Recommandations

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.

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

8.3 Harmonisation nationale de la protection des données dans l'administration

8.3.1 Réglementation technique cohérente de la protection des données à tous les niveaux de l'administration

La LPD régit le traitement de données personnelles aussi bien par des personnes privées que par des organes fédéraux (art. 2, al. 1). Sous réserve de l'art. 37, elle ne s'applique toutefois pas au traitement de données personnelles par des organes cantonaux. Lors des travaux de révision totale de la LPD, on a examiné si cette répartition des compétences entre la Confédération et les cantons en matière de protection des données était toujours indiquée ou s'il ne valait pas mieux viser une harmonisation, autrement dit étendre le champ d'application de la LPD aux organes cantonaux. Élargir ainsi le pouvoir de légiférer de la Confédération dans le domaine de la protection des données ne serait toutefois possible que moyennant une révision partielle de la Constitution. À la demande de la cheffe du DFJP, la Conférence des gouvernements cantonaux (CdC) a organisé une audition des cantons sur cette question. Il en est résulté que la majorité d'entre eux est contraire à l'extension du champ d'application de la LPD au traitement des données par des organes cantonaux. Le projet de 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).

Toutefois, les développements très rapides observés dans le domaine du traitement des données mettent clairement en évidence combien il est important de disposer d'une réglementation cohérente ainsi que de possibilités d'adaptation et de mise en œuvre rapides et souples de la protection des données. Or le risque existe que la diversité des réglementations cantonales s'oppose à la satisfaction de ces exigences. Il convient donc d'examiner s'il y a lieu d'harmoniser la réglementation à l'échelle nationale et, le cas échéant, selon quelles modalités.

Recommandation

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

8.4 L'État comme prestataire de services (cyberadministration)

8.4.1 Situation actuelle, risques et chances

La Confédération, les cantons et les communes appliquent activement une stratégie de cyberadministration depuis plus de dix ans, les questions d'organisation et de procédure étant réglées dans une convention-cadre de droit public. Les rapports annuels de la Commission européenne et de l'ONU sur l'état de la cyberadministration montrent que celle-ci ne cesse de progresser. La Suisse n'occupe toutefois l'une des dix premières places dans aucun des indices établis dans ce domaine. Dans le classement de l'ONU, elle ne figure même qu'au 28e rang, se situant ainsi dans le dernier tiers du peloton des États membres de l'UE.

Le rapport de la Commission européenne sur la situation par pays confirme le besoin de rattrapage de la Suisse. Notre pays se situe en effet juste au-dessous de la moyenne de l'UE pour les quatre indicateurs principaux, à savoir l'orientation vers les services en ligne et les utilisateurs (*user centricity*), la transparence des prestations (*benchmark transparency*), la mobilité transfrontalière (*cross border mobility*) et les infrastructures de base (*key enablers*). Dans le domaine de la transparence des prestations et surtout dans celui des infrastructures de base, telles que l'e-ID, l'envoi de documents électroniques, la collecte unique de données avec stockage centralisé sécurisé, les possibilités de stockage sécurisé et l'authentification unique (*single sign on*, SSO) pour divers sites et services, les notes de la Suisse sont, dans le meilleur des cas, moyennes et parfois insuffisantes. Ces évaluations fournissent de précieuses indications sur les services qui, en raison de la demande, sont jugés importants et par conséquent prioritaires dans les autres pays. La Suisse se doit de combler son retard par rapport à la moyenne européenne, avec pour objectif d'ordre supérieur de procurer un maximum d'avantages à la société au moyen de services numériques, ce qui favorisera également la compétitivité du pays.

Les projets en cours, tels que la création d'un cadre légal régissant un système e-ID reconnu par l'État, le guichet unique pour les entreprises ainsi que les portails eHealth Suisse et eDéménagement Suisse, vont certes dans la bonne direction, mais ils doivent être accélérés et mis en œuvre à l'échelle nationale, puis systématiquement poursuivis et développés, conjointement avec les projets portant sur les infrastructures de base. Du fait qu'en Suisse les autorités assurent une qualité de service supérieure à la moyenne et qu'elles disposent de ressources suffisantes pour fournir leurs prestations par voie analogique ou hybride, le développement de la cyberadministration n'était pas considéré jusqu'ici comme présentant un caractère d'urgence. Pourtant, une numérisation plus poussée des démarches administratives serait non seulement synonyme de gains d'efficacité, de temps et de productivité à la fois pour l'administration et pour les personnes physiques et morales, mais favoriserait également les interactions entre les citoyens et l'État. Il est en outre essentiel que la cyberadministration

garantisse un accès sans barrières aux services de l'État à toutes les personnes handicapées ou présentant des déficiences liées à la vieillesse, comme le prévoit au demeurant la stratégie suisse de cyberadministration. Enfin, il y a lieu de prêter une attention particulière aux personnes qui ne souhaitent pas recourir aux services en ligne, afin qu'elles ne soient pas désavantagées, voire exclues de la société, par la numérisation.

La cyberadministration ne doit donc pas se limiter aux simples échanges numérisés et sécurisés de documents et d'informations entre l'État et ses usagers. Il s'agit plutôt de faire en sorte que tous les processus entre partenaires se déroulent de façon entièrement numérique et sans rupture de média. La numérisation et l'adaptation des processus devraient favoriser l'automatisation, lorsqu'elle est judicieuse. De plus, le pool de données devrait croître de manière significative et conduire à une utilisation secondaire des données, que ce soit dans le cadre de nouveaux modèles d'affaires ou pour améliorer les services de l'État. Le traitement intelligent des données (intelligence artificielle, analyse des big data) pourrait en outre soutenir durablement les autorités, par exemple dans leur travail en relation avec le service de l'emploi ou pour accroître l'efficacité de la mise en œuvre du système des assurances sociales.

La numérisation est donc aussi l'occasion de réfléchir aux processus analogiques et d'en revoir la conception. Tout cela offre certes de nombreuses chances à saisir aux autorités, mais comporte aussi des risques. Cette nouvelle conception du travail et le changement de culture qu'elle implique sont de véritables défis pour les services concernés, ce qui peut avoir un effet ralentisseur sur la numérisation.

8.4.2 Cadre d'action

La numérisation ne permettra de dégager des économies d'échelle que si les infrastructures numériques sont autant que possible normalisées et si le nombre de participants atteint la masse critique nécessaire. Les structures de décision et de mise en œuvre centralisées offrent un environnement favorable à la satisfaction de ces conditions. Ce qui frappe à cet égard dans les pays précurseurs en matière de cyberadministration – tels que le Danemark, mais aussi de plus grands pays comme le Royaume-Uni –, c'est que le succès y repose sur un système descendant, dans lequel les objectifs fixés démocratiquement et en toute transparence sont réalisés transversalement, mais qui encourage, coordonne et intègre également les initiatives ascendantes. Pour réussir, la cyberadministration devra reposer sur une structure continue, avec une coordination et un pilotage assurés de manière participative par les parties prenantes, des communes à la Confédération. L'assemblage de solutions techniques individuelles – sous réserve de leur interopérabilité – se traduit généralement par des coûts élevés, des retards et des problèmes de mise en œuvre. Il ne permet en outre pas d'atteindre la masse critique d'utilisateurs requise. Il est en outre incontestable que le système fédéral, avec ses structures fragmentées et le principe de subsidiarité, contribue de manière déterminante au succès de la Suisse. Il constitue cependant un facteur de résistance systémique aux tendances centralisatrices de la transformation numérique, tout en étant susceptible, dans le même temps, de contribuer à la résilience de la cyberadministration. Enfin, la compatibilité technique et juridique ainsi que l'interopérabilité avec les systèmes de l'UE et avec l'évolution numérique du marché unique devront être garanties.

Conduite, pilotage et coordination

Les organes qui, au niveau fédéral, s'occupent actuellement de la question de la cyberadministration suisse n'ont pas de véritables compétences de pilotage, ni même de mise en œuvre. Il n'y a donc pas pour l'instant de coordination efficace des activités relevant du domaine de la cyberadministration. Pour rapidement progresser et réaliser des économies d'échelle, il est indispensable d'y remédier.

Infrastructure de base
L'infrastructure de base doit inclure une e-ID avec signature qualifiée remplissant les exigences de la forme écrite, un système de gestion des identités et des accès, un processus d'authentification unique, un point de contact unique (interlocuteur central) pour les particuliers et les entreprises ainsi qu'un système sécurisé de stockage des données et des documents, servant de boîte aux lettres numérique pour toutes les parties prenantes. Cette boîte aux lettres numérique remplira la fonction de canal de communication en ligne bidirectionnel entre les autorités et tous les acteurs de la société. L'infrastructure de base devra être disponible dans tout le pays et présenter toutes garanties d'interopérabilité, d'économicité, de sécurité et de confort d'utilisation, car elle devra se mesurer à la convivialité des solutions du secteur privé.

Au cours des 30 dernières années, les systèmes informatiques de l'administration se sont développés de manière organique et ils reflètent donc la structure du système fédéral suisse. Tant dans les divers cantons qu'au sein de l'administration fédérale, l'interconnexion et l'interopérabilité des infrastructures numériques existantes sont insuffisantes pour satisfaire aux exigences de la cyberadministration et du traitement des données au XXI^{e} siècle. Nombre des systèmes de base de ces infrastructures ont été conçus pour des processus analogiques et doivent par conséquent être entièrement renouvelés. Pour atteindre les objectifs – davantage d'efficacité, de synergies et d'interconnexion –, il est indispensable que les administrations définissent des normes et élaborent, sous la forme de modules, des solutions communes permettant d'utiliser les systèmes en place de manière transversale. Ce faisant, elles devront également tenir compte des interfaces avec le secteur privé.

Masse critique
Le succès de la transformation numérique en Estonie, au Danemark, en Finlande et en Suède se mesure au fait que les économies escomptées sont progressivement réalisées, sur fond d'amélioration de la qualité, de la rapidité et de la commodité des services, tant au niveau de l'État qu'à celui des entreprises et des particuliers. Les bases et les conditions de ce succès sont des taux élevés d'enregistrement de toutes les parties prenantes sous leur e-ID, des points de contact uniques, des systèmes d'authentification unique ainsi qu'un vaste assortiment de services couvrant toutes les démarches administratives importantes ou fréquentes.

La comparaison des différentes stratégies de mise en œuvre des États précurseurs en matière de cyberadministration montre quels sont les facteurs de succès déterminants. Parmi les pays cités ci-dessus, seuls le Danemark et l'Estonie obligent légalement leurs habitants à posséder une e-ID. De même, seuls ces deux pays ont adopté de fait un système à option de retrait (*opt out*) en ce qui concerne les prestations numériques des autorités. Cela signifie que pour une majorité de processus administratifs, les citoyens ne peuvent continuer à recourir à des services analogiques que s'ils en font expressément la demande. Grâce à cette politique, 80 à 90 % des démarches administratives se déroulent numériquement et l'e-ID est très largement diffusée. En l'absence d'obligation légale, la Finlande, la Suède et le Royaume-Uni n'affichent certes pas de telles valeurs record, mais les chiffres y sont néanmoins impressionnants. Ce succès s'explique par le fait que soit les habitants y reçoivent d'office leur e-

ID, soit la demande et l'obtention de cette dernière y sont rapides et commodes. L'e-ID est partout gratuite.

Ce qui frappe également, c'est que l'octroi des e-ID est organisé de manière centralisée dans certains pays, et de manière décentralisée dans d'autres et que les deux approches semblent bien fonctionner. En Suède et au Royaume-Uni, par exemple, la délivrance des e-ID a été confiée à divers prestataires privés. Un facteur de succès déterminant semble cependant être le fait que dans tous les pays examinés, l'État a non seulement joué un rôle de coordination et de surveillance en matière d'e-ID, mais s'est également engagé activement, en véritable pionnier. Il a notamment pris l'initiative des contacts avec les fournisseurs privés et activé la réalisation d'une solution technique, tout en veillant à proposer un vaste assortiment de services numériques, afin que la masse critique d'utilisateurs puisse être atteinte. Tous les pays cités ont en outre mis un point de contact unique ainsi qu'un système d'authentification unique à la disposition des entreprises et des particuliers. Les autorités relativisent les charges supplémentaires occasionnées par le passage à la cyberadministration ainsi que les réserves concernant les citoyens n'ayant pas d'affinités pour le numérique en arguant que les services en ligne promettent et garantissent à chacun, dès leur première utilisation, une simplification des démarches ainsi qu'un important gain de temps. L'économie privée a rapidement accepté les solutions mises en œuvre en tant que normes et joue depuis lors le rôle de multiplicateur.

Compatibilité avec le marché unique numérique de l'UE

Le plan d'action de l'UE pour l'administration en ligne joue un rôle important dans le cadre du marché unique numérique. Il a pour base et principal élément moteur le développement des modules du mécanisme pour l'interconnexion en Europe, qui comprennent les infrastructures numériques eDelivery, eID, eInvoicing, eSignature et eTranslation.

Recommandations

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.

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.

8.5 Libre accès aux données publiques et données ouvertes

8.5.1 Situation actuelle, risques et chances

Le libre accès aux données publiques (*open government data*, OGD) a pour objectif de mettre les données de l'administration à la disposition de la société en vue de leur réutilisation. Plus les données sont ouvertes, accessibles et faciles à trouver et à traiter, plus elles sont utiles, que ce soit pour concevoir de nouveaux modèles d'affaires, servir de moteur de croissance économique, faire avancer la recherche ou encore améliorer les services fournis par les autorités. La publication des données contribue en outre à la transparence des activités administratives. Sont toutefois exclues des OGD les données soumises à la protection des données, à la protection de l'information ou à des prescriptions relevant du droit de la propriété intellectuelle. D'après les estimations, rien qu'en tant que moteur de croissance économique, les OGD pourraient être à l'origine d'une augmentation de 0,2 % du PIB. Il faut en outre partir du principe que les OGD peuvent avoir un effet positif non négligeable sur les flux de données, par exemple dans les domaines de la recherche et de l'acquisition d'informations. Enfin, au-delà des aspects quantitatifs, leur valeur économique est jugée comme étant très élevée sur le plan qualitatif également.

En 2014, le Conseil fédéral a approuvé une stratégie de libre accès aux données publiques en Suisse (stratégie OGD), dont les objectifs à remplir pour fin 2018 étaient notamment les suivants: examiner le cadre légal et la politique tarifaire, créer les bases légales nécessaires, préparer la publication coordonnée des données, mettre les infrastructures techniques à disposition et ouvrir la voie à l'instauration d'une culture du libre accès aux données. Cette stratégie devait aussi servir de base à l'établissement d'une collaboration avec les cantons et les communes visant l'application d'une politique globale en matière d'OGD. Soulignons à cet égard que la constitution d'un pool de données aussi important et harmonisé que possible et dépassant les limites de l'administration fédérale est un préalable indispensable à l'exploitation de tout le potentiel des OGD. La Confédération ne peut toutefois pas édicter de normes légales transversales en la matière, car elle ne dispose pas des compétences législatives nécessaires.

La Suisse se situe dans le dernier tiers du classement établi par l'OCDE sur la base du critère de la maturité des OGD. Dans l'étude correspondante de l'UE, la Suisse est considérée comme un *OGD follower*: elle dispose certes d'une vision, de modèles et d'infrastructures techniques, mais il reste encore beaucoup à faire et le volume de données est faible. Dans d'importants baromètres OGD privés également, la Suisse ne se classe pas mieux que dans les cinquante premiers rangs, ce dont une société de services à haute technologie comme celle de notre pays ne saurait se contenter. Les critiques portent aussi sur la qualité des données: celles-ci sont pour la plupart protégées par une licence technique et ne sont donc pas à disposition. Quant à celles disponibles, les utilisateurs ne peuvent pas les télécharger en une seule fois, dans un format ouvert et lisible par machine. De plus, des données importantes, comme celles du registre du commerce ou du registre foncier, ainsi que des géodonnées et des métadonnées ne sont pas intégralement à disposition, ni librement réutilisables.

La collaboration avec les cantons présente aussi son lot de défis: à ce jour, seuls sept cantons ont mis leurs données à la disposition du point de contact unique. La plupart des cantons n'ont d'ailleurs pas encore d'infrastructures leur permettant de préparer leurs données à cet effet, ni les bases légales nécessaires pour le faire. Actuellement, seule une minorité de cantons promeuvent activement les OGD et collaborent intensément avec la Confédération. Les raisons invoquées par les autres sont le manque aussi bien de ressources que de connaissances spécialisées. On peut toutefois supposer que la majorité des cantons se sont mis en position d'attente, jusqu'à ce qu'un service prenne la direction des opérations. Le potentiel de développement de la collaboration entre la Confédération et les cantons est donc très important.

À six mois de la fin de la période de validité de la stratégie OGD 2014-2018, il apparaît que d'importants objectifs ne seront pas atteints. L'approche actuelle basée sur des lois spécifiques ainsi que sur des projets législatifs des autorités compétentes n'a pas abouti au résultat prévu, à savoir la création des bases légales requises dans les délais et dans tous les domaines concernés. Toutefois, plusieurs autres possibilités sont envisageables pour créer les bases légales de l'utilisation de données collectées par des moyens publics: l'une consisterait à compléter la LTrans en conséquence et une autre, à adopter une loi fédérale sur la gestion de l'information. Un tel acte normatif fixerait des lignes directrices cohérentes et appropriées et garantirait la sécurité du droit partout où les nouvelles technologies de l'information remettent en question les relations entre l'État et les citoyens ainsi qu'entre la Confédération et les cantons (et les communes), au niveau du droit administratif comme du droit constitutionnel. D'autres possibilités pourraient également être examinées.

Par ailleurs, la question des tarifs et, par conséquent, des modèles de financement n'est toujours pas clarifiée. Une autre question étroitement liée à celle des tarifs se pose également: dans quelle mesure et à quelles conditions est-il possible d'inciter les entreprises proches de la Confédération à suivre une politique OGD sans enfreindre le principe de proportionnalité s'appliquant aux conditions de concurrence avec le secteur privé? Enfin, tous les services administratifs concernés se doivent d'améliorer leur coordination et leurs échanges, de manière à pouvoir s'accorder sur la définition et sur le format technique de solutions génériques.

Malgré les progrès réalisés, l'exploitation du potentiel des OGD se heurte encore à de nombreux obstacles. Parmi ceux à lever prioritairement, citons l'absence de bases légales, la normalisation insuffisante de la préparation des données, le manque de clarté de la saisie et des conditions d'utilisation des données des entreprises proches de la Confédération ainsi que l'insuffisance des ressources à disposition pour la mise

en œuvre. En résumé, force est de constater que l'actuelle collaboration entre la Confédération et les cantons est insuffisante pour faire avancer le projet OGD à l'échelle nationale.

Recommandation

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.

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.

8.6 Cyberdémocratie

8.6.1 Situation actuelle, évolution, chances et risques

Les effets de la transformation numérique se font clairement sentir sur le système de valeurs et de normes de notre démocratie, né au fil du temps.

La rapide évolution technologique et les nouvelles possibilités d'interactions sociétales entre «savoir» et «information» qui en découlent modifient le contexte dans lequel s'inscrivent les relations quotidiennes entre l'État et les individus. L'évaluation des mécanismes de la cyberdémocratie n'en est toutefois qu'à ses débuts. Dans de nombreux domaines, l'expérience fait encore défaut, et les estimations relatives aux chances et aux risques, aux mesures à prendre et à leurs effets ne sont pour l'instant vérifiables que dans la pratique, selon la méthode «essayer et apprendre de ses erreurs». Des règles édictées par l'État n'auraient guère de sens. C'est pourquoi il faut réfléchir à la création d'espaces d'expérimentation appropriés (sous la forme de compétitions, olympiades urbaines, etc.), pouvant très bien être réalisés dans le cadre d'un système subsidiaire.

8.6.2 Défis et risques

Bien qu'initialement l'idée prévalût qu'Internet allait contribuer à l'émancipation de l'humanité et favoriser une plus grande convivialité politique, force est de constater que la Toile est aujourd'hui surtout un lieu de manipulation. Politiciens dénigrant leurs adversaires sur Twitter, «trolls» postant leurs mensonges dans les colonnes de commentaires des portails médiatiques ou propagandistes diffusant subtilement et à couvert leurs «vérités alternatives» sur les réseaux sociaux: les possibilités de manipulation sont aussi nombreuses que variées.

Le rôle incombant aux médias publics dans une démocratie en pleine révolution numérique est donc d'autant plus important: informer la population, contribuer à la formation de l'opinion par des débats et des discussions critiques et permettre ainsi la participation des citoyens. De manière générale, le risque existe que le quatrième pouvoir manque de plus en plus à ses tâches essentielles pour la démocratie, le dilemme étant le suivant: soit ne miser plus que sur des informations à sensation, soit dispa-

raître à coups de clics. C'est ainsi que les manipulations et les fausses nouvelles abondent et que le lecteur averti se transforme en simple consommateur d'informations, qui plus est non vérifiées. L'accessibilité, la facilité de compréhension et la valeur divertissante ne cessent de grimper sur l'échelle des priorités. Les possibilités offertes par le profilage permettent en outre d'influencer les acteurs de la société de manière ciblée (*bubble filter*, *big nudging*, *social bots*, etc.), avec pour conséquence de saper les fondements de l'intelligence collective (voir aussi ch. 11). Le passage d'une société de l'information à une société du savoir se fait ainsi plus difficile.

Par ailleurs, la dépendance vis-à-vis des plateformes techniques de «monopoleurs» – utilisées pour soutenir les processus démocratiques – comporte d'autres possibilités d'influence, qui sont toutefois difficiles à cerner. Ce problème relève de la responsabilité des grands acteurs concernés du marché, autrement dit des exploitants de ces plateformes d'information, mais ceux-ci ne se considèrent, dans le meilleur des cas, que comme de simples diffuseurs neutres d'informations. Ils ne se sentent donc, pour la plupart, aucunement responsables des contenus, même si l'on observe dans ce secteur également les premiers signes de prise en compte d'une responsabilité sociétale des entreprises.

Il serait possible de compléter, voire de remplacer, ces plateformes numériques sous contrôle d'entreprises privées par des plateformes publiques servant de base à une approche coopérative et au développement de la démocratie participative (cyberparticipation). Citons également les «défis urbains» (*City Challenge*) et les «olympiades urbaines» (*City Olympics*), qui sont des compétitions amicales nationales, internationales ou même mondiales, dans lesquelles la société cherche des solutions à d'importants défis contemporains. Parmi les disciplines de ces compétitions peuvent figurer, par exemple, la lutte contre le changement climatique, le développement de nouveaux systèmes énergétiques plus efficaces, le développement durable, la diversité et la vérification de l'information, la résilience ou l'intégration. Élaborées sur plusieurs mois avec le soutien des pouvoirs publics, les solutions proposées à l'issue de ces compétitions doivent observer le principe du code source ouvert et être labellisées *Creative Commons*, de manière à ce que les villes, les grandes entreprises, les PME, les sociétés créées par essaimage, les chercheurs, les ONG et la société civile puissent les utiliser et les développer librement. De cette manière, le potentiel des nouvelles approches, telles que les données ouvertes, le libre accès, le code source ouvert, la science ouverte, l'innovation ouverte, les marathons de programmation, les ateliers ou espaces de fabrication numérique, les laboratoires publics ou encore la science citoyenne, sera multiplié, donnant ainsi à la société civile la possibilité de contribuer à la recherche de solutions.

Le but est de créer un cadre général positif, nécessaire pour mener à bien la transformation devant conduire à une société numérique durable.

Dans un proche avenir les questions suivantes se poseront en particulier: comment et dans quels domaines l'État doit-il proactivement exploiter lui-même ou promouvoir les nouvelles possibilités numériques, avec pour horizon la «cyberdémocratie 4.0»? Comment la numérisation peut-elle contribuer à augmenter la participation au processus politique? Une fois réduite à des rôles par la mobilisation numérique, la participation démocratique des individus sera-t-elle vraiment améliorée et facilitée? Ne faut-il pas plutôt craindre que le «facteur retardateur» – largement éprouvé – que sont les actuels processus de décision politique ne cède la place à une «cyberdémocratie instantanée»? Les citoyens ne vont-ils pas se sentir exagérément sollicités (onpar ex. par de

trop nombreux scrutins) et vouloir si possible déléguer l'exercice de leur «droit (de vote) éminemment personnel» à des «assistants numériques»?

Les travaux de recherche scientifique qui accompagnent les applications pilotes de vote électronique testées depuis plusieurs années ont permis de recueillir de nombreuses informations concernant les effets du vote en ligne sur les acteurs de la démocratie et sur les scrutins eux-mêmes. Abstraction faite des avantages apportés par des conditions de formation de l'opinion plus souples, indépendantes du lieu et mieux intégrées dans les différentes situations de vie ainsi qu'un mode de participation au scrutin semblable à celui du vote par correspondance, le risque existe que certains groupes de population soient «numériquement» dépassés, si ce n'est exclus, par le développement de la cyberdémocratie, et par conséquent limités dans l'exercice de leurs droits fondamentaux. La sécurité de l'information est par ailleurs le principal défi que pose la mise en œuvre du vote électronique à l'échelle nationale. Les informations à disposition sont par contre moins nombreuses pour ce qui est de l'initiative populaire électronique, de la formation de l'opinion électronique, de la documentation électronique, etc. Soulignons dans ce contexte que la collecte électronique de signatures pourrait avoir sur la démocratie un impact beaucoup plus fort que celui de la participation en ligne aux élections ou aux votations.

Les élections et le droit des citoyens d'y participer et d'exprimer leur opinion politique font partie des biens les plus précieux de la démocratie. Il est donc primordial que le risque de fraude électorale soit aussi faible que possible et que les résultats des élections et des votations soient parfaitement transparents et documentés. L'acceptation de ces résultats est une condition fondamentale du bon fonctionnement de la démocratie. Or, vu l'augmentation des cyberincidents, la société s'inquiète de plus en plus de la sécurité des processus démocratiques.[14]

Les dispositions de protection des systèmes de vote électronique arrêtées dans l'ordonnance de la Chancellerie fédérale du 13 décembre 2013 sur le vote électronique (OVotE) se fondent sur des présomptions de fiabilité et sur l'indépendance de quatre composants de contrôle:

- utilisation de différents matériel informatique, logiciels et systèmes d'exploitation,
- ségrégation des réseaux pour les divers composants,
- utilisation de logiciels aussi simples que possible, limités aux fonctions cryptographiques, et
- séparation stricte entre l'exploitation et la surveillance du système, moyennant l'application de mesures organisationnelles *ad hoc* auprès du personnel responsable.

L'attaquant qui voudrait manipuler le vote sans se faire remarquer devrait corrompre les quatre composants de contrôle. Le système de contrôle par vérification universelle permet en outre de repérer les éventuelles manipulations sur la base des incohérences qu'elles produisent.

[14] Voir notamment l'étude de l'EPFZ et de l'armée suisse: Sicherheit 2018: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend. Tibor Szvircsev Tresch et Andreas Wenger (éd.), Zurich 2018.

La manipulation des quatre composants de contrôle présuppose que l'attaquant soit un acteur puissant disposant d'un vaste savoir-faire et prêt à mobiliser d'importantes ressources. Si l'on prétend à une sécurité inconditionnelle (voir aussi ch. 4.2.1.6), on ne peut certes pas exclure la survenance d'un tel cas, mais il faut tenir compte, lors de l'évaluation des risques opérationnels, de la qualité spéciale de cette menace, qui tend à être essentiellement théorique.

Même si aucune incohérence n'est constatée, des groupements d'intérêts pourraient contester de manière générale le résultat d'un vote électronique, en invoquant le risque décrit ci-dessus, et demander la répétition du vote. Une telle demande devrait cependant se heurter à une large opposition de la société et des milieux politiques, plus large dans tous les cas que dans le second scénario ci-dessous.

Dans ce scénario, le système de détection signale des irrégularités. Ce risque, à la différence de celui du premier scénario, a la qualité de situation la pire pouvant vraisemblablement survenir. Elle peut résulter d'une corruption délibérée du système, mais aussi d'erreurs techniques ou humaines ayant entraîné des incohérences entre les quatre composants de contrôle. Si ces incohérences du résultat du vote dépassent une certaine marge de tolérance, un appel demandant que le vote soit répété pourrait être lancé et trouver un écho suffisant au sein de la population pour que ce soit le cas. La multiplication de telles répétitions pèserait lourdement sur le système démocratique et finirait par remettre en question le principe même du vote électronique. Ainsi, même sans indices de corruption intentionnelle, toute irrégularité peut déclencher un débat de fond sur le vote électronique, attiser les craintes de manipulations et soulever la critique à l'égard de la fiabilité des systèmes numériques.

La diffusion à large échelle du vote électronique présuppose donc que la société soit suffisamment informée des risques techniques et politiques qu'il présente. Dans le même temps, le niveau de maturité technique du système, en termes aussi bien de disponibilité que de stabilité, doit être assez élevé pour que le risque résiduel soit jugé acceptable par la société.

8.6.3 Expériences

Des approches innovantes de la démocratie de base, notamment sa modernisation au moyen de plateformes dites de «délibérations en ligne massives et ouvertes» (*massive open online deliberation*, MOOD), pourraient trouver une place prioritaire dans l'action de l'État. Ces plateformes permettent à la démocratie de mettre tous les arguments en jeu sur une table virtuelle, d'examiner les perspectives qu'ils offrent et d'élaborer des solutions innovantes et intégrées. Les collectivités choisissent ensuite la solution qui leur convient le mieux. Tout le processus peut en outre être soutenu par des systèmes d'intelligence artificielle. Les solutions issues de cette approche sont meilleures que celles élaborées quand les décisions sont prises de haut en bas ou à la majorité, car elles tiennent également compte des objections justifiées et des bonnes idées des minorités. Fondé sur le consensus, le système politique suisse suit déjà l'essentiel de cette approche. L'utilisation des technologies numériques promet cependant de nettement accélérer les processus décisionnels, tout en améliorant encore les possibilités de participation.

Recommandations

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.

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 publics et défis urbains), afin d'accélérer à la fois la transformation numérique, le gain de résilience et le développement durable.

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.

9 Champ d'analyse blockchain

9.1 Technologie et infrastructure

9.1.1 Conception de la blockchain

Une blockchain est, au sens littéral du terme, une chaîne de blocs de données qui forment ensemble une structure organisée et gérée de manière décentralisée, permettant d'effectuer des transactions sécurisées et vérifiables en toute indépendance et sans organe de contrôle central. Chaque transaction doit être signée numériquement pour en garantir l'infalsifiabilité et la vérifiabilité complète. Les nouvelles transactions s'ajoutent en bout de chaîne, bloc par bloc, dans l'ordre chronologique de leur exécution. Chaque bloc ajouté est associé au précédent par une empreinte digitale cryptographique, de manière à former une chaîne unique et traçable sans équivoque possible.

Depuis quelque temps, on entend souvent parler de «registre» (*ledger*), car une blockchain fonctionne effectivement comme un registre comptable (inscription et conservation des transactions). Les transactions peuvent se dérouler sur un réseau pair-à-pair et sans intermédiaires. Techniquement parlant, il serait donc plus juste de parler de technologie de registre distribué (*distributed ledger technology*), mais c'est le terme plus ancien de blockchain qui s'est imposé dans l'usage commun.

Les utilisateurs de la technologie blockchain doivent s'accorder sur la manière dont les blocs se succèdent et s'assurer qu'une fois ajoutés à la chaîne, ils ne puissent plus en être supprimés. Se servant de leur propre puissance de calcul, ils fournissent une preuve de travail ou de calcul (*proof of work*), qui protège contre les falsifications.

Il existe d'autres modèles de technologie blockchain, qui ne sont toutefois guère utilisés dans la pratique. Citons en particulier ceux fondés sur la preuve d'espace ou de capacité (*proof of space*; utilisation d'espace mémoire au lieu de puissance de calcul) ou sur la preuve d'enjeu ou de participation (*proof of stake*; niveau de participation de l'utilisateur basé sur le nombre de transactions). Des adaptations techniques sont toutefois possibles dans la pratique sous certaines conditions, comme l'a montré la division de la chaîne (*fork*) opérée lors de la création du Bitcoin Cash le 1er août 2017. Cette division s'est accompagnée de l'adoption d'un nouveau protocole permettant de former de plus gros blocs de données et de maîtriser ainsi le volume croissant de transactions sans pertes de temps.

9.1.2 Défis technologiques

Du point de vue de sa fonction, la technologie blockchain constitue une (nouvelle) infrastructure. Il faut donc garantir que tous les acteurs intéressés peuvent y accéder et que les données enregistrées (et éventuellement cryptées) sont accessibles aux ayants droit, et uniquement à eux. Étant donné que les blockchains se passent d'intermédiaires (tiers jouant le rôle d'«administrateurs»), il est nécessaire de concevoir le déroulement des transactions à contenu numérique de manière à ce qu'il soit sûr et efficace. À la différence de la blockchain ouverte, largement diffusée et échappant effectivement à toute influence de tiers, la blockchain permissionnée (*permissioned*

blockchain), appelée à gagner en importance, confie certaines fonctions à des intermédiaires.

Les transactions sont effectuées moyennant l'application d'un processus cryptographique. Les utilisateurs doivent recourir en l'occurrence au chiffrement et à la signature asymétriques (cf. ch. 4.4.1). Les normes de sécurité usuelles doivent aussi être appliquées aux processus des blockchains.

Suite au développement des blockchains utilisées pour les monnaies virtuelles (par ex. le bitcoin), il est aujourd'hui possible de créer également des «pièces colorées» (*colored coins*): lors du transfert d'un minimum de bitcoins, un champ de saisie permet de leur «annexer» un jeton (*token*), représentant par exemple une action. Le transfert des bitcoins sert alors de preuve du transfert de propriété de l'action «annexée».

D'autres systèmes (p. ex Ethereum) permettent de définir n'importe quels jetons indépendants les uns des autres et ne devant pas nécessairement être «annexés» à d'autres valeurs. Il est ainsi possible de définir des programmes ou des conditions avantageusement et à sa convenance, par exemple en relation avec des transactions effectuées sur la base de contrats intelligents. Avec les contrats intelligents, les blockchains incluent des algorithmes capables de définir des règles de transmission ou des transactions qui s'appliquent ou s'exécutent lorsque certaines conditions sont remplies.

9.1.3 Infrastructure décentralisée sans contrôle de l'État

La technologie de registre distribué est délibérément conçue comme une infrastructure décentralisée, autrement dit ne comportant pas d'organisation centrale devant être à même de gagner la confiance des utilisateurs. L'État ne peut pas exercer de contrôle sur les transactions effectuées, car en raison de la décentralisation du réseau, il ne dispose pas des moyens techniques nécessaires à cet effet.

L'utilisation de blockchains présuppose donc que la population fasse confiance au bon fonctionnement du système technique, sans que l'État ne puisse contribuer à renforcer cette confiance. À cet égard, le choix d'un tel système est aussi une question de politique et de valeurs sociétales.

9.1.4 Aspects sécuritaires de la technologie blockchain

Étant donné qu'elle repose sur les mécanismes de la cryptographie asymétrique, la technologie blockchain doit elle aussi faire face au défi de la cryptographie post-quantique (cf. 4.4.1). On ne peut donc pas partir de l'idée que la sécurité de la technologie blockchain soit garantie à long terme. Ce risque de sécurité est en outre accru par le fait que les mécanismes blockchain ne prévoient pas de possibilités de mise à jour. La structure de base des blockchains est anonyme et non définie. De plus, au moins en ce qui concerne la blockchain ouverte, il n'existe pas d'organe supérieur qui, en cas d'avancée décisive de la cryptographie, puisse actualiser le système. Une telle actualisation n'est possible que moyennant la mise en œuvre d'un nouveau système de chiffrement et le rechiffrement de toute la blockchain. Chaque projet de blockchain devrait donc prévoir un mécanisme de mise à jour, car si le mécanisme de chiffrement ne peut pas être renouvelé, la traçabilité à long terme des transferts de valeurs n'est plus garantie.

Toutefois, cette nécessité est en contradiction avec l'un des grands principes de sécurité et avec les avantages de la blockchain ouverte: aucun organe central ne doit avoir la possibilité de modifier la blockchain. Il faudrait donc prévoir un mécanisme permettant à la fois de transcrire les blockchains et de prévenir les modifications malveillantes, ce qui présuppose la collaboration de tous les services de vérification (mineurs) ainsi que de la communauté de base. Avec la blockchain permissionnée ou privée, qui dispose d'un administrateur central en charge de la gestion du chiffrement, ces questions ne se posent certes pas, mais ces infrastructures ne bénéficient pas de l'architecture sécuritaire décentralisée de la blockchain ouverte. Elles dépendent du niveau de sécurité des infrastructures numériques environnantes et ne sont par conséquent pas garantes en elles-mêmes d'un gain de sécurité.

Outre le chiffrement asymétrique, il faut également adapter le niveau de sécurité des sommes de contrôle (valeurs de hachage) aux progrès de la cryptographie. Avec le passage de l'actuelle norme SHA-256 à la norme SHA-384, la sécurité sera également garantie pour la première génération d'ordinateurs quantiques.

Les attaques contre l'intégrité globale d'une blockchain sont possibles lorsque l'attaquant, lors de la vérification et de la validation d'un nouveau bloc, autrement dit lors du minage (*mining*), contrôle plus de 51 % de tous les mineurs et peut toujours ajouter et implémenter ses blocs. Toutefois, ce scénario d'attaque présuppose, pour les principales cryptomonnaies, d'énormes capacités de calcul sur une longue période, ce qui relativise la rentabilité de l'attaque.

En raison de leur vaste surface d'agression et des valeurs qu'elles recèlent, les blockchains publiquement accessibles, surtout les levées de fonds initiales (*initial coin offering*, ICO) et les cryptomonnaies, sont des objectifs attrayants pour les attaquants. Les bourses d'échange de cryptomonnaies subissent donc régulièrement des attaques menées avec succès. Le manque de normes de sécurité claires, à même de protéger le système et tous les investisseurs, se fait ainsi cruellement sentir. Les tentatives de réglementation de la Chine montrent cependant combien il est difficile de contrôler et de réguler les bourses d'échange numériques: à peine ont-elles été interdites en Chine qu'elles sont renées sous un nouveau nom à Hong Kong. Des problèmes de sécurité se posent également pour les portefeuilles numériques (*wallet*) des détenteurs de cryptomonnaies, qui sont aussi régulièrement attaqués. Une approche envisageable pour réduire ce risque serait de diffuser des alertes de sécurité à l'intention des clients.

La blockchain est communément considérée comme une technologie d'avenir dans le domaine des registres, par exemple le registre foncier et le registre du commerce, ou plus généralement dans celui de l'enregistrement de l'historique des rapports de propriété de biens de valeur (cf. ch. 9.3.3). Toutefois, eu égard aux questions de sécurité non encore résolues, la compatibilité de la blockchain avec de telles tâches dans la pratique ne pourra être examinée en détail que dans un horizon temporel encore très lointain. La perte de la clé cryptographique, par exemple, peut conduire, dans le pire des cas, à l'impossibilité d'établir clairement les rapports de propriété tels qu'ils existent. Les biens et les valeurs concernés peuvent alors devenir impossibles à vendre ou à faire l'objet de transferts de propriété illégitimes. Malgré tous les avantages de la technologie blockchain, il serait problématique de faire reposer sans réserve des infrastructures de première importance du point de vue de la sécurité du droit sur une technologie encore sujette à de telles failles de sécurité.

Il faut également considérer, en relation avec l'utilisation de la technologie blockchain, que les attributs de sécurité que sont l'intégrité et la traçabilité sont couverts par la

structure de base même de la blockchain. C'est un net avantage par rapport aux bases de données, car dans une blockchain la traçabilité des transferts est un élément inhérent au système, ce qui n'est pas le cas dans une base de données. De plus, lorsque des systèmes décentralisés sont nécessaires et en cas de défaillance d'un ordinateur, la blockchain est un système plus tolérant aux erreurs qu'une base de données traditionnelle. Il faut cependant aussi prendre en considération les inconvénients de la technologie blockchain: les données figurant dans la blockchain elle-même sont accessibles et visibles par tous, d'où une absence totale de confidentialité. Pour une utilisation dans des domaines soumis à des obligations de confidentialité (élections, utilisations tombant sous le coup de la loi du 23 juin 2006 sur l'harmonisation de registres [LHR] ou de la législation sur la protection des données; voir aussi ch. 9.4.1), il est nécessaire de mettre également en œuvre un système de gestion des identités et des accès ainsi qu'un système de chiffrement, intégrés à la blockchain ou séparés. Or tous deux présentent un risque de sécurité, qui ne remet certes pas en question la plus-value sécuritaire de la blockchain, mais prête pour le moins à discussion.

Les avantages de la blockchain en matière de gestion des transactions résident dans la spécification claire des transactions qui doivent être exécutées. Les contrats intelligents sont un développement permettant de définir des règles de transaction au moyen d'algorithmes. Dès que les conditions fixées dans le contrat sont remplies, la transaction est automatiquement exécutée. Un risque lié aux contrats intelligents consiste en ceci qu'ils peuvent ne pas couvrir toutes les situations possibles. Si l'infrastructure blockchain devait prendre en charge à l'avenir des tâches complexes et sensibles précisément dans le domaine des contrats, il y aurait lieu d'en améliorer la sécurité, ainsi que de développer des systèmes d'assurance qualité appropriés ayant force obligatoire.

Recommandation

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).

9.2 Efforts de réglementation accomplis à ce jour

La technologie blockchain met une infrastructure mondiale à disposition. Pour être efficace, sa réglementation devrait donc aussi être mondiale. Vu les réalités politiques, il est cependant peu probable qu'une convention multilatérale soit conclue.

En matière de réglementation, les efforts (inter)étatiques suivants méritent d'être relevés: plusieurs initiatives sont à mettre au crédit d'organisations financières internationales concernées par les monnaies virtuelles, comme le Fonds monétaire international (FMI) et le Conseil de stabilité financière (CSF). En mai 2016, le Parlement européen a publié un rapport détaillé sur les monnaies virtuelles. On s'active également beaucoup au Royaume-Uni: un rapport du gouvernement de janvier 2016 présente, sur près d'une centaine de pages, les chances et les risques de la technologie de registre distribué. La Banque d'Angleterre et la *Financial Conduct Authority* britannique s'occupent aussi intensément de cette thématique.

Ce sont cependant les efforts de réglementation des organisations privées qui occupent le devant de la scène, en particulier ceux des organisations de normalisation,

basés sur le principe de l'autorégulation. Abstraction faite d'un projet de la Fondation Linux, c'est surtout l'Organisation internationale de normalisation (ISO) qui est très active, au travers de son comité technique sur les technologies des chaînes de blocs. Se fondant sur une proposition détaillée de *Standards Australia* (une organisation non étatique), ce comité travaille à l'élaboration de normes internationales en matière de technologie blockchain.

D'un point de vue général, l'insécurité du droit en relation avec la technologie blockchain n'en reste pas moins relativement importante, comme le montrent notamment les changements qu'Ethereum a dû apporter à sa technologie, suite à son exploitation abusive par une organisation décentralisée autonome (ODA) durant l'été 2016.

9.3 Domaines du droit particulièrement concernés par la technologie blockchain

9.3.1 Monnaies virtuelles

À ce jour, dans la pratique, c'est dans le domaine des monnaies virtuelles (surtout le bitcoin) que l'application de la technologie blockchain a pris le plus d'importance. La chaîne de blocs du bitcoin est conçue comme une base de données ouverte: l'accès n'en est pas contrôlé et il n'est pas nécessaire de s'enregistrer sous son propre nom pour l'utiliser. Chaque processus de paiement est inscrit dans la blockchain comme il le serait dans un registre comptable.

La sécurité des transactions est garantie par validation informatique, sur la base d'une opération mathématique. Le bitcoin émis ne peut être transmis qu'à un seul et unique destinataire. Nécessitant une grande puissance de calcul, ce processus n'est pas très efficace. Comme il est également onéreux et long, il faut s'attendre à ce que de nouveaux algorithmes soient bientôt développés pour l'améliorer.

Selon le domaine d'activité concerné, l'anonymat complet, tel qu'il est garanti par l'utilisation traditionnelle du bitcoin, est indésirable, du fait que les partenaires commerciaux souhaitent se connaître ou que les autorités (par ex. administration des douanes ou des contributions) sont intéressées à connaître l'identité des particuliers ou des entreprises effectuant les transactions. C'est pourquoi IBM et Microsoft, entre autres, sont en train de développer des blockchains avec contrôle d'accès, qui peuvent être utiles en particulier aux banques exerçant des activités de financement du commerce international (*trade finance*). L'accès à la blockchain est alors réservé aux utilisateurs disposant d'une autorisation spécifique. Dans la plupart des cas, ces infrastructures ne sont pas que de simples systèmes de paiement: les blockchains couvrent l'intégralité du processus de livraison des marchandises.

9.3.2 Relations entre l'État et les individus

L'utilisation de la technologie blockchain pour assurer la tenue d'élections est très discutée, mais n'a encore jamais été mise à l'épreuve de la pratique. Cette retenue dont on fait preuve dans le monde réel s'explique par la nécessité de garantir un niveau élevé d'intégrité des données (respect des normes de sécurité). Par rapport à celles d'autres pays, les expériences faites en Suisse ont montré que la possibilité de participer à des scrutins par voie électronique (vote électronique) est loin d'être facilement

conciliable avec le respect du principe de légalité et avec la garantie de la liberté de vote. Les normes de sécurité de l'information doivent en effet protéger le secret du vote et prévenir tout risque technique de manipulation des résultats. Or il est encore douteux que la technologie blockchain soit en mesure d'offrir ces garanties.

Le dossier électronique du patient, adopté en application de la loi fédérale correspondante entrée en vigueur en avril 2017, ne concerne pour l'instant que la numérisation des informations et la simplification de l'accès à ces dernières et ne prévoit pas de recourir à la technologie blockchain.

Dans le cadre de l'organisation de l'administration, il serait possible d'appliquer la technologie blockchain pour améliorer la communication entre les autorités et la société civile, notamment en termes de sécurité et de rapidité, à condition toutefois que l'infrastructure nécessaire soit technologiquement utilisable sans charges excessives. Dans les discussions à ce sujet, on se réfère souvent au programme de cyberadministration de l'Estonie et à la numérisation au Danemark. Il convient cependant de souligner que dans la plupart des cas (par ex. pour l'e-ID), ces deux pays ne s'appuient pas sur la technologie blockchain. Au Royaume-Uni, en revanche, on est en train d'analyser la faisabilité de plusieurs projets blockchain, notamment en relation avec le droit fiscal et le droit des assurances sociales.

Il ne faut cependant pas perdre de vue que dans tous les exemples d'application examinés, l'infrastructure est décentralisée et non contrôlée par l'État.

9.3.3 Registres

L'utilisation de la technologie blockchain est par nature particulièrement bien adaptée aux activités relevant du domaine des registres. Les blockchains fonctionnent en effet elles-mêmes comme des registres, qui enregistrent les transactions et les mémorisent de manière inaltérable dans l'ordre chronologique de leur exécution. Différentes possibilités d'utilisation de cette nouvelle technologie sont à la veille d'être exploitées, en particulier dans des domaines relevant exclusivement du droit privé, par exemple pour assurer le suivi du transport de conteneurs sur des navires de haute mer ou en relation avec la production et la distribution de denrées alimentaires. La technologie blockchain est en outre utilisée par exemple pour certifier la provenance d'objets d'art ou de diamants.

Des exigences particulières devront cependant être remplies en matière de respect des normes de sécurité, dès lors qu'il s'agira de gérer dans une blockchain des registres remplissant (aussi) une fonction publique. Cette remarque vaut non seulement pour les registres de personnes (future e-ID), mais également pour le registre du commerce et le registre foncier.

La tenue du registre du commerce dans une infrastructure blockchain faciliterait la communication avec le registre et en augmenterait l'efficacité. Étant donné toutefois que les inscriptions au registre du commerce sont réputées «exactes» et sont régies par le principe de la bonne foi (art. 933 CO), la fiabilité des informations devra impérativement être garantie. Eu égard à cette nécessaire «garantie d'exactitude», l'État ne pourra pas se soustraire, pour assurer la sécurité de l'information et la tenue irréprochable du registre en cas d'utilisation d'une blockchain, à l'obligation de remplir activement au moins une «fonction de surveillance» (cf. ch. 9.1.3).

La technologie blockchain offre des avantages similaires (efficacité, économicité) également pour la tenue du registre foncier. Ce registre étant aussi régi par le principe de

la foi publique (art. 971 et 973 CC), l'État sera également dans l'obligation de remplir certaines tâches de contrôle et de surveillance. Les processus présenteront en outre une complexité technologique accrue, car la plupart des inscriptions au registre foncier reposent sur l'établissement préalable d'un acte notarié. Les gains d'efficacité auront donc pour conditions que ces actes soient aussi délivrés électroniquement et puissent être directement transmis à la blockchain du registre foncier.

9.3.4 Organisations privées

Depuis quelque temps, on parle de plus en plus d'intégrer les processus organisationnels internes des entreprises dans une blockchain. Il est d'ailleurs prévu de créer le cadre légal qui permettra la tenue d'assemblées générales électroniques lors de la prochaine révision du droit de la société anonyme, même si ce ne sera d'abord que sur la base d'informations numérisées, sans recours à la technologie blockchain. L'utilisation de cette technologie est également envisageable en relation avec la comptabilité et les états financiers des entreprises, ainsi qu'avec les exigences de la gouvernance d'entreprise. Enfin, il ne faut pas négliger les défis particuliers que posera la communication avec les autorités de surveillance (mot clé: RegTech).

Le débat n'a guère porté jusqu'ici sur la légalité des sociétés dont l'existence est exclusivement numérique. Les traités d'État relevant du droit international privé ne sont pas axés sur ces formes d'entreprise, du simple fait qu'une organisation purement numérique n'est pas géolocalisable. Ce qui serait envisageable en l'occurrence, c'est de renvoyer aux pages Internet légalement pertinentes, par analogie avec le droit des consommateurs, qui prévoit souvent que les fournisseurs de biens ou de services doivent publier un impressum et des mentions légales sur leur site Internet.

9.3.5 Transactions

a) Contrats individuels

Le terme de contrat intelligent a d'ores et déjà trouvé sa place dans l'usage commun. On parle de contrat intelligent lorsque les relations contractuelles reposent sur un algorithme connecté et autoexécutable: au lieu de négocier le texte du contrat, on se réfère à des accords conclus antérieurement et intégrés dans un code source (généralement sous la forme de dispositions «Si..., alors...»). Les conditions contractuelles et les mécanismes de paiement sont fixés dans des protocoles cryptographiques. La participation personnelle des parties à la conclusion du contrat n'est pas forcément nécessaire. En cas de communication intermachines (telle qu'elle a lieu sur l'IdO grâce à l'interconnexion intelligente des objets), la «machine» (par ex. un robot) émet une déclaration obligeant fermement son propriétaire.

Les difficultés en matière de contrats intelligents commencent lorsque la loi prévoit que pour être valable, le contrat doit impérativement être conclu en la forme écrite. C'est le cas par exemple des contrats individuels conclus avec des consommateurs, mais aussi des contrats de cession de créances (art. 165 CO), ce qui a toute son importance pour la négociation d'actions. En cas de forme écrite obligatoire, il y a lieu de respecter les conditions fixées dans la SCSE, lesquelles impliquent un travail technique non négligeable et sont donc compliquées à appliquer.

Du point de vue du droit sociologique, les contrats intelligents (en raison du déroulement entièrement automatisé de la relation contractuelle) ne conviennent pas lorsqu'il faut tenir compte d'éléments personnels. Une telle perspective individuelle peut être

nécessaire en particulier dans un contexte d'exécution imparfaite des prestations. Des problèmes se présentent également lorsqu'un désaccord oppose les parties et qu'il ne peut pas être réglé par une modification du contrat déjà intégrée dans le code du programme. Dans ce cas, il est possible de prévoir un organe de médiation externe accessible par l'intermédiaire d'une interface technologique reliant la blockchain au monde réel (généralement Oracle).

b) Opérations de négoce normalisées

La technologie blockchain convient en principe bien à la négociation de papiers-valeurs, pour laquelle seuls sont généralement nécessaires des numéros de série, permettant une identification des titres garantie légalement. La forme écrite obligatoire des cessions de créances (art. 165 CO) et des transferts de droits-valeurs (art. 973*c* CO) se traduit toutefois par les complications techniques évoquées plus haut (SCSE).

Une autre possibilité d'exécuter des opérations de négoce normalisées dans une blockchain consisterait à considérer les *colored coins* comme des titres intermédiés. Les titres intermédiés sont des créances et des droits sociaux fongibles à l'encontre d'un émetteur, qui sont inscrits au crédit d'un compte de titres et dont le titulaire du compte peut disposer conformément aux prescriptions de la loi fédérale du 3 octobre 2008 sur les titres intermédiés (LTI). L'inscription des droits-valeurs a lieu par comptabilisation dans le registre principal d'un dépositaire. L'exploitant devrait donc gérer dans la blockchain à la fois le registre des droits-valeurs et le registre principal. Les actes de disposition sur les titres intermédiés interviendraient ensuite conformément aux instructions de l'aliénateur, qui ne sont soumises à aucune exigence de forme et peuvent aussi être données de manière implicite.

c) Systèmes organisés de négociation

La technologie blockchain se présente comme une infrastructure appropriée non seulement du point de vue des participants au marché qui effectuent des transactions normalisées, mais également pour les exploitants de systèmes organisés de négociation.

La loi du 19 juin 2015 sur l'infrastructure des marchés financiers (LIMF) prévoit des systèmes organisés de négociation (art. 42) et des systèmes multilatéraux de négociation (art. 26). Ces derniers ne conviennent pas à l'exécution de transactions blockchain, car tous leurs utilisateurs sont soumis à réglementation. Pour les systèmes organisés de négociation, l'exécution de transactions blockchain (négociation de valeurs mobilières et d'autres instruments financiers) est en revanche possible selon des règles discrétionnaires.

Ni les instruments financiers cotés ni les utilisateurs ne sont soumis à réglementation, mais l'exploitant du système de négociation doit généralement disposer d'une autorisation en tant que négociant en valeurs mobilières.

S'ils sont émis uniquement sur Internet (levée de fonds initiale), les *colored coins* constituent des droits-valeurs (art. 973*c* CO) et doivent par conséquent – comme indiqué plus haut – être considérés comme des titres intermédiés, afin de pouvoir être inscrits au crédit d'un compte de titres en tant que droits fongibles et pour que le titulaire du compte puisse en disposer (art. 3 et 6 LTI). Dans le même temps, le paiement est effectué avec une monnaie virtuelle. Toutefois, différentes questions concernant la post-

négociation, la compensation et le règlement doivent encore être clarifiées sur le plan juridique. Les commentaires qui précèdent ne s'appliquent pas aux instruments financiers «traditionnels», mais valent en particulier pour les droits-valeurs ou les certificats «alternatifs», tels que les certificats sur les matières premières, les métaux précieux, l'énergie ou le changement climatique.

9.4 Matières juridiques transversales

9.4.1 Blockchain et protection des données

La blockchain publique, en particulier, place la protection des données face à de nouveaux défis pour plusieurs raisons. Son principal atout réside incontestablement dans la combinaison de l'inaltérabilité des données avec le système de consensus et de vérification reposant sur la participation de tous les utilisateurs de la chaîne. De plus, la conception même de la blockchain publique part du principe que les données enregistrées sont exactes et qu'il faut donc en assurer l'intégrité. Ainsi, de nouveaux blocs peuvent être ajoutés à la chaîne, mais aucun ne peut ensuite en être supprimé. Il est certes possible de diviser la blockchain après une modification, mais le principe de base de la garantie de l'intégrité des données n'est pas remis en question pour autant. Or ces caractéristiques sont contraires à certaines dispositions fondamentales du droit de la protection des données, telles que le droit à l'oubli, le droit de correction et le droit d'opposition. La recherche en matière de blockchain et le droit de la protection des données sont donc appelés à trouver de nouvelles approches à même de résoudre ces difficultés, en appliquant à cet effet le principe de la protection de la vie privée dès la conception (*privacy by design*).

Par ailleurs, à y regarder de plus près, on constate que les données d'identité des utilisateurs d'une blockchain publique ne sont pas suffisamment anonymisées ou pseudonymisées pour pouvoir être considérées comme des données non personnelles. Rien que le transfert de pièces ou de jetons d'une personne à une autre moyennant l'utilisation de liens soulève déjà des questions. Le Tribunal fédéral et la Cour de justice de l'UE ont classé les adresses IP, y compris les adresses IP dynamiques, comme des données rendant identifiable la personne se trouvant derrière le raccordement Internet. Les identités peuvent en outre être déterminées sur la base des portefeuilles, grâce aux clés privées et publiques et aux valeurs de hachage. On peut donc objectivement présumer que les charges occasionnées par l'identification ne sont aujourd'hui plus si importantes que les utilisateurs refuseraient de les prendre en charge, si bien que l'identification serait assurée.

Les tensions existant entre blockchain et protection des données pourraient augmenter selon les contenus qui seront finalement adoptés dans le règlement de l'UE sur la vie privée et les communications électroniques (respect de la vie privée en ligne). Ce règlement pourrait en effet remplacer le critère de l'«identité» par celui de la «singularité». Cela signifie que non seulement l'identité des personnes, mais également ce qui permet de les distinguer des autres personnes relèverait des données à caractère personnel, obligeant ainsi à traiter toutes les informations et les communications concernées de manière confidentielle. Enfin, les jetons utilisés par exemple en relation avec le droit des registres, le droit des sociétés ou le droit des marchés financiers, ou encore lors d'élections, pourraient aussi contenir des données à caractère personnel, qu'il ne

serait toutefois pas possible de traiter de manière confidentielle en raison de la conception même des blockchains, axée sur la transparence.

La blockchain soulève également la question de l'applicabilité du RGPD (UE) et de la LPD à raison du lieu. Si une blockchain privée contient des données à caractère personnel, la validité extraterritoriale du RGPD impliquerait que tous les exploitants proprement dits d'un nœud de réseau et même tous les mineurs soient considérés comme des responsables du traitement ou des sous-traitants, et ce dans le monde entier si la blockchain concernée a été proposée au sein de l'UE. Ils devraient alors respecter tous les principes de la protection des données, tels que celui de l'obtention du consentement de chaque utilisateur, ce qui ne serait absolument pas praticable. La législation, les autorités de surveillance et la technique se trouvent donc face à une tâche difficile: préserver les possibilités qu'offrent les blockchains sans porter atteinte à la protection de la vie privée ni au droit à l'autodétermination en matière d'information.

9.4.2 Questions relevant du droit de la responsabilité

Toute nouvelle technologie soulève de nouvelles questions en matière de responsabilité. Il s'agit en l'espèce de déterminer qui est responsable en cas d'«erreur» se produisant lors de l'utilisation de la technologie blockchain, autrement dit de régler la problématique de l'attribution des responsabilités.

Un autre défi concerne la gestion des prétentions des lésés en cas de faillite de l'exploitant d'une infrastructure blockchain. Étant donné que les personnes concernées pourront prétendre non pas à certains biens provenant de la masse en faillite – comme dans une faillite traditionnelle –, mais plutôt à la restitution de données, il sera nécessaire d'inscrire dans la procédure d'exécution forcée un droit de revendication assorti de garanties suffisantes (modification de la LP). Enfin, les prescriptions de procédure civile relatives au règlement des litiges devront être adaptées aux particularités de la technologie blockchain (règlement en ligne des litiges).

Recommandation

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), par la tenue de registres numériques et par la protection des données.

10 Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche

10.1 Situation actuelle et perspectives de développement

Ce chapitre présente tout d'abord les processus, les facteurs et les caractéristiques de la numérisation qui revêtent une importance particulière pour l'effort visant à sensibiliser la population à cette évolution et à développer ses compétences en la matière. Il brosse ensuite un rapide portrait du système éducatif suisse en se concentrant sur les aspects liés au numérique.

10.1.1 Quatre défis fondamentaux

1. Le premier aspect qui caractérise la numérisation réside dans l'**accélération de l'automatisation** de nombreux procédés dans le monde du travail. L'automatisation n'est pas un phénomène nouveau. Intervenant de façon récurrente, elle a déjà engendré de profondes mutations durant la seconde moitié du XX^{e} siècle, notamment dans la production industrielle. On peut cependant prévoir que les nouvelles technologies numériques s'orientent de plus en plus vers l'automatisation, de sorte que des robots et des systèmes logiciels seront à même d'assumer des tâches plus complexes. Il n'en demeure pas moins difficile de prévoir les conséquences pratiques de la numérisation sur le monde du travail. Certaines études prédisent une chute dramatique des emplois, tandis que d'autres se fondent sur les expériences recueillies jusqu'ici pour nuancer ces prédictions. Dans l'ensemble, l'emploi a plutôt augmenté ces dernières années en Suisse malgré les avancées de l'automatisation, alors qu'il a reculé dans d'autres pays.

Nul ne saurait nier que nous traversons un changement structurel et que le domaine de l'emploi subira inévitablement un bouleversement. Tout comme les ouvriers à la chaîne ont été remplacés par des robots industriels, des tâches traditionnelles pourraient laisser la place à de nouveaux champs d'activité dans un avenir proche. Cette perspective soulève une question fondamentale: quel genre de compétences et de formation la population doit-elle acquérir pour faire face à ces changements. À l'heure actuelle, il est impossible de prévoir les spécificités – type, nombre, exigences et profil – des emplois futurs. La numérisation rendra sans doute nombre de métiers beaucoup plus exigeants, mais elle pourra aussi fournir des outils, telle la réalité augmentée, pour en faciliter l'exercice.

Dans l'ensemble, il est certain que le défi de la numérisation accroîtra le besoin de formation continue. Il importe dès lors de sensibiliser les gens au rôle de l'apprentissage tout au long de la vie et de leur proposer des formations appropriées.

2. Le deuxième trait caractéristique de la numérisation réside dans la **quantification de tous les domaines de la vie**. Bien qu'il soit impossible de pleinement chiffrer certains aspects de l'existence humaine, tels l'amour, la dignité ou la confiance, les technologies actuelles facilitent la quantification de nombre d'entre eux: des appareils mo-

biles dénombrent les pas franchis ou surveillent le pouls, des tachygraphes numériques enregistrent le style de conduite et des compteurs électriques intelligents identifient des schémas dans la consommation de courant. L'accent mis sur des valeurs telles que l'efficacité, la maximisation du profit et l'accroissement des performances, qui occupent une place de choix dans la plupart des sociétés modernes, ne fait que renforcer cette propension à tout quantifier. Les nouvelles technologies de mesurage permettent d'ailleurs à tout un chacun d'optimiser le «soi» de manière inouïe. Elles accroissent ainsi la pression qui pousse l'individu à comparer son efficacité et ses performances avec celles d'autrui.

La quantification de nombreux domaines de la vie encouragée par la numérisation soulève une question fondamentale: comment le système éducatif doit-il réagir face aux nouvelles possibilités qui s'ouvrent de la sorte dans le monde du travail et dans la vie privée? Il importe en particulier de sensibiliser les citoyens aux chances et aux risques de la quantification. Se «mesurer soi-même» présente en effet une ambivalence: dans certains cas (maladies chroniques, par ex.), un individu peut adapter son mode de vie pour son propre bien; dans d'autres, il court le risque d'une concurrence effrénée, voire l'épuisement professionnel ou mental. Ces effets pourraient notamment toucher l'employabilité et détermineraient ainsi directement l'avenir des formations initiale et continue de la main-d'œuvre. Il faut aussi s'attendre à des conséquences positives et négatives au niveau des organisations et des collectivités publiques. Les nouvelles technologies numériques peuvent par exemple optimiser la logistique, le trafic et la distribution d'énergie et donc atténuer les risques environnementaux. Elles peuvent toutefois également inciter ces organisations à se concentrer uniquement sur ce qui est mesurable, de sorte que le pouvoir de décision des humains sera de plus en plus remplacé par des algorithmes. Ce type de transfert peut entraîner des problèmes tels que la discrimination ou l'amenuisement du potentiel créatif humain. Ces problèmes sont abordés au chapitre 11, consacré à l'éthique.

Pour ce qui est de sensibiliser la population et de développer ses compétences, le défi lié à la quantification consiste à promouvoir une dose suffisante d'esprit critique, afin d'aider les gens à considérer les chances et les risques de la mesurabilité et de la transcription de nombreux processus en algorithmes avec réalisme, pour qu'ils puissent utiliser les nouvelles possibilités de manière responsable et autonome.

3. La troisième grande caractéristique réside dans la multiplication, grâce aux technologies numériques, des **possibilités de créer, de diffuser et de modifier des contenus médiatiques**. Des médias tels les livres, la radio et la télévision ont largement contribué à l'évolution de la société. Désormais, les réseaux modernes de communication, à l'instar d'Internet et de la téléphonie mobile, et les technologies numériques qui leur sont associées permettent en principe à tout un chacun de créer et de diffuser des informations. Dans le même temps, les moyens de manipuler sciemment des contenus médiatiques deviennent de plus en plus sophistiqués, de sorte qu'il sera toujours plus difficile de déterminer si certains contenus (images, vidéos ou enregistrements sonores) sont authentiques ou s'ils ont été falsifiés. Dans le flux actuel de l'information, il est pratiquement impossible d'identifier des contenus qui ont peut-être été modifiés. Dans ces conditions, l'individu devient de plus en plus manipulable, notamment parce que les réseaux sociaux divulguent également des renseignements sur chaque utilisateur et que ces informations peuvent servir à les influencer (tant en matière de consommation que de choix politiques).

Les «gardiens» traditionnels de la circulation de l'information, tels les journalistes ou les distributeurs de musique ou de vidéos, assument un rôle nouveau. Les conséquences économiques dans des domaines comme la presse, le cinéma et la musique sont énormes.

Cette évolution place en particulier les professionnels des médias face à des défis inédits en matière de formation et de formation continue. L'ensemble de la population aura cependant besoin d'une éducation aux médias. Les changements que la numérisation implique pour les médias se retrouvent à tous les niveaux de la société. Preuves en sont des phénomènes tels que le cyberharcèlement et l'apparition de nouveaux acteurs médiatiques (les producteurs de chaînes populaires sur YouTube, par ex.), voire l'influence de la propagande numérique sur des processus démocratiques, cette dernière faisant actuellement l'objet d'études qui se penchent sur les élections américaines et le référendum sur le Brexit. Ces changements apportent de nouveaux problèmes. L'utilisation des réseaux sociaux peut en effet engendrer une dépendance et mettre en danger la cohésion sociale en isolant l'individu.

Le défi consiste dès lors à fournir aux citoyens la compétence médiatique requise pour utiliser de manière responsable les outils disponibles. Cette remarque vaut en particulier pour les professionnels des médias numériques.

4. Enfin, la quatrième caractéristique réside dans une **dépendance croissante vis-à-vis de systèmes autonomes**. Nous utilisons des ordinateurs, Internet et les smartphones dans tous les domaines de la vie. Même si notre monde actuel est déjà fortement dépendant de la technologie, les liens et les interconnexions entre les systèmes techniques laissent encore largement la possibilité à l'être humain de les contrôler, d'intervenir et de décider. Avec la mise en réseau croissante d'objets physiques et virtuels (Internet des objets) et la généralisation de l'intelligence artificielle (IA), la dépendance face à des systèmes décisionnels autonomes s'accroît rapidement. Or cette évolution risque de priver de plus en plus l'être humain de ses chances de décider, de participer et de créer.

Cette perte se manifeste également lorsque des décisions individuelles concernant une norme donnée conduisent à une situation où cette norme devient contraignante pour tous les autres. Selon Rousseau, il s'agirait de l'expression d'une «volonté de tous», mais pas d'une «volonté générale». Autrement dit, des individus prendraient des décisions sans tenir compte des intérêts de l'ensemble de la société. Même si un individu est libre de décider ou non de respecter une norme et, donc, d'appartenir ou non à un réseau (d'appliquer une technique), il ne peut pas négocier lui-même cette norme et il existe rarement d'autres options appropriées auxquelles il pourrait recourir. Pour participer par exemple à un forum de clavardage sur WahtsApp, force est d'accepter les conditions d'utilisation correspondantes. Ces conditions impliquent souvent la collecte de données sur les utilisateurs, indications qui alimentent ensuite des systèmes d'intelligence artificielle, qui se familiarisent ainsi avec le comportement humain. Grâce aux masses de données énormes qu'elles traitent, les machines peuvent puiser dans une expérience beaucoup plus vaste qu'un être humain ne le pourra jamais. Les propriétaires de machines intelligentes peuvent donc exercer un pouvoir sur d'autres personnes. Quant aux utilisateurs, ils ne peuvent pas s'opposer efficacement à ces mécanismes, car ils ne possèdent pas d'informations suffisantes à leur sujet. Il ne saurait alors être question d'un consentement éclairé. Des idées illusoires, comme l'espoir que «l'économie se chargera bien de trouver de bonnes solutions», pourraient empêcher l'État et la population d'exiger la mise en place de conditions optimales.

Le principal défi posé par les efforts déployés pour sensibiliser la population et développer ses compétences consiste à fournir aux individus les moyens d'exercer un contrôle humain et un pouvoir de décision suffisants pour ne pas devenir de simples «unités fonctionnelles» dans un système sociotechnique complexe. Un tel rôle contreviendrait à la notion de dignité humaine (voir le chapitre consacré à l'éthique).

10.1.2 Spécificités du système éducatif suisse

Compte tenu de l'évolution en cours, il est indispensable de sensibiliser la population et de lui donner les moyens de reconnaître les mutations sociales induites par l'automatisation, la quantification, la médiatisation et la dépendance croissante envers l'informatique, d'identifier les changements qui la touchent plus particulièrement et de contribuer à les façonner. Dans ce domaine, un gros travail incombe au système éducatif et aux médias. Le système éducatif englobe toutes les institutions qui dispensent une formation, soit aussi bien les écoles des degrés primaire, secondaire et tertiaire, que les établissements chargés de la formation professionnelle, les universités populaires et les instituts de formation continue. En ce qui concerne la formulation de recommandations, il convient de tenir compte de deux particularités.

Premièrement, le système éducatif suisse regroupe un grand nombre d'acteurs, dont chacun a sa propre idée sur la manière de réagir aux défis de la numérisation. Ces dernières années, les propositions de réforme se sont multipliées, entraînant une certaine lassitude (surtout au sein du corps enseignant), voire des excès. Il n'est par ailleurs pas facile, en Suisse, de réunir une majorité favorable à des modifications dans l'éducation de base. Toutes les propositions visant le système éducatif devraient tenir compte de ces obstacles.

Deuxièmement, l'organisation du système éducatif suisse relève pour l'essentiel des cantons. D'où la difficulté de mener une démarche cohérente. Cette réalité a le mérite de laisser de la place aux essais pratiques et à la diversité. Les recommandations ci-après sont dès lors des propositions qui devraient inciter à exploiter la variété des possibilités offertes, de manière à élaborer un large ensemble de mesures pour faire face à la grande incertitude que suscitent les changements et les défis à venir.

10.2 Possibilités et limites

L'objectif de sensibilisation, d'autonomisation et de formation est de développer l'«habileté numérique» la population, soit ses capacités d'utiliser de façon responsable les chances offertes par la numérisation et d'aborder ses défis de manière adéquate. L'habileté numérique englobe tout ce qui accroît les possibilités et les compétences de chaque citoyen de réussir sa vie dans un monde numérique. Cela ne signifie toutefois pas que l'éducation puisse se contenter de laisser l'individu relever tous les défis de la numérisation, car l'habileté numérique ne suffit pas pour résoudre tous les problèmes. Certaines solutions passeront par l'adoption de lois, par exemple pour imposer des obligations aux fournisseurs de prestations numériques. À titre de comparaison, considérons que les gens suivent une formation générale et spécifique (en vue d'obtenir le permis de conduire) pour devenir des usagers de la route responsables; il n'en demeure pas moins que les pouvoirs publics doivent édicter des mesures de sécurité et

de protection de l'environnement. Les lois et les prescriptions d'application garantissent plutôt que les constructeurs et les vendeurs de véhicules remplissent leurs obligations.

Au vu des défis formulés, voici ce qui découle de ces réflexions.

10.2.1 Accélération de l'automatisation

Tout le monde s'accorde pour dire que la numérisation aura un impact social majeur. Comme nous l'avons mentionné, il est difficile de prévoir l'évolution de l'emploi. Il est dès lors utile d'élaborer des scénarios afin de se préparer à une éventuelle hausse, voire à un taux élevé, du chômage. Sous l'effet des changements, le type d'occupation de la population évoluera par ailleurs vers des activités à caractère social, environnemental et créatif. En conséquence, la formation devra abandonner les modèles standardisés pour privilégier la personnalisation. L'accélération de l'automatisation engendrera aussi de nouvelles formes de collaboration entre l'homme et la machine (intelligence artificielle ou IA) et de collaboration entre êtres humains gérée par l'IA. Le système éducatif devrait ainsi s'interroger sur les possibilités de collaboration entre être humain et IA.

10.2.2 Quantification de tous les domaines de l'existence

Pour ce qui est de la quantification de tous les domaines de l'existence, il importe de poser comme principe que les moyens et les possibilités techniques ne sont que des outils et ne constituent nullement une fin en soi. De plus, le droit des citoyens à décider en toute indépendance de l'utilisation de leurs données devrait faire office de règle suprême. En conséquence, il convient premièrement d'assurer l'autodétermination en matière d'informations et de restreindre le «mesurage» des citoyens par les décideurs publics ou privés. Ce domaine doit être réglé en priorité au niveau législatif et ne relève donc pas directement de l'éducation. Deuxièmement, il faut garantir que le recours croissant aux algorithmes afin de traiter les données collectées pour l'aide à la décision, voire pour les prises de décision automatisées, n'enfreint pas des valeurs fondamentales. Bref, les algorithmes ne doivent ni manipuler ni discriminer, mais au contraire s'avérer équitables et durables. Ces exigences imposent notamment des mesures au niveau de la formation professionnelle initiale et continue des spécialistes qui développent et appliquent des algorithmes. Les fondements de la conception éthique (voir aussi chap. 11) devraient dès lors faire obligatoirement partie de la formation professionnelle des ingénieurs en informatique. Il importe en outre d'éveiller la conscience des individus face aux effets secondaires indésirables et négatifs de la collecte de données personnelles. Ce point pourrait faire partie intégrante d'une éducation numérique de base, à inclure dans l'éducation scolaire.

La mise au point de programmes d'enseignement ainsi que de moyens didactiques destinés à l'éducation scolaire ainsi qu'à la formation professionnelle initiale et continue doit prendre en compte la raison d'être de la quantification. Le mesurage engendre un contrôle croissant aux fins d'efficacité. Or une optimisation absolue entrave cependant l'innovation: dans les processus créatifs (en sciences, par ex.), le progrès résulte fréquemment du hasard ou des tâtonnements. Les erreurs peuvent provoquer des illuminations décisives et s'avérer cruciales pour une percée. De plus, on ignore souvent à l'avance ce qui sera important à l'avenir.

Quantifier ou transformer en algorithme à l'excès ne fait pas que réduire les espaces de liberté individuelle. Une telle dérive compromet aussi le non-conformisme, la diversité et la pensée transversale, pourtant essentiels aux processus d'apprentissage et à la capacité de la société de faire face aux crises. Autrement dit, il convient dans une certaine mesure d'accepter l'inefficacité et le libre arbitre. La liberté de choix ainsi créée ouvre des espaces de débat, des instants de réflexion et de nouvelles marges de manœuvre. De ce point de vue, la quantification en tant qu'instrument de la réflexion et de l'introspection de l'individu ou des institutions mérite d'être perçue de manière plus positive que lorsqu'elle sert à juger et à sélectionner.

Il importe par ailleurs de faire comprendre à tout individu que même les renseignements qu'il décide de divulguer sur lui-même peuvent imposer des contraintes à autrui. Une femme qui déclare, par exemple lors d'un entretien d'embauche, qu'elle ne peut pas ou ne veut pas avoir d'enfants augmente peut-être ses chances de décrocher le poste. Son comportement peut cependant désavantager d'autres femmes qui n'abordent pas ce sujet, car le simple fait de ne pas le mentionner peut constituer une information en soi. Enfin, il convient de relever que l'exactitude des données recueillies et leur pertinence posent toujours problème, de même que la validité des modèles qui serviront à exploiter ces données. Pour éviter de restreindre les libertés, certaines données ne devraient donc pas être collectées ou utilisées. Définir précisément lesquelles exige une large réflexion dans la société, appuyée par toute une série de mesures.

Relevons par ailleurs que les processus d'apprentissage et de formation sont eux-mêmes de plus en plus souvent quantifiés. Plus l'enseignement est dispensé sous forme numérique, plus il est possible de mesurer le processus d'apprentissage: fréquence à laquelle une personne accède aux contenus des cours; temps dont elle a besoin pour lire certains textes; nombre de fautes qu'elle fait en rédigeant une réponse, etc. Tous ces renseignements peuvent être enregistrés et exploités. Leur utilisation peut certes servir à identifier des difficultés spécifiques d'apprentissage, mais soulève nombre d'autres questions: dans quelle mesure l'apprentissage est-il altéré lorsque chaque étape est jaugée et que les relevés collectés sont transmis sous forme agrégée à l'apprenant ou à un employeur potentiel? Quel est l'impact sur le rôle de l'enseignante ou de l'enseignant? À qui appartiennent les indications recueillies durant la formation: à l'étudiant ou à l'école/la haute école? Est-il possible de baser les décisions de sélection non pas sur des examens, mais sur le «profil d'apprentissage»? Quel effet aura sur la candidature d'une personne à un poste un dossier dans lequel le *curriculum vitae* rédigé par cette personne est remplacé par une analyse de son mode d'apprentissage? La recherche pédagogique doit se pencher de plus près sur ce genre de questions afin de prévenir des effets indésirables, telles que de nouvelles formes de discrimination.

Enfin, il importe de tirer au clair le rôle de l'accroissement de données et d'algorithmes disponibles pour le processus éducatif en soi. Des jeux de données comportant un grand potentiel d'innovation sociétale (données anonymisées sur les modèles de déplacements de véhicules ou sur la consommation d'électricité, par ex.) devraient, même s'ils ont été réunis par des entreprises privées, être librement accessibles moyennant des conditions appropriées (sous forme anonymisée et agrégée, par ex.). La manière exacte d'organiser ces conditions dépendra des cas individuels. De nouvelles approches – données ouvertes *(Open Data),* code source ouvert *(Open Source),* libre accès *(Open Access),* science ouverte *(Open Science)* et innovation ouverte *(Open Innovation)* – recèlent un potentiel d'innovation combinatoire. Si les élèves, les enseignants, les étudiants ou les professionnels en formation continue y ont accès, ils

peuvent tester de nouvelles idées et contribuer eux-mêmes à l'innovation. Ces approches ouvertes et la science citoyenne revêtent aujourd'hui une grande importance. Dans ce cas aussi, il faut cependant souligner que toutes les données ne peuvent pas être divulguées, notamment pour des raisons de confidentialité ou de sécurité. En matière d'analyse des données, il serait toutefois possible de fixer le volume de données disponibles et les fonctions activées en fonction de la qualification, de la réputation, de l'équité et de la responsabilité de l'usage des données, tout en assurant des possibilités d'accès identiques à tous.

10.2.3 Éducation aux médias

Ces dernières années, l'éducation aux médias est devenue un élément incontesté de l'offensive sur le front de la formation numérique. Cette éducation repose avant tout sur la transmission de connaissances de base concernant le traitement et l'utilisation de l'information, les technologies des médias et les conséquences individuelles et sociétales de leur application, l'effet culturel des médias et la possibilité de s'en servir dans les domaines de la création et de la conception. Sur le plan du contenu, cela revient à promouvoir la capacité de trouver les informations pertinentes et de les évaluer d'un œil critique, de structurer les renseignements et de produire de nouvelles connaissances. La transmission de capacités servant à surmonter les aspects problématiques des réseaux sociaux (telles les fausses nouvelles) ainsi que le risque d'addiction ou le cyberharcèlement complètent cette éducation. Pour dispenser l'éducation aux médias, il importe d'adapter en conséquence les programmes d'études et la formation des enseignants, adaptations souvent déjà en voie de réalisation.

Les formations initiale et continue des professionnels des médias méritent une attention particulière. Compte tenu des profondes mutations que la numérisation impose au secteur des médias, on a pris conscience de la nécessité d'assurer aux professionnels une formation approfondie pour leur transmettre les compétences mentionnées. Les efforts déjà lancés devraient être soutenus et ce soutien peut conduire à la création de nouveaux profils professionnels, comme celui de journaliste de données. Un accent devrait être mis sur la formation (technique) permettant de mieux identifier tous les types de falsification numérique. Les moyens de manipuler les données ne cessant de se multiplier, le domaine numérique verra sans doute apparaître de nouveaux gardiens, qui garantiront la qualité et la fiabilité des informations diffusées.

10.2.4 Dépendance croissante à l'égard de systèmes autonomes

L'interconnexion croissante d'objets physiques et virtuels (Internet des objets) et la généralisation de l'intelligence artificielle augmentent rapidement la dépendance à l'égard de systèmes décisionnels autonomes. Même dans le cas de systèmes complètement autonomes, il faudrait désigner clairement les responsables qui, le cas échéant, seraient appelés à rendre des comptes. De plus, l'être humain devrait dans l'idéal au moins vérifier le processus. Il importe en outre d'anticiper les risques de perte de contrôle et de s'interroger sur la manière de les contrer. Parmi les mesures à mettre en œuvre, mentionnons par exemple la suspension du négoce ou l'invalidation et la révocation d'opérations lors de mini-krachs (chutes brusques et inattendues des cours sur les marchés financiers). Dans le domaine de la collecte de données, il serait possible de prévenir le risque de perte de contrôle en recourant à une sphère privée distincte. Les données seraient alors traitées de telle sorte que l'individu ne soit plus identifiable et que sa vie privée reste protégée. Une solution de ce genre pourrait aussi

s'appliquer en cas de revente ou de sous-traitance des données. Enfin, il importe, autant que possible, de favoriser le droit à la codécision de la personne concernée. Il est également envisageable de recourir à des normes telles que la compatibilité, la transparence et l'adaptabilité (codécision). C'est cependant le domaine qui offre la marge de manœuvre la plus étroite pour sensibiliser et autonomiser la population.

Tout le monde s'accorde pour dire que la transformation numérique modifiera de plus en plus les aptitudes requises dans le monde du travail. Les compétences en matière informatique seront certainement très demandées. La principale d'entre elles est la pensée dite computationnelle (voir. ch. 4.3.3), à savoir la «capacité individuelle d'identifier les données d'un problème et d'en établir une modélisation abstraite en le décomposant en étapes ou éléments partiels, à concevoir et à développer des stratégies de solution et à les présenter de manière formelle, de telle sorte qu'un être humain, mais aussi un ordinateur puissent les comprendre et les mettre en œuvre»[15]. Il est possible d'acquérir cette compétence cruciale en utilisant un langage de programmation et en programmant un ordinateur ou en collaborant avec l'intelligence artificielle. À l'école, il est aisé de la transmettre aux enfants, par exemple en les chargeant de concevoir des jeux informatiques basiques ou de programmer des robots simples.

Il serait toutefois contre-productif de tout concentrer sur les TIC ou de tout limiter aux TIC, car d'autres aptitudes sont tout aussi cruciales. Tous les degrés du système éducatif – du primaire au tertiaire, de même que la formation professionnelle et la formation continue – pourraient, s'ils ne l'ont pas déjà fait, formuler, en collaboration avec tous les acteurs concernés, les compétences requises pour relever les quatre défis mentionnés plus haut (et les éventuels autres défis).

Nous ne formulons nullement ici un archétype des compétences nécessaires à l'avenir, une telle formulation dépasserait largement le cadre du présent rapport. Elle devrait résulter d'un travail réunissant tous les acteurs (y compris les personnes à former et les enseignants) et suivre une approche ascendante. À titre d'exemple, nous esquissons ci-après quelques-unes des compétences qui peuvent s'avérer utiles pour aborder les défis évoqués.

Vu l'accélération de l'automatisation, il est indispensable de fournir à tous les individus les moyens de la comprendre, d'apprendre rapidement à l'intégrer et de s'adapter avec souplesse aux nouvelles chances et possibilités offertes. Comme déjà mentionné ci-dessus, la pensée computationnelle constitue une clé à cet effet. D'autres capacités seront également essentielles: partager des connaissances, collaborer et concevoir conjointement des produits et des services. Les facultés créatrices, sociales et environnementales gagneront autant en importance. D'autres dispositions encore s'avéreront fort utiles, comme celle de penser de manière autonome et critique (esprit critique), c'est-à-dire la capacité de penser consciemment par soi-même, pour analyser, interpréter ou évaluer et tirer des conclusions, mais aussi la faculté de se concentrer plus longtemps sur une activité, de même que des aptitudes manuelles.

En matière de quantification de tous les domaines de la vie, il sera essentiel de savoir gérer (au sens large) des données avec compétence, c'est-à-dire de savoir ce qu'elles représentent, comment les traiter, comment interpréter les résultats et connaître les incertitudes qui leur sont associées). Une meilleure compréhension de la notion de probabilité ainsi que des calculs de probabilité occupera sans doute une place plus grande dans la formation de base de tout individu.

[15] https://www.nzz.ch/feuilleton/soll-der-mensch-wie-ein-computer-denken-ld.1292090, (état en novembre 2018)

La formation aux médias pourrait aborder les conséquences sociales, éthiques, juridiques ou économiques de la transformation numérique ou de la fracture numérique, de même que la protection des données, la sphère privée, les droits de l'homme, la dignité humaine et l'attitude à adopter face aux fausses nouvelles. La capacité de réfléchir, celle de trouver des renseignements pertinents et de les évaluer d'un œil critique ainsi que celles de structurer l'information et de produire de nouvelles connaissances joueront aussi un rôle important.

Pour pouvoir réagir aux défis posés par la dépendance croissante face aux systèmes autonomes, il sera par ailleurs essentiel à tout individu de comprendre les bases du traitement de l'information et de connaître les chances offertes par la conception collaborative et créative à l'ère numérique de même que par le travail au sein d'équipes interdisciplinaires. Il pourrait également s'avérer crucial de sensibiliser les gens à la nature sociotechnique des systèmes d'information, c'est-à-dire leur expliquer que les systèmes informatiques ont des implications sociétales, qu'ils engendrent des changements (parfois indésirables) et qu'un système de valeurs est, implicitement ou explicitement, intégré à tout système informatique.

Quelles que soient les compétences requises, nous apprendrons tout au long de notre vie. À l'ère numérique, nous vivrons dans une société de l'information et de la connaissance; il apparaît donc souhaitable que nous accordions tous une grande place à l'apprentissage tout au long de la vie. Cet apprentissage désigne les cours classiques de formation continue, l'apprentissage autonome basé sur la littérature spécialisée, l'apprentissage au travail, l'apprentissage en ligne ou en groupe, la participation à des manifestations culturelles, la réception ou la consultation des médias[16], les MOOC (cours en ligne ouverts à tous), l'apprentissage dans des ateliers (de fabrication) collaboratifs (*fab labs* ou *maker spaces*).

10.3 Conclusions

Les canaux appropriés pour sensibiliser la population et lui fournir les moyens requis comprennent la formation, la culture et l'espace public. Pour ce qui est de la formation, nous partons du principe qu'elle relève du système éducatif suisse.

10.3.1 École obligatoire et filières de culture générale jusqu'au degré tertiaire

Il importe de collaborer avec tous les acteurs concernés afin d'établir un référentiel, adapté à chaque degré de l'école obligatoire et de toutes les filières de culture générale (jusqu'au tertiaire), des compétences de base requises pour se préparer à la transformation numérique. Ce référentiel devra être revu et mis à jour à intervalles réguliers. Les modalités de la transmission du «savoir-faire numérique fondamental» doivent inclure tous les éléments de l'apprentissage humain et ne pas se limiter à l'apprentissage au moyen de l'ordinateur.

La CDIP doit exploiter les différents sites éducatifs cantonaux pour mener des expériences et encourager les échanges ainsi que l'apprentissage mutuel. Voici quelques considérations qui mériteraient d'être prises en compte:

[16] https://www.nzz.ch/wissenschaft/bildung/weiterbildung--gebot-oder-fluch-der-zeit-1.18179900 (état en novembre 2018)

- La transmission des connaissances sur les principaux aspects de la numérisation devrait respecter la neutralité de genre et tenir compte des différents contextes de formation.[17]
- L'élaboration d'un dossier pédagogique électronique mérite d'être saluée. Il importe néanmoins de préserver l'autodétermination des apprenants dans le domaine de l'information, c'est-à-dire qu'ils doivent pouvoir décider de l'utilisation des données. (Dans le monde du travail, il en va de même pour les employés.) Le groupe d'experts recommande de ne quantifier qu'avec parcimonie le comportement individuel en matière d'apprentissage et de restreindre la transparence à ce sujet. Ce point devrait être inclus dans la révision de la loi fédérale sur la protection des données (LPD).
- Malgré le décalage entre la vitesse de l'évolution actuelle (des compétences) et la lenteur des processus démocratiques, il faut trouver un moyen de progresser pour que les décisions relatives au système éducatif (plans d'études, compétences, etc.) restent d'actualité.
- Il serait possible d'encourager des écoles modèles au bénéfice de la latitude requise pour tester dans la pratique de nouveaux contenus et formes d'enseignement. Elles pourraient, par exemple, réduire la place de l'enseignement de type frontal pour laisser les élèves élaborer des projets personnels dans des espaces de travail collaboratif ou recourir au modèle de l'«enseignement inversé» (acquisition de l'information par un travail personnel accompagné). De telles écoles pourraient en quelque sorte devenir des organismes apprenants à même de fournir des points de repère à la politique en matière de formation, aux administrations responsables, à d'autres écoles ou aux hautes écoles pédagogiques.
- L'éducation de base – où il est impossible, comme nous l'avons indiqué, d'introduire rapidement au niveau des structures des changements décidés par les autorités centrales – est justement le domaine où le corps enseignant et les directions scolaires jouent un rôle décisif. Il convient de les motiver, de les encourager et de leur donner les moyens de préparer les élèves à la numérisation. La formation des enseignants revêt donc une importance décisive: l'école a besoin de personnel compétent en matière numérique, capable d'élaborer ses propres solutions et disposant de la liberté et du temps nécessaires. Il importe aussi de mettre à sa disposition les outils pédagogiques correspondants (pour l'éducation aux médias ou l'apprentissage de techniques telles que la programmation ou la robotique, par ex.).
- Dans les degrés inférieurs, on pourrait également envisager de multiplier les projets utilisant le numérique (telles des imprimantes 3D). Des professionnels externes, des spécialistes ou des étudiants en informatiques pourraient en outre contribuer à l'enseignement.
- Les enfants et les adolescents s'approprient souvent très vite les technologiques numériques. En d'autres termes, les enseignants pourraient aussi apprendre de leurs élèves. Il s'agirait donc de promouvoir le co-apprentissage.

[17] https://ictswitzerland.ch/media/dateien/Bildung/ICTswitzerland-Positionspapier-Frauen_staerken_die_Informatik.pdf (état en novembre 2018); https://ictswitzerland.ch/publikationen/attraktivitaet-von-ict-berufen/ (état en novembre 2018)

- Il faut vérifier s'il convient d'accorder moins d'importance à l'évaluation des performances et réserver plus de place à la motivation, à la créativité, à la curiosité et à la collaboration des élèves.
- Il importe d'encourager (davantage) l'enseignement personnalisé et l'initiative individuelle, mais aussi le développement du caractère et l'intelligence collective.
- On pourrait s'interroger sur les moyens d'introduire des espaces d'expérimentation ou des options spécifiques du numérique dans les écoles.
- Les ateliers collaboratifs (de conception ou de fabrication) pourraient constituer de nouvelles formes d'enseignement et d'apprentissage; ils pourraient, par exemple, offrir un cadre moderne, numérique et créatif pour les travaux pratiques.
- La conception et l'utilisation des bâtiments scolaires devraient tenir compte des nouvelles formes d'enseignement et d'apprentissage.
- Il convient d'accorder une grande priorité à la mise en œuvre des compétences en matière de médias et d'informatique.
- La Confédération pourrait examiner si elle entend maintenir son modèle d'affaires basé sur l'édition ou si les ressources éducatives libres (matériel didactique et pédagogique libre assorti d'une licence ouverte) constituent une autre option.
- Le monitorage de l'éducation devrait vérifier si les compétences en matière de médias et d'informatique définies dans le Lehrplan 21 sont atteintes
- La Confédération pourrait renforcer educa.ch en lui allouant des compétences et des ressources financières (comme elle le fait pour le projet de cyberadministration), afin d'accroître son potentiel d'innovation.
- La Confédération veille à l'intégration des principaux aspects de l'espace éducatif numérique dans les objectifs communs de la politique en matière de formation.
- Les hautes écoles pédagogiques se chargent d'inclure les connaissances les plus récentes sur la formation numérique dans la formation initiale et continue des enseignants.

10.3.2 Hautes écoles

L'enseignement numérique fait aujourd'hui défaut dans les hautes écoles suisses. Or il faudrait l'intégrer dans le programme d'études (au même titre que l'enseignement de la culture générale). Les structures internes actuelles sont par ailleurs insuffisantes pour garantir la collaboration interdisciplinaire; il faut donc les renforcer tout en tenant compte des spécificités de chaque établissement.

Les remarques ci-après pourraient être prises en compte dans la mise en œuvre de ces recommandations générales:

- L'enseignement numérique mentionné ne devrait pas seulement servir à transmettre des compétences numériques (telles que la pensée computationnelle) et des connaissances de base sur la cybersécurité, mais aussi les connaissances appropriées relevant des sciences humaines (histoire, sciences sociales et économiques, philosophie, éthique et droit) qui servent à étudier la numérisation de la société.

- Il convient de recourir davantage aux formes d'apprentissage numériques, aux MOOC (cours en ligne ouverts à tous), aux mondes virtuels interactifs ou aux plateformes d'apprentissage personnalisé, les étudiants devant toutefois conserver le contrôle sur les données ainsi générées concernant leur comportement d'apprenants.
- La recherche soutenue par les moyens publics devrait, autant que possible, mettre à disposition (en libre accès) les résultats obtenus (données et publications). Il convient également de promouvoir la participation de scientifiques amateurs aux travaux de recherche (science citoyenne).
- Pour faciliter le transfert de connaissances, il faudrait encourager les étudiants à acquérir des compétences entrepreneuriales de même que favoriser la création de start-up universitaires. Des espaces d'expérimentation et des plateformes devraient aussi permettre aux PME d'accéder plus facilement au savoir et aux connaissances universitaires.
- Comme pour les enseignants des degrés inférieurs, il convient de motiver, d'encourager et d'habiliter les professeurs à se préparer à la numérisation et à suivre une formation continue appropriée, de même qu'à tester les nouvelles possibilités et à les étudier.
- Il faudrait tester de nouveaux modèles pour financer la recherche. Dans certains domaines, les fonds pourraient être accordés non pas sur la base d'ébauches de projets, mais sur celle des résultats obtenus et de leur impact (refinancement). Un tel système permettrait de récompenser les travaux qui fournissent (rapidement) des résultats utiles sur des sujets importants.
- Des programmes ou des centres de recherche idoines devraient favoriser l'élaboration d'éléments essentiels pour un encadrement responsable de la transformation numérique, par exemple dans les domaines de l'éthique du numérique et de la conception éthique.

Recommandation:

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.

10.3.3 Formation professionnelle initiale et formation continue

Les structures qui aideraient les professionnels de tous les secteurs à se former tout au long de la vie font défaut. Après mûre réflexion, il faudrait en particulier définir les points suivants: qui est responsable de l'apprentissage tout au long de la vie, qui doit le payer, comment le mettre en œuvre, le financer et l'encourager (allégements fiscaux, bourses d'études, journées rémunérées de formation continue, etc.)?

Les propositions ci-après pourraient être prises en compte:

- Les professionnels de tous les domaines pourraient se voir attribuer un «compte formation» à vie, qui leur permettrait d'interrompre leur carrière afin d'acquérir de

nouvelles compétences. Certaines taxes incitatives existantes pourraient contribuer à le financer.

- Les professionnels de tous les domaines devraient acquérir des connaissances de base sur la cybersécurité. Ils pourraient ensuite les approfondir à l'aide de modules consacrés aux besoins spécifiques de certains groupes de métiers. La formation pourrait recourir à du matériel qui a déjà fait ses preuves pour favoriser la sécurité informatique dans l'entreprise et l'administration publique. Pour disposer rapidement d'un matériel approprié, il serait même possible de recourir à celui de pays voisins (Allemagne, Autriche, France et Italie) en fonction des régions linguistiques suisses.[18]
- La formation en informatique devrait inculquer aux futurs développeurs l'importance qu'il y a à considérer les implications éthiques, sociales, économiques, culturelles, juridiques et sociétales de leur travail. Les concepteurs d'algorithmes devraient comprendre qu'évaluer les conséquences de leur activité fait partie de leurs tâches et ils devraient apprendre à procéder à cette évaluation.
- Tous les professionnels des médias devraient suivre une formation ciblée, incluant les connaissances techniques et judiciaires requises pour être à même d'assurer la crédibilité des médias numériques.
- La maturité professionnelle devrait inclure des matières propres à la numérisation (informatique et médias, par ex.). La formation aux médias devrait être étendue à la filière générale du secondaire II.
- Dans le domaine de la formation continue, il serait envisageable de créer un portefeuille de formations, individuel et électronique. À ce propos, il importe de répondre à des questions du genre: des certificats sous forme électronique sont-ils admissibles? Que faut-il encore enregistrer? Comment faut-il utiliser ces données? Quelles sont les prérogatives dans ce domaine et à qui reviennent-elles? Il serait possible de répondre à ces questions en créant une identité numérique. Il importe en priorité de réduire la quantité des données et de préserver l'autodétermination en matière d'information.
- En ce qui concerne le matériel didactique, il conviendrait de développer des applications adaptées aux différentes branches scolaires ou à la matière à enseigner.

Recommandation:

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.

10.3.4 La culture pour sensibiliser au numérique

[18] En voici un exemple: *Leitfaden zur Umsetzung der Basis-Absicherung nach IT-Grundschutz: In 3 Schritten zur Informationssicherheit* de l'Office fédéral allemand pour la sécurité des technologies de l'information: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 (état en novembre 2018)

La culture est un excellent moyen de communication pour éveiller l'esprit critique. La promotion culturelle doit dès lors chercher davantage à inciter les artistes en tout genre à mener une réflexion critique sur la transformation numérique.

Les propositions ci-après pourraient être prises en compte:

- L'art pourrait susciter l'enthousiasme pour l'ère numérique: art numérique interactif, jeux informatiques, courts ou longs métrages, etc. Les activités appropriées pourraient être menées dans des musées ou lors de festivals. L'art pourrait également contribuer à sensibiliser la population à des sujets tels que la numérisation ou l'intelligence artificielle (IA), à aborder ces sujets de manière ludique et à les considérer d'un point de vue critique. Les romans policiers et les séries télévisées peuvent également servir à sensibiliser au numérique.
- Il serait possible d'encourager l'art numérique, en créant par exemple un prix national. Un plus grand nombre de subventions pourraient être accordées aux œuvres relevant de ce domaine.
- Il faudrait encourager des lieux permettant de tester une utilisation du numérique à des fins créatrices et artistiques. De tels lieux comprennent des espaces libres et créatifs, comme des ateliers de production participatifs, mais aussi des bibliothèques qui proposent des animations socioculturelles. Il convient aussi de recommander les compétitions publiques de programmation et une notion élargie des «défis urbains» ou «olympiades urbaines» (voir chap. 11). Une initiative du genre «A Nation of Makers[19]» offrirait l'occasion aux citoyens «ordinaires» ainsi qu'aux adolescents de développer des idées novatrices et de les tester. D'autres exemples comprennent l'initiative «Open Innovation» (qui consiste à ouvrir le processus d'innovation au savoir externe et interne à une organisation afin d'accroître le potentiel innovant) ou l'idée de la recherche participative (qui fait intervenir le plus rapidement possible de futurs utilisateurs dans le processus de développement de nouveaux produits et d'applications mobiles). Mentionnons également que des centres communautaires peuvent se convertir au numérique (*fab labs* ou ateliers collaboratifs[20]). Un atelier de ce genre existe à Amsterdam (De Waag[21]) et un autre à Fribourg (Bluefactory[22]). La Confédération pourrait encourager des projets similaires dans chaque ville, afin de susciter l'enthousiasme pour le numérique.
-

Recommandation:

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.

[19] https://nationofmakers.us/about.html (état en novembre 2018). Nation of Makers (une nation de concepteurs) est une organisation américaine sans but lucratif qui apporte un appui aux adeptes états-uniens du mouvement «faites-le vous-même» en les aidant à créer des communautés et à partager des ressources ainsi qu'en leur offrant une assistance juridique.

[20] Ateliers d'innovation ouverts, où les intéressés peuvent utiliser des outils de pointe (imprimantes 3D, cutters laser, fraises CNC, microcontrôleurs, logiciels CAD, etc.), mais aussi des outils traditionnels, des machines pour travailler le bois et pratiquement tous les autres outils utiles à un bricoleur ou à un inventeur.

[21] http://waag.org/en (état en novembre 2017)

[22] https://www.bluefactory.ch/ (état en novembre 2017)

11 Champ d’analyse transformation numérique et éthique

11.1 Situation actuelle et évolution future

11.1.1 Remarques préliminaires

L’éthique constitue le fondement d’une société durable. En encadrant les comportements, la morale garantit depuis des siècles une coexistence pacifique et prospère dans les différents contextes culturels et historiques. Certains conflits sociaux ont résulté certes sur des écarts fondamentaux dans l’acception de valeurs morales, différences qu’il n’est pas facile d’aplanir. Au fil du temps, des normes éthiques ont néanmoins fait leurs preuves et forment la base du vivre ensemble dans des sociétés modernes et pluralistes. Les droits de l’homme servent par exemple à mener une existence autonome et responsable et à protéger l’individu contre les agressions de l’État, d’entreprises et d’autres personnes. Des libertés fondamentales telles que la liberté d’opinion, de conscience et d’information devraient favoriser le développement personnel dans l’intérêt économique et social, pour autant qu’elles ne restreignent pas l’épanouissement d’autrui. La sphère privée garantit des espaces de loisirs et d’épanouissement, qui permettent d’expérimenter de nouvelles idées et formes d’existence tout en protégeant l’individu dans son développement et contre les agressions externes.

Bien que la conception des valeurs morales fondamentales décrites ci-dessus se soit surtout imposée dans la culture occidentale et que les sociétés diffèrent dans la manière dont elles conçoivent les valeurs éthiques comme la liberté, l’égalité et la justice, les droits de l’homme fondamentaux constituent un cadre de référence éthique largement reconnu au niveau international. Des conflits de valeurs sont bien sûr inévitables; il peut ainsi arriver que les libertés publiques de l’individu s’opposent aux revendications de solidarité formulées par le groupe. Dans ces cas, l’éthique a pour tâche de soumettre les arguments de chaque point de vue à un examen critique et d’intégrer les appréciations correspondantes dans la réflexion sur la société. L’un des défis que posent les sociétés modernes et pluralistes réside dans l’impossibilité de présupposer qu’il existe une notion «correcte» ou «juste» des valeurs éthiques, car cette notion doit être négociée pour chaque conflit à résoudre. Quelle est, par exemple, la limite du devoir de solidarité dans une assurance-maladie lorsque certains prennent sciemment des risques de santé? Voilà le genre de questions éthiques qui sont au cœur de nombreux débats sociaux.

Lorsque des évolutions sociétales ou des innovations technologiques modifient une société, elles ont un impact sur la morale qui règne dans cette société. La conception de certaines valeurs peut ainsi varier ou alors ces valeurs peuvent perdre ou gagner en importance dans certains domaines. Si l’on considère la démocratie comme une valeur fondamentale de l’organisation d’une société, il est certes possible de retracer ses origines jusqu’aux cités-États de la Grèce antique. Depuis cette époque, la notion de la valeur «démocratie» a cependant nettement changé: aujourd’hui, il est par exemple normal d’inclure les femmes et les personnes aux moyens financiers limités dans les processus de décision. Même s’il existe différentes formes de démocratie – comme la démocratie directe ou représentative –, nous estimons que cette forme de

régime offre une solution pérenne qui mérite d'être protégée, car elle permet de tenir compte de points de vue différents et de trouver un équilibre entre eux. Selon les connaissances actuelles, c'est le régime qui offre les meilleures conditions pour garantir la paix, la prospérité et la stabilité. Les principaux traits caractéristiques et principes de fonctionnement des démocraties comprennent notamment la liberté (y compris la liberté de la presse et la liberté d'opinion), l'autodétermination, l'épanouissement de soi, la responsabilité, le pluralisme, la séparation des pouvoirs, le partage du pouvoir, l'équilibre des pouvoirs, la protection des minorités, la codécision, la participation, la transparence, l'équité, la justice, la légitimité et la protection de la sphère privée. En fin de compte, il est possible d'affirmer que nombre de ces valeurs ont été inscrites dans la Constitution en réaction à des événements graves comme les guerres, les génocides ou les conséquences de systèmes politiques totalitaires. Elles forment ainsi le fondement de l'ordre qui sous-tend la société moderne.

11.1.2 Valeurs fondamentales touchées par la numérisation

Quelles sont donc les valeurs éthiques que la numérisation met plus spécialement en jeu? Sans prétendre à l'exhaustivité, voici celles qui méritent d'être mentionnées:

- **Dignité humaine et vie privée:** La Déclaration universelle des droits de l'homme de 1948 (Charte internationale des droits de l'homme adoptée par l'ONU) débute par cette phrase: «Tous les êtres humains naissent libres et égaux en dignité et en droits.» Bien qu'il ne soit pas facile de formuler une définition juridique de la dignité humaine, ce texte lui accorde une valeur inaliénable et souligne l'obligation de protéger l'être humain. La dignité humaine signifie notamment que les êtres humains ne peuvent pas être utilisés comme des moyens pour atteindre un objectif ou qu'ils ne doivent pas être considérés comme une «marchandise». Dans le cadre de la numérisation, le droit de tout individu à maîtriser les informations qui le concernent et la protection de la vie privée sont une composante essentielle de la dignité humaine. Son respect exige en particulier que nul ne puisse faire l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Ce principe est mentionné explicitement dans la Charte de l'ONU des droits de l'homme, dont l'application relève des États qui l'ont signée. Cette disposition a pour objectif de protéger des domaines de la vie qui garantissent la liberté de mouvement, de développement et de comportement à tout individu. La sphère privée ne comprend donc pas seulement une protection contre la mise à nu, mais également le droit d'«être laissé tranquille», c'est-à-dire le droit de se prémunir contre des influences manipulatrices personnalisées et d'être à l'abri de ces influences dans le cadre privé. La sphère privée inclut également le droit de s'isoler, de ne pas être sans cesse accessible et de se mettre «hors ligne».
- **Égalité et non-discrimination:** L'égalité est une règle fondamentale de la société, qui se reflète dans le principe d'égalité devant la justice. Elle ne signifie pas qu'il soit incorrect, du point de vue éthique, de différencier le traitement réservé à diverses personnes (par exemple en versant des salaires différents pour des prestations différentes). La différenciation poserait problème si elle devait tenir compte de critères tels que la couleur de la peau, le sexe ou la religion, qui sont dépourvus de pertinence dans l'accès à certains biens, possibilités ou postes. On parle alors de discrimination, c'est-à-dire d'une inégalité de traitement dépourvue de justification objective.

- **Autonomie et autodétermination:** Le principe d'autonomie attribue des droits (et des obligations) aux êtres humains pour ce qui est de choisir et de maîtriser leur propre existence. L'autonomie et l'autodétermination se retrouvent dans le principe du consentement éclairé. Dans le cadre numérique, on parle de l'autodétermination en matière d'information, notion qui désigne le droit de l'individu de se prononcer sur la collecte, la conservation, l'utilisation et la diffusion de données qui le concernent.
- **Transparence:** Pour pouvoir exercer leur autonomie et leur droit de participation, les individus ont besoin de disposer de connaissances sur les affaires qui les concernent. Le monde politique requiert une communication ouverte et pertinente sur les décisions qui font l'objet des débats. C'est le seul moyen qui permette aux différents acteurs de se faire une opinion bien informée et de prendre librement leurs décisions. La transparence est donc également indispensable à un consentement éclairé quant à l'utilisation de données personnelles.
- **Solidarité:** La solidarité désigne le lien qui unit les individus d'une communauté. Elle signifie que les individus ne seront pas abandonnés à eux-mêmes face à certains risques et dangers auxquels leurs activités ou leur existence les exposent. La collectivité leur apporte un appui dans des situations critiques, telles que la maladie et les accidents, ainsi que pour lutter contre la pauvreté. Ce principe admet que quiconque peut tomber malade ou devenir pauvre sans que sa responsabilité soit mise en cause et que l'absence de solidarité diminue le goût du risque, alors que celui-ci est justement indispensable à l'innovation et à l'esprit d'entreprise, qui servent les intérêts de la société.
- **Sécurité:** L'une des principales tâches de la collectivité est de protéger la vie et la propriété. Au sens de valeur fondamentale, la sécurité ne désigne dès lors pas seulement une protection directe contre le vol, les blessures ou une mort violente, mais aussi la préservation de conditions matérielles permettant de profiter pleinement des valeurs mentionnées plus haut. Il s'agit donc également de garantir la paix, car les droits fondamentaux peuvent perdre leur validité en période de conflit ou de guerre.

Même s'il leur arrive d'entrer en conflit – lorsque certaines libertés s'opposent au devoir de solidarité, par exemple – ces valeurs sont des repères aussi essentiels que fondamentaux. Il appartient au monde politique et à la société d'établir un équilibre stable entre ces valeurs et de veiller à trouver des solutions novatrices pour éviter ou surmonter les éventuels dilemmes.

11.1.3 Problèmes éthiques concrets

La numérisation à laquelle nous assistons modifie la société en profondeur et exerce donc une influence sur ses fondements éthiques. Si la comparaison avec l'industrialisation qui a débuté au XVIII^{e} siècle s'impose, les bouleversements s'annoncent cette fois plus rapides et plus absolus. Le défi consiste à encadrer cette transformation historique de telle sorte qu'elle se déroule de manière pacifique et sans provoquer des révolutions ou des conflits violents.

Que l'on considère la gestion des connaissances, les réseaux logistiques et même l'établissement de relations humaines, le numérique s'impose désormais dans pratiquement tous les domaines de la vie, modifiant les flux de l'information et l'organisation

de nombreux processus. De plus en plus de sphères sociales sont peuplées de systèmes numériques, dotés de capteurs et de terminaux «effecteurs» entre lesquels s'inscrit le traitement de l'information. Ils agissent comme des intermédiaires techniques dans les procédés de production et les relations humaines. De plus, l'informatique – science sur laquelle repose la numérisation – véhicule une certaine vision du monde: celui-ci est considéré comme un conglomérat d'informations et de flux d'informations. Aussi la tentative de dominer le monde s'exprime-t-elle dans la volonté de mesurer et d'influencer ces flux d'informations.

Concrètement, le risque existe que les outils de la numérisation puissent également servir à atteindre des objectifs contraires à l'éthique (double usage). De l'avis de nombreux spécialistes, ils sont à même de menacer les réalisations sociales. Voici des exemples du recours à des technologies numériques qui pourraient entraîner des effets indésirables:

- **Numérisation du monde du travail:** L'impact de la numérisation sur le monde du travail a récemment fait l'objet d'intenses débats. L'accélération de l'automatisation, grâce à l'intelligence artificielle et à la robotique, peut menacer des postes et la participation à l'activité économique, d'où le risque d'inégalités sociales. Une nette diminution de l'emploi pourrait saper le droit au travail et à un revenu, de même que la possibilité de s'épanouir par le travail. Une telle évolution pourrait finalement porter atteinte à la dignité humaine, que l'État doit veiller à protéger. De plus, une part importante des recettes de l'État proviennent des impôts prélevés sur le revenu du travail, de sorte que l'éventuel manque à gagner pourrait remettre en cause le bien-être général et la stabilité politique. La transition technologique offre naturellement aussi d'énormes chances économiques et sociales. La transformation numérique peut toutefois provoquer des évolutions disruptives dont il importe d'atténuer autant que possible les effets par des moyens politiques afin de garantir la sécurité et la paix. Il est évident en outre que la numérisation du monde du travail aura une incidence marquée sur les aptitudes professionnelles qui seront requises à l'avenir pour répondre aux exigences de l'économie. Le système éducatif est donc appelé à réagir. Ce sujet est traité au chapitre 10 (Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche).
- **Surveillance massive:** Une surveillance généralisée, englobant par exemple de grandes portions des échanges sur Internet, porte atteinte à la vie privée des citoyens et, partant, à leur liberté individuelle de même qu'à leur droit à l'autodétermination et à l'épanouissement. Une surveillance de ce genre peut ainsi conduire indirectement à de l'autocensure et à une diminution de la variété des opinions et de l'engagement social, conséquences qui peuvent réduire la capacité de fonctionnement des collectivités démocratiques. Les programmes de surveillance de la NSA et de la CIA ainsi que le programme britannique «Karma Police» illustrent la portée de la surveillance massive. Nombre d'États appliquent des techniques éprouvées pour soumettre les dissidents à une surveillance ciblée et entraver leurs actions, voire les menacer.
- **Réseaux sociaux:** L'utilisation actuelle des réseaux sociaux et le recours croissant à des «social bots» (agents conversationnels spécifiques) favorisent des phénomènes tels que les *shit storms* (déferlement de commentaires haineux) et la diffusion de fausses nouvelles *(fake news).* Ces réseaux ne sont pas garants d'une information de bonne qualité ou pondérée et ni leurs bulles de filtres ni

leurs chambres d'écho n'atténuent la polarisation sociale. Dans le même temps, les moyens permettant de manipuler des contenus médiatiques deviennent de plus en plus sophistiqués, de sorte qu'il sera toujours plus difficile de déterminer si certains contenus (images, vidéos ou enregistrements sonores) sont authentiques ou s'ils ont été falsifiés. Ces moyens multiplient les possibilités de manipuler les processus politiques, même par des États tiers, ce qui pourrait menacer la stabilité sociale d'un pays. Des réactions par trop hâtives risquent de conduire à la création de ministères de la Vérité (comme dans le roman *1984*, de George Orwell) et mettre en danger des droits démocratiques fondamentaux, comme la liberté de la presse et la liberté d'expression. Le bon usage des réseaux sociaux et de leurs avantages constitue dès lors un autre défi de taille pour le système éducatif. Les enjeux de la formation sont abordés plus en détail dans le chapitre 10 (Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche).

- **Manipulation numérique *(big nudging):*** La manipulation numérique désigne l'activité qui consiste à utiliser des informations personnalisées pour exercer une influence sur le comportement d'un grand nombre d'individus, et ce, au niveau du subconscient également, afin de poursuivre par exemple des objectifs politiques. Une telle manipulation englobe un conflit de valeurs entre le bien-être et l'autonomie des citoyens et devient particulièrement problématique sur le plan éthique lorsqu'il manque de transparence et qu'il est inévitable. La personnalisation de certains messages, dans la publicité par exemple, fait partie intégrante du modèle d'affaires de certaines sociétés qui offrent des prestations sur Internet (moteurs de recherche ou réseaux sociaux, par ex.) et qui collectent ainsi les données des usagers. La plupart des clients de ces plateformes savent certes qu'ils reçoivent de la publicité ciblée en échange du recours gratuit aux services proposés. Les exemples récents (facebook, par ex.) ont mis en lumière le problème que pose l'utilisation abusive des données pour mener des campagnes de manipulation en prévision de votes populaires. En 2016, ce problème a été largement débattu dans le cadre du scrutin sur le Brexit et les élections présidentielles aux États-Unis. L'efficacité de ces manipulations est certes controversée. Il n'en demeure pas moins indéniable qu'elles reposent sur une utilisation abusive et non transparente de données et qu'elles portent également atteinte à la vie privée des utilisateurs. La collecte croissante des flux de données (concernant la consommation d'électricité, le trafic, etc.) peut par ailleurs inciter l'État à tenter, de manière antidémocratique, de contrôler l'attitude des individus, contrôle qui restreint le libre arbitre et un comportement responsable. Si la manipulation numérique devait être largement utilisée à l'avenir, elle pourrait saper le principe – qui va aujourd'hui de soi – selon lequel notre société repose sur la participation libre et responsable de tous.
- **Modélisation prédictive et contrôle:** L'utilisation des technologiques numériques pour prévoir les résultats de processus sociaux et vérifier leur déroulement est étroitement liée à la problématique de la manipulation numérique. La participation d'un individu aux décisions qui le concernent est une caractéristique essentielle de la dignité humaine et constitue un pilier immuable de la démocratie. Le respect de la dignité humaine veut que les sujets humains ne soient pas traités comme des animaux, des objets ou des données. Dans un État de droit démocratique, les individus sont donc amenés à rendre des comptes sur la base de leur comportement effectif, en application du droit pénal par exemple. Ils doivent

alors bénéficier d'un droit d'opposition. Le traitement moderne des données pourrait remplacer la pondération qu'un individu responsable entreprend à l'aide d'une «boussole éthique» afin de décider par des algorithmes prévisionnels. La modélisation prédictive pourrait ainsi généraliser le recours à la gestion des risques dans de nombreux domaines de la société. Des algorithmes capables de prédire un comportement inapproprié, comme ceux de la «prévision policière», risqueraient non seulement de bafouer la présomption d'innocence dans le système judiciaire, mais aussi d'entraver des essais faisant appel à des solutions innovantes. De telles applications réduiraient sensiblement le poids de la responsabilité personnelle. Les individus pourraient, en fin de compte, être privés de la liberté d'assumer la responsabilité de leurs actes.

- **Crédit social:** Le système de «crédit social» (qui consiste à attribuer des notes à chaque citoyen), actuellement en voie d'implémentation en Chine, est l'un des projets concrets destinés à influencer le comportement individuel. Déjà en place dans certaines régions, ce programme, qui utilise le numérique pour exercer un contrôle social, vise à obtenir par la contrainte certains comportements politiques et économiques, dans la mesure où la note décrochée par l'individu déterminera par exemple son accès à des postes de travail, à des services ou à certaines conditions de crédit. Un tel système détruit le pluralisme social et favorise l'esprit de soumission et non pas la responsabilisation des citoyens. Lorsque les ressources sont rares, le crédit social peut désavantager de nombreux individus. Les méthodes de ce genre menacent les fondements mêmes d'une existence digne.
- **Algorithmes décisionnels entièrement automatisés:** Un rôle croissant des données dans l'accès numérique au monde et un recours accru à des algorithmes décisionnels entièrement automatisés peuvent constituer une menace pour l'équité et la justice. Un problème général réside dans le fait que de tels algorithmes «apprennent» à partir de données issues du passé et qu'ils peuvent ainsi tendre à consolider des préjugés et des solutions obsolètes. Les véhicules autonomes et, plus généralement, les systèmes d'intelligence artificielle ayant une fonction décisionnelle peuvent être amenés à se prononcer sur des questions de vie ou de mort. Ces logiciels sont alors confrontés à des dilemmes éthiques, aujourd'hui déjà implicites (lors de certains rares accidents, le conducteur doit décider rapidement entre deux mauvaises solutions), mais qu'il faudrait expliciter, si des algorithmes devaient à l'avenir être appelés à les résoudre. Or cette explicitation comporte le risque d'attribuer une «valeur» plus ou moins élevée à certaines personnes. Les juristes et les éthiciens estiment cependant qu'une telle distinction (fondée sur l'âge, la formation, le revenu, etc.) n'est pas admissible, car le droit exige que tous les individus bénéficient du même traitement. Il importe donc de recourir à des solutions techniques, politiques et sociales appropriées pour éviter l'apparition de dilemmes qui mettent en jeu la vie d'un être humain. Des systèmes techniques peuvent s'avérer utiles à cet effet dans la mesure où leur application diminue le nombre de situations problématiques et si la programmation générale, par exemple, réduit au minimum l'ampleur des dommages corporels. Pour éviter que des valeurs différenciées soient attribuées aux individus, il est aussi possible d'appliquer des solutions aléatoires. Lorsque le recours à de tels systèmes conduit à accroître le nombre de dilemmes à expliciter (c'est-à-dire des dilemmes pour lesquels l'algorithme doit contenir une solution), leur emploi ne se justifie pas. Dans ce contexte, la mise au point et l'utilisation de

systèmes d'armes autonomes posent un problème particulier. Lors de l'implémentation et de l'application d'algorithmes décisionnels automatisés, la transparence est dès lors de mise sur les fondements de la prise de décision, la traçabilité et la responsabilité («contrôle humain significatif). Cette exigence s'impose également lorsque les algorithmes décisionnels ne risquent pas d'être confrontés à un dilemme. Ces systèmes sont de plus en plus souvent déployés dans la communication avec les êtres humains. Si le contexte n'indique pas qu'un être humain s'adresse à une machine, la situation équivaut à une tromperie, qui pourrait engendrer des inconvénients pour l'interlocuteur humain (les réactions de ce dernier pourraient, par exemple, être enregistrées afin d'améliorer la fonction vocale de l'algorithme). Il convient donc d'informer au préalable l'interlocuteur humain qu'il est en interaction avec une machine.

- **Cyberrisques:** Les technologies numériques s'imposant toujours plus dans les différents domaines de la vie (Internet des objets, par ex.), des infrastructures essentielles se prêtent davantage à la manipulation, au vol, au sabotage et à la destruction, d'où une menace pour la sécurité et la paix. Réagir aux cyberrisques en mettant par trop l'accent sur la cybersécurité peut de plus entrer en conflit avec des valeurs fondamentales et remettre leur respect en cause. Dans ce contexte, un problème réside dans le fait que des services de renseignement ne rendent pas publiques les vulnérabilités qu'ils découvrent dans des logiciels (vulnérabilités *zero-day*), attitude qui empêche de protéger les systèmes en question (mentionnons, à titre d'exemple, les attaques du rançongiciel WannaCry en mai 2017). Dans l'ensemble, les cyberrisques représentent un danger croissant non seulement pour la souveraineté individuelle, mais aussi pour la souveraineté des entreprises et des États.

11.1.4 Défis éthiques fondamentaux

Ces exemples de différents aspects éthiquement contestables des technologies numériques renvoient à quelques problèmes fondamentaux associés à la numérisation et qui ont déjà été abordés au chapitre 10 (Champ d'analyse information de la population en matière de numérique, développement des compétences, participation des utilisateurs et recherche).

Premièrement, la numérisation permet de quantifier de nombreux domaines de l'existence, dans la mesure où elle explicite des informations jusqu'ici implicites, le mesurage de la société atteint dès lors des proportions inouïes. Il offre aux individus de nouvelles possibilités de se comparer réciproquement. Ceux qui souhaitent se soustraire à ce mesurage apparaissent de plus en plus suspects ou subissent des pressions qui les poussent à divulguer eux aussi leurs données. De plus, la place de l'individu dans la société et sa vie se réduisent toujours davantage à ce qui est mesurable. Cette tendance crée une représentation simplifiée, voire parfois unidimensionnelle, de l'être humain et de la réalité (que ce soit sous forme de crédit social, d'argent ou d'une autre unité de grandeur). Une telle approche conduit tôt ou tard à accorder trop de place ou de pouvoir aux chiffres et à une dérive de la société.

Il y a lieu de se demander dans ce contexte si l'idée d'une forme de «propriété des données» constituerait un moyen de rendre la quantification plus éthique. D'une part, cette solution inciterait toutefois à créer encore davantage de données. D'autre part, il est difficile de déterminer dans quelle mesure des «données personnelles» n'appar-

tiennent effectivement qu'à la personne considérée. Nombre de ces indications concernent en effet des interactions avec des tiers: une personne ne figure pas nécessairement seule sur une photo, mais peut-être avec des membres de sa famille; les données relatives aux relations qu'un individu entretient avec des tiers sur les réseaux sociaux fournissent également des renseignements sur ces personnes. Dans nombre de cas, ces données n'appartiennent donc pas exclusivement à une seule personne, à l'instar des données génétiques, qui permettent de faire des observations sur la parenté. En conséquence, le défi de la quantification consiste à encourager un esprit critique suffisant et à garantir l'autodétermination en matière d'information pour qu'il soit possible d'évaluer avec réalisme le mesurage engendré par la numérisation et de le contrôler. Ce point est expliqué plus en détail dans le chapitre 10.

Deuxièmement, la numérisation fait passer à un niveau supérieur la dépendance de l'être humain à l'égard de la technologie, car les machines agissent de plus en plus de manière autonome, en prenant des décisions qui concernent les êtres humains. Cette évolution entrave l'influence humaine et pourrait conduire à une situation où les humains devraient être rendus plus «compatibles avec la machine», par exemple pour faciliter la saisie automatique de l'identité d'une personne. De nombreuses opérations numériques (transactions financières et contrôles d'accès, par ex.) passent par la vérification de l'identité de personnes. Cette vérification ne pose aucun problème tant que la personne concernée en est consciente et l'accepte librement. Cette condition ne serait plus remplie si une personne a été «marquée» (c'est-à-dire qu'on lui aurait implanté une micropuce servant à la saisie automatique de son identité. Ce point est également abordé au chapitre 10.

Troisièmement, l'utilisation de technologies numériques dénote une tendance à standardiser toujours davantage les systèmes, les processus et le déroulement des opérations, parce que certaines solutions s'imposent face à d'autres. Il pourrait en résulter une uniformisation à l'échelle mondiale, qui saperait la résilience (résistance face aux crises) de la société humaine, car celle-ci a besoin de diversité et d'espace de liberté et d'expérimentation pour garantir à long terme la survie de l'espèce. En toute logique, le défi consiste ici à préserver le contrôle de l'être humain et sa capacité de décider pour que les individus ne soient pas réduits au statut d'«unités fonctionnelles» dans un système sociotechnique complexe, statut qui contreviendrait à la notion de dignité humaine. Une telle évolution aurait de graves conséquences sur les chances d'épanouissement des êtres humains, qui forment pourtant le fondement de la force d'innovation de notre société. Rappelons cependant que toutes les grandes innovations sociales ont commencé par violer les principes du système existant. L'impossibilité de perpétrer des violations mûrement réfléchies (appelées «innovations disruptives») entravera sérieusement le développement futur de la société, pourtant indispensable pour résoudre les nombreux problèmes mondiaux. Force est donc de craindre que la société ne soit pas à même de relever ses défis à temps et qu'elle connaisse dès lors de graves crises.

Un quatrième point essentiel réside dans la menace que la numérisation représente pour les fondements éthiques et dans l'ampleur de cette menace. Une approche cruciale pour répondre à cette question repose sur la notion d'intégrité contextuelle: le milieu dans lequel vit l'être humain est subdivisé en plusieurs domaines qui fournissent différentes références à l'individu. Dans un contexte familial, les gens s'attendent à être traités d'une autre manière que lorsqu'ils interagissent avec un organisme étatique. Dans un cadre économique, ils acceptent des formes d'inégalités de traitement, qui seraient inadmissibles dans les domaines de la santé, du droit et de l'éducation.

L'interprétation de valeurs morales fondamentales, telles l'équité et l'autonomie ainsi que les règles qui en découlent (dans le cas de l'équité, il s'agit de règles de répartition comme «une part égale à chacun», «à chacun ce qu'il mérite» ou «à chacun selon ses besoins»), varie en fonction de la sphère sociale. De la même manière, les renseignements qui sont produits dans ces différentes sphères et que les individus divulguent avec parcimonie diffèrent également. On parle alors de l'intégrité contextuelle de l'information.

Lorsqu'une personne met par exemple, dans le contexte de la santé publique, des données personnelles à disposition de la recherche médicale, le désir de venir en aide à autrui constitue souvent sa motivation première. Si ces données sont détournées pour offrir des couvertures d'assurance taillées sur mesure ou maximiser des profits, ces activités ne correspondent plus à l'intention initiale. L'intégrité contextuelle est dès lors violée, et cette atteinte sape l'esprit d'entraide.

Certaines techniques de la numérisation, comme l'analyse des *big data*, qui visent à collecter un maximum de renseignements différents sur les individus et à les conserver sous forme non structurée, comportent le risque inhérent de violer cette intégrité contextuelle. Les données étant de plus en plus souvent négociées par des courtiers en données et qu'elles alimentent des modèles statistiques complexes de groupes de personnes, une telle violation de l'intégrité contextuelle devient difficilement perceptible, voire imperceptible, même pour l'utilisateur commercial des données. Il n'est pas facile d'estimer l'ampleur du problème éthique que constitue la violation de l'intégrité contextuelle, car les limites de différentes sphères sociales ainsi que des normes morales qui s'y appliquent ne sont pas immuables. La pondération des valeurs peut par exemple varier lorsque des individus sont prêts à divulguer davantage de renseignements sur leur vie privée en contrepartie d'avantages individuels ou collectifs et qu'ils en attendent autant de leurs semblables. Dans ce cas, la conception habituelle de la vie privée tendrait à changer. Il convient toutefois de considérer que l'ordre du monde, avec sa structure de valeurs, occupe une place centrale dans différentes sphères sociales. Nombre de personnes s'offusqueraient que des informations privées sur leur cercle d'amis servent à fixer des prix individualisés ou à offrir des couvertures d'assurance. De ce point de vue, le caractère universel de la numérisation constitue un problème éthique fondamental, car cette technologie estompe les limites des sphères sociales.

11.2 Possibilités et limites (situation souhaitée)

11.2.1 Initiatives en cours

Vu la variété des défis éthiques que pose la numérisation, les solutions ne sont pas toujours éthiquement simples. Les évaluations des technologies et leur réglementation constituent un moyen de gérer les effets secondaires indésirables et fréquemment inattendus ainsi que les risques d'abus des technologies numériques. Dans le cadre de la révolution numérique, les innovations évoluent cependant si vite que ces instruments peinent souvent à suivre au même rythme. Dans le domaine de la numérisation, ils atteignent donc leurs limites.

En matière de réglementation, quelques initiatives visent à maîtriser les risques de la numérisation. Au niveau de l'UE, une initiative a été lancée pour définir les droits fondamentaux à l'ère du numérique. L'ancien ministre allemand de la Justice, Heiko

Maas, avait entrepris un projet similaire. Ces initiatives débordent du Règlement général sur la protection des données (RGPD) de l'UE, car elles ont pour principal objectif de faire valoir des droits fondamentaux dans l'espace du contenu numérique. Face aux nombreux avis critiques, issus des milieux scientifiques et économiques, qui avaient alerté sur le danger que représentaient les systèmes superintelligents et les systèmes d'armes, le gouvernement des États-Unis avait organisé, bien auparavant, une série d'ateliers sur l'avenir de l'intelligence artificielle. Ces ateliers ont débouché sur l'adoption des normes IEEE pour une «conception conforme aux règles éthiques».[23] Pour la première fois, les cinq géants de l'informatique (Alphabet [Google], Amazon, Facebook, IBM et Microsoft) se sont alliés dans le cadre d'une initiative commune, afin de définir au plus vite une conception éthique de systèmes utilisant l'intelligence artificielle. Le but est de mettre au point des IA morales et responsables.

L'éthique n'a cependant pas uniquement pour tâche d'avertir contre d'éventuelles anomalies. Elle se doit aussi de considérer d'un point de vue critique les peurs et les espoirs excessifs, souvent associés à la numérisation dans le débat public. Une perception erronée des problèmes peut mener à des conclusions erronées et à des solutions inappropriées, qui risqueraient également de poser des problèmes éthiques. Dans les développements les plus récents du débat public, d'aucuns ont soutenu l'hypothèse selon laquelle les réseaux sociaux auraient largement favorisé la polarisation politique. Les preuves corroborant cette hypothèse sont cependant tout sauf manifestes et les spécialistes ont obtenu des résultats contradictoires. Si des mesures de censure globales étaient prises sur la base de telles hypothèses pour atténuer le problème des fausses nouvelles, cette intervention n'en demeurerait pas moins une mesure mettant en danger les valeurs fondamentales de la démocratie. Il importe donc de procéder à une évaluation soigneuse du problème, qui tienne compte de solutions alternative et décentralisée (mot-clé: conception de mécanisme). À cet effet, on pourrait très bien songer à renforcer l'utilisation de mécanismes de réputation, de qualification et de modération.

11.2.2 L'éthique comme moteur de l'innovation

L'éthique n'a par ailleurs pas seulement une fonction de «gardienne»; elle est aussi censée expliquer comment elle peut favoriser des solutions novatrices. Elle a donc pour tâche d'informer sur les moyens de développer de meilleures technologies numériques. Il importerait en particulier d'amener les concepteurs de ces technologies à considérer dans quelle mesure leur application peut porter à atteinte à des valeurs fondamentales ou les renforcer. La conception éthique ou conforme aux règles éthiques (*ethically aligned design)* est l'une des notions essentielles dans ce contexte. Elle part de l'observation que les instruments et les outils techniques impliquent, expriment voire rendent impossible le respect de certaines valeurs. Cela vaut notamment pour des systèmes informatiques le plus souvent mis en œuvre dans des cadres complexes définis par les êtres humains: comme aides à la communication (téléphone mobile, Skype, etc.), instruments de planification (allant de Doodle, organisateur simple, à des outils sophistiqués utilisés dans la construction d'avions), moyens de développer des idées (rédaction collective de documents, par ex.) ou instruments de commande de systèmes techniques. Nombre de ces systèmes comprennent des options par défaut qui sont difficiles à modifier, voire en partie non modifiables, et qui

[23] Ethically Aligned Design, http://standards.ieee.org/news/2016/ethically_aligned_design.html (état en novembre 2018)

exercent une influence sur la perception de valeurs. La conception éthique revêt dès lors deux aspects: premièrement, les architectes de systèmes informatiques doivent adopter une attitude proactive en se rappelant sans cesse que leurs produits influent sur des valeurs importantes comme l'autonomie, la propriété, l'équité, la liberté, l'identité, le consentement éclairé, la confidentialité, la confiance, la prospérité ou la dignité humaine. Deuxièmement, il importe d'appliquer une systématique qui permette de structurer ces influences de telle sorte qu'elles soient compatibles avec les valeurs fondamentales et les valeurs culturelles. Voici des éléments essentiels de cette démarche:

- *définition des concepts:* Quelles valeurs sont touchées par une technologie donnée? Comment cette valeur (la confiance, par ex.) se distingue-t-elle? Qui est directement ou indirectement concerné par chaque valeur considérée?
- *études empiriques:* Les utilisateurs remarquent-ils que le recours à certaines technologies implique un échange de valeurs (un certain confort d'utilisation en échange de la vie privée, par ex.)? Quelles différences existe-t-il entre les avis sur certaines actions et les actions effectivement réalisées avec l'aide des technologies?
- *analyses techniques:* Quelles caractéristiques techniques expriment-elles une valeur dans les technologies? Comment la conception d'une technologie peut-elle encourager une valeur spécifique (la collaboration, par ex.)? Comment prévenir que la technologie intègre la notion d'une valeur (telle que la confidentialité) qui ne correspond pas à la notion qu'en a l'utilisateur de cette technologie?

Enfin, l'éthique a également pour tâche de souligner que la numérisation peut aussi jouer un rôle positif pour relever des défis futurs, comme le changement climatique ou la raréfaction des ressources. Des olympiades urbaines ont par exemple[24] été proposées afin d'accélérer l'élaboration et la diffusion de solutions respectueuses des sources d'énergie, de l'environnement et des ressources. En associant l'Internet des objets et la technologie des blockchains, il est possible de mobiliser d'autres forces du marché, qui pourraient contribuer à instaurer une économie circulaire respectueuse des ressources, efficace et compétitive. Elles pourraient également engendrer une évolution économique qui soit conforme aux valeurs fondamentales de la société et qui tienne compte des externalités (c'est-à-dire les conséquences pour l'être humain et son environnement). L'approche correspondante est connue sous le nom de «système financier socio-écologique» ou de «système financier 4.0». Il est en outre souvent recommandé de doter l'économie numérique d'une structure participative et de lui donner largement la forme d'un écosystème innovant, pour que l'innovation combinatoire soit possible. À ce titre, des principes tels que code source ouvert, libre accès, données ouvertes et innovation ouverte jouent d'une part un rôle essentiel; d'autre part, des principes tels que co-création, co-évolution, intelligence collective, autogestion et gouvernance fondée sur la subsidiarité ne sont pas en reste. Pour accélérer l'innovation, d'aucuns ont par ailleurs proposé d'instaurer le «capitalisme démocratique», une sorte de financement participatif alimenté par l'État ou un nouveau mécanisme de création de monnaie. De nouvelles voies et de nouveaux systèmes incitatifs ont en outre été découverts afin d'accroître l'intelligence collective et d'améliorer sensiblement la démocratie et les marchés. Ces possibilités se sont fait connaître sous

[24] http://futurict.blogspot.de/2017/06/propositions-on-perspective-global.html (état en novembre 2017)

les noms de «démocratie numérique» ou «mise à niveau numérique pour la démocratie». Enfin, il est possible de générer des outils pratiques pour favoriser l'autonomie numérique. Un assistant numérique de gestion des données (fondé sur la technologie de l'intelligence artificielle) a récemment été proposé, qui devrait offrir un moyen simple permettant aux citoyens de consulter et de comprendre l'utilisation de leurs données personnelles et d'exerce une influence sur cette utilisation.

11.3 Conclusions

Contrairement aux questions soulevées dans les autres champs d'analyse, il est en général impossible de partir des questions éthiques présentées dans ce chapitre et des solutions envisagées pour formuler des solutions simples à même de venir définitivement à bout des problèmes. Nombre de ces derniers sont en effet complexes et requièrent une série de mesures dont toutes ne relèvent pas directement de l'éthique. De plus, nombre des actions proposées par ailleurs dans ce rapport affichent des liens naturels avec des valeurs éthiques fondamentales, dans la mesure où ils favorisent l'autodétermination en matière d'information et la protection de la vie privée. Voilà pourquoi nous ne formulons ici que deux mesures d'ordre général:

1) **L'éthique dans la formation initiale et la formation continue**: Les professionnels de tous les secteurs qui exercent une influence sur la transformation numérique devraient être confrontés régulièrement à des questions pratiques relevant de l'éthique au cours de leur formation initiale et de leur formation continue. L'intégration de l'éthique devrait être constructive, c'est-à-dire qu'il ne s'agit pas d'attribuer à l'éthique une fonction de «surveillance et de contrôle». Il s'agit au contraire de souligner, par des approches telles que la conception axée sur les valeurs ou la conception éthique, comment la réflexion éthique peut apporter une contribution utile aux solutions numériques. Cela ne vaut pas seulement pour les ingénieurs et les informaticiens, mais pour tous les groupes de métiers (professionnels des médias, dirigeants, etc.) qui interviennent de manière notable dans la transformation numérique de la société. Afin d'aider la Suisse à jouer un rôle de leader dans ce domaine, il faudrait notamment intensifier la recherche sur l'innovation responsable et la conception axée sur les valeurs.

Voici des suggestions pour appliquer ces mesures:

- Il convient d'**intensifier la recherche sur les problèmes éthiques de la transformation numérique** dans les hautes écoles suisses. Cet effort comprend la création de nouvelles chaires et de nouveaux centres de recherche consacrés par exemple à la conception éthique. Ce faisant, il importe de savoir que ces chaires et ces centres de recherche auront une forte orientation interdisciplinaire et qu'ils coopéreront étroitement avec des groupes de recherche des domaines technique et social.
- Il importe de promouvoir la **recherche en sciences sociales et dans les domaines techniques** qui ont des conséquences directes sur les problèmes éthiques évoqués. Mentionnons en particulier les recherches visant à déterminer dans quelle mesure la manipulation numérique engendre des effets concrets, comment améliorer la transparence et les moyens de contrôler les systèmes d'IA dotés de fonctionnalités décisionnelles, les moyens de lutter contre les bulles de

filtres ou sous quelle forme il serait possible d'instituer judicieusement une propriété des données.

- Par analogie avec le développement de capacités de recherche dans les domaines cités, il convient de garantir plus spécialement que la **formation des techniciens spécialisés** accordera une place suffisante aux considérations éthiques. Relevons à ce propos le domaine de la cybersécurité, dans lequel il importe par exemple de renforcer la prise de conscience quant aux possibles conflits de valeurs (sécurité de l'information contre l'accès aux données dans le secteur de la santé, par ex.) et d'élaborer des pratiques d'excellence pour gérer de tels conflits.

2) **Protection des valeurs fondamentales:** Les mesures concrètes qui découlent logiquement de la transformation numérique devraient se fonder sur l'idée que cette transformation exerce une influence sur les valeurs fondamentales de notre ordre social. Cela ne signifie nullement que toute modification dans l'interprétation de ces valeurs soit a priori négative. Il incombe cependant aux forces sociales qui remettent certaines valeurs en question par des innovations numériques concrètes de démontrer que ces innovations contribuent à l'intérêt général ou, du moins, qu'elles ne lui nuisent pas. Cette exigence abstraite s'appliquera de manière différente selon les situations. Elle souligne toutefois que le point de vue éthique doit être pris en considération dans toute évaluation des innovations numériques. Il faudrait en particulier veiller à inclure dans la numérisation l'«autonomisation numérique» et l'autodétermination en matière d'information. Afin de protéger la démocratie et la dignité humaine, il importe de trouver d'urgence des solutions et des instruments pour promouvoir l'autodétermination en matière d'information.

Voici des suggestions pour appliquer ces mesures:

- Une large utilisation des technologies numériques pour générer des données sur de vastes portions de la population ne doit pas avoir d'influence sur le **respect des droits fondamentaux**, c'est-à-dire déterminer par exemple l'accès à des prestations de l'État (comme c'est le cas dans le système de crédit social). Il importe de veiller à ce que tout individu puisse exercer ses droits fondamentaux, même s'il ne veut pas utiliser certaines technologies numériques (les smartphones, par ex.). Il convient donc de vérifier que le système juridique en vigueur contient les garanties réglementaires requises.
- Les solutions apportées aux **problèmes qui résultent de l'utilisation de technologies numériques** (efficacité accrue de la propagande, par ex.) ne doivent en aucune manière restreindre les droits fondamentaux (telle la création d'un «ministère de la Vérité» qui décide quelle information politique est vraie ou fausse).
- Toute forme de **manipulation**, à l'aide de moyens numériques ou autres, doit posséder une légitimité démocratique et être transparente. Il faut de plus vérifier régulièrement si cette manipulation atteint les objectifs et en informer l'opinion publique. Si les objectifs ne sont pas du tout ou insuffisamment réalisés, il convient de mettre fin à la manipulation.
- Le recours à des **systèmes décisionnels automatisés dans des domaines sensibles** doit toujours réserver une place appropriée à la capacité humaine de

décision (intégration d'un «second avis humain»). Dans les domaines où il faut s'attendre à des dilemmes éthiques, il ne faudrait développer des systèmes décisionnels automatisés que s'ils diminuent nettement l'apparition de ces dilemmes.

- Les gains d'efficacité que les technologies numériques permettraient d'obtenir en portant atteinte à droits fondamentaux ne justifient **aucune mesure contraignante ni intervention physique** (telle une éventuelle obligation de se faire implanter une micropuce pour faciliter la vérification de l'identité).
- Il importe d'encourager la recherche afin de développer des **instruments** (numériques) **qui soutiennent le respect des droits fondamentaux**. Il s'agit par exemple de concevoir des outils pour l'autodétermination en matière d'information ou des mécanismes de réputation, de qualification et de modération.

Recommandations:

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.

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.

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 et de la conception axée sur les valeurs.

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).*

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.

12 Annexe 1: Composition du groupe d'experts

Présidente:

Brigitta M. Gadient, ancienne membre du Conseil national

Science et recherche:

Markus Christen, privat-docent à l'Université de Zurich

Nicolas Gisin, professeur à l'Université de Genève

Dirk Helbing, professeur à l'EPF de Zurich

Jean-Pierre Hubaux, professeur à l'EPF de Lausanne

Matthias Kaiserswerth, ancien directeur du centre de recherche d'IBM, directeur de la fondation Hasler

Adrian Perrig, professeur à l'EPF de Zurich

Droit:

Rolf H. Weber, professeur émérite à l'Université de Zurich

Ursula Widmer, ancienne présidente d'Information Security Society Switzerland

Économie:

Thomas Pletscher, membre de la direction d'economiesuisse

Communication et société:

Regula Hänggli, professeure à l'Université de Fribourg

Administration:

Peter Fischer, délégué au pilotage informatique de la Confédération

Adrian Lobsiger, préposé fédéral à la protection des données et à la transparence (depuis juin 2016)

Luzius Mader, directeur suppléant de l'Office fédéral de la justice

Hanspeter Thür, préposé fédéral à la protection des données et à la transparence (jusqu'à fin 2015)

Secrétariat

Arié Malz (direction)

13 Annexe 2: Experts et représentants de groupes d'intérêts consultés

Thomas Dübendorfer
Président de l'association Swiss ICT Investor Club (SICTIC), Zurich

Raoul Egeli
Président de Creditreform, représentant de l'USAM

Alain Gut
Président de la commission de la formation, ICTswitzerland

Franz Grüter
Conseiller national, vice-président de ICTswitzerland, CEO et président du conseil d'administration de green.ch

Christian Kunz
Cofondateur et CEO de BitsaboutMe AG, Berne

Dale Kutnick
Senior Vice President et Director of Research, Gartner Inc. Stamford USA

Friedemann Mattern
Professeur au sein du département de l'informatique, EPF de Zurich

Patrick Schmid
Senior Account Executive, Gartner Inc. Switzerland

Sara Stalder
Directrice de la fondation Stiftung für Konsumentenschutz (SKS)

Martin Vögeli
Chef de la division Group Strategy & Board Services, Swisscom

14 Annexe 3: Abréviations et glossaire

Accord Safe Harbor: du point de vue de la Suisse, la législation des États-Unis n'offre pas une protection des données adéquate. C'est pourquoi, afin de faciliter les transferts de données entre eux, les deux pays ont élaboré un ensemble de règles garantissant un niveau suffisant de protection des données pour les entreprises enregistrées. Établi en 2008 par un échange de lettres, ce cadre réglementaire a été remplacé en 2017 par un nouvel accord baptisé «Privacy Shield» (bouclier de protection des données personnelles).

Actionneur: élément de commande qui transforme des impulsions électriques en grandeurs mécaniques.

Analyse des vulnérabilités: (*vulnerabilities scan*) examen des vulnérabilités des infrastructures numériques destiné à identifier les lacunes de sécurité et les comportements non conformes des systèmes examinés.

Antivirus: logiciel à même de détecter, bloquer et éventuellement supprimer les virus, vers et chevaux de Troie informatiques connus.

Apprentissage automatique: (*machine learning*) apprentissage basé sur des algorithmes utilisant généralement des approches statistiques du traitement des données, afin d'identifier des modèles et apprendre de ces derniers.

Apprentissage profond: (*deep learning*) désigne un sous-domaine de l'apprentissage automatique (*machine learning*). Il se distingue de ce dernier en ceci que le système apprend de lui-même – à l'aide de réseaux de neurones artificiels – à reconnaître des caractéristiques distinctives et à les appliquer.

B2B: relations interactives entre des fournisseurs et producteurs et d'autres fournisseurs et producteurs.

B2C: relations interactives entre des fournisseurs et producteurs et des consommateurs.

Blocage géographique ou **géoblocage:** (*geo-blocking*) technologie utilisée sur Internet pour bloquer des sites web dans une zone géographique donnée.

Botnet: appelé également «réseau zombie», un botnet est un groupe de maliciels automatisés, ou «bots». Il est créé par la mise en réseau des ressources d'un grand nombre d'ordinateurs, utilisées ensuite pour lancer des attaques. Les ordinateurs sont

préalablement infectés par l'agresseur à l'insu de leur propriétaire, puis utilisés comme bots.

BSI: *Bundesamt für Sicherheit in der Informationstechnik*. Autorité civile allemande en charge des questions de sécurité informatique.

BSIG: *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*. Loi fédérale allemande sur l'autorité civile en charge des questions de sécurité informatique (cf. BSI).

C&C: commande et contrôle. Fonctions de contrôle des botnets exécutées au moyen de serveurs de commande et contrôle.

CC: code civil suisse, RS *210*

CO: code des obligations, RS *220*

Confidentialité différentielle: (*differential privacy*) processus d'anonymisation par lequel les données originelles liées à une requête sont complétées par un si grand nombre d'éléments factices (bruit de fond) qu'il est certes encore possible d'effectuer une analyse statistique des données mais non d'identifier la personne qu'elles concernent. Ce terme relève du domaine de la publication sécurisée d'informations sensibles. Les mécanismes qui répondent aux exigences de la confidentialité différentielle empêchent les agresseurs de distinguer si une personne déterminée figure ou non dans une base de données.

Convention 108: Convention du Conseil de l'Europe sur la protection des données (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel). La Convention 108 est un traité international ayant pour objet la protection des données des personnes physiques. Elle est entrée en vigueur pour la Suisse le 1er février 1998 (RS *0.235.1*).

DDoS: *distributed denial of service*. Déni de service distribué: lors d'une attaque par déni de service distribué, un très grand nombre de systèmes infectés sont mobilisés pour attaquer une seule et même cible. Le système visé est généralement débordé par cet assaut et n'est dès lors plus accessible à ses utilisateurs ordinaires.

Deepnet ou darknet: partie du web reposant sur un réseau pair à pair (réseau entre partenaires disposant des mêmes droits et établissant des connexions entre eux). Formant de loin la plus grande partie du réseau, le deepnet ou darknet échappe aux moteurs de recherche Internet.

Désintermédiation: (*disintermediation*) désigne la suppression des intermédiaires dans la chaîne de distribution entre les fabricants de produits ou les prestataires de services et les consommateurs, grâce à Internet et aux moyens de communication modernes.

Économie de plateformes: (*gig economy*) nouveau secteur du marché du travail apparu dans le sillage de la numérisation, dont le fonctionnement est généralement basé sur l'offre de mandats à court terme sur des plateformes en ligne. Les destinataires des mandats sont des travailleurs indépendants ou exerçant l'activité concernée à titre accessoire. Les exploitants des plateformes jouent souvent le rôle d'intermédiaires entre les clients et les mandataires. Ils fixent les conditions-cadres et perçoivent une commission pour leurs services. Exemples: Uber et Upwork.

e-ID: identité électronique.

Exploit zero-day: (*zero-day exploit*) attaque qui exploite pour la première fois un point faible matériel et surtout logiciel.

Externalisation / Infogérance: (*outsourcing / managed services*) externalisation des tâches et des structures informatiques des entreprises auprès de prestataires de services externes.

Fracture numérique: (*digital divide*) désigne l'inégalité d'accès aux ordinateurs, à Internet et aux technologies de la communication due à la pauvreté ou à d'autres facteurs structurels, comme le genre ou le manque de connaissances linguistiques.

Freemium: modèle économique consistant à proposer des services de base gratuits, alors que les services plus étendus ou l'offre complète sont payants.

Freenet: logiciel pair à pair permettant de construire un réseau dont le but est de stocker les données de manière distribuée, afin de déjouer la censure et de garantir l'anonymat des échanges de données.

G2Ci: *Government to Citizen*. Relations interactives entre l'État et les citoyens.

Hameçonnage: (*phishing*) le terme anglais *phishing* est une contraction des mots *password* (mot de passe), *harvesting* (moisson) et *fishing* (pêche). L'hameçonnage est un type d'attaque consistant à envoyer de faux courriels ou SMS à des internautes, afin de les diriger vers des sites Internet de banques, etc. contrefaits et de leur soutirer leurs données d'accès (nom d'utilisateur et mot de passe).

I2P: (*invisible Internet project*) projet à code source ouvert (*open source*), qui permet de construire un réseau anonyme de communication sur Internet.

IAM: *identity and access management*. Gestion des identités et des accès: désigne une solution de sécurité centralisée permettant d'assurer l'intégralité de la gestion des identités et des accès.

IDE: numéro d'identification des entreprises, attribué à chaque entreprise opérant en Suisse.

IdO: Internet des objets (*Internet of Things, IoT*). Désigne l'interconnexion d'objets s'y prêtant dans un réseau numérique universel, principalement Internet. Les appareils deviennent ainsi omniprésents, tout en restant autonomes. L'IdO associe le monde des données et celui des objets.

IdT: Internet de tout (*Internet of Everything, IoE*). Désigne l'ensemble des connexions entre les personnes, les processus, les données et les objets et représente une évolution de l'Internet des objets (cf. IdO).

Ingénierie sociale: (*social engineering*) manipulation psychologique directe de personnes, ayant pour but d'accéder à des données confidentielles ou d'amener la victime à exécuter des actions déterminées.

k-anonymat: (*k-anonymity*) technique répandue de mesure scientifique du degré d'anonymat des données. Lorsque des données qui ont été modifiées afin de les anonymiser peuvent être attribuées non plus à des personnes déterminées mais à un groupe comptant k personnes ou plus, on parle de k-anonymat.

LAAM: loi du 3 février 1995 sur l'armée, RS *510.10*

LAr: loi fédérale du 26 juin 1998 sur l'archivage, RS *152.1*

LBI: loi du 25 juin 1954 sur les brevets, RS *232.14*

LCart: loi du 6 octobre 1995 sur les cartels, RS *251*

LCD: loi fédérale du 19 décembre 2013 contre la concurrence déloyale, RS *241*

LDA: loi du 9 octobre 1992 sur le droit d'auteur, RS *231.1*

l-diversité: (*l-diversity*) mesure de l'anonymat des données; la l-diversité est une amélioration minime mais essentielle du k-anonymat. Ce dernier n'est en effet pas entièrement fiable en tant que mesure du degré d'anonymat. La l-diversité garantit qu'un groupe comptant k personnes présente au moins l valeurs différentes pour chaque caractéristique.

LHR: loi du 23 juin 2006 sur l'harmonisation de registres, RS *431.02*

LIMF: loi du 19 juin 2015 sur l'infrastructure des marchés financiers, RS *958.1*

LJAr: loi fédérale du 29 septembre 2017 sur les jeux d'argent, RS ..., FF *2017* 5891

LP: loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite, RS *281.1*

LPD: loi fédérale du 19 juin 1992 sur la protection des données, RS *235.1*

LRens: loi fédérale du 25 septembre 2015 sur le renseignement, RS *121*

LRFP: loi fédérale du 18 juin 1993 sur la responsabilité du fait des produits, RS *221.112.944*

LSCPT: loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication, RS *780.1*

LSPro: loi fédérale du 12 juin 2009 sur la sécurité des produits, RS *930.11*

LTI: loi fédérale du 3 octobre 2008 sur les titres intermédiés, RS *957.1*

LTrans: loi fédérale du 17 décembre 2004 sur la transparence, RS *152.3*

M2M: *machine to machine*. Désigne l'échange automatique d'informations numérisées entre machines ou terminaux.

Menace persistante avancée: (*advanced persistent threat*, APT) désigne une attaque complexe, ciblée et de longue durée, visant des infrastructures informatiques et des données confidentielles spécifiques et impliquant la mobilisation d'importantes ressources de la part de l'agresseur.

MPLS: *multiprotocol label switching*. Technologie permettant de transférer des données en déterminant à l'avance le chemin des paquets de données, ce qui n'est pas le cas sur un réseau IP. Le MPLS permet de construire des réseaux distincts sécurisés sur la couche OSI 2 (Ethernet), avec des liaisons point à point.

NIS: directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016

OGD: *open government data*. Modèle à la croisée de deux principes: d'une part, celui d'une action gouvernementale et administrative ouverte (*open government*), d'autre part, celui du libre accès aux données (*open data*), notamment publiques (*government data*). Ces deux derniers aspects privilégient certaines caractéristiques spécifiques de la mise à disposition des données concernées (extrait de la Stratégie en matière de libre accès aux données publiques en Suisse pour les années 2014 à 2018).

OIP: ordonnance du 11 décembre 1978 sur l'indication des prix, RS *942.211*

OVotE: ordonnance de la Chancellerie fédérale du 13 décembre 2013 sur le vote électronique, RS *161.116*

Pair à pair: (*peer-to-peer*) dans un réseau pair à pair, tous les ordinateurs sont sur un pied d'égalité et peuvent aussi bien utiliser des services qu'en mettre à disposition.

Paradoxe de la vie privée: (*privacy paradox*) d'un côté, les utilisateurs dévoilent de plus en plus de données personnelles (nom, photos, numéro de téléphone mobile et même croyances religieuses) sur le net et, de l'autre, ils s'inquiètent de la protection de leur sphère privée. Une analyse plus précise de ce phénomène montre toutefois que le paradoxe n'est qu'apparent, car il n'existe pas de lien significatif entre le souci de protection de la sphère privée et la diffusion de données. La majorité des utilisateurs donne la priorité à cette dernière, privilégiant ainsi leur participation aux réseaux sociaux.

Pare-feu: (*firewall*) dispositif à composantes logicielles et matérielles destiné à contrôler et à filtrer les flux de données entrants et sortants. Il sert à assurer la protection des infrastructures numériques (ordinateurs, réseaux) et constitue une mesure fondamentale de prévention des accès non désirés au réseau.

PFPDT: préposé fédéral à la protection des données et à la transparence.

Privacy Shield: voir Accord Safe Harbor.

Protection de la vie privée dès la conception: (*privacy by design*) consiste à prévoir des mesures techniques destinées à empêcher toute violation de la protection des données dès la phase d'élaboration d'un processus de traitement des données. Font partie de telles mesures notamment l'anonymisation, le chiffrement et la minimisation des données.

Protection de la vie privée par défaut: (*privacy by default*) consiste en des mesures de protection des données appliquées par défaut et visant à garantir que seules sont traitées les données personnelles nécessaires à la réalisation de la finalité du traitement.

Protection de périmètre: (*perimeter protection*) assure la sécurité de l'interface entre un réseau privé ou un réseau d'entreprise et un réseau public, comme Internet. La protection de périmètre forme la première ligne de défense d'un réseau contre les cyberattaques.

Rançongiciel: (*ransomware*) logiciel malveillant qui chiffre les données des ordinateurs et ne les déchiffre que contre paiement d'une rançon.

RegTech: *regulatory technology*. Terme générique désignant l'ensemble des mesures et des technologies modernes permettant de répondre aux exigences de la conformité à la réglementation (*compliance*) et de la gestion des risques.

RGPD: règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1

RSA: algorithme de chiffrement asymétrique nommé d'après les initiales de ses trois inventeurs, Rivest, Shamir et Adleman. Comme d'autres processus de chiffrement asymétrique, le RSA repose sur des fonctions à sens unique.

SCSE: loi du 18 mars 2016 sur la signature électronique, RS *943.03*

SDN: *software defined networking*. Technologie permettant de gérer un réseau au niveau logiciel, en le découplant du niveau matériel. Dans ces réseaux à définition logicielle, l'administrateur peut définir le chemin des paquets de données, ce qui n'est pas le cas dans les réseaux ordinaires.

SD-WAN: *software defined wide area network*. Technologie permettant de construire un réseau étendu à définition logicielle. Comme avec le SDN, il est possible de gérer

le réseau au niveau logiciel, de sorte que les structures d'interconnexion peuvent être conçues avec davantage de souplesse et selon des principes de sécurité spécifiques.

Sécurité dès la conception: (*security by design*) principe fondamental selon lequel les systèmes doivent être si possible conçus dès le départ – autrement dit dès la phase de développement de leurs composantes matérielles et logicielles – de manière à ne présenter aucun point faible et à être insensibles aux attaques.

SHA: *secure hash algorithm*. Processus de chiffrement standardisé, qui exécute une fonction de hachage (sommes de contrôle dérivées mathématiquement d'une valeur quelconque).

Système cyberphysique: (*cyber-physical system*, CPS) système intégré dans lequel des composantes techniques informatiques et logicielles sont associées à des éléments mécaniques ou électroniques. Grâce à l'intégration de capteurs et d'actionneurs, les CPS mettent à disposition en temps réel des fonctions système d'un genre nouveau, permettant d'intégrer des informations, des données et des fonctions. L'Internet des objets repose sur les CPS.

TIC: technologies de l'information et de la communication.

Tor: *The onion routing*. Routage en oignon, qui protège ses utilisateurs contre l'analyse des flux de données et leur permet d'accéder à Internet de manière largement anonyme.

15 Annexe 4: Normes et obligations de notifier en comparaison internationale

Introduction

Le développement rapide des infrastructures numériques, l'augmentation de la dépendance vis-à-vis de ces dernières et leur importance croissante pour la société placent les structures de l'État face à de nombreux défis. En particulier, où et comment l'État doit-il intervenir pour garantir une gestion ordonnée des chances et des risques de la transformation numérique? L'analyse comparative ci-après montre comment les différentes infrastructures critiques et les services en ligne importants sont réglementés dans d'autres pays et quels axes stratégiques ces derniers poursuivent.

Étendue de l'analyse

L'analyse repose sur une enquête que le groupe d'experts a pu réaliser grâce au soutien du DFAE et d'une douzaine de ses représentations extérieures[25]. Établie sur la base des informations reçues de ces dernières, la vue d'ensemble ci-dessous présente la situation en matière de prescriptions étatiques relatives aux normes de sécurité informatique dans les pays suivants: Allemagne, Autriche, France, Royaume-Uni, Suède, Norvège, Finlande, Singapour, Hong Kong, Australie, Chine et États-Unis.

Situation en Europe

De manière générale, les États européens se conforment aux prescriptions contraignantes de la directive (UE) 2016/1148 (directive NIS), qui s'applique aux infrastructures critiques et au secteur de la communication numérique. Les États membres de l'UE sont tenus de transposer dans leur droit national les dispositions de la directive NIS. Au moment de la présente analyse, tous ne l'avaient pas encore fait.

L'**Allemagne** dispose depuis juillet 2015 d'une loi sur la sécurité informatique (*IT-Sicherheitsgesetz*) applicable aux exploitants d'infrastructures critiques. Sont considérés comme des infrastructures critiques les équipements, les installations et les composants relevant des secteurs de l'énergie, des technologies de l'information, des télécommunications, des transports, de la santé, de l'eau, des produits alimentaires, de la finance et des assurances, et qui sont importants pour le fonctionnement de la collectivité. Les exploitants d'infrastructures critiques sont définis par voie d'ordonnance légale et s'engagent à observer des normes techniques minimales ainsi qu'une obligation de notifier. En tant que service de l'État en charge des questions de sécurité informatique, le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) remplit de nombreuses tâches et dispose de larges compétences en relation avec la sécurité de l'information au niveau national (§ 3 de la loi sur le BSI). Par exemple, les exploitants d'infrastructures critiques et leurs associations de branche peuvent proposer des normes de sécurité propres à leur branche au BSI, auquel il incombe alors de déterminer si ces normes sont propres à garantir le respect des exigences prévues. Les

[25] Le groupe d'experts remercie le DFAE pour sa précieuse collaboration, sans laquelle cette comparaison internationale n'aurait pas pu être effectuée.

exploitants sont en outre tenus de prouver au moins tous les deux ans qu'ils remplissent les exigences légales.

Concrètement, les normes de sécurité sont arrêtées dans les différentes lois régissant les réseaux de télécommunication publics (*Telekommunikationsgesetz*, TKG), les réseaux d'approvisionnement en énergie et les installations énergétiques (*Gesetz über die Elektrizitäts- und Gasversorgung*, EnWG) ainsi que les centrales nucléaires et les dépôts de déchets nucléaires (*Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren*, AtG).

En **Autriche**, le projet de loi sur la sécurité des réseaux et des systèmes d'information (*Netz- und Informationssystemsicherheitsgesetz*, NISG) prévoit que des normes de sécurité devront être édictées pour les opérateurs de services essentiels (ordonnance du chancelier fédéral). La directive NIS[26] distingue entre les opérateurs de services essentiels (secteurs selon la note [27]) et les fournisseurs de service numérique (au sens de la directive [UE] 2015/1535). Le projet de NISG reprend cette systématique. De plus, tout comme la directive NIS, le plan directeur 2014 du programme autrichien de protection des infrastructures critiques (*Österreichisches Programm zum Schutz kritischer Infrastrukturen*, APCIP) prévoit aussi l'élaboration de normes de sécurité (y c. dans le secteur informatique). Ce programme n'est pas encore appliqué, car on attend de connaître les normes de la future NISG. Selon le projet de NISG, les opérateurs de services essentiels et les fournisseurs de service numérique auront l'obligation de notifier les incidents de sécurité à un service de communication, qui sera rattaché à l'autorité opérationnelle en matière de sécurité des réseaux et de l'information (*NIS-Behörde*). Seront également soumises à cette obligation légale de notifier les PME et les organisations à but non lucratif, dans la mesure où elles fourniront des services essentiels. De plus, la NISG et les normes qui y seront arrêtées s'appliqueront aussi à l'administration publique. Certaines entreprises stratégiques considérées comme des infrastructures critiques n'auront certes pas l'obligation légale de notifier dont il est question ci-dessus, mais elles seront néanmoins tenues de porter les incidents de sécurité à la connaissance du service de contact et de communication de l'Office fédéral pour la protection de la Constitution et la lutte contre le terrorisme (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, BVT). Le BVT et les exploitants concernés concluront à cet effet des conventions de coopération sur l'échange d'informations classifiées.

En **France**, l'Agence nationale de sécurité des systèmes d'information (ANSSI) a commencé à publier, depuis juillet 2016, des prescriptions obligeant les exploitants d'infrastructures critiques à appliquer des mesures de protection. Les premiers secteurs concernés sont la santé, les produits alimentaires et l'économie de l'eau, et d'autres vont suivre. Relevons que le nombre d'exploitants des secteurs public et privé soumis à ces prescriptions s'élève à environ 250, mais que leur liste est confidentielle. La base

[26] Aux fins de la mise en œuvre de la directive (UE) 2016/1148 du 6 juillet 2016 (directive NIS), l'Autriche prépare une loi sur la sécurité des réseaux et des systèmes d'information (*Netz- und Informationssystemsicherheitsgesetz*, NISG).

[27] Selon l'annexe II de la directive NIS, les services essentiels relèvent des secteurs suivants: énergie, transports, banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable et infrastructures numériques (IXP, fournisseurs de services DNS, registres de noms de domaines de haut niveau).

légale correspondante a été créée suite à l'adoption de la loi de programmation militaire de décembre 2013. Les quelque 250 exploitants d'infrastructures critiques concernés sont soumis à une obligation d'informer l'ANSSI et de lui notifier certains incidents prédéfinis[28]. Les institutions non soumises aux prescriptions mentionnées plus haut n'ont actuellement pas d'obligation de notifier vis-vis de l'ANSSI. Toutefois, avec la mise en œuvre de la directive NIS, l'application des prescriptions de l'ANSSI devrait s'étendre à d'autres secteurs, si bien que le nombre d'exploitants qui leur sont soumis devrait augmenter.

Au **Royaume-Uni**, le processus d'élaboration et d'adoption de prescriptions conformes à la directive NIS est en cours, la conception et la mise en œuvre de ces prescriptions incombant en l'occurrence à plusieurs acteurs étatiques[29]. Il existe cependant déjà certaines prescriptions générales de sécurité informatique, qui ont été élaborées par le *National Cyber Security Centre* (NCSC). Elles doivent être considérées comme des lignes directrices visant à assister l'administration publique (*government departments*, *agencies*) et les infrastructures critiques nationales dans le domaine de la sécurité informatique. Ces lignes directrices valent cependant aussi pour les administrations locales (*local government*) et le secteur public élargi (*wider public sector*). Il n'est pas possible de déterminer dans quelle mesure elles ont force obligatoire.

Situation en Scandinavie

À ce jour, la **Suède** n'a pas édicté de prescriptions étatiques contraignantes pour les exploitants d'infrastructures numériques et les fournisseurs de services en ligne. Toutefois, pour les exploitants d'infrastructures critiques, l'agence gouvernementale *Swedish Civil Contingencies Agency* (MSB) renvoie en particulier aux méthodes et aux normes bien établies de la suite ISO27k. Par ailleurs, hormis dans certains secteurs, les exploitants d'infrastructures critiques ne sont apparemment pas soumis à une obligation de notifier les incidents. La législation en vigueur en matière de protection prévoit cependant certaines obligations de notifier (par ex. dans les secteurs de l'électricité et des télécommunications)[30]. Les exploitants publics et l'administration sont quant à eux tenus de notifier les incidents à la MSB.

En **Norvège**, les autorités publiques émettent des recommandations et fixent des exigences en matière de sécurité informatique. La plupart sont définies à l'échelle sectorielle par les ministères compétents. Les recommandations émises par l'État peuvent avoir force obligatoire ou simplement tenir lieu de lignes directrices. Une certaine obligation de notifier découle du *National Security Act*, qui oblige les différents ministères à présenter au ministère de la justice un rapport annuel sur l'état du respect des prescriptions dans leur secteur de compétence.

---

[28] Les opérateurs d'importance vitale (OIV) sont obligés de transmettre différentes informations: 1) des déclarations d'incidents; 2) une «cartographie» de leurs systèmes d'information d'importance vitale; 3) un tableau de bord de suivi de certains indicateurs de sécurité des systèmes d'information.

[29] *Department for Digital, Culture, Media & Sport*, *Cabinet Office*, *Governement Digital Service* et *Department for Business, Energy & Industrial Strategy*

[30] *Incident reporting in the telecoms sector (EU telecoms package Article 13a)*

En **Finlande**, la *Finnish Communications Regulatory Authority* (FICORA) est habilitée à édicter des prescriptions régissant la sécurité de l'information dans le secteur des télécommunications. La coordination entre la FICORA et le secteur des télécommunications est assurée en collaboration avec le *National Cyber Security Centre* (NCSC-FI). Les opérateurs de télécommunication ont l'obligation d'informer la FICORA de tout incident de sécurité affectant leurs réseaux. Dans le domaine des infrastructures critiques, la *National Emergency Supply Agency* (NESA) apporte un certain soutien aux exploitants par l'émission de lignes directrices sur la sécurité de l'information. Les directives du NCSC-FI ne sont apparemment pas contraignantes pour les exploitants. En revanche, il semblerait, en règle générale, que les recommandations émises à l'échelle sectorielle par les ministères compétents ont force obligatoire, en particulier pour l'administration. Enfin, on peut supposer qu'avec la mise en œuvre de la directive NIS, les exploitants d'infrastructures critiques ainsi que d'autres secteurs seront soumis à une obligation de notifier les incidents de sécurité de l'information.

Situation en Asie et en Australie

En règle générale, il existe en **Chine** des normes de sécurité informatique s'appliquant aux exploitants d'infrastructures numériques et aux fournisseurs de services en ligne, ainsi que dans d'autres secteurs. En raison de la complexité des dispositions en vigueur à l'échelle nationale, il est actuellement difficile d'établir avec certitude s'il existe un service de communication auquel les incidents de sécurité informatique importants doivent être notifiés et, le cas échéant, de juger de l'étendue de cette obligation de notifier. Cette difficulté est en outre aggravée par le fait que les compétences décisionnelles, tant stratégiques qu'opérationnelles, sont revendiquées par deux institutions gouvernementales différentes[31]. Ce qui est sûr en revanche, c'est que les organisations sous influence étrangère tendent à être soumises à des contrôles plus étendus en matière aussi bien de sécurité informatique que de sécurité de l'information et doivent donc respecter les prescriptions étatiques correspondantes.

Le gouvernement de **Hong Kong** a déjà adopté différentes dispositions réglant la question de la sécurité de l'information dans sa globalité. Lors de la conception et de la mise au point des documents concernés – prescriptions de sécurité, directives, instructions, processus, etc. –, il s'est largement appuyé sur des normes ayant déjà fait leurs preuves (ISO, Commission électrotechnique internationale, etc.). Les réglementations adoptées ont force obligatoire pour toutes les unités d'organisation gouvernementales. Le *Government Computer Emergency Response Team Hong Kong* (GovCERT.HK) remplit la fonction de service de coordination et de communication pour les cyberincidents de sécurité de l'information. Toutes les organisations étatiques (exploitants d'infrastructures aussi bien critiques que non critiques) sont soumises à une obligation de notifier vis-à-vis du GovCERT.HK. De plus, le *Hong Kong Computer Emergency Response Team Coordination Centre* (HKCERT) joue le rôle de service d'information public, menant des actions de prévention et de sensibilisation générales visant les autres acteurs concernés comme les PME.

[31] La *Chinese Administration for Cyber Security* et le *Ministry of Public Security* se disputent le pouvoir de décision dans ce domaine, au niveau tant stratégique qu'opérationnel.

À **Singapour** la *Cyber Security Agency of Singapore* (CSA) est l'unique responsable de la coordination et de la surveillance de tout ce qui est en rapport avec la cybersécurité. En matière de réglementation et de prescriptions, le gouvernement singapourien suit généralement une approche de haut en bas, ce qui signifie que les tâches, les responsabilités et les compétences de la CSA sont très étendues[32]. Le *Cyber Security Act* règle les prescriptions applicables aux exploitants d'infrastructures critiques. Il s'agit d'une loi-cadre intersectorielle intégrée au *National Security Masterplan 2018*. Elle fixe des exigences minimales en matière de mesures préventives et constitue la base légale de l'action de la CSA. Singapour a défini onze secteurs que l'État juge importants du point de vue sécuritaire. Dans chacun d'eux, il incombe à l'autorité sectorielle compétente d'assurer la surveillance de tout ce qui relève de la sécurité. Dans le secteur financier, il s'agit par exemple de la *Monetary Authority of Singapore* (MAS). Elle fixe notamment des lignes directrices (*Technology Risk Management Guidelines*) relatives à la gestion générale des risques technologiques et des cyberrisques dans le secteur financier. En règle générale, les divers secteurs et l'administration sont tenus de notifier les incidents de sécurité de l'information à la CSA.

Avec l'*Australian Cyber Security Center* (ACSC), l'**Australie** dispose d'une institution chargée d'assurer la coordination entre les autorités, les instances de réglementation et le secteur privé. L'ACSC collecte des informations, évalue les menaces et conseille le secteur privé en conséquence. De plus, deux institutions responsables de la coopération avec les exploitants d'infrastructures critiques ont été créées au sein du *Federal Attorney-General's Department*. La première, le *Computer Emergency Response Team* (CERT), travaille en étroite collaboration avec les autres autorités de l'État et tient lieu de principal interlocuteur pour les incidents de sécurité survenant dans le secteur des infrastructures critiques. La mission du CERT consiste à donner en temps utile aux exploitants et aux institutions d'intérêt national des conseils appropriés et efficaces visant à prévenir les cyberattaques. Il n'existe apparemment pas d'obligation de notifier les incidents de sécurité. La seconde institution, le *Trusted Information Sharing Network* (TISN), est un organisme de coordination. Fonctionnant en réseau, il est chargé d'assurer des échanges d'informations réguliers entre les exploitants d'infrastructures critiques, les autres secteurs et les entreprises publiques[33]. En fait partie par exemple l'*Australian Securities and Investment Commission* (ASIC), compétente en matière de réglementation du secteur financier. Il n'existe pas de prescriptions étatiques contraignantes en matière de normes de sécurité informatique, mais l'ASIC attend des banques qu'elles prennent des mesures appropriées de gestion des risques.

Situation aux États-Unis

[32] Tâches de la CSA: «[...] également chargée d'élaborer les règles, les politiques et les pratiques de cybersécurité et de les faire appliquer. Elle assure la coordination des efforts du gouvernement, de l'industrie, des milieux académiques, des milieux d'affaires et de la société civile, ainsi que celle des efforts déployés à l'échelle internationale.»

[33] Les secteurs concernés comprennent les banques, la finance, la santé, les produits alimentaires, les transports, l'énergie, les télécommunications, la fourniture et la distribution d'eau et les services relevant du *Commonwealth Government*.

Les **États-Unis** comptent plusieurs départements d'État ayant des responsabilités en matière de sécurité de l'information. Il s'ensuit que la distribution des diverses tâches, responsabilités et compétences en matière de prescriptions étatiques relatives aux normes de sécurité informatique présente une grande complexité. Le *Department of Homeland Security* (DHS) semble jouer à cet égard un rôle central de coordination. On peut en outre partir du principe qu'il existe une obligation de notifier les incidents, en particulier ceux concernant la sécurité nationale. Abstraction faite du DHS, on peut également supposer que, dans une certaine mesure, les divers départements édictent des recommandations contraignantes relatives aux normes de sécurité informatique applicables dans leur secteur de compétence. De manière générale, il n'existe pas de normes étatiques de sécurité informatique s'appliquant aux exploitants d'infrastructure numériques et aux fournisseurs de services en ligne. Il est en revanche probable que les autorités compétentes édictent des prescriptions sectorielles pour les exploitants d'infrastructures critiques et pour l'administration publique. Citons pour exemple le *National Institute of Standards and Technology* (NIST), qui, dans son cadre de cybersécurité, a élaboré des «quasi-normes» relativement détaillées régissant les infrastructures critiques.

Comparaison entre pays

	Normes nationales obligatoires en matière de TIC pour						
État	Exploitants d'«infrastructures numériques» et de «services en ligne»	Bureau de notification	Tous les exploitants d'«infrastructures critiques»	Bureau de notification	«Administration»	«Secteurs spécifiques»	Bureau de notification
Suisse	**A**	**A**	**A**	**A**	**AAA**	**AA**	**AA**
Allemagne	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AA**
Autriche	**AAA**	**AA**	**AAA**	**AA**	**AAA**	**A**	**AA**
France	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Grande-Bretagne	**A**	**A**	**AA**	**AA**	**AA**	**AA**	**AA**

Suède	**A**	**A**	**AA**	**AA**	**AA**	**AAA**	**AAA**
Norvège	**AA**	**A**	**AA**	**AA**	**AA**	**AA**	**AA**
Finlande	**AA**	**AA**	**AA**	**AA**	**AAA**	**AA**	**AA**
Singapour	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Hong Kong	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**
Australie	**AA**	**AA**	**AA**	**AA**	**AA**	**AA**	**AA**
USA	**A**	**A**	**AA**	**AA**	**AAA**	**AAA**	**AAA**
Chine	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**	**AAA**

Remarque: tous les pays analysés disposent actuellement d'une cyberstratégie nationale. Selon les pays, les efforts concernant les prescriptions de l'État ou celles posées à un bureau de notification sont néanmoins très différents sur le plan institutionnel, juridique et sectoriel. La «pondération» figurant dans le tableau indique la tendance concernant les prescriptions des États correspondants.

Le pays concerné dispose de prescriptions ou de bureaux de notification: **AAA = *«excellents»*, AA = *«médiocres»*, A = *«nuls»*** ou ***«très faibles»***.