economiesuisse
DOSSIER POLITIQUE

# # 03 / 2018

# Une politique des données basée sur la confiance, pour le progrès et l'innovation

12.03.2018

## L'essentiel en bref

L'utilisation innovante des données ouvre des perspectives insoupçonnées, de nouveaux champs d'application et favorise la création de nouveaux modèles d'affaires. En même temps, les changements induits par la transformation numérique sont source d'incertitude. Qu'advient-il des données dans les limbes du cyberespace? Que faire pour garantir qu'elles ne tombent pas entre de mauvaises mains? Comment assurer et constamment améliorer la sécurité dans des systèmes de réseaux? Cela soulève des questions subsidiaires. Comment la politique devrait-elle réagir à ces transformations? Quel rôle incombe alors aux individus, aux milieux économiques et à l'État? economiesuisse répond à toutes ces questions en proposant sa politique des données pour l'économie. Celle-ci a été développée avec des représentants de toutes les branches, ainsi que de grandes et petites entreprises. La politique des données permet – en dépassant largement le simple cadre de la protection des données – de discuter des questions ouvertes et de présenter les différents intérêts à l'œuvre lorsqu'il s'agit de renforcer la capacité d'innovation et la compétitivité de la Suisse. Susciter la confiance des individus dans le traitement des données est crucial dans ce contexte.

**Contact et questions**

**Erich Herzog**
Membre de la direction, responsable du département Concurrence et Réglementation

**www.dossierpolitik.ch**

## Position d'economiesuisse

- **Éviter une réglementation étatique préventive en matière de politique des données:** dans un environnement technologique dynamique, des règles restrictives décidées à la hâte risquent d'entraver la création de valeur et les développements futurs.

- **Équilibrer durablement la protection des données et l'innovation:** les données sont le moteur de l'innovation pour les nouveaux modèles d'affaires. L'espace pour l'innovation doit alors être proportionnel à la protection des données individuelles.

- **À l'État de reconnaître et d'encourager l'autorégulation des entreprises:**une approche basée sur l'autorégulation convient mieux qu'une réglementation étatique rigide pour relever les nombreux défis dans le domaine des données. L'État dispose en outre de moyens suffisants pour responsabiliser les entreprises le cas échéant.

- **Adopter les standards économiques comme recommandations:** dans de nombreux domaines, la sécurité juridique peut être assurée par les standards de branche fixant une norme communément acceptée pour l'utilisation des données.

- **Préserver la liberté des particuliers d'agir en toute responsabilité:** une mise sous tutelle par l'État n'est pas efficace en matière de traitement des données. Les particuliers devraient pouvoir contrôler leurs données de manière responsable, dans les limites du cadre technologique disponible.

- **Utiliser des moyens techniques pour gagner la confiance:** les nouvelles technologies et les nouveaux outils devraient être utilisés de manière cohérente. Cela garantit un traitement des données fiable et favorise la responsabilité individuelle.

- **Utiliser les instruments juridiques existants:** les instruments en place permettent de répondre à pratiquement toutes les questions de droit. La loi fédérale contre la concurrence déloyale (LCD), la loi sur le droit d'auteur (LDA), d'autres droits de la propriété immatérielle ou encore la loi sur les cartels (LCart) conviennent notamment à cet effet.

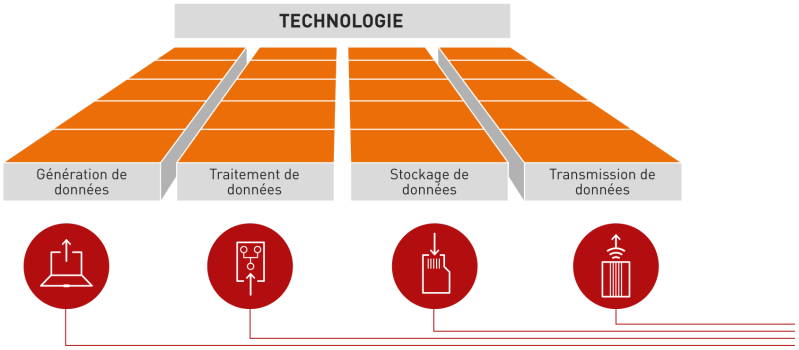
## Numérisation et données

→ **Les données sont le moteur de l'innovation.**

La digitalisation est la base sur laquelle les milieux économiques, les sciences et la société se développent. Dans sa publication sur l'économie numérique [1] , economiesuisse indique ce que la Suisse devrait faire pour tirer parti de ces transformations technologiques et rester dans le peloton de tête. Le cœur de la numérisation est constitué par la possibilité de générer des données, de les traiter, de les stocker et de les transmettre [2] . Les données sont ainsi le véritable moteur de l'innovation à l'ère du numérique. Tous les nouveaux modèles d'affaires se fondent sur l'utilisation de données, comme détaillé dans les exemples suivants.

**Figure 1**

**Processus liés aux données au centre de la numérisation**




Source: economiesuisse
www.economiesuisse.ch

→ **Des exemples pour montrer les avantages des données dans tous les domaines.**

**Simplification de la mobilité**

Aujourd'hui déjà, il est possible de réunir dans une même application plusieurs moyens de transport, comme les taxis, les transports publics, les véhicules et vélos de location. L'application calcule l'itinéraire le plus direct. Elle peut aussi intégrer d'autres paramètres individuels et permettre la livraison d'achats ou de plats au domicile.

**Diagnostic (précoce)**

Si une photo prise avec le flash montre une tâche blanche, et non rouge, dans l'œil d'un enfant, il peut s'agir d'une tumeur. L'application «White eye detector» examine les photos stockées sur le téléphone mobile à la recherche de signaux d'alerte pour le cancer des yeux. Les yeux jugés inhabituels sont immédiatement identifiés et signalés par l'application. Celle-ci peut procéder à un test rapide de détection du cancer de l'œil avec l'appareil photo du téléphone mobile. De même, certains algorithmes utilisés par Google permettent de détecter des maladies oculaires à partir de photos des yeux. Une application a été développée récemment pour détecter une pression artérielle élevée et un risque d'infarctus. Ces solutions sont

plus avantageuses, plus rapides et moins invasives que les méthodes conventionnelles.

**Soutien aux patients dans le domaine médical et développement de nouvelles thérapies**

Les outils de traitement (comme un inhalateur) pourront bientôt, grâce à des capteurs et une application, fournir des données et des mesures au médecin traitant. Cela permettra d'améliorer son évaluation. Le médecin et le patient recevront directement des informations sur le déroulement de la thérapie, les effets secondaires ou des infections et pourront, si nécessaire, intervenir immédiatement. Cette collecte de données à grande échelle permet de développer de nouvelles connaissances et contribue à améliorer les thérapies pour les patients.

**Découverte de planètes et de galaxies**

En 2017, la NASA (National Aeronautics and Space Administration) a découvert, avec l'aide de Google, un nouveau système solaire, similaire au nôtre, qui compte huit planètes. Avec ses moteurs de recherche, le groupe a analysé des données du télescope Kepler. Cela a permis d'analyser très rapidement un volume de données bien plus important que ce qu'il serait possible de faire manuellement. En quatre ans, le télescope Kepler a observé 200 000 étoiles et pris une photo toutes les 30 minutes. Il a ainsi collecté des billions de données. Des astronomes auraient mis beaucoup plus de temps pour effectuer ce travail.

→ **Les processus numériques génèrent d'énormes volumes de données.**

**Quelques données sur des données**
En 2016, le volume de données produites à travers le monde a atteint 16,1 zettaoctets. Sous forme de textes écrits à l'ordinateur, cela représenterait 230 000 billions de pages A4, soit une pile représentant 82 fois la distance entre le Soleil et Neptune. La lumière d'une lampe placée sur la dernière feuille mettrait 14 jours et 8 heures pour venir éclairer la première, sur terre (cf. economiesuisse/W.I.R.E., La Suisse numérique, page 15.).

# Politique des données pour l'économie

→ **Les milieux économiques définissent sept lignes directrices de la politique des données.**

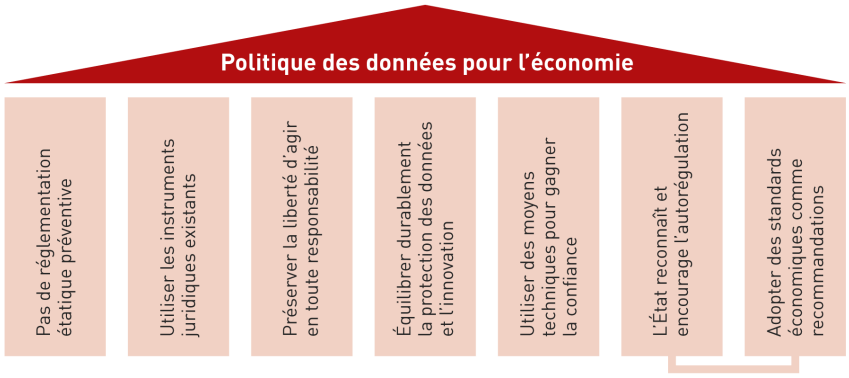
L'un des défis pour les entreprises est de garantir la confiance de tout un chacun lors du traitement de données. Sans confiance, il ne peut y avoir de gestion durable des données, car les individus ne mettent leurs données à disposition que s'ils savent qu'elles seront gérées de manière adéquate. La transparence dans la saisie et le traitement des données permet à chacun de décider quelles offres il veut utiliser ou non.

## Les piliers de la politique des données

Avec ses lignes directrices, l'économie définit les piliers d'une politique des données. Ceux-ci sont la base des besoins et des champs d'action identifiés dans le présent dossier. Il s'agit de montrer, de manière constructive, comment traiter les données dans un contexte où plusieurs intérêts s'affrontent.

**Figure 2**

**Lignes directrices de la politique des données**




Source: economiesuisse
www.economiesuisse.ch

→ **Demandes et champs d'action identifiés**

Les individus et leur environnement produisent sans cesse des données. Que ce soit en utilisant Internet ou des produits, en effectuant des transactions financières, en allant au club de gym ou en remplissant une déclaration fiscale. Les machines aussi génèrent des données, en enregistrant des états de fonctionnement ou en communiquant des données de production, par exemple. Partout et en permanence, des données sont créées.

## Demandes et champs d'action

Voici les demandes et domaines d'action identifiés à partir des lignes directrices de la politique des données:

1. Renoncer à un droit de propriété des données

2. Renoncer à de nouvelles lois restreignant le transfert de données

3. Utiliser les instruments de droit existants pour garantir l'accès aux données et la sécurité des investissements dans les produits basés sur les données

4. Instaurer la confiance comme base du traitement des données et de l'innovation

5. Renoncer à un droit fondamental à la portabilité des données

6. Établir des normes d'anonymisation de l'économie

7. Promouvoir l'approche basée sur le risque pour la gouvernance des données

8. Soutenir les données ouvertes de l'administration publique (open governement data)

9. Établir des normes minimales et sectorielles pour la cybersécurité et améliorer la gestion des risques et des crises.

**Bonnes pratiques bien plus efficaces qu'une la réglementation étatique préventive**

## Neuf demandes et champs d'action

→ **Corseter les données dans un cadre légal entrave les innovations.**

### 1. Pas droit de propriété des données

Certains vantent aujourd'hui le droit de propriété des données, comme solution pour les particuliers de conserver la souveraineté sur leurs données et de protéger leurs investissements. D'aucuns font d'ailleurs déjà valoir cette exigence sur le plan politique. Mais un droit de propriété des données est-il justifié et comment pourrait-il être mis en œuvre?

Les réflexions juridiques ont gagné en dynamisme, au rythme des évolutions technologiques. Certaines manières d'exercer la possession et la propriété, jusqu'ici purement théoriques ou difficilement réalisables, sont possibles aujourd'hui. La disponibilité des informations élimine les frais de recherche et réunit des personnes aux besoins similaires, à l'instar des nouvelles formes de location (Uber, Airbnb) ou de la tendance à utiliser les contenus en ligne plutôt que de les posséder (plateformes de diffusion continue). Un film sur DVD ne peut être visionné que par l'utilisateur qui le détient physiquement. Un film sur Netflix est accessible à une multitude de personnes en même temps.

Actuellement, les données ne sont pas définies comme objets de droit et ne permettent donc pas de faire valoir des droits absolus comme des droits de propriété. Cependant, la législation en vigueur garantit, pour toutes les personnes concernées, un traitement sûr des données. Il n'est donc pas nécessaire pour cela de créer un objet de droit – et donc une propriété des données. La patrimonialité des données entre notamment en contradiction avec les exigences et les acquis de la numérisation. S'il devient nécessaire d'adapter la législation dans certains domaines, pour la blockchain [3] par exemple, ces ajustements peuvent s'effectuer de manière ponctuelle et ciblée sans que cela n'ait d'effets collatéraux involontaires sur l'économie numérique.

Un autre problème est que les exigences quant à la configuration de tels droits ne sont pas tangibles. En l'absence d'une harmonisation internationale, un cadre légal rigide pour les données menacerait fortement la sécurité du droit et de la planification. D'autres méthodes sont plus appropriées pour garantir la protection des données et la sécurité des investissements. Les droits de la personnalité, par exemple, permettent de protéger les personnes jusque dans le domaine de la gestion des données.

**Cas des algorithmes**

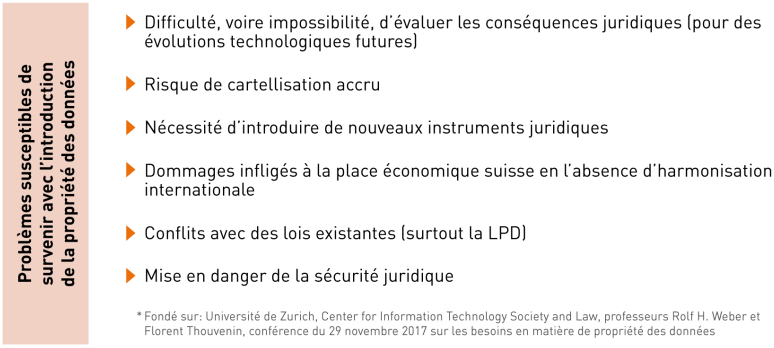
Les algorithmes sont des instructions opératoires pour les machines, comme une recette donne les indications pour cuisiner. Une nouvelle restriction en droit des algorithmes serait tout aussi peu pertinente qu'un droit de propriété sur les données et freinerait l'évolution dans ce domaine. Les algorithmes créent en effet une valeur ajoutée considérable à partir de données:

- les moteurs de recherche en ligne répondent aux requêtes sur la base d'algorithmes;

- les applications de navigation montrent le chemin grâce à des algorithmes;
- dans le secteur bancaire, les algorithmes permettent d'évaluer le risque dans les opérations de crédit.

**Figure 3**

**Problèmes induits par un droit de propriété des données***




* Fondé sur: Université de Zurich, Center for Information Technology Society and Law, professeurs Rolf H. Weber et Florent Thouvenin, conférence du 29 novembre 2017 sur les besoins en matière de propriété des données

Source: economiesuisse
www.economiesuisse.ch

→ **Les dispositions légales ne sont utiles que dans les cas exceptionnels.**

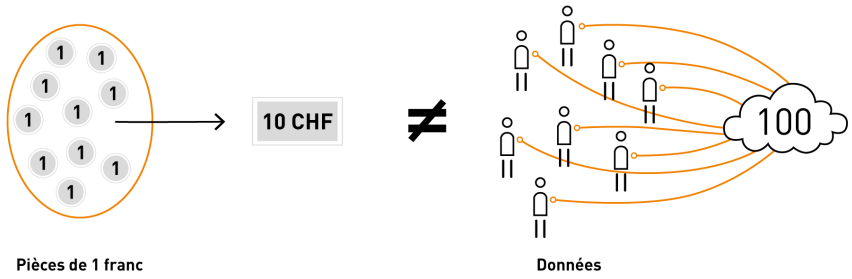
Avec les nouveaux modèles d'affaires, il peut y avoir des besoins, exceptionnels, de clarification comme pour les données dans le cadre d'une faillite. En délocalisant des photos vers un nuage, l'on peut augmenter l'espace mémoire du téléphone mobile au-delà de l'appareil. Les entreprises utilisent elles aussi la mémoire en nuage, à cause de l'accès facilité et d'autres prestations des fournisseurs de nuage informatique. Si un fournisseur de solutions en nuage fait faillite, l'entreprise n'a aucune possibilité d'exiger la restitution de ses données stockées dans le nuage, même si celles-ci sont essentielles pour ses opérations. Du point de vue légal en effet, les données ne constituent pas des choses mobilières pertinentes au regard de la faillite. Dans pareil cas, une réglementation des droits concernant les données [4] peut être justifiée à titre exceptionnel.

**Les données n'acquièrent de la valeur que dans un certain contexte**

Avec une pièce d'un franc en poche, l'on peut acheter de la marchandise à hauteur de la contre-valeur. Avec dix personnes donnant un franc chacune, le montant passe à dix francs. Pour les données, la valeur se calcule d'une autre manière. Une donnée isolée n'a pas de valeur en soi. Il faut placer les données dans un contexte par rapport à l'origine ou à d'autres jeux de données pour qu'elles acquièrent de la valeur. Par exemple, des données isolées de déplacement à vélo ne servent à rien, mais combinées pour un système de location de vélos, elles deviennent intéressantes parce qu'elles se muent en informations pouvant être interprétées par l'entreprise. Cette valeur ne peut pas être calculée à partir de la donnée individuelle.

Figure 4

Valorisation des données




Source: economiesuisse
www.economiesuisse.ch

→ **Une circulation des données sans restriction et une confiance solide dans le traitement des données sont souhaitables.**

## 2. Pas de nouvelles lois restreignant le transfert de données

Par transfert de données, il faut entendre le flux de données empruntant les voies de transmission numériques entre différentes parties prenantes. Chaque fois que des informations sont transmises, cela alimente la circulation des données au sens large. Les parties participant au transfert de données ont des droits et des obligations. L'absence de toute restriction à l'égard du transfert de données, indépendamment du lieu où se trouvent les parties prenantes (c'est-à-dire aussi au niveau international) est fondamentale pour l'économie. Toute limitation ou nouvelle réglementation à l'échelle nationale est à éviter. Cela vaut notamment pour les blocages de réseaux.

### Refuser les blocages de réseaux

Les blocages de réseaux ou limitations d'accès sont des mesures techniques qui, sur ordre de l'État, restreignent l'accès à certains prestataires sur Internet. Le projet de loi sur les jeux d'argent prévoit ainsi des blocages de réseaux, afin que les fournisseurs étrangers sans concession en Suisse puissent être exclus du marché des jeux d'argent. Les internautes seraient empêchés d'accéder aux pages web proposant ces offres, grâce à des barrières techniques contrôlées par l'État et mises en place par les fournisseurs d'accès à Internet. De tels blocages sont totalement inappropriés en la matière et, en plus, dangereux parce qu'ils perturbent la sécurité et la stabilité des réseaux.

### Transfert de données: avantages de l'autonomie privée et des bonnes pratiques

Aujourd'hui déjà, les parties prenantes – particuliers ou entreprises – règlent le transfert de données entre elles, généralement par arrangements contractuels, conditions d'utilisation et application des dispositions légales en vigueur. Une réglementation additionnelle par la loi n'est pas nécessaire.

Les bonnes pratiques sont des règles de comportement que les branches ou l'économie dans son ensemble s'imposent à elles-mêmes. Pour la circulation des

données, celles-ci permettent d'éviter une information insuffisante des parties prenantes les plus faibles et de promouvoir la sécurité du transfert de données en garantissant un traitement des données responsable. Les bonnes pratiques peuvent prendre les formes suivantes:

- clauses standard/éléments de contrat instaurant un juste équilibre des droits et obligations des parties prenantes, pouvant être repris par ceux-ci dans le cadre de contrats;
- normes techniques en matière de technologie et de sécurité;
- description commune des rôles des parties prenantes dans le transfert de données.

En plus de garantir la responsabilité des parties prenantes dans le transfert de données, les bonnes pratiques contribuent aussi à le rendre plus fluide et plus simple, par exemple par des éléments de contrat standardisés. En fin de compte, elles créent de la sécurité juridique.

**Bonne marche des affaires ralentie par les ruptures de médias**

Rupture de médias signifie que, dans un contexte de transfert ou de traitement numérique d'informations, des éléments doivent être transmis manuellement (par saisie manuelle sur un ordinateur, par exemple). Ces ruptures de continuité peuvent engendrer d'importantes charges additionnelles, notamment dans les contacts avec les autorités. Lorsqu'une information traitée par voie électronique dans l'entreprise doit être préparée à la main (couchée sur papier, saisie dans un masque en ligne) pour être soumise à une autorité de surveillance, cela représente un travail supplémentaire, de nouvelles sources d'erreur et donc une perte de qualité dans le processus concerné. Dans les rapports avec l'État notamment, ces changements de support d'information plombent régulièrement l'efficacité des échanges. En été 2017, le SECO a mené auprès de l'économie une enquête sur l'adéquation des lois face à la digitalisation (test numérique). De nombreuses dispositions entravant l'échange numérique avec les autorités ont été identifiées.

## 3. Les instruments juridiques en vigueur garantissent l'accès aux données et assurent les investissements dans les produits reposant sur les données

Les données qu'une personne communique échappent en partie à son contrôle. Elles peuvent être détenues par une administration publique, une entreprise ou une autre personne. Des droits d'accès sont conférés aux personnes autorisées à accéder à des données. Cela s'applique aussi aux relations entre deux entreprises.

La protection des investissements vise à protéger, d'une manière adéquate, les dépenses liées à des données contre une exploitation non autorisée par des tiers. Un développement dans le domaine des produits basés sur les données ne doit pas pouvoir être utilisé par un tiers (ou du moins pas sans une indemnisation).

**Les lois telles que la LCD, la LCart et la LDA offrent de nombreuses possibilités d'action**

Utilisé correctement, notre arsenal juridique permet de réglementer l'accès aux données de manière raisonnable et d'assurer la protection des investissements dans

les produits basés sur les données:

- La loi fédérale contre la concurrence déloyale (LCD) contient un droit dit de la protection des prestations qu'il est possible d'invoquer devant un juge pour empêcher l'utilisation d'une prestation propre par un tiers.
- Le fait que des entreprises revendiquent l'accès à des données d'autres entreprises pour déployer leurs activités sur un marché déterminé n'est pas nouveau. La question a toujours été traitée sous l'angle du droit des cartels et du contrôle des abus de position dominante (LCart). Le terme d'essential facility devrait être évoqué immédiatement à chaque fois que des données sont en jeu.
- Une protection spécifique des banques de données [5] qui constituent une création intellectuelle propre à leurs auteurs est prévue dans le droit de l'UE. Il est possible de se passer de cette réglementation. En droit suisse, les banques de données peuvent être placées sous la protection du droit d'auteur (LDA) à certaines conditions. Une protection suffisante est garantie ici aussi, en particulier par la protection des prestations de la LCD.

**Les instruments juridiques existants permettent aux tribunaux de rendre des jugements équitables**

En 2005, le Tribunal fédéral a dû statuer sur un litige entre plusieurs prestataires d'annonces immobilières en ligne. L'un d'eux recherchait systématiquement sur Internet les nouvelles annonces immobilières pour les publier sur son site dans un but commercial. Le Tribunal fédéral s'est penché sur la recevabilité de cette pratique. Après une évaluation juridique approfondie, le Tribunal fédéral a réglé le différend en s'appuyant sur la loi fédérale contre la concurrence déloyale (LCD).

## 4. Le traitement des données et l'innovation reposent sur la confiance

Aujourd'hui, les utilisateurs veulent toujours plus accéder en tout lieu et en tout temps à des contenus qu'ils jugent intéressants et qui correspondent à leur profil. L'obtention de l'information, de la marchandise ou de la prestation passe souvent avant la loyauté à un prestataire. De nouveaux modèles d'affaires sont créés pour répondre aux attentes de ces utilisateurs. La numérisation favorise l'apparition de nouvelles prestations qui facilitent la vie et augmentent la diversité de l'offre. Le traitement de grandes quantités de données est au cœur de ces nombreux nouveaux modèles d'affaires. Celui qui met des données à disposition doit pouvoir être sûr que celles-ci seront utilisées à bon escient et qu'elles ne serviront pas à des fins abusives. Ce qui est acceptable pour un utilisateur peut aller trop loin pour un autre. La réponse à la question de savoir ce qui est admis et ce qui est interdit doit être individuelle. Une protection des données démesurée et infantilisante dans ce domaine freinerait sensiblement tout nouveau développement. Il appartient aux utilisateurs et aux prestataires de trouver un juste équilibre entre protection des données d'une part et capacité d'innovation d'autre part.

→ **En matière de traitement des données, les milieux économiques doivent respecter des considérations éthiques.**

**Considérations éthiques, autorégulation et bonnes pratiques des entreprises dans le domaine du traitement des données**

Les possibilités offertes par l'analyse de grandes quantités de données sont énormes. La Chine par exemple pratique le big nudging pour essayer d'influencer le comportement de toute sa population dans le sens voulu par le gouvernement. Ces tentatives de manipulation et de contrôle doivent être clairement rejetées. Souvent, c'est l'État lui-même qui, pour diverses raisons, accède à des données concernant ses citoyens. L'affaire Snowden et les programmes de stockage préventif des données sont là pour le rappeler.

Il est fondamental, pour les milieux économiques, de tracer, sur la base de principes éthiques, les limites de ce qui peut être fait. Le risque que des clients soient manipulés ou que des processus opaques les incitent à prendre des décisions malheureuses doit être évité. L'économie est prête à s'autoréguler dans le domaine du traitement de données en s'appuyant sur une réflexion éthique. Elle veut se montrer digne de la confiance de ses clients.

→ **La portabilité des données ne doit pas être absolue. L'anonymisation et l'approche basée sur les risques sont à saluer.**

**Révision actuelle de la loi sur la protection des données et relation avec la numérisation**

Les entreprises connaissent l'importance d'une protection adéquate des données. En Europe, les règles [6] ont été durcies récemment, avec des répercussions directes sur la Suisse. La loi fédérale sur la protection des données (LPD) est également en cours de révision.

La protection des données se réfère au premier niveau d'utilisation des données (collecte, sauvegarde et définition des données). Mais cette approche de la protection des données ne permettra pas de suivre le rythme de la transformation numérique encore longtemps.

## 5. La portabilité des données ne doit pas être garantie dans la loi

La portabilité des données règle la question de la transmission des données vers d'autres systèmes. Une personne active sur Facebook, par exemple, transfère toutes sortes de données sur la plateforme: les noms de ses amis, ce qu'elle aime, des photos, etc. À partir de ces données révélatrices d'un comportement, l'exploitant de la plateforme peut en déduire d'autres. Si la personne opte à présent pour une autre plateforme, peut-elle récupérer ses données ainsi que les conclusions qui ont été générées et les transférer sur la nouvelle plateforme? La portabilité des données pose ainsi la question de savoir s'il faut obliger les entreprises à transférer, c'est-à-dire à transmettre à des tiers désignés, les données saisies par leurs utilisateurs sous une forme structurée.

**Un droit absolu à la portabilité des données est disproportionné**

En vertu de la nouvelle législation de l'UE, les entreprises et les autorités seront obligées de garantir la portabilité des données. Cette obligation doit permettre aux utilisateurs de mieux contrôler leurs données et encourager la concurrence entre prestataires. Les utilisateurs auront le droit de réclamer par exemple des données brutes ou des données issues de compteurs électriques intelligents, de moteurs de

recherche ou de bracelets connectés. Un droit absolu à la portabilité des données n'existe pas en droit suisse.

L'exemple du réseau social mentionné plus haut montre les limites d'un droit aussi absolu. En règle générale, recevoir ses données n'est d'aucune utilité pour l'utilisateur d'un réseau social. Ce qui l'intéresse en premier lieu, ce sont les enseignements et les conclusions générés, par le réseau ou par des tiers, à partir de ses données. Toutefois, il n'est pas possible d'extraire ses données du système sans porter atteinte à ses intérêts.

**Pour une portabilité des données différenciée**

Les entreprises investissent régulièrement des montants considérables dans le domaine de la protection des données. Il est possible à tout moment de remettre les données à l'utilisateur quand les deux parties, le client et l'entreprise, en conviennent ainsi. Il serait cependant malvenu d'obliger l'entreprise à rendre des données dans tous les cas et de lui dire comment elle doit procéder. Qui plus est, ces données sont souvent déjà enregistrées dans le système de manière anonymisée, voire ne peuvent tout simplement plus être attribuées à un seul individu. Il convient aussi de noter que le transfert de données d'une entreprise à un particulier peut, selon les règles en vigueur sur les formats, s'accompagner de difficultés techniques.

Il existe d'autres possibilités pour garantir un droit de regard raisonnable sur ses données:

- utilisation d'instruments juridiques et techniques existants;
- ententes entre les parties, éventuellement par des contrats;
- bonnes pratiques

## 6. Normes d'anonymisation de l'économie

**6. Normes d'anonymisation de l'économie**

L'anonymisation et la pseudonymisation sont deux procédés concourant à la protection des données. Dans la pseudonymisation, le nom de la personne ou un autre caractère d'identification est remplacé par un pseudonyme (combinaison de lettres ou de chiffres). Dans l'anonymisation, les données sont modifiées de manière à ne plus pouvoir reconnaître la personne.

Exemple: pour que ses étudiants puissent accéder facilement aux résultats d'un contrôle écrit, le professeur d'une haute école peut leur demander d'inscrire, sur les feuilles, un pseudonyme librement choisi. Une fois les épreuves corrigées, le professeur peut publier une affiche (y compris sur Internet) qui permet de découvrir les résultats pour chaque pseudonyme. L'attribution du pseudonyme à l'étudiant ne peut dépendre que du professeur ou de l'étudiant lui-même. Il s'agirait d'une anonymisation si les feuilles d'examen avec mention des pseudonymes des étudiants étaient détruites après coup. Les indications figurant sur l'affiche seraient anonymisées, car il ne serait plus possible de les attribuer aux étudiants respectifs.

**Avantages des normes d'anonymisation de l'économie**

Pour une entreprise qui élabore un nouveau concept, travailler avec des données peut se révéler fastidieux si elle doit obtenir à chaque fois une autorisation du fournisseur de données. En règle générale, le volet personnel des données ne l'intéresse pas non plus. L'anonymisation et la pseudonymisation lui permettent d'utiliser ces données de manière simplifiée tout en garantissant la protection de la personnalité.

Les solutions d'anonymisation incluant aussi des possibilités de pseudonymisation deviennent rapidement obsolètes. Des standards techniques développés par les branches économiques évoluent en continu et protègent les droits de la personnalité.

L'anonymisation permet aussi de surmonter une autre difficulté: dans la pratique, il n'est guère possible de séparer les données personnelles de celles générées par des objets. De nombreuses données, y compris les données d'exploitation d'une fraiseuse par exemple, peuvent être liées à une personne. Les données de l'horloge interne de la machine pourront être couplées avec le plan d'intervention des collaborateurs. Il sera possible de tirer des déductions sur le comportement de l'utilisateur de la machine. L'utilisation des données d'exploitation pour améliorer les processus de production risque d'être limitée par la protection des droits de la personnalité de l'utilisateur de la machine. L'anonymisation offre l'avantage de pouvoir exploiter et analyser les données tout en protégeant au mieux les droits de la personnalité.

## 7. Pour une gouvernance des données basée sur les risques

La gouvernance des données d'une entreprise représente l'ensemble des règles sur la mise à disposition, l'utilisation, l'intégrité et la protection des données de l'entreprise. La mise en œuvre d'un système de gouvernance des données dans l'entreprise comporte différentes mesures: définition des banques de données, encadrement des responsabilités internes en fonction des données traitées, institution d'un mécanisme de contrôle et formation des collaborateurs.

Dans l'approche fondée sur les risques, les plus gros investissements dans la protection des données sont effectués là où le potentiel de risques est le plus grand. Si une entreprise recueille des données par exemple au moyen d'une carte client personnalisée qui donne des points de fidélité lors de chaque achat, la collecte de ces données ne présente pas, en soi, de risque particulier. Le big data [7] présente cependant de nombreuses possibilités de traitement des données. Si l'on croise les points de fidélité avec les données de la caisse-maladie de la même personne, cela est loin d'être anodin. Dans ce domaine, les entreprises engageront plus de moyens que dans d'autres pour protéger les données et respecter les normes éthiques.

**Seule l'approche fondée sur les risques permet leur prise en compte adéquate**

L'approche par les risques est nécessaire pour tenir compte de la complexité d'une entreprise et des diverses possibilités d'association et d'utilisation des données. En raison des multiples formes de combinaison entre elles, les données génèrent des risques plus ou moins marqués. De plus, d'autres facteurs doivent être pris en compte dans une entreprise: existence de données non structurées; possibilité pour des tiers d'accéder à des données; processus recourant à des données personnelles

sensibles; données n'existant qu'au niveau de l'application. L'approche axée sur les risques permet d'accorder toute l'attention requise aux situations les plus à risque. Les ressources sont ainsi allouées à des risques effectifs, sans risque d'éparpillement.

### 8. Soutien aux données ouvertes de l'administration publique (open government data, OGD)

Les bases de données du secteur public sont nombreuses et très volumineuses. Les administrations recueillent régulièrement des données dans l'exécution de leurs tâches. Il s'agit notamment des statistiques de la population, de données météo, de cartes topographiques des frontières communales de la Suisse, de documents historiques, de données du transport ou de répertoires de la littérature suisse. Ces données peuvent être utilisées tant par l'administration que par des tiers, entreprises ou particuliers, dans un but de création de valeur. L'entreprise peut, le cas échéant, avoir un intérêt à exploiter ces données ou à les utiliser d'une nouvelle manière. Une association de données inédite peut donner naissance à un nouveau modèle d'affaires mais aussi générer de la valeur ajoutée pour toute la population.

**Pour des OGD accessibles au public**

Toutes les données que l'État prélève dans l'accomplissement d'une tâche régalienne et qui ne sont pas personnelles (c'est-à-dire qui ne peuvent pas être rattachées à une personne) doivent être accessibles au public et donc également aux entreprises. Il faut cependant poser des limites: les particuliers qui travaillent avec l'État ou les entreprises publiques ayant des activités de droit privé ne seront pas soumises à l'obligation de publier des données. En parallèle, les entreprises publiques qui ont des activités de droit privé devront être assujetties aux règles de la concurrence.

→ **Les données OGD sont des données obtenues par l'État. Leur obtention est financée par les impôts et les taxes.**

**Qu'est-ce que les données OGD?**
Par open government data (OGD), il faut entendre les données que l'État obtient dans l'accomplissement d'une activité régalienne. L'obtention de ces données est financée par les impôts et les taxes.

→ **La réglementation étatique seule ne suffit pas en matière de cybersécurité. Un système décentralisé et flexible est nécessaire.**

### 9. Élaborer des normes minimales et sectorielles en matière de cybersécurité et améliorer la gestion des risques et des crises

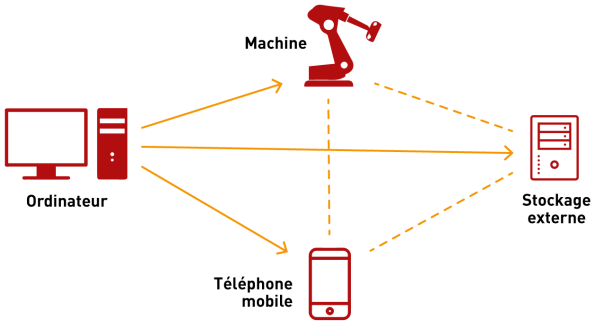
La numérisation et l'interconnexion des systèmes qu'elle implique nous rendent vulnérables dans de tous nouveaux domaines. En effet, l'utilisation de technologies, leur mise en réseau, leur complexité et leur dynamique comportent des dangers. Les médias s'en font l'écho presque quotidiennement, avec des articles sur des attaques et des manipulations. Ces activités criminelles sont perpétrées pour des raisons et avec des méthodes très diverses. À l'instar de ce qui se fait dans le monde physique, il faut se protéger pour éviter de subir des actes criminels de tiers dans le monde numérique.

**Les milieux économiques préconisent des normes minimales et sectorielles**

Un standard de sécurité uniforme prescrit par l'État ne peut pas répondre aux multiples défis de la cybercriminalité, car on risque ainsi une cybersécurité unilatérale et donc insuffisante. Il faut, au contraire, privilégier un système décentralisé et flexible. Les milieux économiques peuvent contribuer à augmenter le niveau de cybersécurité au moyen de standards minimums «prêts à l'emploi», là où des normes sectorielles sont requises. À cet égard, il faut porter une attention particulière aux maillons faibles de la chaîne, car, avec la mise en réseau, toute entité ayant un niveau de protection inférieur à la moyenne fragilise l'ensemble de la chaîne. Des standards minimaux élaborés par les milieux économiques sont d'autant plus importants dans ce domaine: des entreprises mal protégées peuvent bénéficier du savoir-faire d'autres entreprises. Cela évite également une asymétrie entre les branches dans le domaine de la cybersécurité. Par ailleurs, la création de standards minimaux permet d'aborder la question sous l'angle des risques. Sa mise en œuvre intègre de manière appropriée le risque encouru par l'entreprise. La mise en réseau comprend également celle des appareils entre eux. Si une entreprise ne veille pas à une maintenance régulière de ses appareils, ceux-ci peuvent être le point d'entrée d'une attaque.

Figure 5

**Propagation de cyberrisques en raison de la mise en réseau d'objets et d'entreprises**




Source : economiesuisse
www.economiesuisse.ch

**Répartir les tâches entre le secteur privé et l'État en cas de crise et encourager le signalement de cyberattaques**

Une définition claire des tâches entre le secteur privé et l'État est nécessaire pour anticiper les cas de crise. L'État doit être doté des instruments nécessaires pour poursuivre des crimes dans l'espace virtuel international. Parallèlement, il doit veiller, par des incitations appropriées, à ce que les incidents soient signalés. Ainsi, il sera en mesure de réagir et de formuler des recommandations. Ses relations avec les entreprises doivent se fonder sur une culture de la coopération et non de la contrainte. Ainsi, une communication doit avoir lieu si l'entreprise le souhaite et sous une forme qui lui paraît adaptée. Encourager le signalement d'incidents permettrait d'accroître la transparence, de mieux appréhender les menaces et de réduire les conséquences pour des tiers.

**Sensibiliser la population, les entreprises, l'administration et la politique**

La cybersécurité est une tâche collective classique qui concerne non seulement les entreprises et l'État, mais également les particuliers. La compréhension des cyberrisques doit être améliorée de façon générale afin d'induire un changement des comportements. Les banques, par exemple, envoient régulièrement des informations à leurs clients pour les sensibiliser aux cyberattaques ou les mettre en garde contre des courriels et des appels téléphoniques frauduleux.

## Déclaration des milieux économiques

→ **L'adoption par les milieux économiques d'une déclaration suscitera la confiance.**

Les lignes directrices et les champs d'action identifiés sont le point de départ de bonnes pratiques des milieux économiques. Adopter des standards généralement reconnus dans le domaine du traitement et du transfert de données permet d'éviter un écart important entre le niveau d'information des différentes parties, de promouvoir la sécurité du transfert de données et d'accélérer ce dernier. De tels standards contribuent à la sécurité juridique sans entraver les évolutions. Les bonnes pratiques ont des avantages pour toutes les parties concernées, y compris quand il s'agit de traitement des données. Un standard d'anonymisation en évolution régulière au sein des entreprises permet de se maintenir à la pointe et d'assurer la protection de la personnalité. Dans le domaine de la cybersécurité, des standards minimaux sectoriels peuvent conduire à un système décentralisé et flexible et éviter des failles dans le dispositif. Les bonnes pratiques favorisent en outre des réflexions éthiques et techniques en lien avec les données et remplacent de manière appropriée un droit légal absolu à la portabilité des données. L'application de bonnes pratiques dans les domaines indiqués permet d'éviter des réglementations préventives inutiles.

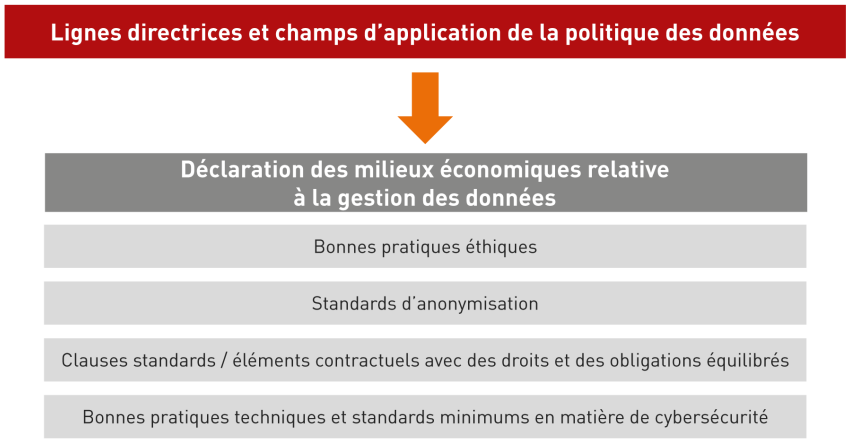
### Conclusion

Les évolutions technologiques sont rapides. La Suisse doit veiller à rester à la pointe dans ce domaine. La gestion des données et les nombreux champs d'application qui en résultent, de l'économie du partage à l'intelligence artificielle, modifieront en profondeur les activités économiques. À cet égard, il est de la plus haute importance de maintenir l'équilibre entre les différents intérêts de manière à conserver la confiance des individus et à préserver la capacité d'innovation de la place économique.

Les milieux économiques sont prêts à assumer leurs responsabilités. Pour ce faire, ils expliquent avec quels instruments il est possible de renforcer la confiance dans nos entreprises et, simultanément, de donner à la Suisse les outils dont elle a besoin face à la concurrence internationale et de rester dans le peloton de tête. Il est essentiel d'éviter d'entraver ou d'empêcher des évolutions par des règles trop rigides. La politique des données présentée ici par les milieux économiques donne les outils nécessaires pour ce faire.

Figure 6

**Bonnes pratiques comme solution pour la politique des données**




Source: economiesuisse
www.economiesuisse.ch

## Remerciements

Nous remercions tout particulièrement les membres du groupe de travail Politique des données d'economiesuisse ainsi que les personnes ci-dessous qui ont géré les sous-groupes et, par extension, les nombreux participants:

- Matthias Bossardt, responsable Cybersecurity KPMG Suisse, KPMG SA, en charge du sous-groupe Cybersecurité au sein du groupe de travail Politique des données d'economiesuisse;
- Maria Chiara Atzori, head Data privacy CH, Novartis International SA, responsable du sous-groupe Autodétermination pour les informations concernant la personne et big data au sein du groupe de travail Politique des données d'economiesuisse;
- Werner W. Wyss, head Regulatory affairs, Zürcher Kantonalbank, en charge du sous-groupe Transfert de données au sein du groupe de travail Politique des données d'economiesuisse;
- Gema Olivar Pascual, designated General counsel, PricewaterhouseCoopers SA, en charge du sous-groupe Données et algorithmes en tant que sujets de droit au sein du groupe de travail Politique des données d'economiesuisse;
- Jean-Marc Hensch, directeur, swico, en charge du sous-groupe Droits d'accès et d'utilisation au sein du groupe de travail Politique des données d'economiesuisse;
- Nadine Büchler, collaboratrice scientifique Concurrence et réglementation chez economiesuisse, secrétaire et coordinatrice du groupe de travail Politique des données jusqu'en septembre 2017.

1. economiesuisse/W.I.R.E., La Suisse numérique: imaginer l'économie et la société de demain, août 2017
2. Sample Tootlip
3. La blockchain est une technologie de stockage et de transmission d'informations décentralisée, transparente et sécurisée. Elle repose sur une chaîne de jeux de données liés les uns aux autres, qui s'agrandit à chaque transaction. Une fois sauvegardées, les données peuvent être lues, mais pas modifiées. La blockchain est donc résistante aux manipulations.
4. Initiative parlementaire 17.410 M. Dobler: Les données étant le bien le plus précieux des entreprises privées, il convient de régler leur restitution en cas de faillite.
5. Directive 96/9/CE concernant la protection juridique des bases de données
6. Règlement général sur la protection des données (RGPD), qui entrera en vigueur le 25 mai 2018; convention n° 108 du Conseil de l'Europe sur la protection des données, ratifiée par la Suisse
7. Terme générique employé pour différentes technologies de collecte et/ou d'analyse de grandes quantités de données. Ces données sont trop volumineuses, trop complexes, trop changeantes ou insuffisamment structurées pour pouvoir être exploitées avec les méthodes traditionnelles de traitement des données.