UNE NOUVELLE GOUVERNANCE POUR LES DONNEES AU XXIEME SIECLE

DES STANDARDS POUR LA CIRCULATION ET LA PROTECTION DES DONNEES PERSONNELLES

10 avril 2019

WWW.PRIVACYTECH.FR

PRESENTE L'ASSEMBLEE NATIONALE,

LE 10 AVRIL 2019

AVEC LE SOUTIEN DE :

MAZARS afnor CERTIFICATION Capgemini invent onecub

VISIONS SERAPHIN .LEGAL Infhotep

RÉDACTEURS-EN-CHEF :

PARTIE A & D : MAZARS onecub

PARTIE B : VISIONS

PARTIE C : Infhotep

LES CONTRIBUTEURS DE PRIVACY TECH

EXECUTIVE SUMMARY

RESUME

Une économie digitale performante et éthique nécessite une libre circulation des données personnelles sous le contrôle des individus. Le RGPD (Règlement Général sur la Protection des Données), lancé le 25 mai 2018, est un pas en avant majeur vers une nouvelle économie centrée sur l'individu grâce :

- au nouveau droit à la portabilité (Article 20) qui encourage la circulation des données,

- à une série de mesures et principes visant à augmenter la protection des individus comme le consentement spécifique et informé et le privacy by design.

Le RGPD s'inscrit dans la stratégie de Marché Unique du Digital (Digital Single Market) de l'Union Européenne et a pour but de créer les conditions pour une économie sans barrière qui bénéficierait autant aux individus et aux entreprises qu'à la société dans son ensemble. Presque un an après le lancement du RGPD, nous observons un paysage prometteur d'organisations qui commencent à s'adapter au nouveau règlement, autant en Europe que dans le reste du monde. Mais il reste encore beaucoup à faire, particulièrement en ce qui concerne la mise en oeuvre du contrôle des données par l'individu et de la portabilité. La tâche est éminemment complexe et requiert une coordination internationale, multisectorielle et multi-expertises. Pour réussir nous avons définitivement besoin d'une nouvelle approche ambitieuse qui pourrait partir de l'Europe pour s'étendre à l'international.

Dans un tel contexte, nous proposons d'engager un échange constructif entre tous les acteurs de la donnée personnelle (entreprises, administrations, académies, associations) qui voudraient joindre leurs efforts au sein d'une nouvelle forme d'organisation dont le but serait de construire, harmoniser et proposer des standards technologiques, terminologies et bonnes pratiques pour la circulation et la protection des données personnelles, ainsi qu'une gouvernance adaptée.

Les grandes problématiques à aborder sont les suivantes :

1. faciliter la circulation des données en s'appuyant sur le nouveau droit à la portabilité (Art. 20 RGPD) et en créant de nouveaux outils et standards dédiés

2. redonner de la confiance aux individus en s'appuyant sur le RGPD dans son ensemble et en harmonisant les bonnes pratiques relatives aux droits des personnes concernées

3. créer de la confiance entre les acteurs économiques en créant et en harmonisant des labels et des certifications

Dans le développement de ce document nous présenterons les enjeux, l'état d'avancement et des exemples concrets d'application pour chacune de ces problématiques.

Nous verrons que l'ensemble de ces défis requiert un niveau de coopération et de coordination très élevé au niveau Européen et au-delà. Nous présenterons également un mouvement émergent d'initiatives internationales.

Nous proposerons des recommandations pour structurer cette nouvelle économie et poserons les bases d'un futur organe de collaboration internationale dont la vocation sera de coordonner tous ces acteurs pour proposer des standards, labels et bonnes pratiques communs.

SOMMAIRE

Paula Forteza :

Paula Forteza est députée pour LREM de la 2e circonscription des français de l'étranger (Amérique latine et Caraïbes). Elle a 32 ans, née en France et grandi en Argentine. Elle a travaillé au sein du gouvernement de la ville de Buenos Aires puis s'est lancée dans une expérience entrepreneuriale avant de rentrer en France pour poursuivre ses études à Sciences Po. En 2015, elle a rejoint la mission Etalab rattachée au Premier Ministre, où elle a suivi des dossiers relatifs à la modernisation de l'administration publique, l'ouverture de données et la mise en place de politiques de transparence ainsi qu'à l'organisation du Sommet Mondial pour un Gouvernement Ouvert à Paris. Avant son élection, en tant que société civile, elle a travaillé dans l'utilisation d'outils numériques pour dynamiser la participation citoyenne et pour renouveler la démocratie. Aujourd'hui, elle œuvre chaque jour pour ouvrir et moderniser l'Assemblée nationale. Elle a ainsi mis son agenda en ligne, son IRFM est consultable en open data et elle propose un espace de collaboration avec la société civile lors de son Bureau Ouvert hebdomadaire. Rapporteure du groupe de réforme de l'Assemblée nationale « Démocratie numérique » elle espère généraliser toutes ces pratiques. Elle s'engage aussi dans le travail législatif de sa commission (commission des lois), elle a été rapporteure du projet de loi protection des données personnelles qui a intégré au droit français le RGPD.

Préface :

Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) est entré en application. Créateur de nouveaux droits pour les citoyens, il en proclame quatre principaux : un droit à l'oubli, à la rectification, à la portabilité et l'exigence d'un consentement libre et éclairé.

La proclamation de ces droits, bien que préalable nécessaire, ne peut être suffisante. L'enjeu principal, aujourd'hui, est celui de faire connaître, et comprendre, ces nouvelles possibilités données aux utilisateurs afin qu'ils s'en saisissent. Cela est d'autant plus nécessaire que tout l'équilibre du RGPD repose sur cette idée :

les citoyens détenant de nouveaux droits, les acteurs du numérique n'ont plus, par principe, de déclaration préalable à faire auprès de la CNIL pour commencer une activité traitant de données personnelles. Le contrôle devient donc, dans un premier temps, citoyen.

Il s'agit d'une nouvelle forme de régulation plus équilibrée permettant à la fois de ne pas brider l'innovation, tout en respectant les droits des utilisateurs. Cependant, un enjeu majeur demeure : donner les moyens aux utilisateurs d'exercer ses droits.

Aujourd'hui, qui lit les conditions générales d'utilisation ? Qui sait comment demander le transfert de ses données d'un service à l'autre ? Qui souhaite ne pas cocher la case mais le fait par habitude ou désabusement ?

Un an après le RGPD, le défi majeur est l'application de ces droits. Si le RGPD est instrument européen qui a parfaitement illustré la capacité des pays membres de l'Union européenne à se mettre d'accord sur des sujets majeurs en adoptant une position commune, il doit se montrer exigeant en matière d'application harmonisée de ses règles. La réponse à ce défi est la standardisation des normes par les acteurs du numérique. L'utilisateur doit être en capacité de se construire des repères sur ses droits et devoirs en ligne, les identifier facilement. Le déploiement du Marché Unique Numérique au sein de l'Union européenne se fait certes au niveau législatif, mais il ne pourra pas se faire sans une mise en œuvre harmonisée. La standardisation doit donc se faire de manière coordonnée et compréhensible par tous au-delà des frontières.
Pour y parvenir plusieurs voies existent : celle de l'innovation et celle du travail entrepris par la société civile, l'une n'ira pas sans l'autre. Le RGPD est l'occasion de faire naître tout un nouvel écosystème innovant chargé de mettre en œuvre ces nouveaux droits pour les citoyens. Il peut prendre la forme de RegTech permettant une réponse plus rapide aux exigences de conformité en déployant des solutions intuitives, en phase avec les besoins des utilisateurs. Une mise en garde doit tout de même être faite, les RegTech ne doivent pas devenir la compliance low cost des services numériques. A ce titre, plusieurs collectifs peuvent jouer ce rôle de lanceurs d'alerte, en posant des standards de qualité. Tim Berners-Lee, un des pères fondateurs du Web, a ainsi annoncé fin 2018, la création du projet Solid, plateforme open source destinée à héberger les données des utilisateurs où il le souhaite en en gardant le contrôle.

L'enjeu de demain sur la protection des données personnelles résident donc bien là : parvenir à une mise en œuvre harmonisée pour faire vivre ce cadre législatif européen coordonné. Il revient maintenant au politique d'être attentif aux initiatives qui pourraient naître, et aiguiller de manière concertée les propositions naissantes.

Axelle Lemaire :
Roland Berger, Ancienne Secrétaire d'Etat chargée du Numérique et de l'Innovation.

Introduction :

Le 21ème siècle est marqué par l'avènement massif et la démocratisation de l'accès à internet et de l'économie associée aux plateformes numériques, dont le modèle repose sur les données. Aujourd'hui, le socle légal des démocraties (droits et libertés fondamentaux) doit trouver sa forme d'expression dans ce phénomène d'avènement des plateformes. L'enjeu consiste à définir le cadre règlementaire le plus pertinent, mais également le cadre technologique et les usages qui permettront d'affirmer ces droits et libertés dans ce nouvel environnement.

Le RGPD répond en partie aux enjeux relatifs aux données personnelles et est en cela considéré comme un succès. Toutefois, le texte reste aussi perçu comme une contrainte, générateur de coûts et de démarches administratives. Les non-Européens ne partagent pas toutes les préoccupations européennes vis-à-vis de la protection des données. Pourtant, en réalité, le RGPD offre un avantage concurrentiel fort aux entreprises se soumettant à ces normes et principes. Cette exigence est intrinsèque à l'identité propre du numérique, qui repose sur la confiance des utilisateurs.

Malheureusement, cette vision n'est pas acquise partout aujourd'hui, même en Europe, car le RGPD est parfois vécu comme un fardeau. Politiquement, le RGPD peut être considéré comme une arme : la norme de droit n'est pas uniquement présente pour contraindre. Il sert également à accompagner un essor technologique pouvant bénéficier aux entreprises. Il est vrai que la situation actuelle peut sembler schizophrène : d'un côté, l'Union Européenne impose le plus haut standard de protection des données personnelles au monde, de l'autre, le marché européen est le dernier à en bénéficier, puisqu'il n'existe pas d'outils pour mettre en place le RGPD. Un vrai travail technique de mise en place est nécessaire.

Ce travail nécessaire n'est pourtant pas dû à un écueil du texte, mais à des lacunes dans la capacité de l'écosystème (communautés de développeurs, Etats, entreprises, organisations diverses), à le transformer en outil concurrentiel. Si les objectifs sont bons et nécessaires, mais il manque aujourd'hui un accompagnement des membres de l'écosystème pour permettre un changement de perception et une pleine exploitation du RGPD. Ceci nécessite notamment un travail sur la Privacy UX, sur la définition d'ergonomie, de design et de standards d'usage afin que le RGPD protège, mais que cela ne soit pas dommageable pour l'expérience utilisateur. Il faudra également réaliser un effort considérable en matière de standardisation des normes.

Pourtant, les standards sont trop souvent sous-évalués par les pouvoirs publics, en particulier dans le secteur des technologies. Ils sont perçus comme techniques et donc agnostiques, non politiques. Il faut cependant bien se rappeler que dans le secteur numérique, c'est le standard technique qui créer la norme. Prenons par exemple les technologies de télécommunication : le chantier de standardisation des normes mobiles avait été bien identifié par l'Union Européenne, avec des résultats remarquables pour définir le GSM et permettre l'interopérabilité des réseaux. Mais les progrès, depuis, sont beaucoup plus lents, au point que l'Europe est quasiment absente dans la définition des standards 5G. Pour le RGPD, il n'est pas trop tard pour agir, en s'appuyant sur un écosystème favorable.

Pour le moment, les industries européennes se rendent compte qu'elles se sont fait imposer des standards américains. Les technologies chinoises sont quant à elles utilisées à des fins de surveillance. On pourrait à ce propos demander à l'Europe de prendre le parti de créer un écosystème basé sur l'usage éthique des données. Les entreprises sont désormais conscientes de ces problématiques, et le RGPD a permis une réelle prise de conscience du pouvoir des données au sens général, et pas uniquement les données personnelles. Il a également permis d'accélérer l'entrée dans l'ère de la donnée. Ainsi, ces sujets qui n'étaient considérés que sous l'angle de la "compliance" (conformité) deviennent des sujets hautement stratégiques économiquement. Il n'en demeure pas moins que la stratégie doit être refondue, et ne plus être fondée sur la seule menace de la sanction financière et de la dégradation d'image. Il s'agit plutôt de responsabiliser les acteurs via un transfert de l'enjeux de conformité de l'amont vers l'aval. A ce propos, tout reste encore à construire en matière de "privacy by design" : ce transfert a donc pour objectif de sortir du schéma de pensée et d'action selon lequel « je me conforme à peu près, et j'espère ne pas être rattrapé par la patrouille ». Les standards préconisés dans ce rapport permettront de définir la voie idéale pour faire de la compliance au RGPD un atout éthique ET économique.

Les enjeux sont considérables : le RGPD est mal reçu même par les utilisateurs finaux ! Le recueil de leur consentement est complexe et opaque, d'autant plus que l'utilisateur n'a pas conscience du parcours des données, et ne maîtrise pas la chaîne de données qui le concerne. Le consentement éclairé est aujourd'hui plus un fantasme qu'une réalité.

Il ne faut pas oublier que le droit doit rester flexible : une interprétation trop rigide du RGPD pourrait bloquer les évolutions technologiques. Pour autant, il ne faut pas revoir à la baisse le statut des droits et libertés. La conciliation de l'innovation et de la protection est donc nécessaire. Le droit civil continental prend du temps à s'appliquer et se met en place sur un temps long à l'inverse du besoin technique qui nécessite des itérations constantes et systématiques. Cette remarque est aussi valable s'agissant du rapport entre les autorités de régulation et les nouvelles technologies. A cause d'un manque de moyens de suivi et de mise en œuvre, la régulation perd de son influence et de son efficacité. On assiste là à un décalage entre la promesse et la réalité. Il faudrait plus de moyens. Une autre réponse pourra être l'action de groupe, pour peser dans les débats, peut-être plus adaptée au monde numérique. La tendance est également désormais à la certification des personnes, mais on peut imaginer dans le futur la certification des référentiels techniques voire de solutions logicielles.

Il n'en demeure pas moins qu'il faudra continuer à rappeler l'importance de croire en la valeur de la mutualisation des données par plusieurs acteurs lorsque la sécurité est assurée. Le RGPD ne doit pas

servir d'excuse injustifiée pour s'opposer à toute forme de partage et de mutualisation. Il faut continuer à imaginer des alliances et avancer, sans trouver d'excuses pour ne rien faire. Ce sera le sujet de la privacy dans son ensemble qui devra évoluer, et le droit n'a jamais autant été prescripteur de pratiques nouvelles et de promesses d'innovation. Il faut en profiter, et définir des standards d'utilisation pour toutes les données, pour conquérir de nouveaux espaces.

A/ FAIRE CIRCULER LES DONNEES PERSONNELLES

Olivier Dion :
Est le président fondateur de Onecub qu'il a créée en 2011 afin de redonner la maîtrise de leurs données aux individus. Onecub est un outil de portabilité des données personnelles, permettant à ses utilisateurs de faire circuler leurs données tout en gardant le contrôle, et aux entreprises de mettre en oeuvre un droit à la portabilité innovant. Depuis plusieurs années Olivier est un membre actif des communautés Open Data et Self Data en Europe comme aux Etats-Unis.

L'étude sur la portabilité RGPD présentée dans cette partie du document a été réalisée au moyen de plusieurs dizaines d'interviews d'acteurs de l'écosystème de la donnée et de leurs précieuses contributions :

- Grandes entreprises
- Administrations
- Cabinets de conseil
- Experts de la donnée
- Startups
- Associations de protection des données et de Self Data
- Universités
- Cabinets d'avocats spécialisés dans la donnée

Dès l'origine de la construction européenne, la vocation essentielle des traités consistait à organiser et à fluidifier les échanges commerciaux à l'intérieur de l'espace européen. L'économie de la donnée (personnelle) est aujourd'hui une réalité à l'échelle Mondiale, avec le développement d'Internet, des contenus multimédias personnalisés, et des divers objets connectés de notre quotidien.

Néanmoins, la donnée personnelle n'est pas seulement une marchandise, son utilisation et sa circulation non régulées sont susceptibles d'impacter le domaine intime des individus. En outre, **la dynamique des échanges de données repose sur la confiance des utilisateurs.** C'est donc pour arbitrer entre ces enjeux a priori contradictoires, que le régulateur européen a défini les contours d'une utilisation à la fois dynamique des données personnelles, mais également respectueuse de la vie privée des personnes concernées, et sous leur contrôle.

1. Le nouveau droit à la portabilité des données personnelles RGPD [2] :

Qu'est-ce que le droit à la portabilité ?

Le droit à la portabilité consiste pour toute personne physique concernée par le traitement de données, à **pouvoir recevoir ses données collectées par un responsable de traitement,** dans un format structuré et interopérable, **afin de pouvoir les réutiliser pour ses propres finalités ou les transmettre à un autre responsable de traitement,** conformément à l'article 20 du RGPD, et aux lignes directrices du groupe de travail "article 29" (G29)[3] . **Le droit à la portabilité doit favoriser la circulation des données à la demande de l'individu.**

Cependant, le droit à la portabilité ne s'applique pas dans tous les types de traitement de données personnelles. Le considérant 68 du RGPD précise les conditions dans lesquelles le droit à la portabilité s'exerce. Ainsi, **ce droit ne doit pas porter atteinte aux droits et libertés des autres personnes concernées.** Le droit à la portabilité ne doit pas non plus faire obstacle au droit à l'effacement des données de la personne concernée : les responsables de traitement ne pourront valablement s'en prévaloir pour conserver des données personnelles.

En effet, les données ne sont obligatoirement portables que lorsque le traitement est fondé sur le consentement de la personne, ou dans le cadre de l'exécution d'un contrat. De même, seules les données fournies par la personne concernée sont portables. La notion de données "fournies" doit être entendue au sens large. Ainsi, le G29 recommande aussi d'inclure « les données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif » qui sont par exemple des données de localisation, des données comme le rythme cardiaque ou encore l'historique d'utilisation d'un site web. Ainsi, les données fournies sont celles qui « résultent de l'observation du comportement d'une personne, mais excluent les données résultant d'une analyse subséquente de ce comportement »[4] .

Néanmoins, **les données enrichies ou inférées par le responsable de traitement ne sont pas obligatoirement portables,** l'utilisation de celles-ci étant par ailleurs protégées par la réglementation sur la propriété intellectuelle. Les données "anonymisées" ne le seraient pas non plus. Dès lors, les données créées lors d'un processus de recommandation et de personnalisation par catégorisation ou profilage restent en dehors du champ de l'article 20 en ce qu'elles appartiennent au responsable de traitement. Par exemple, les scorings des assureurs, qui permettent d'évaluer les risques d'un assuré potentiel, sont exclus du droit à la portabilité des données.

L'article 20§1 du RGPD exige que les données soient transmises **« dans un format structuré, couramment utilisé et lisible par machine ». Cela implique l'interopérabilité du traitement des données, et la généralisation d'un ou plusieurs formats "standards".** Le Groupe 29 encourage l'adoption de formats ouverts communément utilisés, sans prescrire de formats précis[5]. Comme le relève B. Van Asbroeck « une incertitude demeure quant à la question de savoir si le format en tant que tel doit être interopérable, ou si ceci est une question de bonnes pratiques que les responsables du traitement sont encouragés à adopter »[6]. **En l'absence d'obligation de comptabilité et d'un système d'interopérabilité universel, les opérateurs privés conservent une marge de manœuvre dans la mise en œuvre du droit à la portabilité.**

Les contours du droit à la portabilité :

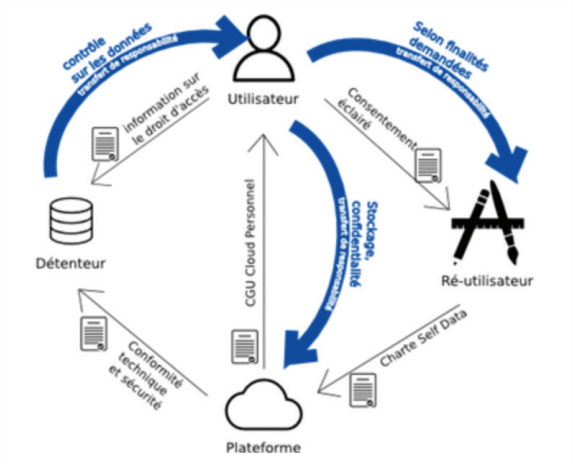
Plusieurs droits découlent du droit à la portabilité. D'abord, ce nouveau droit permet à la personne concernée de recevoir ses données à caractère personnel dans un format qui permette leur réutilisation. Ce droit permet aussi et surtout de transmettre les données à caractère personnel d'un responsable de traitement à un autre opérateur, sans que le premier n'y fasse obstacle. L'article 20 du RGPD indique que ce transfert peut se faire directement, lorsque cela est techniquement possible.

Le droit à la portabilité des données personnelles se veut donc être un outil qui aille dans le sens d'un contrôle croissant des individus sur leurs données personnelles. Cependant, si la standardisation est une condition nécessaire, elle ne semble pas suffisante pour rendre effectif l' « empowerment » de l'individu sur ses droits. En effet, **la portabilité directe d'un responsable de traitement à un autre soulève une interrogation quant au respect du consentement** et aux modalités de son retrait. Si la personne concernée autorise le transfert de ses données d'un responsable de traitement initial vers un autre, quelle sera la garantie que le flux de données s'interrompra automatiquement en cas de retrait de consentement ? La réutilisation des données par le responsable de traitement récipiendaire sera-t-elle conforme à la finalité consentie ?

Une portabilité directe entre responsables de traitement qui ne saurait pas limiter les finalités de réutilisation n'est pas souhaitable, elle diminuerait largement la confiance des utilisateurs qui perdraient rapidement la maîtrise de l'utilisation de leurs données entre tous leurs responsables de traitement et n'offrirait aucun moyen de contrôle efficace.

Pour répondre à un objectif de réutilisation des données portables, dans le respect des droits des individus, ce nouveau paradigme de transfert de données centré sur l'utilisateur **ne pourra se développer que si les utilisateurs ont confiance dans la capacité des responsables de traitement à respecter les conditions de traitements consenties.** Les responsables de traitement doivent donc développer un comportement éthique, être transparents vis-à-vis de ceux qui les ont autorisés à accéder à leurs données.

Ce climat de confiance pourrait être favorisé par le recours à des fournisseurs de système de gestion des informations personnelles (PIMS - Personal Information Management Systems), sur lesquels nous reviendrons au paragraphe A.4, qui offriront aux utilisateurs des outils pour faciliter les transferts et contrôler notamment que les données transférées ne sont pas traitées de manière non autorisée.



Dans son essence même, on constate donc que le droit à la portabilité est éminemment rattaché à la personne concernée : c'est elle qui a le droit de recevoir puis de transmettre ses données. Le droit à la portabilité est donc centré sur l'humain qui contrôle la circulation de ses données.

---

[2] Contribution Aurore Troussel, Justice.cool

[3] Lignes Directrices WP 242, du groupe de travail "article 29" (G29), révisées le 5 avril 2017

[4] 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

[5] Groupe de travail « Article 29 » sur la protection des données Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 5.

[6] « Les obligations de « compliance » des entreprises » Van Asbroeck, B., Debussche, J., in Vers un droit européen de la protection des données, Bruxelles, Éditions Larcier, 2017, p. 89-133

2. Les enjeux et opportunités :

a. Bénéfices généraux :

Quel est l'impact de la portabilité ?

La portabilité peut être interprétée comme une contrainte. En effet, elle a un coût et peut être vue comme un risque. Malgré des perspectives plus que prometteuses[7], le marché manque encore de maturité sur les cas d'usage et les modèles de revenus. **Cependant les bénéfices attendus de la portabilité à court comme à long terme sont gigantesques.**

Dans les faits, deux modèles de portabilité des données coexistent ayant des finalités différentes.

[7] Contribution GS1

a1. Portabilité concurrentielle :

La portabilité concurrentielle recouvre la situation dans laquelle une personne concernée est en mesure de transférer ses données personnelles d'un service à un service concurrent.

A titre d'exemple, la portabilité concurrentielle permet à un utilisateur d'une plateforme de streaming musical de passer vers un autre acteur proposant un service similaire, sans perdre l'historique de ses usages, comme ses playlists musicales (i.e. Spotify vers Deezer).

L'organisation actuelle des acteurs du web enferme de facto les individus, dans un usage captif d'une plateforme spécifique. A titre d'exemple, le partage de photos avec des membres d'une famille ou des amis est devenu le terrain quasi-exclusif de quelques réseaux sociaux. Les sociétés qui souhaitent innover, en créant par exemple un fil d'actualités plus équilibré, n'ont pas l'occasion de le faire, étant donné que la concurrence se joue plutôt au niveau de la collecte des données à caractère personnel qu'au niveau de l'innovation elle-même[8]. Par conséquent, la portabilité des données à caractère personnel peut permettre de changer la donne et de créer une réelle émulation entre les acteurs, notamment au travers de la portabilité concurrentielle. Aussi, **la portabilité concurrentielle permet de fluidifier le marché.**

[8] Contribution UGent

a2. Portabilité complémentaire :

La portabilité complémentaire offre la possibilité aux personnes concernées de transférer des données personnelles d'un service vers un autre acteur proposant un service complémentaire. Cette dynamique implique donc des échanges intra et intersectoriels.

La portabilité complémentaire permettra l'exploration de cas d'utilisation innovants et le développement d'écosystèmes foisonnants. Par exemple, un individu pourra transférer ses playlists de musique vers une plateforme de vente de billets de concerts en ligne (i.e. Spotify vers le site de billetterie concerts de la Fnac).

La portabilité complémentaire peut profondément remodeler le paysage des services en ligne dans le monde entier grâce à la libre circulation des données qu'elle induit, **elle peut être un vecteur majeur d'innovation pour les entreprises.** Une infinité de cas d'utilisation innovants et de bénéfices d'usage peuvent être imaginés et rendus possibles grâce cette portabilité.

La portabilité complémentaire permet aux nouveaux entrants, les startups par exemple, d'avoir accès aux données détenues par les acteurs en place. Elle ouvre le marché. Tout autant que la portabilité concurrentielle, la portabilité complémentaire est donc une affaire de concurrence.

b. Bénéfices généraux :

b1. Enjeux politiques :

La portabilité au service du Digital Single Market :

Le marché unique du digital (ou Digital Single Market) de l'UE **vise à réduire les entraves pour les entreprises et à leur permettre d'exercer davantage leurs activités par-delà les frontières** au sein de l'UE, d'une manière légale, sûre, sécurisée et abordable.

Même si certaines startups peuvent craindre que cette stratégie ne favorise les grands groupes au détriment des petits acteurs, il n'en demeure pas moins que peu de PME de l'UE vendent à l'étranger, à peine 7% : cela pourrait changer en cas d'avènement du marché unique pour les services en ligne, avec la libre circulation des biens, des personnes, des services et des capitaux. L'objectif est globalement de numériser les services publics et les entreprises, favoriser la circulation des mégadonnées (Big Data), stimuler la création et l'utilisation d'objets connectés, etc.

Plusieurs exemples concrets existent :

- **Roaming :** disparition des frais d'itinérance pour les communications depuis l'étranger
- **Portabilité des services :** accès pour les consommateurs qui ont payé pour des services de contenu en ligne dans leur pays d'origine lorsqu'ils se rendent dans un autre pays de l'UE
- **Geoblocking :** interdiction des blocages géographiques injustifiés sur les sites de commerce en ligne

Mais un autre aspect de cette stratégie est le partage d'informations et la libre circulation des données numériques au sein de l'Union européenne. **La libre circulation des données personnelles s'accorde pleinement avec cette approche stratégique.**

Portabilité et émergence de l'IA

On regroupe habituellement sous le terme d'« intelligence artificielle » ou IA un ensemble de notions s'inspirant de la science cognitive, faisant référence à des technologies destinées à assister ou suppléer l'individu dans le traitement des informations massives (Big Data) [9]. **Longtemps, l'intelligence artificielle relevait des films, séries et romans de science-fiction. Aujourd'hui, cette technologie devient partiellement une réalité.**

Le marché de l'intelligence artificielle pour les applications en entreprise est estimé à plus de 36 milliards de dollars d'ici à 2025 contre 643 millions de dollars en 2016, soit une tendance d'augmentation de plus de 52% par an. Cumulé avec le marché du data analytics, il est estimé à 70 milliards de dollars en 2021 selon l'étude de la Banque Américaine Merrill Lynch [10].

L'IA repose sur l'utilisation de nombreuses données, personnelles ou non, comme le rappellent l'avis "Big Data" du CEP, publié en décembre 2016 [11]. Les solutions Smart City, e-Santé, basées sur l'IA, pour ne citer qu'elles, ont besoin d'une grande quantité de données, suffisamment diversifiées pour fonctionner [12].

Ces données sont récoltées, entre autres par les objets connectés (ou IoT). Ces appareils permettent de mieux décrypter certains besoins non formulés par les usagers.

Or, les quantités de données ne semblent pas suffisantes pour développer significativement cette technologie. En effet, en l'absence de confiance, l'individu crée un camouflage numérique où l'idée est de saisir de fausses informations pour bénéficier du service sans être ciblé, ce qui rend les données collectées erronées et non pertinentes, en d'autres termes, inutilisables. Cette attitude est d'autant plus compréhensible que les effets du Big Data sont très difficiles à comprendre pour les individus, et même pour les grandes entreprises.

Au moment de l'adoption du RGPD, plusieurs acteurs économiques, et personnalités politiques européennes ont craint que cette nouvelle régulation n'affaiblisse la dynamique de l'économie numérique européenne et le développement de l'intelligence artificielle, en favorisant davantage les Etats-Unis et la Chine.

D'un autre point de vue, la circulation et l'exploitation des données basées sur le consentement éclairé des individus pourrait fournir, de manière éthique et saine, aux algorithmes d'intelligence artificielle une base de connaissance améliorée des souhaits, habitudes et comportement humains, tout en intégrant les individus à ce développement technologique. **La portabilité pourrait servir un développement éthique de l'intelligence artificielle.**

---

[9] Rapport de Synthèse France IA, "état des lieux de l'intelligence artificielle en France",Page 5

[10] Rapport de Synthèse France IA, "état des lieux de l'intelligence artificielle en France",Page 1 et http://about.bankofamerica.com/assets/davos-2016/PDFs/robotic-revolution.pdf

[11] https://www.cep-pub.org/avis/avis-publicite-et-big-data/

[12] Contribution Médéric Collas

b2. Quelques chiffres :

Il est estimé que 50 milliards d'appareils et d'objets seront connectés à Internet d'ici 2020, dont 28 milliards répondant à la définition des IoT [13]. Or, on sait que les données sont importantes pour l'IoT, ainsi que pour l'IA. Aussi est-il intéressant de corréler le marché disponible pour la portabilité des données avec les explosions du nombre de données et des IoT.

La valeur de l'économie de données de l'UE s'élevait à plus de 285 milliards d'euros en 2015, et continue à croître. Il est même considéré que **la valeur de l'économie européenne des données pourrait atteindre 739 milliards d'euros d'ici 2020**, soit 4% du PIB global de l'UE [14], voire même mille milliards d'euros selon une étude du Boston Consulting Group [15].

Au Royaume-Uni, l'impact de la circulation des données personnelles sur la productivité est estimé à environ 27,8 milliards de livres sterling d'augmentation du PIB. Ce n'est qu'une partie de l'opportunité de valeur. La contribution à l'économie de l'innovation numérique tirée par les opérateurs historiques, les nouveaux entrants, les marchés de pair à pair et les particuliers eux-mêmes sera probablement beaucoup plus importante [16].

Si ces tendances économiques et technologiques témoignent d'un avenir prometteur pour l'économie des données personnelles, celle-ci ne se fera pas sans le concours des consommateurs / clients qui prennent une part de plus en plus importante dans les processus de valorisation [17], dans un contexte où 72 % des internautes européens s'inquiètent toujours de devoir communiquer en ligne trop de données à caractère personnel [18].

Au travers des chiffres exposés ci-dessus, il apparaît que **la portabilité constitue une opportunité unique de créer une réelle arme économique**, à condition que les barrières soient levées.

---

[13] https://lexpansion.lexpress.fr/high-tech/cinq-graphiques-pour-mesurer-le-boom-des-objets-connectes_1794945.html

[14] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

[15] CIGREF, « Economie des données personnelles, les enjeux d'un business éthique », Octobre 2015 Page 8

[16] CtrlShift, rapport p10

[17] CIGREF, « Economie des données personnelles, les enjeux d'un business éthique », Octobre 2015 Page 8

[18] Commission Européenne, « Le marché unique numérique est nécessaire, voici pourquoi »

b3. Opportunité sociale :

Le G29 le rappelle, le droit à la portabilité permet à l'individu de prendre conscience du traitement de ses données, et des enjeux qui en découlent, notamment en terme de valeur économique. Si l'individu est encore trop souvent vu comme un acteur du "digital labor", qui fournit des éléments de sa vie, de ses usages, ou de son profil psychologique, il peut, en mobilisant ce droit, s'émanciper de sa captivité numérique.

Renforcer la liberté de choix du consommateur [19] :

Le droit à la portabilité est novateur en ce qu'il permet à la personne concernée de transmettre les données à caractère personnel d'un responsable de traitement à un autre, sans que le premier n'y fasse obstacle. Il s'agit donc de permettre à la personne de **changer plus facilement de fournisseur de service en empêchant un « verrouillage »** de ses données personnelles [20]. Cette conception du droit à la portabilité va dans le sens de « l'autonomisation de la personne concernée (**« data subject empowerment »**).

La référence à un déséquilibre entre la personne concernée et le responsable de traitement renvoie aux concepts du droit de la consommation. A cet égard, selon le Groupe 29, « En affirmant les droits et le contrôle des particuliers sur les données les concernant, la portabilité des données représente une occasion de mieux «rééquilibrer» la relation entre les personnes concernées et les responsables du traitement » [21] et de **bousculer le monopole**. Dans le même sens, l'ancienne présidente de la Commission Nationale de l'Informatique et des Libertés (CNIL), Isabelle Falque-Pierrotin, estime que l'objet principal de la régulation des données est de réduire l'asymétrie informationnelle entre les utilisateurs et le détenteur de données, en **favorisant la transparence, gage de confiance.**

Ainsi, le **droit à la portabilité constitue un outil juridique, et pratique, afin que les consommateurs acquièrent ou développent leur " empowerment " numérique** [22], autrement dit en favorisant leur autonomie à l'égard d'un acteur spécifique de l'écosystème de la donnée.

Permettre aux individus de gérer leur identité numérique :

Pour le détenteur, que ce soit dans le cadre de la restitution de données, ou le cas échéant de leur(s) réutilisation(s) par les personnes ou d'autres opérateurs, il est nécessaire d'encadrer la mise à disposition des données à la seule personne concernée. Ce qui implique la vérification de l'identité de la personne, dans un contexte dématérialisé. En effet seule la personne concernée doit pouvoir avoir accès aux données. Cela implique donc la mise en place d'un mécanisme robuste de signature électronique, ou la création d'une véritable identité numérique.

Plusieurs projets en cours impliquent qu'un Etat ou qu'une entreprise fournisse à l'individu, devenu citoyen numérique, une véritable identité numérique (i.e. projet France Connect pour l'administration publique française). Certains pays en Europe sont déjà avancés sur ce sujet, on pourra citer par exemple l'Estonie[23]. Du côté des entreprises certaines s'appuient sur **la technologie blockchain pour proposer une identité numérique souveraine indépendante des administrations**, on peut citer le projet de blockchain SOVRIN[24] .

---

[19] Contribution Aurore Troussel, Justice.cool

[20] Groupe de travail « Article 29 » sur la protection des données Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 4.

[21] Groupe de travail « Article 29 » sur la protection des données Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 4.

[22] « Section 6. - Droit à la portabilité des données (art. 20 du RGPD) » Tombal, T., in Le règlement général sur la protection des données (RGPD/RGPD), Bruxelles, Éditions Larcier, 2018, p. 482-523

[23] https://www.france24.com/fr/20181221-afrique-estonie-diplomatie-numerique-nouveaux-amis-benin-kersti-kaljulaid-e-gouvernance

[24] https://sovrin.org/

c. Bénéfices par typologie d'acteur :

c1. Individus :

Depuis l'avènement du RGPD, nous assistons à une préoccupation croissante de la population concernant l'utilisation des données à caractère personnel.

Les individus ne cernent pour autant pas clairement la nouvelle capacité qui leur est proposée et les possibilités qu'offre le nouveau droit à la portabilité des données à caractère personnel. Le droit à la portabilité reste un droit abstrait et sans intérêt pour les individus, dans la mesure où rien de compréhensible et de pratique ne leur est proposé.

Mais que peuvent espérer les individus avec leur nouveau droit à la portabilité ? Pour les individus, que ce soit en tant que consommateurs, usagers ou citoyens, il s'agit de :

- **Simplifier la transmission d'informations d'un service à un autre** sous leur contrôle (en lieu et place de formulaires web ou papier à compléter à chaque demande) ;
- **" Monétiser " la fourniture de leurs données contre un service, un avantage ou une contrepartie financière ;**
- **Maîtriser leur identité numérique ;**
- **Explorer pleinement la valeur d'usage des données**, et en tirer un enseignement, pour leur propre besoin ou une thématique faisant sens (recherche médicale, respect de l'environnement, etc...).

En résumé il s'agit pour les personnes concernées de **récupérer leur « pouvoir d'agir ».**

c2. Grandes entreprises :

Les grandes entreprises peuvent largement bénéficier de la portabilité et de la circulation des données à caractère personnel. Actuellement, chaque entreprise ne peut avoir accès qu'aux données qu'elle crée elle-même. Mais **si demain le contrôle de ces données est remis entre les mains du client, ce dernier peut décider de partager davantage de données avec les entreprises** (y compris des données générées par des concurrents).

Mettre le contrôle des données à caractère personnel entre les mains des individus signifie donc aussi que ces derniers peuvent « dépenser » sélectivement ces données, comme s'il s'agissait d'une monnaie. Les grandes entreprises peuvent alors prendre du recul dans leurs efforts de collecte de données et se concentrer sur des capacités concurrentielles et innovantes plus fructueuses.

Aujourd'hui, ce sont les grandes entreprises, y compris les opérateurs historiques tels que les opérateurs de mobilité (compagnies aériennes, trains, autoroutes et parkings…), les banques et les assureurs, les services publics et les fournisseurs de réseaux Internet et mobiles, **qui collectent le plus grand nombre de données à caractère personnel et pourraient être à l'origine du mouvement pour la portabilité**.

Le RGPD a mis le sujet de la portabilité au cœur du débat pour les grandes entreprises. Néanmoins, elles sont encore peu matures sur le sujet, considéré comme un peu " flou ". **Pour le moment, les grandes entreprises se sont contentées d'une mise en conformité a minima du RGPD concernant la portabilité**, et à cet égard, la portabilité ne semble pas une priorité pour elles.

Mais que peuvent espérer les grandes entreprises avec la portabilité ? Les avantages pour les entreprises sont nombreux :

- Elles pourraient grandement **faciliter l'expérience utilisateur et les démarches de leurs clients** en permettant des imports de données provenant de services tiers pour remplacer les formulaires et imports de documents.
- **Augmenter la connaissance de leurs clients** et ainsi personnaliser les usages en s'appuyant sur des données provenant de services tiers.
- **Améliorer la sécurité** via la simplification de la connaissance du client (ou « Know Your Customer (KYC) ») pouvant engendrer une lutte plus efficace contre l'usurpation d'identité.
- **Proposer de nouveaux modes de gestion des données à leurs clients**, plus transparents et centrés sur l'individu.
- Enfin elles auraient **la possibilité de développer de nouveaux usages et services innovants** en permettant la réutilisation de leurs données vers des services partenaires et complémentaires**.**

c3. Nouveaux entrants :

Dans le climat actuel, où la concurrence est basée sur la collecte de données à caractère personnel, **les entreprises nouvelles et innovantes ne peuvent pas gagner, car elles n'ont pas les données [25].**

Les nouveaux entrants, à savoir les start-up et les petites et moyennes entreprises, semblent donc pouvoir être les principaux bénéficiaires de la portabilité des données à caractère personnel. Les nouveaux entrants aimeraient réellement avoir accès aux données à caractère personnel collectées par les grandes entreprises ou l'administration par le biais de la portabilité.

Les nouveaux entrants ne joueraient alors pas obligatoirement le rôle de disrupteur pour les grandes entreprises, ils pourraient devenir leurs premiers partenaires dans le cadre d'usages de portabilité complémentaire innovants, créant ainsi un écosystème collaboratif autour de la donnée personnelle.

---

[25] Contribution UGent

c4. Administrations :

Même si l'obligation de portabilité des données ne concerne pas celles qui sont issues de la fourniture d'un service public, les opérateurs publics (Etats, établissements publics, collectivités territoriales, regroupement de communes, ...) **ont également intérêt à s'intéresser à ce droit pour faciliter les démarches et mieux anticiper les besoins des administrés.**

Il s'agira notamment de simplifier les démarches administratives des usagers, en remplaçant le système actuel, qui consiste à leur demander de multiples copies « papier » de documents justificatifs ou informations nécessaires au traitement de leur(s) demande(s), par un mécanisme de partage par voie numérique de documents et informations [26].

La portabilité permettra également au citoyen de réutiliser facilement ses données administratives auprès d'opérateurs privés afin de faciliter toutes ses démarches (banque, assurances, immobilier, emploi, etc.).

---

[26] Contribution Thierry Roby

3. Les problématiques à adresser :
a. Education des individus :

La mobilisation du droit à la portabilité reste encore marginale. Pour la startup Fair & Smart, qui propose à ses utilisateurs un outil facilitateur de l'exercice de leurs droits sur les données, **le droit à la portabilité représente moins de 6% de l'ensemble des requêtes de droit formulées par les utilisateurs** [27].

Il est donc nécessaire de **sensibiliser les consommateurs** au sujet de la donnée personnelle. La signification de ce qu'est une donnée personnelle et/ou sensible reste floue pour une majorité d'individus. Pour que ces derniers puissent se saisir de leurs nouveaux droits, il faut d'abord clarifier cette définition pour le non initié [28].

Le business model qui prédominait jusqu'ici (donnée personnelle contre gratuité) était d'une grande simplicité pour l'individu et ne lui demandait aucun effort particulier. Il y a donc un compromis à trouver entre le respect des droits des consommateurs, qui passe par une information potentiellement dense, et la commodité dans l'usage pour leur outil numérique.

Mais cela ne se fera qu'avec la confiance des usagers. Les polémiques et scandales récurrents, concernant des collectes de données à l'insu des personnes, d'atteinte à la confidentialité des données détenues, ont amenés à **une certaine défiance des utilisateurs**.

Le défi sera de leur permettre :

- l'**identification des données traitées** les concernant ;
- la **connaissance des possibilités d'agir sur la collecte** ;
- le **contrôle des traces** ;
- la **maîtrise de leur identité numérique** ;
- la **simplification de la transmission d'informations sous leur contrôle**.

Ces défis seront remplis lorsque l'utilisateur sera en mesure de comprendre et tirer un enseignement des données, pour son besoin propre ou dans le cadre d'une thématique faisant sens. **Pour gagner la bataille de l'adoption, il faut passer par une phase d'acculturation des individus** concernant l'impact de leurs actes et leurs droits, pour développer une conduite éclairée dans l'espace numérique [29].

---

[27] Contribution Fair & Smart

[28] Médéric Collas

[29] Médéric Collas

b. Stratégie des entreprises :

Presque un an après le RGPD, la portabilité est loin d'être une réalité économique ou sociétale, et peu d'entreprises la proposent de manière pratique pour les utilisateurs. En août 2018 la société Onecub avait sollicité 5000 services en ligne parmi les plus prisés par les internautes français pour des demandes de portabilité : **moins de 5% des services avaient répondu favorablement à la demande de portabilité**, la plupart des sollicitations avaient été simplement ignorées et aucun moyen de portabilité pratique ou automatisé n'avait alors été proposé.

b.1.Peur de la désintermédiation :

La démarche de portabilité des données s'inscrit dans une logique d'ouverture (type « open model »). Cette démarche pourrait sembler dangereuse au premier abord pour les entreprises.

En effet le contexte doit bien être re-précisé : **les données concernées constituent un actif informationnel, et même souvent stratégique pour l'entreprise**. C'est pourquoi **les données sont conservées en « silo »,** c'est à dire qu'elles restent enfermées dans le système d'information de l'entreprise et n'en sortent qu'en de très rares occasions, créant des silos disjoints entre les entreprises. D'ailleurs, si comme cela a été évoqué au paragraphe précédent les individus doivent être éduqués, nous rappellerons ici que **les enjeux de l'éducation concernent aussi les métiers de l'entreprise.**

Restituer les données entraînerait une prise de risque, et notamment :

- **Laisser fuiter des trésors cachés** et ignorés dont des concurrents pourraient s'emparer ;
- **Révéler une non-conformité** dans la gouvernance existante des données.

Mais surtout, **l'entreprise craint de s'exposer à une désintermédiation** : en effet, la personne concernée, une fois les données restituées suite à l'exercice du droit à la portabilité, pourrait décider de changer d'opérateur, ou de traiter elle-même ses données et n'avoir plus recours aux services de l'entreprise.

Aussi la restitution des données devra-t-elle être questionnée :

- S'agira-t-il d'une démarche proactive, pour développer des services innovants ou un nouveau mode relationnel ?
- Le détenteur est-il bousculé par un nouvel intermédiaire ou concurrent ?
- Le détenteur entend-il collaborer avec un acteur tiers (plateforme ou service) ?

Plus précisément, ces questions impliquent une interrogation plus profonde sur le sens même de la désintermédiation :

- Quels sont les motivations et les stratégies recherchées ? Il peut s'agir de construire un nouvel écosystème, suivre une tendance, renforcer une image;
- Quel est le contenu à ouvrir et à quelle fin ? ;
- Quelles actions seront permises sur le contenu ? Une multitude peut être envisagée, telle la consultation, la modification, la réutilisation, la diffusion, la monétisation.
- Quels seront les modalités et mécanismes ? les outils, la gouvernance, l'authentification, les formats de diffusions, qu'ils soient lisibles et interopérables à la fois ;
- Quelle chronologie d'ouverture ? La diffusion peut être réalisée à court terme, comme à plus long terme.

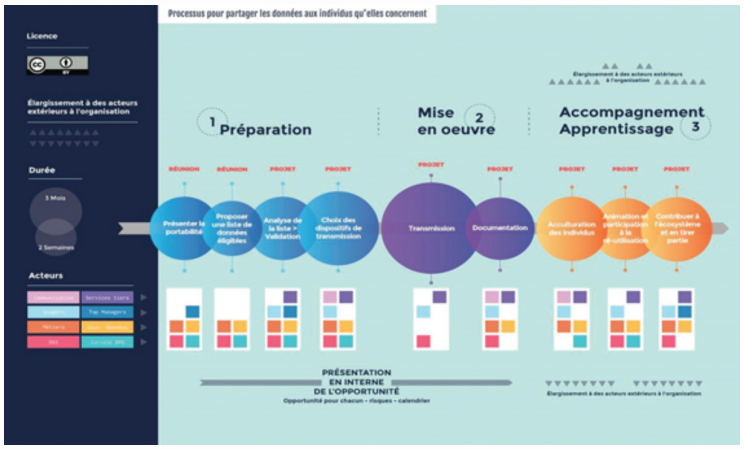
On comprend donc que **l'entreprise peut tout à fait décider de conserver ses données précieusement, au risque de les garder non utilisées, tout comme elle peut décider de les exploiter avec le consentement de l'individu et de les laisser circuler**. Dans ce dernier cas, elle devra s'interroger sur tous les aspects évoqués ci-dessus pour être en mesure de ne plus craindre la désintermédiation. **Plutôt que de penser en silo elle pourra réfléchir à des stratégies d'alliances** avec des services pouvant lui fournir des données et des services pouvant exploiter des données qu'elle collecte et transforme.

L'entreprise est face à un dilemme mais elle doit comprendre que sa crainte n'est pas nécessairement justifiée, et qu'elle peut également tirer pleinement parti de cette nouvelle opportunité. **Ne pas s'ouvrir si les autres s'ouvrent signifie également prendre le risque d'être désintermédié.**

b.2.Faiblesse des preuves de marché :

Après quelques mois d'application du RGPD, les acteurs de l'écosystème se rendent compte que **la portabilité n'est pas encore généralisée**, et que **la faiblesse des preuves de marché commence à peser sur le marché** : les cas d'utilisation commerciale sont difficiles à imaginer pour les entreprises, en particulier pour les opérateurs historiques, car ils ont rarement eu à l'imaginer auparavant. En conséquence, ils ne proposent **pas de cas d'utilisation réels à leurs utilisateurs, qui n'en comprennent pas les avantages en retour**. Le nouveau droit à la portabilité est encore abstrait tant pour les individus que pour les organisations, à l'exception de quelques startups et autres acteurs précurseurs que nous détaillerons plus loin dans ce document.

Cette perception d'inutilité par les individus se corrèle au fait que les organisations détentrices de données ont souvent également comme inquiétudes la complexité, le coût et le temps qu'un projet d'ampleur sur la portabilité implique. La Fing et ses partenaires, en se basant sur l'expérience terrain du pilote MesInfos, ont établi la description des étapes types d'un projet de portabilité, exposé ci-dessous[30].



Pourtant la partie n'est pas perdue, car si à ce jour les POC (Proof of Concept) ne sont pas totalement concluants, il ne faut pas oublier que :

- Le droit à la portabilité tel que compris aujourd'hui est un **droit récent qui ne demande qu'à se construire,** il faut donc laisser le temps au temps sur ce point ;
- **Certains investissements ont été réalisés par des acteurs, mais le retour sur investissement n'est pas encore prouvé.**

Dans ce dernier cas, **il est probable qu'une démonstration de la viabilité de modèles économiques aboutisse à un déblocage potentiellement brutal, mais tout à faire libératoire**, des opportunités. Autrement dit, le marché est actuellement en pleine zone de défrichage : les premiers succès sont en attente, et le marché devrait se structurer et offrir plus de garanties par la suite.

[30] Fing, Cahier #4, « la portabilité des données en pratique »

c.Business model :

La monétisation de l'usage des données est un choix complexe de modèle de revenus conforme, éthique et viable. La valeur des données résulte bien souvent du croisement des données et des services qui en découlent. Il s'agit ici d'établir un plan pour le succès de la portabilité, en identifiant un modèle de revenus viable, une clientèle cible, ainsi que les produits et détails du financement[31]. En d'autres termes, comment **permettre une pérennisation d'un modèle économique de développement.**

La circulation des données, et la production de valeur, dépend de la confiance des utilisateurs. L'enjeu consiste à déterminer **un compromis entre un modèle économique viable pour les acteurs de l'écosystème, et une démarche transparente et éthique à l'égard des individus.** Sachant que le droit à la portabilité doit, par principe, rester gratuit pour l'individu. Seuls les nouveaux services seront payés par l'utilisateur, mais en aucun cas la portabilité au sens strict du terme. Il ne s'agit alors pas de réaliser une utilisation en dehors du contrôle des personnes concernées, mais bien d'**une utilisation conduite avec le consentement, et la confiance, de l'utilisateur.**

Le marché étant considéré comme étant « multifaces », impliquant l'interdépendance des opérateurs, nous retiendrons que les acteurs suivants interviennent dans le cadre de la portabilité :

- **Les individus :** qui souhaitent disposer de nombreux services et d'usages simples et personnalisés, ils doivent donc fournir de la donnée ;
- **Les fournisseurs de services (détenteurs ou réutilisateurs)** : qui ont tout intérêt à avoir le plus de clients possible, ils doivent donc proposer des services et générer des interactions ;

On parle également de réseaux croisés[32].

Plusieurs modèles de revenus sont possibles :

c.1.Monétisation B2B user-centric :

Lors d'un transfert de données directe, pour une finalité précise, entre un service détenteur et un service réutilisateur, **le service détenteur est celui qui a réalisé un investissement pour collecter ou produire la donnée. Le service réutilisateur lui n'a pas eu à réaliser cet investissement,** la donnée lui ayant été directement transmise à la demande de l'utilisateur.

Dans de nombreux cas d'usage, grâce aux données du détenteur, le réutilisateur va pouvoir :

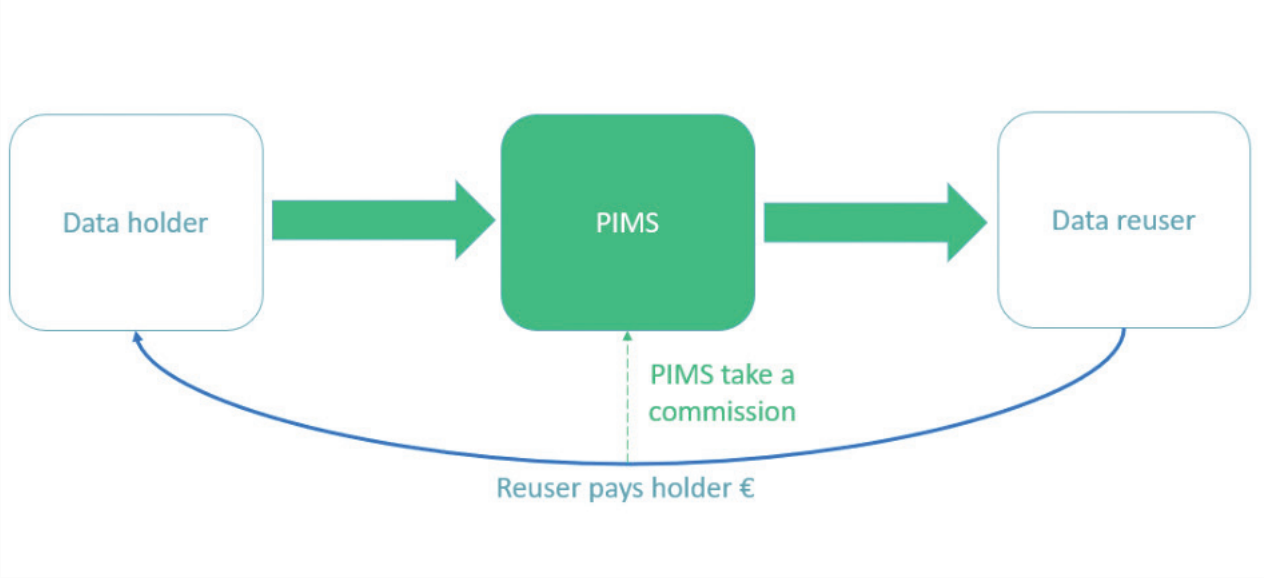
- **soit simplifier son service et son expérience utilisateur** grâce aux données du détenteur (exemple : éliminer un formulaire et le remplacer par un import),
- soit **réaliser une plus-value en proposant un service basé sur la donnée** du détenteur (exemple : le site de vente de concerts se basant sur une playlist provenant de Spotify).

Dans ce cas **il paraît naturel que le détenteur initial puisse être rémunéré pour avoir fourni de la valeur au réutilisateur**. En particulier s'il s'agit d'un transfert de données répétitif (exemple : Spotify qui transmettrait chaque nouvelle chanson écoutée au site de vente de concerts).

Il ne s'agit pas ici de revente cachée de données personnelles entre partenaires, le transfert ayant été activé (gratuitement) par le consentement éclairé de l'utilisateur. **Un tel modèle de revenu doit présenter une transparence exemplaire pour être accepté par l'utilisateur**.

Si le transfert est géré par un PIMS :

- le PIMS peut faciliter les paiements entre le détenteur et le réutilisateur puis se rémunérer par une commission
- Il peut aussi facturer les consentements pour la réutilisation (Consent as a Service).



[31] CtrlShift (full) p201

[32] MesInfos p92

c.2.Business model B2C :

Cette valorisation passe par le biais de nouveaux services qui peuvent directement être facturés, et donc de nouveaux marchés à destination et au bénéfice du consommateur[33]. Ce dernier bénéficiera de services et le prestataire de services pourra lui tirer différents avantages :

- Bénéfices indirects en termes de confiance ou de fidélité pour la marque (si le prestataire est la marque) ;
- Bénéfice direct lors de la vente du produit.

Un PIMS qui permettrait la gestion des données pour l'utilisateur pourrait facturer des services additionnels (modèle freemium) à l'utilisateur. Par exemple, si le PIMS stocke les données de l'utilisateur il pourra facturer un espace de stockage additionnel.

[33] MesInfos p106 et CtrlShift p38

c.3.Monétisation des données par l'individu :

Les données sont aujourd'hui, à tort ou à raison, parfois appelées le "nouvel or noir". A tort pour certains auteurs[34], la donnée n'étant pas un bien consomptible mais un bien reproductible à l'infini. Cette image reste pertinente en ce que le pétrole et **les données ont de la valeur**[35]. A titre d'exemple, le marché de la publicité en ligne représentait en 2017 plus de 48 milliards d'euros (source : IAB Europe)[36], l'objectif étant soit de cibler les individus soit de suivre l'évolution des comportements.

On comprend donc que l'accès à ces données personnelles est stratégique car il permet de créer de la valeur. Les données font aujourd'hui clairement l'objet d'un marché évolutif, mais il reste toutefois difficile de quantifier la valeur propre des données d'un individu (d'un état brut à des données exploitées et valorisées). Valent-elles des centimes ou des centaines d'euros ? Tout au plus, sait-on que Facebook considère que l'accès à des données personnelles vaut $20 par mois, en tout cas dans le cadre de son projet Atlas.

La monétisation des données est un sujet sensible, qui oppose la personne concernée, qui a fourni les données, et les acteurs de l'écosystème, qui les exploitent pour leurs intérêts légitimes.

Le refus de la patrimonialisation :

Les auteurs défendant cette thèse rejettent la notion de propriété des données :

- soit pour des raisons de droit (une donnée est un droit attaché à la personne humaine, et pas une propriété) et la loi de nombreux pays (dont la France) pose le principe d'indisponibilité du corps humain (la vente d'organe est interdite) ;
- soit pour des raisons liées à la nature des données numériques (possibilité de copie, modalités de production).

La monétisation consentie par l'individu :

Les partisans de cette thèse soutiennent que les individus sont propriétaires de leurs données et doivent pouvoir les vendre comme ils l'entendent (Gaspar Koenig, « Mes data sont à moi » ; Eric Posner, « Radical Markets »). Il faudrait alors reprendre le contrôle des données qui sont aujourd'hui monétisées en notre nom et que l'utilisateur passif devienne un consommateur actif[38].

Quelles pistes pour une rémunération ou valorisation des données de l'individu ?

Aujourd'hui, les modèles existant sont :

- Soit axés sur la privacy et nécessitent des investissements qui peuvent être coûteux, bien que les données personnelles soient protégées et non exploitées ;
- Soit gratuits mais basant leur modèle économique sur l'exploitation des données recueillies (GAFAM), sans que l'usage qui en est fait soit réellement connu. Cette gratuité est aujourd'hui un frein pour les approches protectrices des données car elle a abouti à une normalisation de l'offre gratuite[39].

Aussi un modèle de valorisation des données personnelles par le particulier lui-même permettrait de proposer une alternative raisonnable qui se situerait entre les deux modèles exposés ci-dessus. Ce modèle permettrait de donner une valeur commerciale juste au service de protection, et serait basée sur le libre arbitre éclairé des citoyens[40].

HUBERT LE LIEPVRE :

Hubert Le Liepvre est le fondateur de Ze Profile, une application mobile qui donne le pouvoir au consommateur en lui permettant d'obtenir des promotions, à la demande, en échange de données personnelles. Hubert a auparavant développé plusieurs activités sur les marchés de capitaux.

ERIC ZEYL :

Eric Zeyl est le fondateur de My Data is Rich, le premier tiers de confiance en matière de collecte, gestion et valorisation des données personnelles : rendre les particuliers acteurs et bénéficiaires de l'exploitation de leurs données, tout en protégeant leur anonymat et leur vie privée.

[34] Ruben Verborgh

[35] Ruben Verborgh & E Zeyl / MyDataIsRich

[36] Hubert le Liepvre / Ze Profile

[37] Hubert le Liepvre / Ze Profile

[38] Ruben Verborgh

[39] E Zeyl / MyDataIsRich

[40] E Zeyl / MyDataIsRich

d.Les problématiques juridiques :

La plupart des entreprises craignent une circulation des données non encadrée, et aimeraient préciser les conditions d'utilisation des données ainsi "portées", notamment à l'égard d"autres acteurs de l'écosystème, afin de **se protéger en termes de responsabilités.**

D'une manière générale, **le droit à la portabilité pose un défi juridique**, qui appelle probablement à un compromis entre d'une part les droits légitimes du responsable de traitement détenteur initial des données, les opérateurs « concurrents » du secteur ou de secteurs intéressés par le traitement des données concernées, et d'autre part les droits et attentes des personnes concernées, en tant que citoyens, usagers, consommateurs ou patients.

Ces questions pourront être encadrées par des licences d'utilisation des données personnelles, qui auront vocation à déterminer le modèle de revenus et la répartition du coût de fonctionnement de l'ensemble[41], afin que la " privacy " ne soit pas exclusivement réservée aux individus ayant les moyens de payer pour cela.

Les opérateurs « concurrents », ou de secteurs complémentaires (intéressés par le traitement des données en « seconde main ») devront ne collecter que les données strictement nécessaires à leur besoin. Il faudra donc convenir d'un standard, avec vraisemblablement la mise en œuvre de métadonnées juridiques, afin de « filtrer » la collecte des données et de protéger les différents acteurs de la chaîne. **Un " framework juridique pour la circulation des données " est encore à construire pour rassurer l'ensemble des acteurs et préciser la chaîne des responsabilités.**

Le rôle, et les droits et obligations, des opérateurs de plateforme de gestion des données personnelles (les PIMS), devront être précisés, dans le cadre d'une charte de bonne conduite, ou autre instrument juridique et engageant pour l'opérateur adhérent. Quel est le rôle de l'opérateur, à l'égard de la personne concernée (utilisateur), du détenteur des données (responsable de traitement), ou des opérateurs tiers intéressés à pouvoir réutiliser ces données ? Qui est responsable du transfert des données, par ce biais, de responsable de traitement (détenteur) à un autre responsable de traitement ? Est-ce que l'opérateur récupère les données de la personne ? Ces données font elles par ailleurs l'objet d'un traitement spécifique par l'opérateur du PIMS ? L'utilisateur peut-il réutiliser ses données, et les croiser avec d'autres données …. etc ?

Enfin **il faudra reconnaître un droit suffisamment large de réutilisation des données**, par l'utilisateur ou une communauté d'utilisateur. Pour cela **les utilisateurs, ou des associations représentant l'intérêt commun des utilisateurs, auront vocation à être partie prenante au cadre de la gouvernance de ces sujets**. Là encore, il faudra définir le juste niveau de gouvernance. A noter que le RGPD prévoit à l'article 80, la possibilité d'une représentation des personnes concernées.

Plus spécifiquement **le droit à la portabilité amène à s'interroger sur l'adaptation des moyens de protection des intérêts économiques, « légitimes », des responsables de traitement (sa propriété intellectuelle et industrielle), à concilier avec le droit des personnes à profiter des avantages du traitement de leurs données (droit de réutilisation).**

Adapter les moyens de protection de la propriété intellectuelle et industrielle :

Le responsable de traitement, en particulier les fabricants d'objets connectés ou éditeurs d'applications mobiles, aura investi des moyens importants en recherche et développement, et voudra légitimement **protéger ses « secrets industriels ».** L'application du droit à la portabilité ne doit pas permettre à des concurrents de « décortiquer » un processus technologique sous-jacent (rétro-ingénierie). Quid des métadonnées dans le cas des données relevées directement par un capteur ou appareil connecté ?

Des exemples sont indiqués dans les lignes directrices établies par le G29 (reprises par le Comité Européen de la Protection des Données), concernant les catégories de données pour lesquelles le droit à la portabilité s'applique, et a contrario celles non concernées par ce droit. Il faudra probablement que les responsables de traitement se questionnent en amont, sur le format et l'organisation des données, afin que ces données ne puissent révéler indirectement le procédé technologique développé et exploité.

---

[41] Hubert le Liepvre / Ze Profile

e.Les problématiques médiatiques :

Nous l'avons déjà évoqué plusieurs fois, **le développement de la portabilité des données personnelles repose sur la confiance des utilisateurs**. Pour cela, il est impératif d'établir un cadre d'utilisation organisé et régulé par les acteurs de l'écosystème (responsable de traitement, co-traitant, sous-traitants ...), conduit avec la plus grande transparence.

En effet, **cette confiance peut être altérée, voir anéantie, à l'occasion d'un scandale** en matière de données à caractère personnel.

L'exemple le plus parlant et le plus récent concerne l'affaire « Cambridge Analytica ».

Cambridge Analytica est une société de publication stratégique combinant des outils d'exploration et d'analyse des données. En croisant des données qualitatives et quantitatives, la société est en mesure d'identifier et prédire les réactions psychologiques des individus dans le but de leur adresser des messages qui feront changer leur comportement. Cette technique s'appelle le micro-ciblage (i.e. micro-targeting). La société Facebook a longtemps autorisé, sans réserves ni contrôles, à des entreprises tierces d'exploiter largement les données des utilisateurs Facebook via une API.

Ainsi, le Dr Aleksandr Kogan a eu accès aux données personnelles de plusieurs dizaines de millions de personnes dans le monde, au moyen d'une API développée par lui-même, et a été en mesure de réutiliser ces données. Cela lui a permis de générer des profils de personnalité de ces utilisateurs concernant leurs opinions politiques, sans qu'aucune alerte ne semble se déclencher au niveau de facebook, sans que ces derniers n'aient été informés que de telles informations étaient collectées et sans que leurs consentements n'aient été requis pour cette finalité.

Facebook n'a pris conscience de l'utilisation de l'application tierce en contravention avec sa politique de plateforme qu'en décembre 2015. Après investigations par l'autorité de contrôle britannique (l'ICO), Facebook s'est vu infliger une amende à hauteur de 500.000 £. Depuis cet incident, Facebook a mis en place une politique de contrôle beaucoup plus restrictive en ce qui concerne le transfert de données à caractère personnel.

Une tel événement a un impact très négatif en matière de circulation de données.

Depuis Cambridge Analytica les entreprises, qui n'étaient déjà pas très ouvertes sur la question de la circulation des données, craignent qu'en cas de problème lié à un transfert de données vers d'autres entités, la responsabilité ne leur soit imputée.

A ce stade, deux possibilités existent :

- **Soit chaque entreprise met en place des politiques contraignantes et coûteuses en matière de contrôle des services destinataires** des données à caractère personnel, ce qui impactera lourdement le droit à la portabilité et la circulation des données avec un coût prohibitif ;
- **Soit l'écosystème dans son ensemble organise un cadre applicable à tous les acteurs, concernant la circulation des données**, en précisant le rôle, les responsabilités et les pratiques admises. Dans cette hypothèse, l'acteur qui ne respecterait pas ce cadre, serait considéré comme peu fiable et devrait pouvoir être reconnu comme tel par l'ensemble de la communauté.

La confiance entre les responsables de traitement devrait être envisagée comme une question de gouvernance globale, plus que comme un problème spécifique à une entreprise. Dans le cas contraire seuls les acteurs aux moyens conséquents pourront se permettre de faire circuler leurs données.

f.Une réglementation adaptative :

Le bon fonctionnement des marchés exige une réglementation et une législation solides. Pour suivre le rythme de l'évolution d'un marché connaissant une évolution rapide, comme celui de la portabilité des données à caractère personnel, les régulateurs et les gouvernements ont besoin de niveaux de connaissances, de compétences et d'adaptabilité élevés afin d'assurer le succès du développement du marché au même rythme[42].

Sans une réglementation adaptative, il est difficile de garantir la sécurité des individus et de leur permettre d'accéder aux avantages qui leur sont offerts par la portabilité. La réglementation adaptative, en parallèle du développement des infrastructures, garantit le fait que l'environnement législatif et réglementaire reflète le rythme et l'orientation du marché. **La réglementation adaptative permet d'assurer un équilibre dynamique entre croissance et sécurité[43].**

Grâce à une approche collaborative, la réglementation adaptative développe également la confiance des entreprises à l'appui de l'innovation et, pour les particuliers, une mauvaise utilisation sera évitée. Vu l'évolution rapide du marché des données à caractère personnel, une approche traditionnelle de la réglementation pourrait être un obstacle et limiter le potentiel du marché des données à caractère personnel.

Dans le cadre de son projet britannique, CTRL-Shift propose quelques recommandations en matière de réglementation adaptative à savoir[44] :

- **Création d'une structure pour permettre l'élaboration d'une réglementation itérative et adaptative** qui permettra aux organismes gouvernementaux de réagir rapidement aux nouvelles possibilités et aux nouveaux défis du marché ;
- **Collaboration étroite entre les gouvernements, les innovateurs et les organismes de réglementation,** au moyen d'ateliers de détermination de la portée en tant qu'outil d'élaboration des politiques.

Pour CTRL-Shift, en l'absence d'une réglementation adaptative, **la réglementation risque d'être mal conçue et/ou inadaptée aux opportunités et aux risques**, ce qui ralentit considérablement le développement de l'opportunité de marché. Cela peut créer des contraintes sur la valeur du marché qui, à leur tour, peuvent limiter l'investissement[45].

La création d'une réglementation adaptative exige une concentration, des investissements et des changements importants de la part des gouvernements et des organismes de réglementation. Cette question a fait l'objet de nombreuses discussions de la part des gouvernements et des entreprises, et **de nombreuses entreprises réclament désormais clairement ce changement[46].**

[42] CTRL-Shift, Unleashing the power of trust, Department for Digital, Culture, Media & Sport, 2018, p.5

[43] CTRL-Shift, Unleashing the power of trust, Department for Digital, Culture, Media & Sport, 2018, p.16

[44] CTRL-Shift, Unleashing the power of trust, Department for Digital, Culture, Media & Sport, 2018, p.104

[45] CTRL-Shift, Unleashing the power of trust, Department for Digital, Culture, Media & Sport, 2018, p.53

[46] CTRL-Shift, Unleashing the power of trust, Department for Digital, Culture, Media & Sport, 2018, p.53

g.Enjeux techniques :

g.1.L'architecture des données :

Modèle de « restitution directe à l'utilisateur » :

La plupart du temps les données sont "portées" dans **une archive brute sous la forme d'un tableur Excel / CSV** ou de plusieurs tableaux dans une archive .zip que l'individu récupère directement sur sa machine. **Les données transférées ne sont pas forcément les données que l'utilisateur souhaite réutiliser**, il s'agit simplement de l'ensemble des donnée portables du point de vue de l'article 20. Aussi les responsables de traitement ayant jusqu'à 30 jours pour envoyer les données demandées, ce procédé n'est jamais temps réel.

Un tel modèle de portabilité, pourtant répandu et vu comme conforme aujourd'hui, pose plusieurs problèmes de taille :

- **La sécurité des données peut difficilement être assurée** ;
- **La minimisation des données n'est pas respectée**, l'utilisateur souhaite rarement récupérer l'ensemble de ses données mais juste une partie ;
- **L'expérience utilisateur est médiocre** elle ne permet à aucun moment de construire des cas d'usage innovants à partir de la portabilité et pourrait presque être considérée comme un "obstacle à la portabilité".

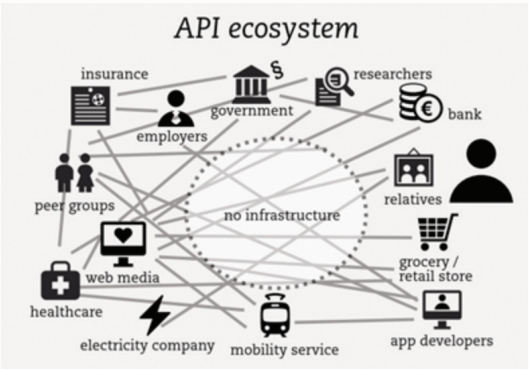
Un tel modèle, très "artisanal" ne peut prospérer. Il est donc déterminant de travailler aussi l'encadrement technique par des API fonctionnelles, qui respectent l'esprit du texte et les exigences de sécurité.

Modèle API B2B[47] :

L'économie de l'API est déjà en train de développer un écosystème de services en expansion organique permettant l'échange de données personnelles sur des connexions point à point.

Cependant, **les entreprises ont du mal à gérer leurs intégrations d'API**, **tandis que les individus sont perdus en raison de la difficulté à bénéficier d'une vue d'ensemble de leurs flux de données personnelles** entre services.

À long terme, une certaine restructuration systémique sera nécessaire. L'économie actuelle de l'API peut être considérée comme une étape d'incubation pour la prochaine économie des données. Cependant, nous aurons également besoin d'une infrastructure plus robuste en plus des simples API.



48

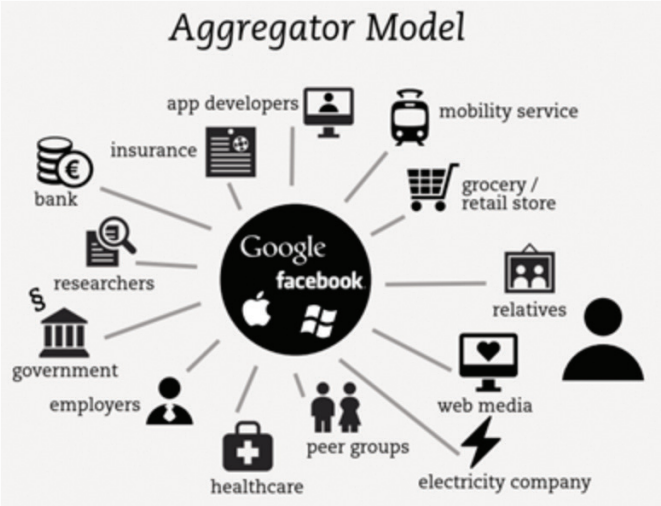
Modèle des agrégateurs de données[49] :

Dans l'état actuel des choses, **des agrégateurs de données personnelles apparaissent dans des secteurs spécifique**s, tels que Validic et Human API pour la santé, en plus des centrales de données bien établies que sont les GAFAM qui rationalisent le flux et l'interopérabilité des données personnelles au sein de leurs propres écosystèmes. Le modèle « d'agrégation » de données évolue naturellement en dehors de l'économie de l'API, mais il présente deux inconvénients fondamentaux.

Premièrement, **le manque d'interopérabilité entre les agrégateurs** de données signifie que les particuliers et les entreprises s'enferment dans des fournisseurs de services de données spécifiques et que le marché des données est fragmenté d'une manière qui **étouffe l'innovation et la concurrence, et incommode les individus.**

Deuxièmement, **les agrégateurs de données actuels ne reconnaissent pas toujours le respect de la vie privée comme fondamental** et ne s'engagent pas de manière transparente sur le sujet.

Plusieurs initiatives visent à créer un modèle plus ouvert et plus respectueux de la vie privée (telles que Qiy, The Good Data, Respect Network), mais en l'absence d'une infrastructure commune, elles souffrent également d'un manque d'interopérabilité.



50

Modèle des PIMS avec « API centrée utilisateur »[51] :

Le modèle « API centré utilisateur », notamment développé dans le projet MyData (dont nous reparlerons dans la partie D de ce document), **est une nouvelle approche**, un changement de paradigme dans la gestion et le traitement des données personnelles qui vise à transformer le système actuel centré sur l'organisation en **un système centré sur l'humain** mais également un modèle considérant les données personnelles comme une ressource à laquelle personne d'autre que l'utilisateur ne peut contrôler.

L'objectif est de **fournir aux individus les moyens pratiques d'accéder à leurs données personnelles, de pouvoir les récupérer et ainsi les utiliser (des PIMS - Personal Information Management Systems)**.

Il s'agira des données sur l'historique des achats, les déplacements, les télécommunications, les dossiers médicaux, la gestion bancaire et financière, l'historique de navigation Internet, etc.

Nous détaillerons ce modèle, centré utilisateur et basé sur les PIMS, dans le paragraphe A.4 de ce document.

[52]

[47] MyData - A Nordic Model for human-centered personal data management and processing, Finnish Ministry of Transport and Communications, September 2014

[48] Source : MyData – A Nordic Model for human-centered personal data management and processing, Antti Poikola, Kai Kuikkaniemi & Harri Honko, Septembre 2014

[49] MyData - A Nordic Model for human-centered personal data management and processing, Finnish Ministry of Transport and Communications, September 2014

[50] Source : MyData – A Nordic Model for human-centered personal data management and processing, Antti Poikola, Kai Kuikkaniemi & Harri Honko, Septembre 2014

[51] MyData - A Nordic Model for human-centered personal data management and processing, Finnish Ministry of Transport and Communications, September 2014

[52] Source : MyData – A Nordic Model for human-centered personal data management and processing, Antti Poikola, Kai Kuikkaniemi & Harri Honko, Septembre 2014

g.2.Interopérabilité technique :

Formats :

Le RGPD indique que des processus organisationnels et techniques doivent être mis en place pour que le RGPD puisse atteindre efficacement ses objectifs, tels que la portabilité des données.

Dans le même temps, **la nouvelle réglementation européenne reste neutre en ce qui concerne la technologie et ne mentionne aucun format ou norme spécifique**. Par conséquent, une étude allemande menée par la Stiftung Datenschutz (fondation pour la protection des données allemande) a examiné comment l'exigence légale d'un « format structuré, couramment utilisé et interopérable » peut être remplie en pratique.

L'étude allemande a conclu que l'exigence minimale en matière de portabilité et d'interopérabilité des données devrait être **l'utilisation du format « CSV »**. A cela s'ajoute une simple description de la manière dont les données sont organisées dans le document.

Pour des solutions plus complexes, les formats « XML » ou « JSON » doivent être utilisés. Ces formats permettent des niveaux de granularité plus fins, contiennent des données sur le contenu ainsi que des métadonnées descriptives et, grâce à leur structure, ont une profondeur suffisante, leur permettant même de représenter des structures de données complexes.

L'information contenue dans ces documents n'est pas seulement lisible par machine mais peut également être lu par les personnes concernées elles-mêmes en ayant recours à un logiciel standard, qui permet en même temps à l'utilisateur d'exercer son droit d'accès à l'information.

En ce qui concerne la réutilisation efficace des données transférées, **le format « PDF » ne devrait pas être utilisé** comme un standard dans le domaine de la portabilité des données, et ce, même s'il s'agit d'un format électronique efficace dans le cadre du droit d'accès en ce qui concerne la transparence de l'information[53].

Aucun vocabulaire, ni aucune ontologie standard n'est mentionnée par le règlement, c'est au marché de définir ses références.

Protocoles de transfert données :

La portabilité des données personnelles doit être conforme à la portabilité syntaxique, sémantique et politique des données, conformément à la NORME ISO/CEI 19941:2017.

Étant donné que le champ d'application englobe tous les processeurs de données et que les systèmes existants utilisent une grande variété de formats et d'interfaces, la normalisation doit être en place **pour permettre le transfert des données, sans demander de changements majeurs à l'un ou l'autre des responsables de traitement.**

L'évolutivité et l'interopérabilité peuvent être obtenues en tirant parti des plates-formes d'intégration

hybrides entre les systèmes d'émission et de réception (au travers d'un PIMS par exemple), en assurant un **découplage complet entre ces systèmes et une conversion appropriée vers et à partir du format standard défini** pour la portabilité des données personnelles.

La plateforme intermédiaire d'intégration hybride appliquera les dispositions de l'article 20 du RGPD et facilitera l'échange de données à caractère personnel entre systèmes hétérogènes **sans nécessiter de mises à jour coûteuses des applications d'envoi et de réception et sans conserver aucune copie des données transférées** après leur transmission réussie au système récepteur.

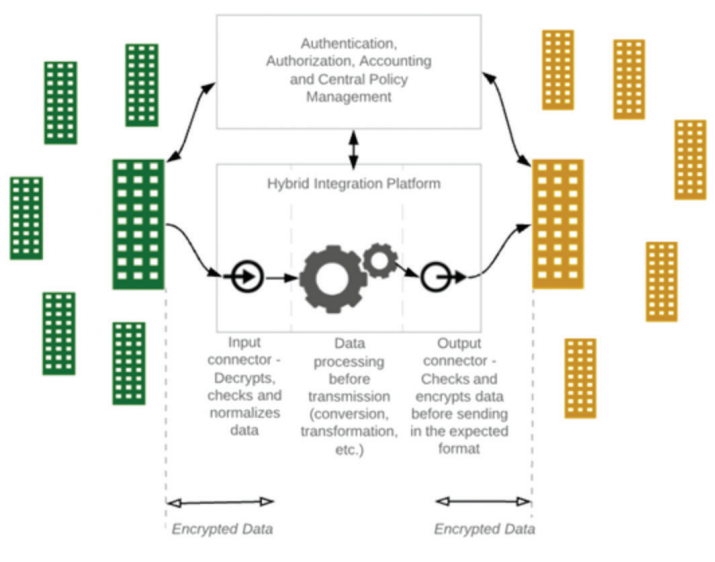
Ses composantes de base fonctionneraient en trois (3) grandes étapes, comme suit :

- **Connecteur d'entrée** : Connexion au système émetteur, chargé du décryptage, du contrôle et de la normalisation des données dans le standard défini ;
- **Système de traitement interne** : Réalisation de toutes les conversions et transformations nécessaires aux données avant qu'elles ne soient transmises au système récepteur par le connecteur de sortie ;
- **Connecteur de sortie** : Vérification, chiffrage et transmission des données transférées au système récepteur dans le format qu'il prend en charge.

Des connecteurs standard et/ou open source peuvent être développés et entretenus pour prendre en charge des systèmes largement utilisés. Les systèmes à petite échelle peuvent tirer profit de la normalisation de l'interface et du format des données pour **réduire au minimum les coûts de mise en œuvre.**

L'approche en trois étapes de la plateforme d'intégration hybride serait définie par le biais de « contrats», fonctionnant à chaque étape. Le contrat définit les règles selon lesquelles les données sont ingérées, transformées et/ou livrées et comment ce traitement est réellement effectué. Ces contrats permettront le transfert de données à caractère personnel en streaming ou de manière asynchrone en fonction de l'occurrence d'un événement ou d'une condition.

C'est cette approche événementielle qui, à son tour, offre une plus grande flexibilité en permettant à des systèmes hétérogènes d'échanger de manière transparente des données personnelles spécifiques.



JACOPO TENCONI :

Jacopo Tenconi est directeur commercial & responsable des alliances chez Primeur, une société Suisse, née en Italie, avec 30 ans d'expérience dans l'intégration de données, en particulier dans le domaine de la finance.Jacopo a auparavant travaillé avec ABB et Siemens en Europe et en Asie.

[53] Praktische Umsetzung des Rechts auf Datenübertragbarkeit, Stiftung Datenschutz

g.3 Consentement :

La portabilité est un droit activé par l'individu lui-même auprès de ses fournisseurs de service. Cependant, les transferts de données qui en découlent, qu'ils soient directs entre services ou qu'ils s'effectuent via ou vers des outils PIMS, doivent offrir le plus grand contrôle possible à l'utilisateur sur la circulation de ses données. **Sans contrôle sur les flux de données et les finalités de réutilisation, la portabilité n'offrira pas la confiance nécessaire à une généralisation de la pratique.**

Pour ce faire **nous recommandons de baser la circulation des données sur la notion de consentement du RGPD.**

L'approche décentralisée de la blockchain paraît très prometteuse quant à la gestion du consentement par l'ensemble des acteurs de l'écosystème. Ces acteur pourraient ainsi bénéficier d'un registre global des consentement robuste, commun et avec une valeur de preuve importante en cas de litige.

Cette problématique sera détaillée dans la partie B de ce document.

g.4 Sécurité[54]

Afin de déployer les solutions les mieux adaptées, l'ensemble des problématiques de sécurité listées ci-dessous demandent un travail collaboratif et collectif entre différents métiers. L'enjeu est de **réunir suffisamment d'acteurs pour constituer une « masse critique » capable de générer un consensus et une adoption** suffisamment large par les utilisateurs finaux. A contrario des approches verticalisées non concertées ne permettront pas d'obtenir un niveau d'adoption suffisant.

Renforcement des mécanismes d'identification/authentification :

Le recueil d'un consentement, le renforcement de l'intermédiation dans les interactions entre une entreprise et ses clients par exemple pour collecter les données personnelles (exemple des PISP/AISP[55] dans le cadre de la DSP2[56] pour une banque) nécessitent de contrôler plus fortement l'identité des utilisateurs via **l'usage d'identités numériques certifiées et/ou d'authentifications renforcées.**

Recherche d'alternatives à la sécurisation par mot de passe et chiffrement bout en bout des échanges de données :

L'implémentation d'une meilleure circulation des données va faire émerger de nouveaux intermédiaires (de type PIMS), agissant au nom de l'utilisateur pour collecter ses données personnelles auprès d'un fournisseur et les partager à un tiers. En plus de la **nécessité d'un chiffrement bout en bout des données, dans le cas où l'accès aux données** de l'utilisateur est sécurisé par mot de passe, ces intermédiaires auront accès à ce dernier (ou à des jetons d'authentification), ce qui constitue un risque sécurité aggravé par le manque d'hygiène régulièrement observé dans le domaine de la gestion des mots de passe.

Besoin de standards d'authentification et d'identités numériques transverses :

L'usage du droit à la portabilité des données personnelles va se traduire par des parcours clients mélangeant l'usage de plusieurs applications de différents fournisseurs de services (exemple de l'agrégation de comptes bancaires par un AISP pour un client multi-bancarisé dans le contexte de la DSP2). **Si chaque application dispose de sa propre logique d'identification/authentification, l'expérience client sera très dégradée** (identifications/authentifications multiples & hétérogènes) ayant **pour conséquence une non adoption de l'usage** par les utilisateurs finaux.

Mise en œuvre de systèmes d'analyse comportementale :

L'implémentation de la portabilité des données personnelles devra s'appuyer sur des architectures à base d'API s'interfaçant avec **des applications clientes externes (hors du périmètre du système d'information) pour lesquelles il est nécessaire de contrôler les niveaux et profils de sollicitation afin de détecter toute sollicitation anormale.**

---

[54] Médéric Collas

[55] A.I.S.P (Account Information Service Provider) et P.I.S.P (Payment Initiation Service Provider).

[56] Directive des services de paiement

g.5 UX Design

L'UX design, user experience ou UX, est une notion qui a émergé ces dernières années. Elle s'attarde sur le parcours utilisateur dans son ensemble, en faisant valoir la qualité émotionnelle d'expérience et d'engagement entre un service et ses utilisateurs[57]. Il est nécessaire de comprendre que la qualité de l'expérience d'utilisation est devenue le maître-mot de la conception de tout service ou produit numérique, et vise à allier simplicité, personnalisation et multi-modalité[58].

On peut alors se demander quel est le lien à faire entre cet UX et la portabilité des données.
Il faut pour cela garder en tête que **le design est un enjeu crucial pour la vie privée,** et c'est pour cela que le RGPD a introduit la notion de privacy by design, expression utilisée dès 2009[59].

Ainsi, pour se répandre largement, **la portabilité des données doit être extrêmement simple à utiliser pour les individus et doit en même temps respecter les principes de protection de la vie privée dès la conception** (on peut également comprendre le design comme la volonté délibérée), ce qui peut être contradictoire si cela n'est pas fait correctement.

Le recueil d'un consentement éclairé nécessite donc un travail conséquent en matière de conception du parcours utilisateur :

- Afin **d'éclairer efficacement un utilisateur sur la portée de son accord** alors que son objectif personnel n'est pas de donner son accord mais de consommer le service pour lequel on demande son accord
- Afin de **rassurer un utilisateur réticent par des explications et arguments intelligibles et un environnement d'interaction inspirant la confiance.**

Dans un souci d'intelligibilité pour l'utilisateur final et de garantie d'une expérience utilisateur optimale unifiée, l'ensemble des travaux dans le domaine de l'UX doivent dans la mesure du possible déboucher sur des normes, standards ou des bonnes pratiques de conception adoptées par un écosystème de fournisseurs de services large[60].

Cette problématique sera détaillée dans la partie B de ce document.

---

[57] Cnil Linc, Cahiers IP n°06 "la forme des choix"

[58] Cnil Linc, Cahiers IP n°06 "la forme des choix"

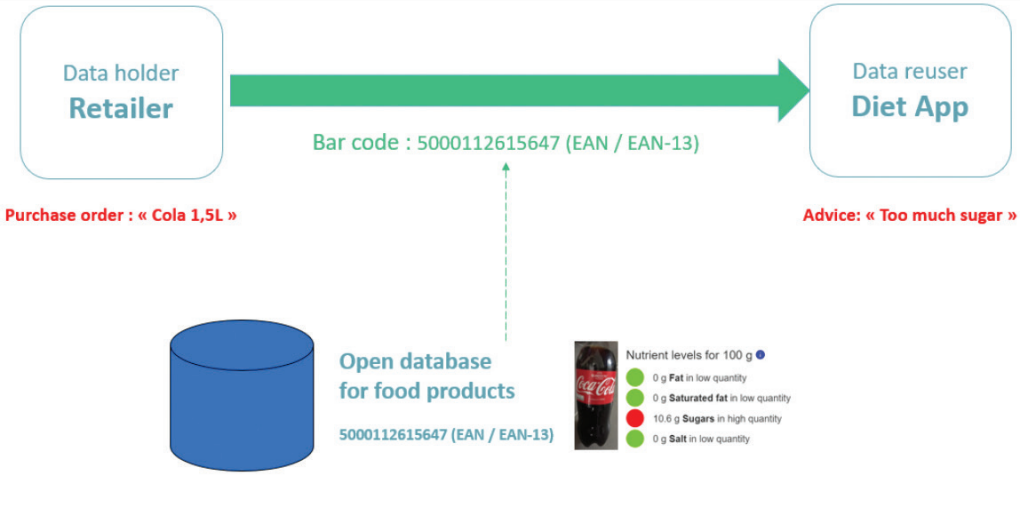
[59] Cnil Linc, Cahiers IP n°06 "la forme des choix"

[60] Médéric Collas

g. 6 Données de référence

Les données de référence sont les données structurées qui vont permettre à deux services qui s'échangent des données de parler le même langage.

Exemple concret : imaginons un cas d'usage où les clients d'un service de vente de produits alimentaires peuvent porter leurs données d'achats vers un service tiers de coach diététique, un fonctionnement optimal du cas d'usage implique que les deux services s'appuient sur une base de données structurée aussi complète que possible sur l'ensemble des produits alimentaires existants avec leurs caractéristiques (valeurs caloriques, composition, allergènes, etc). Si la base de données de référence est bien faite, ni le vendeur, ni le coach n'ont à stocker chez eux les informations nutritive de l'ensemble des produits existants, ils partagent la même base de connaissances publique. L'efficience de la circulation des données personnelles est directement reliée à la circulation, et à la structuration, des données de référence.



Les données de référence peuvent par exemple provenir de bases de données de référence :

- **En Linked Data** une initiative du W3C visant à favoriser la publication de données structurées sur le Web, non pas sous la forme de silos de données isolés les uns des autres, mais en les reliant entre elles pour constituer un réseau global d'informations.
- **En Open Data** données numériques dont l'accès et l'usage sont laissés libres aux usagers. Elle peut être d'origine publique ou privée, produite notamment par une collectivité, un service public (éventuellement délégué) ou une entreprise.

De nombreuses bases de données de référence existent dans de nombreux domaines (produits de consommation, musique, films, etc.). La plupart de ces bases de données, quand elles sont consultables via API, sont proposées par des entreprises privées (exemple : catalogue produit Amazon). Certaines sont en Open Data, on peut citer par exemple Open Food Facts[61] pour les produits alimentaires.

La question du modèle de revenu pour ces bases de données doit être posée. En effet l'investissement peut être lourd et nécessiter d'être rentabilisé pour assurer la maintenance, l'hébergement ou le haut niveau de qualité des références. La portabilité pourrait offrir un moyen de rentabiliser ces bases qui pourraient par exemple être commissionnées à chaque réutilisation.

Il faudra en revanche du temps avant que nous bénéficions de bases de données de référence structurées et ouvertes pour tout type de données, le premier niveau de portabilité doit donc pouvoir être réalisable avec des données non structurées, ou structurées mais non standardisées.

[61] https://fr.openfoodfacts.org/

4 - Les outils facilitateurs

a. Le rôle des PIMS

Le RGPD ne s'oppose pas à la réutilisation massive des données à caractère personnel, mais impose des conditions à leur traitement. Dans cette approche, **le droit à la portabilité instaure un nouveau paradigme de transfert des données plaçant les individus au centre de l'écosystème de leurs données,** et les autorise à choisir quel responsable de traitement pourra réutiliser leurs données et à quelles conditions (finalité, durée de conservation, sécurité, conditions de transferts hors UE). Le développement de cette nouvelle architecture de circulation des données portables, comprenant les données fournies directement et de manière active par les utilisateurs au responsable de traitement ou résultant de l'observation de l'utilisation du service ou du dispositif [62], est conditionné à la transparence sur les conditions de traitement et à la capacité des responsables de traitement à les respecter.

Le recours aux fournisseurs de système de gestion des informations personnelles (PIMS - Personal Information Management Systems), qui consiste à faire des personnes les détenteurs de leurs propres informations personnelles[63] pourrait favoriser le développement de la circulation des données. En effet, les fournisseurs de PIMS vont adopter des mesures technologiques pour garantir aux individus le transfert, et le respect des conditions de réutilisation de leurs données par les responsables de traitement, et ce de manière automatique.

Les systèmes de gestion des informations personnelles (PIMS : Personal Information Management Systems) sont des systèmes qui permettent aux individus de mieux contrôler leurs données personnelles. **Les PIMS permettent aux individus de gérer leurs données personnelles dans des systèmes de stockage sécurisés, locaux ou en ligne et de les partager quand et avec qui ils le souhaitent, ils peuvent aussi simplement faire circuler les données et offrir le contrôle sans le stockage.** Les fournisseurs de services en ligne et les annonceurs pourront interagir avec les PIMS s'ils envisagent de traiter les données de particuliers. Cela peut permettre une **approche centrée sur l'humain** des informations personnelles et de nouveaux modèles commerciaux [64].

Alors que le responsable de traitement est soumis à l'obligation d'adopter des mesures techniques et organisationnelles dès la conception pour garantir les droits des personnes concernées, en tenant compte « de l'état des connaissances, des coûts de mise en œuvre et de la nature de la portée, du contexte et des finalités du traitement ainsi que des risques (...) que présente le traitement pour les droits des personnes concernées » (art 25§1 du RGPD), le fournisseur de PIMS va mettre en œuvre le concept de privacy by design en se rapprochant de celui, initié au Canada par A Cavoukian[65,] issue de la philosophie des Privacy Enhancing Technologies (PET)[66], et dans une logique de smart contract. Ces derniers sont définis comme des programmes informatiques autonomes qui une fois programmés, exécutent automatiquement des conditions préalablement définies. En incorporant les conditions de la portabilité des données dans le code informatique, le fournisseur de PIMS va garantir aux utilisateurs la certitude que leurs données seront traitées comme convenu. Dès lors que le consentement est retiré, le flux des données portables sera automatiquement interrompu. Par cette pratique, l'adage de L. Lessig [67], **« code is law » devient « law is code ».** Cette approche est de nature à favoriser la confiance, la transparence et la traçabilité, nécessaires à l'exercice du droit à la portabilité entre responsables de traitement.

Les PIMS pourront également permettre de réduire grandement le coût de la portabilité. En effet la variété des systèmes d'information des organisations est importante et certains systèmes mettront des années à évoluer. Dans le même temps le nombre de connexions à créer entre ces systèmes est proprement gigantesque, les PIMS pourront prendre à leur charge ce coût et soulager ainsi les organisations. Une démarche open source devra très certainement être couplée à cet effort. Les PIMS joueront le rôle de hub de transfert de données en s'appuyant sur une architecture centrée sur l'individu.

Force est de constater que si ce nouvel acteur, qui peut être considéré comme « un intermédiaire ou une plateforme « qui connecte les deux versants du marché : les personnes qui offrent leurs données en vue de leur utilisation ou réutilisation, d'une part, et les organisations qui souhaitent utiliser ou réutiliser celles-ci, d'autre part »[68], facilite l'exercice du droit à la portabilité, **une incertitude existe sur le régime de sa responsabilité[69].** Cette incertitude pourra être clarifiée dans le cadre d'une gouvernance globale.

ELÉONORE SCARAMOZZINO :

Eléonore Scaramozzino est avocate et fondatrice de Constelletion, cabinet d'avocats spécialisé dans le domaine des données personnelles. Eléonore est spécialiste du droit Européen et a travaillé avec la Direction Générale de la Concurrence de la Commission européenne.

[62] « Lignes directrices relatives au droit à la portabilité des données », WP 242-rev.01, spéc. p.12

[63] Avis du CEPD sur les systèmes de gestion des informations personnelles : vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel, 20 octobre 2016.

[64] European Data Protection Supervisor 2016

[65] CAVOUKIAN (A.): « Privacy by design : The 7 foundational principles », Information and Privacy /Commissioner of Ontario, Canada, 2009.

[66] DEBET (A), MASSOT (J) et METALLINOS (N), Informatique et libertés. La protection des données à caractère personnel en droit français et européen, Lextenso, coll. Les intégrales, 2015, spéc. nos 55, CE : Etude annuelle 2014, le numérique et les droits fondamentaux, Ed. La documentation française, 2014, spéc. p. 179

[67] LESSIG (L.): Code is law, On liberty in cyberspace, Harvard magazine, jan.-fév. 2000, adresse : http://harvardmagazine.com/2000/01/code-is-law-html. Pour une traduction française de l'article, v. http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig

[68] Avis du CEPD sur les systèmes de gestion des informations personnelles : vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel, 20 octobre 2016, p.14.

[69] Contribution Eléonore Scaramozzino, Constelletion Partenaires

b. Les différents modèles de PIMS

PIMS (Personal Information Management Systems), PDMS (Personal Data Management Systes), VRM (Vendor Relationship Management), PDS (Personal Data Store), Personal Cloud, tiers de confiance … Nous retiendrons le terme générique de PIMS pour qualifier un ensemble d'outils destinés à permettre aux individus de gérer leurs données. Le marché des PIMS étant encore à ses débuts, les contours sont encore flous et les définitions à fixer. Ceci pourra d'ailleurs être précisé par un organe de gouvernance des données.

Cependant nous pouvons faire ressortir plusieurs propositions de valeur pour les PIMS :

- le stockages des données,
- le transfert,
- la gestion des consentements (avec ou sans blockchain),
- la gestion des mots de passe,
- le traitement de données à l'intérieur du PIMS au moyen d'applications,
- la monétisation des données par l'utilisateur,
- la monétisation entre services,
- la gestion de la contractualisation entre services,
- etc.

Les PIMS se présentent sous diverses formes et architectures, toujours centrées sur l'individu :

- Certains PIMS fonctionnent seuls, d'autres en marque blanche,
- Certains PIMS stockent les données sur un appareil de l'utilisateur ou sur un cloud, d'autres ne stockent pas les données,
- Certains PIMS ont un business model B2B, d'autres B2C,
- Plusieurs PIMS peuvent s'associer pour proposer une solution de gestion complète.

La FING a proposé une classification des PIMS, voir ci-dessous.

CC-BY-FING : "Les Données personnelles partagées : quels cas d'usage pour quels modèles de Gouvernance" - mars 2019

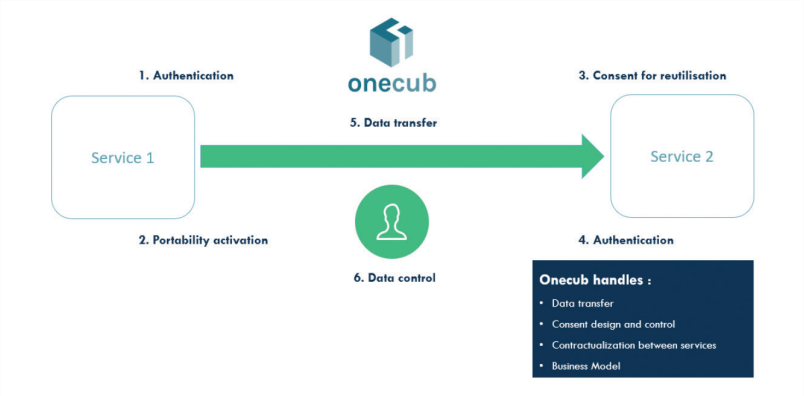
c. Quelques exemples de PIMS

Concernant la concurrence entre PIMS, les PIMS devront montrer l'exemple en offrant une portabilité très fluide entre eux. Cela suppose un grand niveau d'interopérabilité et donc **des standards communs.**

Voici quelques exemples concrets de PIMS et leur modèle.

Le PIMS Onecub :

Onecub facilite la circulation des données en centralisant le contrôle dans les mains de l'individu, tout en laissant les données décentralisées. Onecub s'intègre facilement, à un bouton d'export/import de données (bouton de portabilité) affiché sur le compte d'un utilisateur sur un service en ligne. Onecub présente ensuite à l'utilisateur un écran de recueil de consentement, intégré au service, pour le transfert et la réutilisation de données vers un service tiers qu'il aura sélectionné pour un cas d'usage spécifique. Le cas d'usage aura été prévu et contractualisé, au préalable, entre les deux services. Une fois le consentement donné, l'utilisateur est redirigé vers l'écran d'authentification du service tiers. S'il s'authentifie, Onecub transfère les données sans les stocker, mais en assurant leur interopérabilité. Seul le consentement est conservé. La circulation des données peut être réalisée en continu ou en une fois. Plus tard, s'il le souhaite, l'utilisateur pourra contrôler ses données via un tableau de bord de l'ensemble des consentements qu'il aura donné de manière indépendante de ses services en ligne.



Le business de Onecub est B2B, l'action de transfert est gratuite pour l'utilisateur mais Onecub permet au service réutilisateur de payer le service détenteur de la donnée initiale, de manière transparente pour l'utilisateur, et prend une commission sur l'échange.

CHRISTINE TARTANSON :

Christine Tartanson est une experte de l'innovation data dans l'alimentaire, le retail et la mobilité. Elle est Directrice des Partenariats pour la startup Onecub, plateforme de portabilité des données personnelles (PIMS). Christine a dirigé l'équipe Produit Europe chez NPD Group, cabinet d'étude international.

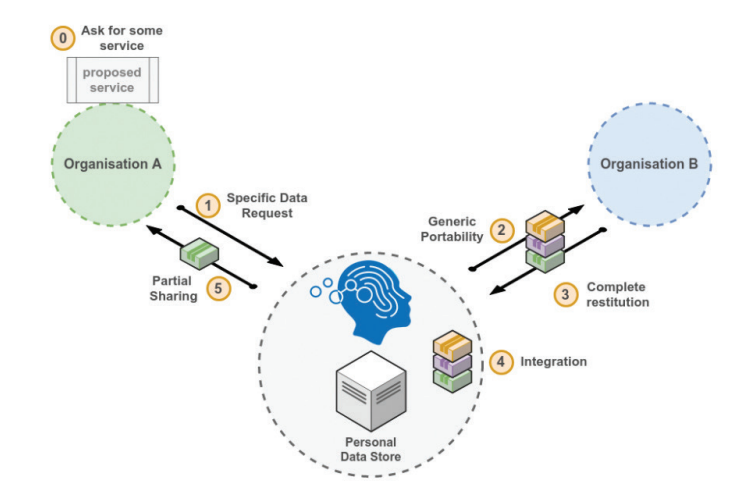
Le PIMS Fair&Smart :

Le PIMS Fair&Smart s'appuie sur une plateforme distribuée de gouvernance des données personnelles accessible aux individus et aux organisations. Il vise à offrir à l'utilisateur une vue centralisée de ses données personnelles, de qui les utilise et pour quelles finalités. Il se positionne ainsi comme un hub d'échanges de données supervisé par l'individu, auditable et historisé, avec un chiffrement des échanges de bout-en-bout. Fair&Smart offre à l'utilisateur les possibilités suivantes :

- L'exercice de ses droits RGPD : droit d'accès, d'opposition, de portabilité, de limitation, d'effacement et de rectification, notamment pour alimenter son espace,
- La gestion centralisée de ses consentements,
- Le transfert chiffré d'informations sélectionnées et éventuellement retraitées (conversion, agrégation, horodatage...),
- Le stockage de toutes données brutes et structurées, fichiers et documents.

Fair&Smart propose un stockage en ligne distribué redondé avec partage ouvert vers l'extérieur.

Le modèle de réutilisation des données peut être représenté comme suit :



XAVIER LEFEVRE :

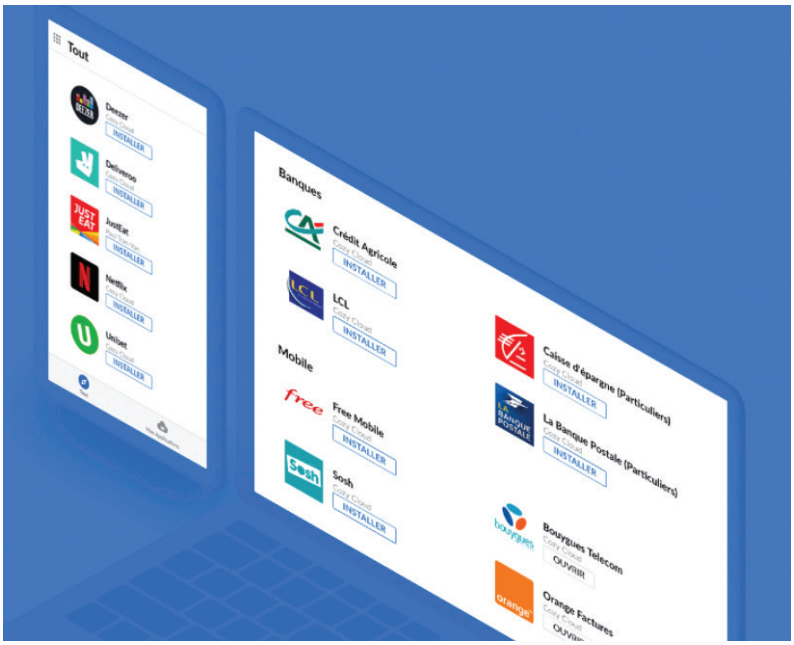
Xavier Lefevre est le fondateur de la startup Fair&Smart, spécialisée dans les solutions de gestion des données personnelles à destination des particuliers et des entreprises (PIMS). Xavier a été entrepreneur dans la distribution, puis a été directeur stratégie pour une SSII spécialisée dans l'innovation

Le PIMS Cozy Cloud :

Cozy est le premier domicile numérique, un espace de stockage intelligent qui permet à l'utilisateur de récupérer automatiquement toutes ses informations et d'ainsi bénéficier de services et d'une intégration qui dépasse celles des silos fermés des GAFA. Alors que chacune de nos décisions sont conditionnées par nos données, leur réappropriation par les individus est l'enjeu majeur des démocraties à l'ère du numérique.

Le risque de la portabilité est qu'au final la portabilité ne favorise que des flux de données allant vers les services déjà existants. C'est la problématique à laquelle répondent les clouds personnels comme Cozy Cloud, des outils permettant aux individus d'agréger, stocker et traiter par eux-mêmes leurs données dans un espace personnel dédié et sécurisé créant ainsi un véritable domicile numérique pour les utilisateurs. Les clouds personnels permettent des propositions de valeur structurellement inaccessibles dans les services en silos comme :

- La personnalisation anonyme grâce aux services numériques « à domicile »
- Le big data en peer-to-peer (P2P)
- L'intelligence artificielle décentralisée

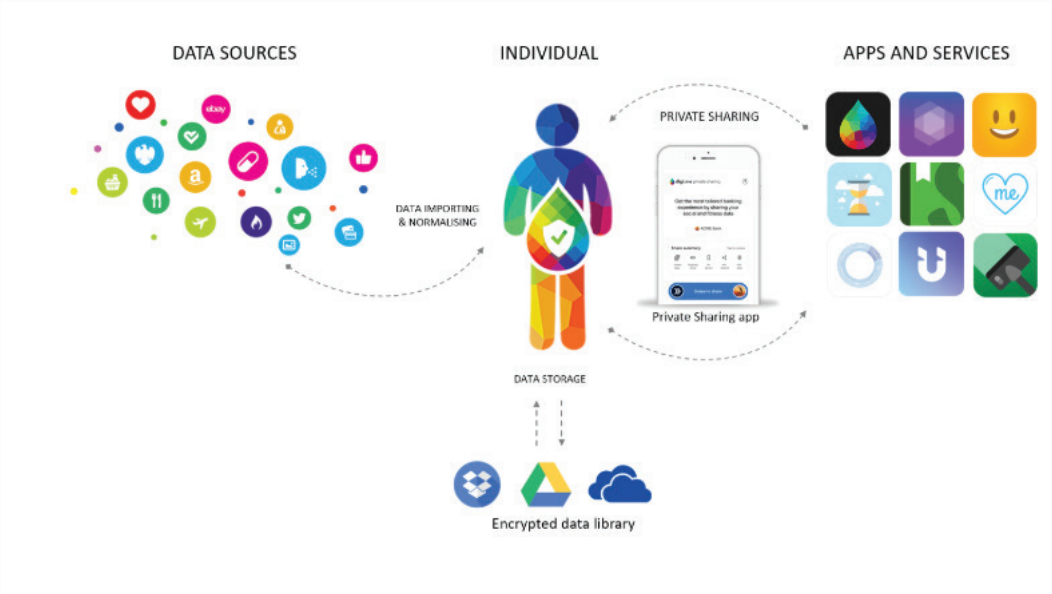


BENJAMIN ANDRÉ :

Benjamin André est le président fondateur de la startup Cozy Cloud, outil de cloud personnel ou domicile numérique (PIMS) permettant aux utilisateurs de récupérer et gérer leurs données. Benjamin a notamment travaillé pour Total et sur des systèmes d'information dans de grandes entreprises.

Le PIMS Digi.me :

Digi.me est une plateforme d'échange de données personnelles qui permet à l'individu de contrôler ses données. Digi.me ne voit, ne touche ou ne détient jamais les données d'un individu. Il permet à l'individu de partager ses données en privé avec des tiers en échange d'un meilleur service, d'une meilleure commodité ou d'une récompense. Les données sont cryptées à l'intérieur de l'application digi.me lorsqu'elles sont importées depuis vos comptes. Vos données cryptées sont ensuite stockées dans un cloud personnel de votre choix (Dropbox, Google Drive, Microsoft OneDrive) jamais sur nos serveurs. Les données ne peuvent être consultées et partagées en privé que lorsque vous êtes connecté et que vous donnez votre autorisation explicite. Toutes les opérations de données se déroulent à l'intérieur de l'application ou dans un cloud personnel virtuel temporaire (pour la synchronisation). Nous ne voyons ni ne stockons jamais votre mot de passe.



RONY DONNELLY :

Rory Donnelly est CEO de Digi.me, plateforme d'échange et de contrôle des données personnelles par l'individu (PIMS). Rory possède une vaste expérience dans la mise en place de réseaux de distribution.

d. Liste de PIMS en activité[70]

PIMS	Pays d'origine
Bali (Microsoft)	Etats-Unis
Bankin	France
BitsAbout.Me	Suisse
CitizenMe	Royaume-Uni
CloudLocker	Pays-bas
Cozy Cloud	France
Datacoup	Etats-Unis
Datum.org	Suisse
Digi.me	Royaume-Uni
Dock.io	Etats-Unis
Fair & Smart	France
Healthbank	Suisse
Helixee	France
Inrupt (Solid)	Etats-Unis
Jolocom	Allemagne
Linxo	France
Lympo	Lituanie
Meeco	Australie
MyDex	Royaume-Uni
My Data is Rich	France
Onecub	France

[70] Contribution CBS - Copenhagen Business School

5 - Etat de l'art et Cas d'usage de portabilité

a. Se déplacer

a1. Les enjeux

La portabilité permettra aux individus de se déplacer plus facilement. Un nouveau sujet est apparu ces dernières années pour les grandes villes et les acteurs de l'industrie de la mobilité : le MaaS (Mobility as a Service) / agrégation de services de mobilité, qui vise à interconnecter l'ensemble des services de mobilité et d'hospitalité (train, avion, métro, voiture individuelle, taxi, hôtel, etc.) afin de proposer aux utilisateurs une expérience de mobilité totalement fluide.

A l'heure des Smart Cities, le droit à la portabilité citoyenne **permettrait en particulier à la ville de s'affranchir de la dépendance aux acteurs globaux du Web,** pour avoir accès aux données des citoyens, notamment des données de mobilité, afin d'être en mesure d'élaborer une politique de transport public adaptée à leurs habitudes de mobilité.

La portabilité est également **une opportunité très prometteuse dans le secteur de l'automobile avec l'avènement prochain du véhicule connecté** qui pourrait se transformer en véritable plateforme de services pour les particuliers.

a2. Initiatives en cours

Projets de la ville de Reims et de Paris Saclay :

Voilà des années que des expérimentations multi-partenariales visent à collecter des données personnelles sur un territoire, notamment dans le secteur des transports et des mobilités. L'idée est souvent de créer une plateforme de collecte, d'échange et de partage de données entre plusieurs acteurs, privés et publics, afin de proposer de nouveaux services mutualisés à destination d'usagers, dans une démarche de collaboration avec ces derniers et de restitution des données, résultats et analyses à leur profit.

Comment organiser cette mise en commun de données entre plusieurs partenaires et organiser, dans le même temps, une gouvernance partagée et ouverte entre tous et au bénéfice des usagers, dans le respect du RGPD ? En instituant un tiers de confiance de la donnée.

L'idée n'est pas nouvelle. Elle a été conceptualisée par le programme Datact, dont les concepteurs (Le Hub et Chronos) ont réfléchi, depuis 2011, à un concept de « régie de données » (Cahier détaché de la Gazette des Communes, n° 2, 19/2221, du 12 mai 2014). Cette réflexion était principalement économique mais les concepteurs de ce programme, conscients qu'il fallait y associer une approche juridique, avaient proposé d'assimiler cette régie de données à un « tiers de confiance dont le statut juridique reste à définir ». C'est une réflexion que Jérôme Giusti, avocat, fondateur et associé du cabinet d'avocats Metalaw, avait à l'époque commencé à interroger (Instituons un tiers de confiance et un nouveau contrat social entre opérateurs de transport et usagers, Quelles stratégies pour l'open data ? La Vie du Rail, Ville Rail et Transports, mai 2014).

A l'origine appliqué à l'open data, il interroge, depuis plusieurs années, ce concept au regard des données à caractère personnel. Profondément inspirée d'une démarche d'autorégulation, cette réflexion est venue s'enrichir à l'occasion de l'entrée en vigueur du RGPD et du droit à la portabilité.

C'est ainsi que la réflexion sur une régie de données à été initiée d'un point de vue juridique, dans le cadre de l'appel à projet Mobilise, financé en 2016 par l'ADEME, dont l'objet est de créer une application qui permettait à la ville de Reims et sa région périphérique de faire remonter des données de mobilités depuis des usagers volontaires, de les partager entre des opérateurs privés et acteurs publics au sein d'un hub et ainsi, de créer des services de mobilités adaptés aux usages du territoire.

Actuellement, sur l'initiative de la communauté d'agglomération de Paris Saclay, un projet similaire s'engage, sous l'appelletion Mov'in Saclay, lequel cherche à développer une plateforme pour organiser la mobilité sur ce territoire dans une démarche d'innovation ouverte, associant les citoyens, les entreprises et collectivités, ainsi que les fournisseurs de services.

Plusieurs acteurs publics et privés pourraient ainsi faire le choix de créer entre eux une structure ad hoc dédiée au traitement commun de leurs données, sous la forme d'une association, d'une SCIC[71] ou d'un GIE[72].

Cette structure tierce serait chargée, en amont, de centraliser les données issues des divers fichiers fournis par les responsables de traitement. Elle serait la seule à maîtriser, gérer puis partager les données personnelles qui en seraient issues, dans le respect du RGPD. En aval, elle déciderait, au cas par cas, de libérer certaines données au bénéfice des utilisateurs pour des besoins spécifiques, en prenant le soin de cloisonner certains fichiers, anonymiser certaines données, exiger certaines conditions d'utilisation spécifiques, en fonction des besoins sollicités. Ces transferts de données, réalisés sous la forme contractuelle, pourraient être soumis à des « binding corporate rules », déjà connus par ailleurs pour les échanges intra-groupes. Les utilisateurs des données connaîtraient ainsi par avance les règles applicables à leur diffusion, pourraient les négocier en amont et bénéficier ainsi d'une sécurité et de standards juridiques leur permettant de les exploiter en conformité avec la loi. Enfin, des standards de « Self Data » pourraient également être imaginés et promus pour permettre aux personnes concernées par la collecte de leurs données de se les voir restituer, selon des modalités et des normes connues d'avance.

Un tel regroupement répondrait ainsi au besoin impérieux de créer en commun des standards d'interopérabilité et de portabilité, ainsi que de rechercher ensemble des modèles économiques partenariaux, tout en associant les territoires à la décision dans une démarche de préservation de leur souveraineté et de sauvegarde de l'intérêt général.

La donnée pourrait ainsi devenir, dans l'intérêt de la puissance publique, comme des entreprises et des particuliers, un commun soumis à des règles de « copyleft ». Un changement de paradigme, à n'en pas douter.

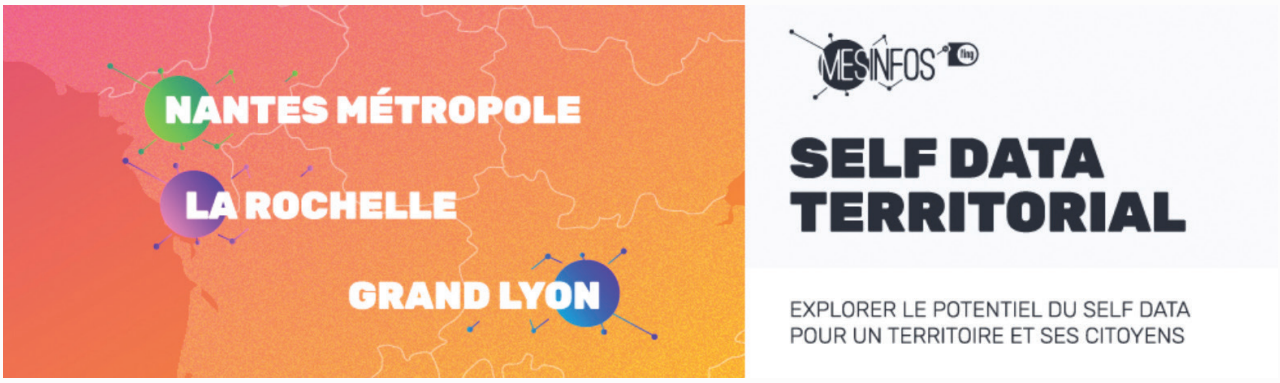
JÉRÔME GIUSTI :

Jérôme Giusti est avocat au barreau de Paris, spécialiste en droit des nouvelles technologies. Fondateur du cabinet d'avocats Metalaw, il accompagne depuis des années des acteurs dans l'élaboration de modèles juridiques innovants autour de la donnée. Il promeut le concept juridique de tiers de confiance de la donnée.

[71] Sociétés coopératives d'intérêt collectif

[72] Groupement d'intérêt économique

Projet de la ville de La Rochelle :



CC-BY-FING : Self Data Territorial Mes Infos - janvier 2019

Le projet self data territorial (SDT) de La Rochelle, en lien avec la Fabrique des Mobilités et la FING travaille sur plusieurs problématiques :

- Celle de l'appropriation des données par le plus grand nombre dans des enjeux de littératie du numérique et d'égalité d'accès aux services (notamment publics)
- Celle de la gestion des données respectueuse de la vie privée, centrée autour de l'usager contributif
- Celle des réutilisations potentielles des données, à forte valeur ajoutée pour l'usager ou pour la collectivité
- Celle de la gouvernance des données à l'échelle d'un territoire

Compte tenu de la culture de la ville de La Rochelle, en terme d'innovation sur les mobilités, et du fait que ce sujet est également central dans la vie de tous les habitants, la thématique de la mobilité durable nous a semblé particulièrement pertinente. Cette thématique repose sur une approche globale incluant les mobilités personnelles et professionnelles. Cela permet aussi de mobiliser les organisations dans leurs pratiques internes, puisqu'elles devront restituer les données liées à la mobilité de leurs agents. La mobilité est aussi questionnée sous tous ses aspects : déplacements, facteurs de pollution et congestion urbaine, et qualité de vie.

Le programme 2018-2019 s'est donc déroulé sur plusieurs temps, avec de nombreux acteurs, selon un principe de co-construction comprenant :

- Une présentation aux relais d'usagers locaux (Conseils citoyens, comité d'usagers, comités de quartiers) ;
- Une conférence participative en septembre 2018 pour informer et questionner l'acceptabilité du partage de données de mobilité via des cas pratiques (présentation du Compte Mobilité de l'ADEME[73]) et questionnant les aspects techniques de la portabilité des données[74] ;
- Des ateliers dans les quartiers ;
- Des ateliers de prospective avec la FING ;
- 4 scénarios ont été co-construits avec les habitants et les différents partenaires ;
- L'intervention d'un coach C02, afin de mesurer et réduire l'empreinte carbone de ma mobilité.

Un scénario sera adopté par les élus pour une exploration fondée sur les mêmes principes d'ouverture au grand public. Un appel à volontaires sera diffusé, y compris dans les organisations des partenaires (Ville, La Poste, Enedis et Université). La création d'une communauté d'expérimentateurs, allant au-delà des classiques fractures intergénérationnelles, sociales et professionnelles, est visée.

En effet, si la thématique choisie est universelle, son approche via la donnée écarte les individus-citoyens qui ne sont pas à l'aise avec l'outil numérique, ou qui entretiennent à ce sujet une forme de défiance. Ainsi seule une minorité de rochelais s'est engagée dans cette phase 2018-2019, et les publics invisibles, citoyens ou professionnels pourtant ciblés, sont restés à l'écart.

Le projet a été porté jusqu'à fin 2018 par la DSI de la Ville et sa cheffe de projets numériques en charge de l'administration des données. En 2019, il est porté par la direction de la Transformation numérique et son administratrice générale des données dans le cadre d'une mutualisation de services Ville-Agglomération.

Si le pilotage est porté par l'institution publique, la gouvernance du projet sera construite avec les utilisateurs et les partenaires. En effet, le projet s'intègre dans un plan d'action « données », plus vaste, de mise en circulation des données sur le territoire via une gouvernance territoriale des données outillée, d'un service public territorial des données et d'une plateforme de données permettant le shared data et l'open data. Si l'institution publique apparaît comme un tiers de confiance légitime pour organiser le crowdsourcing de données personnelles, elle se doit de se doter d'instances de contrôle permettant de garantir cette confiance.

VIRGINIE STEINER :

Virginie Steiner est administratrice générale des données pour la Ville et l'Agglomération de La Rochelle, Virginie Steiner pilote l'ouverture des données publiques dans le respect des cadres légaux et des stratégies locales axées sur le respect de la vie privée, le numérique durable et les Communs. Elle conduit des projets transversaux sur les données sous l'angle territorial en portant notamment la future réalisation d'un service public territorial des données et un programme autour de la valorisation des données personnelles et l'autodétermination informationnelle (Self Data territorial).

[73] Agence de l'environnement et de la maîtrise de l'énergie

[74] https://www.youtube.com/watch?v=h3gnh7mxM2c

a3. Cas d'usage en cours

L'agrégation de services de mobilité basée sur la portabilité :

Le service Citeazy est un agrégateur de services de mobilité. Citeazy permet à un utilisateur de visualiser l'ensemble des services de mobilité correspondant à sa recherche, et de réserver des trajets ou services de mobilité (vélo, scooter, voiture, taxi, transports en commun, etc.) depuis une interface unique. Il peut alors bénéficier d'une expérience d'utilisation totalement personnalisée et intégrée. Citeazy permet aujourd'hui à une entreprise d'assurer la mobilité de ses salariés et pourra demain permettre à un territoire d'assurer la mobilité de ses habitants.

En 2019 Citeazy a fait appel au PIMS Onecub pour organiser la portabilité des données de ses utilisateurs entre son service et l'ensemble des services de mobilité qu'il agrège. L'expérience utilisateur est la suivante :

- un utilisateur Citeazy souhaitant réserver un trajet précise sa demande sur le service Citeazy
- Citeazy lui présente les différentes options de mobilité disponibles
- L'utilisateur sélectionne son trajet et le service associé
- Une pop-up Onecub s'ouvre et propose à l'utilisateur d'envoyer des données Citeazy vers le service de mobilité pour faciliter la réservation (données d'identité, cartes d'abonnement, moyens de paiement, permis, préférences, etc.), puis de récupérer ses données de mobilité (confirmation de réservation) dans Citeazy
- Onecub recueille le consentement de l'utilisateur pour le transfert de données et permet à l'utilisateur de s'authentifier sur le service de mobilité retenu
- Onecub réalise le transfert de données via une API dédiée mais n'enregistre pas les données
- L'utilisateur a réservé son trajet sans sortir de l'interface Citeazy et pourra réutiliser toutes les données collectées dans Citeazy pour des mobilités ultérieures
- S'il le souhaite l'utilisateur peut accéder à un compte personnel, indépendant de Citeazy ou de ses partenaires, dans lequel il retrouve un tableau de bord de ses consentements qu'il peut révoquer à distance à tout moment.

Onecub crée des connecteurs normalisés autour de la plateforme Citeazy et prend en charge toute la complexité de la portabilité pour Citeazy (les aspects techniques, juridiques, UX design, business model).

Le modèle appliqué par Onecub est le suivant :

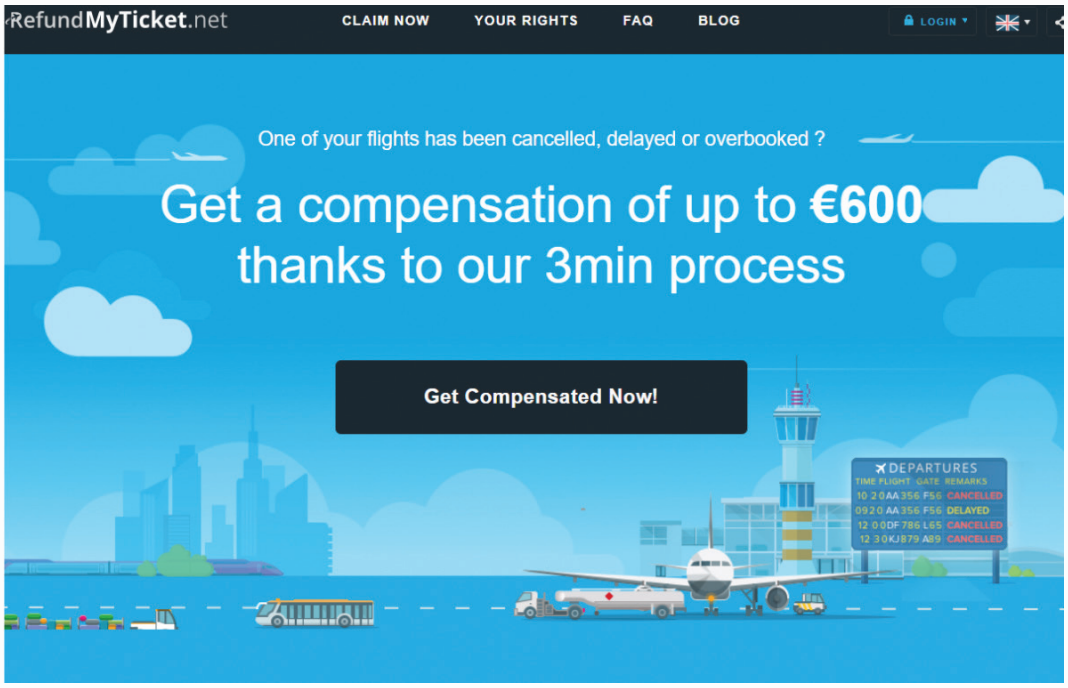
- Onecub permet à Citeazy et à ses services partenaires de s'échanger des données en s'appuyant sur le droit à la portabilité
- Onecub permet à Citeazy et à ses partenaires de définir des cas d'usage précis d'échanges de données et le business model associé
- Onecub s'appuie sur la notion de consentement pour la réutilisation des données et enregistre le consentement de l'utilisateur afin de lui offrir du contrôle
- Onecub fait circuler les données de mobilité selon le souhait de l'utilisateur mais ne les enregistre pas, elles restent décentralisées
- Onecub offre à l'utilisateur un moyen transparent, indépendant de Citeazy et de ses services, de contrôler la circulation de leurs données.

ALMA GUIRAO :

Alma Guirao est la fondatrice de Citeazy, agrégateur de services de mobilité. Alma est une serial entrepreneure, Citeazy est sa 3ème structure. Elle a notamment fondé Handsaway une application mobile qui aide à lutter contre les agressions sexistes. Citeazy déploie ses 2 premières versions chez ses clients et se prépare à lancer la 3ème version.

La portabilité pour faire valoir les droits des passagers :

RefundMyTicket aide les passagers victimes d'un vol retardé, annulé ou surbooké à obtenir une indemnisation conformément à la réglementation européenne. Après une tentative de conciliation amiable, si les compagnies aériennes refusent d'indemniser leurs clients, nos avocats partenaires défendent les droits des passagers devant le juge. Le succès de ces actions en justice dépend de l'obtention des données personnelles des passagers.



Pour pouvoir prétendre à une indemnisation en cas de retard, d'annulation ou de surbooking, les passagers doivent s'être présentés à l'enregistrement de leur vol à l'aéroport. Au fur et à mesure des procès, la question de la preuve de cette présence à l'embarquement est devenue critique et avec elle celle de l'accès aux données personnelles des passagers s'est posée. Actuellement les passagers n'ont aucun document qui puisse définitivement prouver leur présence à l'embarquement ou à bord de l'avion. Le boarding pass, traditionnellement fourni après le check-in, peut désormais être obtenu en ligne plusieurs jours avant le départ du vol et a donc perdu de sa force probante. Il arrive aussi souvent que les voyageurs jettent ou perdent leurs documents de voyage. Pour autant, les compagnies aérienne et certains prestataires intermédiaires détiennent ces preuves indispensables qui apparaissent systématiquement dans ce qu'on appelle les données PNR.

Les données des dossiers passagers (données PNR[75]) sont des informations à caractère personnel qui sont recueillies et conservées par les transporteurs aériens. Ces données comportent différentes informations telles que le nom et le statut du passager, c'est à dire son enregistrement ou sa non-présentation à l'enregistrement. Ces données personnelles sont des preuves déterminantes pour l'issue du litige. Aujourd'hui, les compagnies aériennes conservent ces données PNR (et y sont même contraintes pour des questions de sécurité) qui sont des preuves irréfutables de la présence des passagers à l'aéroport. C'est grâce au droit à la portabilité des données que RefundMyTicket et ses avocats pourraient défendre plus facilement les droits des passagers en apportant les preuves nécessaires au succès de leur réclamation.

Sans le droit à la portabilité, les compagnies aériennes sont les seules à détenir les preuves qui les incriminent et celles-ci refusent systématiquement de les fournir aux passagers, même lorsqu'ils en font la demande expresse. Cette situation pourrait s'améliorer grâce à l'application effective du droit à la portabilité, dans le secteur aérien et dans tous les secteurs. RefundMyTicket plaide en faveur de l'ouverture des données des citoyens pour permettre à chacun d'avoir la main sur les informations qui les concernent et pour favoriser la transparence. La portabilité des données des consommateurs vers des prestataires de services juridiques tel que RefundMyTicket permettrait de rééquilibrer les relations entre les entreprises et leurs clients. Les avocats partenaires de RefundMyTicket ont déjà posé une question préjudicielle à la Cour de Justice de l'Union Européenne pour défendre le droit d'accès des passagers à leurs données personnelles face aux compagnies aériennes. La portabilité des données pourrait renforcer les droits des justiciables grâce à l'obtention de preuves.

AURORE TROUSSEL :
Aurore Troussel est élève-avocate et étudiante à HEC, spécialisée dans la protection des données personnelles et la justice par algorithmes. Juriste à Justice.cool, plateforme de médiation en ligne assistée par intelligence artificielle.

[75] Passenger Name Record

a4. Exemples de cas d'usage

Données portables	Cas d'usage
Réservations de transports (train, avion, VTC, covoiturage,...), hébergement, documents administratifs, documents, de paiement, etc.	je récupère l'ensemble de mes données mobilité dans un agrégateur MaaS ou hub de services à partir duquel j'agrège et réutilise toutes les informations nécessaires à ma mobilité et je peux réserver des trajets multimodaux et services en 1 clic.
Réservations de transports (train, avion, VTC, covoiturage,...)	je transmets les données de mes voyages à des services de mobilité courte distance pour être transporté à mon arrivée (en gare, à l'aéroport, etc.) comme des VTC, covoiturages, taxis, etc. En cas de retard les infos associés seront également transmises.
GPS	je transmets les données de mes trajets (application GPS ou automobile connectée) à un service de covoiturage pour prendre des courses dès que je fais un trajet
GPS, réservations de transports	je transmets mes données à un service de livraison entre particuliers pour prendre des courses dès que je fais un trajet
Réservations de transports (train, avion, VTC, covoiturage,...)	je transmets les données de mes voyages (train, avion, bus, bateau, covoiturage) a un service de conciergerie pour bénéficier de services à mon arrivée
Réservations de transports (train, avion, VTC, covoiturage,...), GPS	je transmets les données de ma mobilité à des services me permettant de calculer mon empreinte carbone
Réservations de transports (train, avion, VTC, covoiturage,...), hébergement	je transmets tous mes lieux visité vers des sites d'évaluation (hôtels, restaurants, lieux de sortie, etc.)

b. Chercher un emploi

b1. Les enjeux

La portabilité est en enjeu clé pour l'emploi où elle va permettre d'optimiser les parcours de recherche d'emploi et de formation. La **simplification administrative** induite par la portabilité se combinera avec la possibilité de générer un CV à partir de multiples traces laissées sur différents services (parcours scolaire, expérience professionnelle, niveaux de langue, etc.). Les données portables de l'éducation (diplômes du secondaire et du supérieur, formations en ligne, MOOC, etc.) pourront également venir enrichir le CV. La portabilité permettra dans l'autre sens le **"multi-posting" d'une recherche vers de multiples services, augmentant ainsi les chances de réussite des candidats.**

Les obstacles à surmonter dans le domaine de l'emploi sont cependant nombreux. **Les référentiels emploi et formation existants doivent être correctement partagés et utilisés par tous les acteurs de l'écosystème.** L'emploi est également un domaine où il est fréquent qu'un acteur public (type Pôle Emploi pour la France) soit le principal détenteur de données tandis que de nombreux sites proposent leurs services en parallèle (acteurs mondiaux, startups de recherche d'emploi spécialisés, conseil formation, etc.). **Les acteurs publics de l'emploi sont face à un choix clair : soit ils se considèrent comme le pivot de leur écosystème national et ouvrent largement leurs données à des acteurs privés, soit ils ferment les portes et les concurrencent, oubliant ainsi leur mission d'intérêt général.**

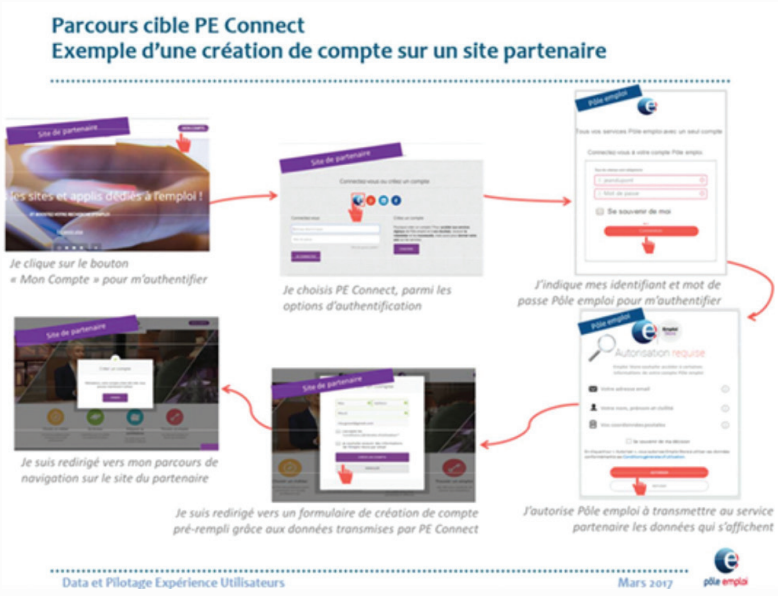
b2. Initiatives en cours

Le cas Pôle Emploi pour la France

Le dispositif de portabilité des données personnelles de Pôle emploi est ouvert depuis Juin 2017. Ce dispositif offre aux utilisateurs plusieurs avantages tels que :

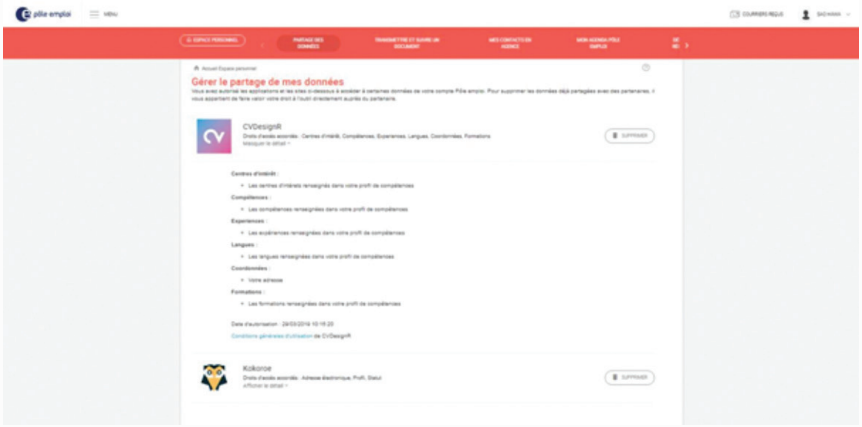
- Un seul identifiant et mot de passe pour accéder à l'ensemble des services Pôle emploi et des services de partenaires ayant souscrit à ce dispositif
- Une navigation fluide (SSO[76]) dès qu'une identification est réalisée sur l'ensemble des services de Pôle emploi et ceux des partenaires
- Une portabilité des données personnelles entre services (avec recueil du consentement au sens RGPD) si ces services sont des services de partenaires
- La possibilité à travers les espaces personnels des candidats (site pole-emploi.fr - rubrique Gestion des consentements) de visualiser l'ensemble des partages de données acceptées et résilier ces échanges de données partenaire par partenaire

Le parcours d'un utilisateur débute par le bouton 'Se connecter avec Pôle emploi'. Ce dispositif permet une lecture des CGU du site du partenaire et un recueil du consentement éclairé de l'utilisateur en amont d'un transfert de ses données vers le partenaire :



Sur l'écran Autorisation Requise, la liste des données à partager vers le partenaire est affichée avec la possibilité d'une case "se souvenir de ma décision". Cette case à cocher est désactivée à chaque fois qu'un partenaire modifie ses CGU afin de laisser aux utilisateurs la possibilité de les relire et/ou si la liste des données partagée évolue.

Ce dispositif de portabilité des données personnelles a été mis en œuvre par Pôle emploi de manière concomitante à la livraison d'un écran de gestion des consentements dans l'espace personnel des candidats sur pole-emploi.fr



Fin Février 2019, ce dispositif était plébiscité par nos utilisateurs : 172 738 utilisateurs du dispositif sur le mois de février 2019, et près de 1,5 millions d'appels sur les 12 derniers mois. Le dispositif est implémenté chez plus d'une vingtaine de partenaires :

Le dispositif repose sur des API mises à disposition via le portail pole-emploi.io. A ce jour, 9 API de données personnelles sont disponibles :

- 1 permettant d'identifier les individus (Se connecter avec Pôle emploi)
- 4 portant l'ensemble des informations d'un CV (Coordonnées, Compétences, Expériences, Formations)
- 1 portant le statut du candidat (demandeur d'emploi : oui/non)
- 1 en lien avec la reconnaissance d'expériences prof. par les employeurs
- 1 portant leur date de naissance
- 1 portant les critères du service d'abonnement aux offres d'emploi sur PE.fr

Pôle emploi ouvre de nouvelles API régulièrement au regard des demandes de nouveaux partenaires. Les périmètres de données sont segmentés afin de garantir à chaque utilisateur que les données partagées par Pôle emploi vers le site d'un partenaire soient "juridiquement nécessaires". A titre d'exemple, Pôle emploi ne partage pas les adresses postales (API Coordonnées) des candidats pour l'accès à des services de cours en ligne car cela n'est pas indispensable pour consommer un service en ligne.

Ce dispositif s'inscrit dans une démarche d'OpenInnovation menée par Pôle emploi depuis plusieurs années. Cette démarche consiste à travailler avec tous les porteurs de projets dans le domaine de l'emploi et/ou de la formation professionnelle afin d'offrir de nouveaux services aux candidats et entreprises : à ce titre, Pôle emploi partage des données, incube des startups internes et externes, répond à toute sollicitation d'un offreur de service. Pôle emploi propose aussi de référencer tout service digital utile aux candidats et de les promouvoir vers les conseillers et candidats.

Dans cette démarche, Pôle emploi

- Accorde une place importante à la collaboration ouverte avec tous porteurs de projets qu'ils soient startups, grandes entreprises privées, collectivités territoriales, institutionnels, acteurs de l'emploi...
- Œuvre à la mise en place de consortiums (plusieurs entités différentes pour construire des projets difficilement réalisables de manière isolé)
- Veille à enrichir le panel des services proposés aux candidats et entreprises
- Personnaliser ses offres de services en direction des candidats et entreprises au regard des innovations du marché

STÉPHANE FRERE :

Stéphane Frere est DG Pôle emploi, Direction Expérience Utilisateur et Digital, Equipe OpenInnovation et Data. Ses spécialités sont l'OpenInnovation, l'accompagnement de startups internes et externes, l'IA et la Gouvernance des données afin développer l'intelligence collective.

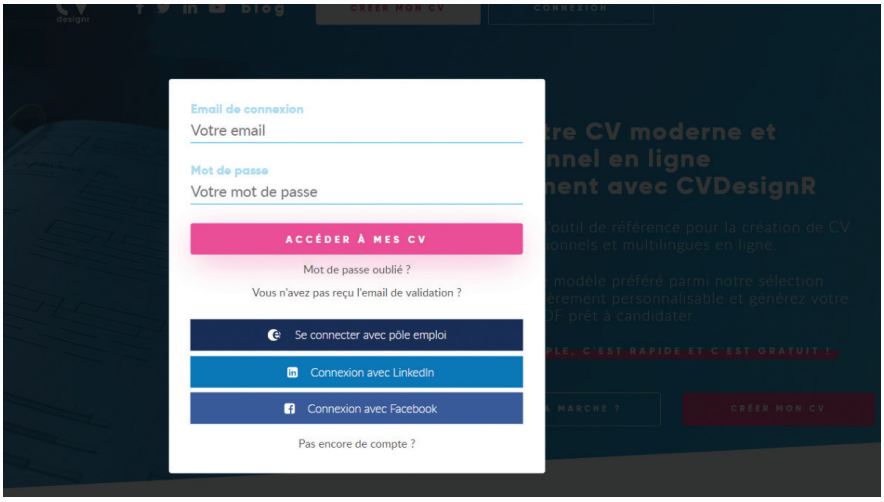
[76] Single Sign-On

b3. Cas d'usage en cours

Le cas CvdesignR :

Par Pôle Emploi

Zoom sur l'un des cas d'usages portabilité Pôle Emploi en lien avec les données liées aux CV :



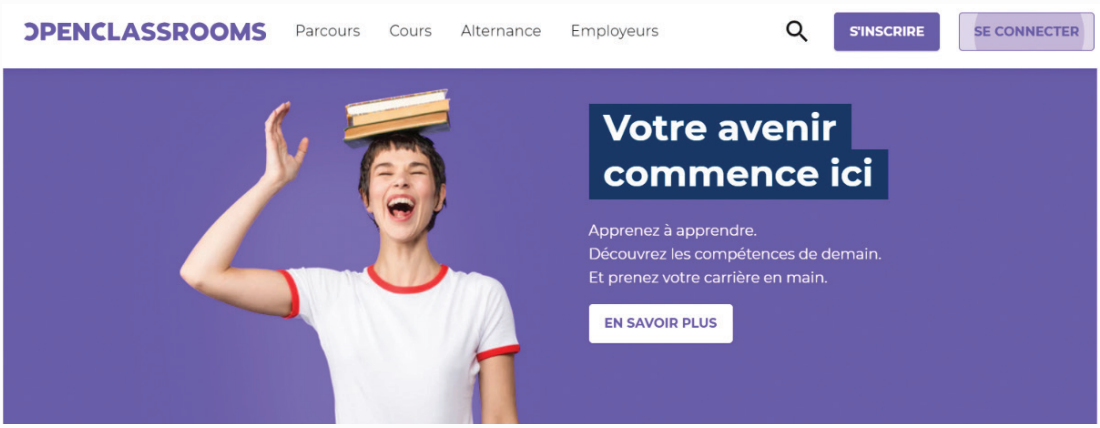
CvdesignR est un site spécialisé dans l'édition de CV proposant des modèles gratuits. C'est le service externe à Pôle emploi le plus sollicité par des candidats. Un service web, qui représente une forte audience soit 203 783 visiteurs uniques sur l'année 2017 et 23 812 sur le mois de mai 2018. Grâce à l'implémentation du bouton Se connecter avec Pôle emploi sur le site du partenaire, les candidats peuvent dupliquer les données CV déjà renseignées sur Pôle Emploi vers ce site. Ils économisent donc une double saisie et peuvent directement exploiter les fonctionnalités de mise en forme des CV proposées par CVDesignR.

Les avantages pour le partenaire sont nombreux :

- Faciliter la découverte du service par des candidats qui n'ont pas à se créer un nouveau compte
- Faciliter l'expérience des candidats en personnalisant le service au regard des données partagées (exemples : éviter les doubles saisies, bénéficier de données actualisées provenant de Pôle emploi à chaque connexion)
- Offrir de nouveaux services freemium ou adaptés au profil des candidats
- Bénéficier d'actions de communications de la part de Pôle emploi en direction des candidats qui pourraient être intéressés par le service d'un partenaire enrichi de cette fonctionnalité
- Ce dispositif est gratuit

Le cas OpenClassrooms

Par Pôle Emploi



OpenClassrooms est une école en ligne (MOOC) qui propose des cours certifiants (reconnus par l'état) et des parcours débouchant sur des métiers d'avenir, réalisés en interne, par des écoles, des universités, ou encore par des entreprises partenaires comme Microsoft ou IBM. La plateforme couvre des thématiques comme la programmation informatique, le marketing, l'entrepreneuriat et les sciences. Les utilisateurs du bouton " Se connecter avec Pôle emploi " qui sont identifiés comme inscrits en tant que Demandeurs d'emploi bénéficient d'un accès à toutes les formations. Si le statut de l'individu change au cours de la formation alors les formations débutées peuvent être achevées.

b4. Exemples de cas d'usage

Données portables	Cas d'usage
Parcours académique, historique professionnel, bulletins de salaire, niveau de langue, etc.	Je récupère mes données auprès de différents services pour enrichir plus facilement mon profil
Dossier de recherche d'emploi, type d'emploi recherché	Je transmets l'ensemble de mon dossier de recherche d'emploi facilement à de multiples sites

c. Se soigner

c1. Les enjeux

L'interopérabilité est déjà un sujet majeur pour l'industrie de la santé où il n'y a pas de débat sur son importance. **Le droit à portabilité pourrait améliorer directement les soins pour tous** en permettant aux individus de **faire circuler facilement leurs données entre les prestataires de soins, vers l'administration, ou vers le monde de la recherche.** En France (avec le DMP : Dossier Médical Partagé) et dans d'autres pays européens, les patients commencent à se voir proposé par leur administration des outils pour stocker et gérer leurs données médicales.

Aujourd'hui les informations collectées dans les centres de soin sont stockées de manière fragmentée et hétérogène, ce qui nuit à la prise en charge des patients et à la réutilisation de ces données pour la recherche. Un établissement hospitalier utilise un nombre important de logiciels médicaux, lesquels stockent des données cliniques et administratives dans des formats qu'ils ont eux-même définis. Ces formats diffèrent d'un logiciel à l'autre et ne sont connus que par leur éditeur, ce qui rend difficile tout partage de données entre les équipes médicales. Cela place l'hôpital dans une position inconfortable : il est propriétaire et responsable des données qu'il collecte mais il est dans l'incapacité technique d'accéder à ces données autrement qu'au travers du logiciel qui les a stockées.

Cette situation est préjudiciable à tous les niveaux :

- Les difficultés de communication entre services médicaux **nuisent à la cohérence du suivi des patients,** et leur font courir de graves danger lorsque l'historique de leurs antécédents, de leurs prescriptions ou de leurs allergies n'est pas accessible.
- La réutilisation des données collectées est très compliquée, et **les équipes de recherche doivent systématiquement effectuer un travail colossal de prétraitement et de mise en forme des données avant de pouvoir les analyser.**
- **L'hôpital est assujetti aux logiciels médicaux qu'il utilise :** il ne peut changer de prestataires sans perdre l'historique des données de ses patients.
- **Les droits des citoyens établis par le RGPD en matière d'effacement et de portabilité des données personnelles ne peuvent être garantis par les centres de soin.**

Ces dysfonctionnements pourraient être corrigés par une gestion consistante des bases de données de santé, c'est-à-dire en adoptant un standard commun intelligible par l'ensemble des acteurs. Cela rendrait aux centres de soin leur souveraineté vis-à-vis des données qu'ils collectent et fluidifierait le marché de l'informatique médicale, ce qui favoriserait l'innovation.

Un point d'attention est à noter du côté des utilisateurs qui identifient les données de santé comme les plus sensibles à faire circuler**. Les utilisateurs craignent de divulguer des informations sur leur état de santé qui pourraient leur porter préjudice** (vis à vis d'une banque, d'un assureur, etc.) sans s'en rendre compte. La peur de perte de contrôle est réelle et pourrait limiter les usages[77].

ARHLN :

Le projet Arkhn est né d'une volonté d'aider les centres de soin à mieux gérer les données de santé qu'ils manipulent. En tant que développeurs et data scientists, nous sommes particulièrement sensibles aux problématiques liées à l'interopérabilité des données, dont les enjeux sont cruciaux dans le domaine médical.

[77] Panels utilisateurs - CEREGE Université de Poitiers

Le standard FHIR

Un tel standard existe et fait déjà consensus : il s'agit du format FHIR[78] , développé par HL7 international ; son adoption au sein des hôpitaux français nécessite néanmoins une retranscription des bases de données existantes. C'est l'ambition du projet Arkhn[79], qui développe plusieurs outils open source visant à permettre cette transition. L'objectif est de comprendre l'architecture des bases de données de santé afin de pouvoir les réécrire au format FHIR. Ce travail de standardisation est effectué grâce à une plateforme collaborative, sur laquelle l'ensemble des membres partagent les cartographies qu'ils ont établies.

Lancé en septembre 2018, ce projet est soutenu par de nombreux acteurs du domaine de la santé. L'appui des services publics permettrait d'accélérer son développement.

[78] https://www.hl7.org/fhir/

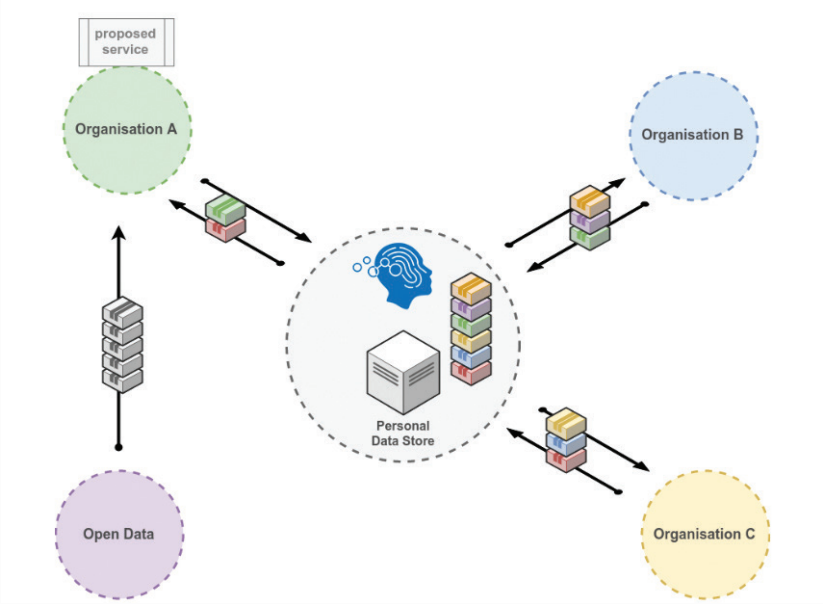
[79] https://arkhn.org

c3. Cas d'usage en cours

L'accompagnement des personnes atteintes de maladies chroniques

Le service envisagé par le PIMS Fair&Smart vise à améliorer l'accompagnement personnalisé des personnes atteintes de maladies chroniques. Pour éviter une communication manuelle fastidieuse de l'historique des données de santé nécessaires, le projet consiste à inviter les personnes à exercer leur droit à la portabilité auprès des différents responsables de traitement (ex : laboratoires d'analyses médicales) qui ont effectués des analyses pour elles. Il s'agit ensuite de convertir les données restituées dans un format pivot standard, d'extraire les résultats utiles, et les résultats utiles seulement, pour les envoyer de façon sécurisée au service d'accompagnement personnalisé. Un suivi individuel historisé plus clair peut alors être proposé, ainsi que des recommandations personnalisées en fonction des évolutions observées ou de facteurs environnementaux. Le projet croise donc des données personnelles analysées à partir d'un référentiel avec des données environnementales disponibles en open data ou via des API dédiées.

L'approche PDS avec transfert chiffré de bout-en-bout et recueil du consentement explicite intégré au parcours utilisateur a été validée et mise en œuvre selon le schéma suivant :



c4. Exemples de cas d'usage

Données portables	Cas d'usage
Historique des soins, prescriptions, allergies, etc.	je transmets mes données d'un soignant à un autre
Prescriptions, données administratives, etc.	je transmets mes données à mon employeur ou à mes organismes pour faciliter mes démarches (remboursements, déclaration maladie, etc.)
Historique des soins, prescriptions, allergies, etc.	je transmets mes données vers des laboratoires de recherche
Historique des soins, prescriptions, allergies, etc.	je transmets mes données vers un service d'aide à domicile automatisé

d. Gérer ses données d'éducation

d1. Les enjeux

La voie à suivre

Dans le secteur de l'éducation, l'importance de la portabilité automatisée des données est évidente depuis des décennies. Bien que le concept existe depuis un certain temps, les efforts à grande échelle visant à permettre la portabilité des données sont tout récents. Cette démarche est cependant confrontée à trois obstacles majeurs :

- Le manque de prise en compte des besoins de l'élève
- Le manque d'interopérabilité réelle des systèmes
- L'absence de normes au niveau des données elles-mêmes.

Les données personnelles d'éducation souffrent malheureusement d'un manque de définition. **Elles sont très diverses et englobent toutes les données de cursus, collectées lors du suivi d'un parcours de formation dans divers établissements. Elles recouvrent également toutes les données et traces créées par l'utilisation des moteurs de recherche, des sites de vidéo, etc. consultés lors de l'approfondissement d'un apprentissage, et au delà, celles qui sont créées en dehors du parcours de formation**, et qui peuvent être néanmoins être exploitées pour éclairer ce dernier.

Ces données sont aujourd'hui principalement utilisées à des fins administratives ou strictement dans le cadre prévu de leur collecte. Mais **une réutilisation plus large pourrait être d'une très grande valeur, notamment dans l'orientation et dans l'adaptation des apprentissages :**

- D'une part, **une approche « Big Data » de ces données permettrait de mieux déceler les forces et les difficultés de l'apprenant**, d'aider le professeur à adapter sa pédagogie et de mieux distribuer les ressources, de mieux orienter l'élève par rapport à des profils observés, etc.
- D'autre part, **la réutilisation par l'individu de ses propres données personnelles d'éducation, en dehors du cadre d'utilisation initial, lui permettrait d'éclairer son propre parcours tout au long de sa vie d'apprenant.**

Une telle réutilisation suppose cependant une maîtrise complète des données et une conscience des opportunités et risques. Faciliter l'accès aux données personnelles d'éducation **peut par exemple être source de discriminations.**

Aujourd'hui **les données personnelles d'éducation sont détenues par un grand nombre d'applications sur lesquelles les établissements et les apprenants ont trop rarement le contrôle.** Soit les applications sont choisies librement par les enseignants et donc **il existe peu de visibilité sur l'éparpillement de ces données,** ce qui rend leur réutilisation compliquée. Soit, les applications utilisées sont strictement encadrées, mais les contraintes externes ou logistiques en empêche l'usage plein et entier, comme c'est le cas pour beaucoup d'ENTs (Espaces numériques de travail) qui sont remis à zéro d'une année sur l'autre.

Au-delà de cet éparpillement de données, **le manque de connaissance du sujet et de conscientisation des enjeux, par les responsables de formation ou d'équipes pédagogiques, constituent les principaux freins dans le développement d'une démarche à la fois éthique et innovante.**

Le levier du droit à la portabilité peut être utilisé pour amorcer des initiatives de transfert et de réutilisations de données personnelles d'éducation.

Il s'agirait donc par exemple de mener des programmes dans les établissements pour permettre aux élèves ou étudiants de s'informer sur leurs données et de demander à exercer leur droit à la portabilité. Ces demandes pourraient ensuite servir de justification pour récupérer les données éparpillées et permettre leur réutilisation. Ces initiatives pourraient également servir d'opportunités de formation des équipes enseignantes aux enjeux des données personnelles d'éducation, ce qui est également une obligation du RGPD. Ces formations s'appuierait alors sur des exemples précis de cas d'usage de portabilité au service de l'élève, des parents, des enseignants et des établissements. Ainsi **le RGPD peut servir d'outil pour tous les pionniers de l'innovation en éducation** pour enclencher une démarche de réutilisation des données personnelles. Une fois la démarche initiée, **il est impératif de pouvoir dégager des standards et bonnes pratiques** diffusables pour facilement implémenter et diffuser la technique.

JB PIACENTINO :
JB Piacentino a dirigé la filiale française de la fondation Mozilla. En 2015, comme DG adjoint de Qwant, il développe en Qwant Junior, le moteur de recherche pour les 6-12 ans. Convaincu que les progrès des sciences humaines et de l'IA vont révolutionner l'éducation, il fonde EdTech One en 2019 pour conseiller les entreprises du secteur.

d2. Initiatives en cours

Il existe actuellement de nombreuses initiatives concernant la portabilité des données traitées dans le cadre éducatif. Toutes ces initiatives ont été lancées avant l'entrée en application du règlement général sur la protection des données (RGPD). Certaines des principales initiatives internationales visant à accroître la portabilité des données dans le contexte de l'éducation.

La déclaration de Groningue :

La déclaration de Groningue vise non seulement à éliminer progressivement les documents papier et les diplômes, mais aussi à accroître le partage et l'accès aux données sur les étudiants en assurant l'interopérabilité sémantique entre les systèmes. En avril 2012, neuf pays, dont les États-Unis, la Chine, l'Inde, la Russie et le Royaume-Uni, se sont réunis dans la ville de Groningue, aux Pays-Bas, pour signer la Déclaration de Groningue sur les dépôts de données numériques pour les étudiants. Depuis, de nombreux autres pays ont signé cette déclaration, dont la France et l'Australie. Selon les termes mêmes de la Déclaration, " le principe primordial est de rechercher la convergence plutôt que l'uniformité ".

Les signataires de la Déclaration de Groningue n'ont pas dicté aux membres la manière dont ils doivent numériser ou échanger les données sur les étudiants. Ils reconnaissent plutôt que de multiples cadres et modèles doivent être utilisés pour faire en sorte que les pays dotés de systèmes centralisés puissent communiquer et échanger des données avec les pays dotés de cadres distribués. Le travail des équipes du Réseau de la Déclaration de Groningue est un exemple de la façon dont la portabilité des données peut être réalisée dans d'autres industries. L'une des principales approches utilisées par le réseau de Groningue pour identifier les obstacles à l'échange de données dans le domaine de l'éducation est l'approche "pilote à petite échelle".

La Déclaration de Groningue représente la tentative la plus développée à ce jour pour mettre en place un cadre international complet pour la portabilité des données à tous les niveaux de l'enseignement, du primaire au secondaire et jusqu'à l'enseignement supérieur. Bien qu'il s'agisse du projet de portabilité des données le plus développé dans l'enseignement supérieur, le Réseau de la Déclaration de Groningue a encore beaucoup de travail à faire avant d'atteindre ses objectifs, à savoir faire de la portabilité automatique de données une réalité.

Le cas des Etats-Unis :

La NSC (National Student Clearinghouse) offre aux États-Unis une sélection de services axés sur l'échange de données et la vérification des titres de compétences. Les services fournis par le CNS comprennent la vérification de l'obtention du diplôme et de l'inscription ainsi que le libre-service des étudiants pour demander leurs relevés de notes. Le transfert sécurisé des relevés de notes est au cœur des services fournis par le NSC aux établissements américains. Une des premières tentatives de normalisation et d'automatisation du transfert de l'information sur les relevés de notes entre les collèges et les universités, le serveur SPEEDE (Standardization of Postsecondary Education Electronic Data Exchange), est maintenant également opéré par la NSC. Ce serveur utilise les protocoles FTPS (File Transfer Protocol Secure) et SFTP (SSH File Transfer Protocol) pour prendre en charge l'échange de données informatisé en utilisant des fichiers formatés ANSI. La NSC fournit une plateforme tierce qui permet de centraliser l'information sur le nombre d'étudiants qui ont terminé leurs études et le nombre d'inscriptions.

La plupart des services fournis par le NSC visent à fournir des preuves générales d'inscription et/ou d'obtention d'un diplôme. Bien que les écoles envoient au CNS des fichiers de données semestriels contenant des renseignements sur les élèves, le CNS ne donne pas accès aux données sur les élèves ni à des statistiques globales. Ainsi, les services de partage de données n'impliquent pas le transfert direct des données d'un système d'information à un autre ; dans la plupart des cas, l'information est au format PDF ou Word qui doit ensuite être traitée par l'institution destinataire. L'absence d'interopérabilité directe des systèmes constitue un obstacle majeur à la facilité de transfert des données des étudiants et à la portabilité.

Le cas de la France :

Beaucoup d'actions politiques ont été entreprises en France depuis 2018 pour fournir une orientation plus personnalisée vers l'enseignement supérieur pour les lycéens : la loi ORE (Orientation et réussite des étudiants) a introduit ParcourSup, une nouvelle plateforme publique d'orientation qui assigne les universités aux lycéens et, fin 2018, le gouvernement français a annoncé la création de ORISUP, une base de données regroupant toutes les données éducatives sur la population du primaire au supérieur afin d'échanger des données pour une orientation " Big Data ".

Le 16 janvier 2019, le Comité d'éthique de Parcoursup a publié un rapport présentant quelques faits intéressants sur l'avenir de l'orientation :

- La réalisation d'une orientation véritablement efficace au service des citoyens, les aidant à trouver leur véritable place dans la société, devra s'appuyer sur une approche " Big Data " et une recherche sur les données éducatives : infrastructures et bonnes pratiques doivent être construites pour permettre la réutilisation de ces données ;
- Aujourd'hui, il n'y a pas suffisamment de recherches effectuées à l'aide de données sur l'enseignement supérieur ;
- Les chercheurs ne sont pas au courant de toutes les données disponibles sur l'enseignement supérieur.

L'avenir de l'éducation, des nouvelles pratiques pédagogiques à une orientation plus personnalisée, réside donc dans la réutilisation des données éducatives qui, jusqu'à présent, n'ont été utilisées qu'à des fins administratives ou statistiques.

Un exemple tiré du cas d'utilisation de l'orientation aide à illustrer cette question : aujourd'hui, les diplômés des lycées français s'orientent grâce à leur intuition, quelques recherches sur internet et quelques heures, au mieux, passées avec un conseiller qui ne connaît pas assez la personne pour lui donner des conseils pertinents.

A l'avenir, un système (privé ou public) peut être imaginé comme ayant dans sa base de données tous les programmes d'enseignement supérieur possibles et faisant de l'apprentissage machine sur les données éducatives de millions d'étudiants de l'école primaire à l'enseignement supérieur. Cet algorithme sera formé pour déterminer à partir d'un profil quel domaine d'études et/ou de travail serait le mieux adapté pour l'étudiant en question. Il proposerait ensuite à l'étudiant une sélection d'universités et de cursus correspondant à son profil. Les résultats d'un tel système aideraient l'élève à avoir une discussion avec son conseiller d'orientation et l'aideraient à mieux se connaître.

TAYLOR BROOKS :

Taylor Brooks est originaire des États-Unis, il vit et travaille actuellement en France et compte près de 10 ans d'expérience dans le traitement de données. Responsable des données à l'Université Américaine de Paris, il s'intéresse à l'ensemble du cycle de vie des données, de la collecte à l'analyse, dans le secteur de l'éducation et au-delà.

L'adaptative learning pour une personnalisation des parcours pédagogiques :

Par Benjamin André - fondateur Cozy Cloud

Tout enfant qui entre dans le système éducatif arrive avec ses forces et ses lacunes : Le PIMS Cozy Cloud permet d'analyser ses difficultés de lecture, d'écriture ou de calcul et d'adapter ses exercices à ses besoins propres. Mais ces données sont extrêmement sensibles : elles concernent des mineurs qui ne sont pas en âge de consentir à l'utilisation de leurs données, elles en disent très long sur leur potentiel scolaire, et il est facile d'en tirer des prédictions qui pourraient aller contre l'intérêt de l'élève. Comment s'assurer qu'on ne décourage pas demain un élève dyslexique de se lancer dans une carrière de journaliste ?

Il ne fait guère de doute que l'IA de Linkedin finira par apprendre sur les données scolaires de Microsoft - et ce potentiellement sans même que Linkedin ne s'en rende compte - et fera ses recommandations sur la base d'informations personnelles renforçant la détermination statistique et ainsi la confortant au détriment de la nécessaire sérendipité sociale.

Dans Cozy Cloud les traces d'apprentissages restent sous le contrôle de l'utilisateur et l'algorithme d'adaptative learning accède localement aux données sans en envoyer aucune à l'extérieur. L'élève dispose ainsi de recommandations très personnalisées sur son parcours pédagogique – exercices, lectures, vidéos… - sans qu'aucune information sur ses faiblesses ne soit partagée avec qui que ce soit.

d4. Exemples de cas d'usage

Données portables	Cas d'usage
Diplômes, bulletins de note, formations, projets réalisés, etc.	je transmets les données de mon parcours scolaire à un service de recherche d'emploi / formation
Diplômes, bulletins de note, formations, projets réalisés, etc.	je transmets les données de mon parcours scolaire à un potentiel employeur
Diplômes, bulletins de note, formations	je transmets mes données à des outils d'adaptive learning qui s'adapteront à mes compétences et à mon niveau
Diplômes, données administratives	je récupère et transmets mes données administratives pour faciliter mes démarches

e. Acheter

e1. Les enjeux

L'industrie du commerce de détail est aujourd'hui sous pression. **De nouveaux modèles comme Amazon ont bousculé le marché.** Pour une grande majorité des détaillants, les données clients sont essentielles. **La libre circulation des données personnelles pourrait permettre aux détaillants de rattraper leur retard.** Par exemple, grâce à la libre circulation des données, les détaillants peuvent développer leur offre de produits en liant l'usage alimentaire à la santé et au bien-être. A ce sujet, la grande distribution ne semble pas avoir suffisamment anticipé sa réflexion stratégiques et les investissements nécessaires.

Dans le secteur de la distribution, ce qu'il s'agirait de rendre portable en premier lieu, c'est probablement la liste de produits du ticket de caisse ou du panier e-commerce. Evidemment le sujet est très sensible. Que l'on puisse aisément récupérer l'ensemble de ses actes d'achats, détenu par une enseigne, pour solliciter les offres d'enseignes concurrentes, voilà un scénario qui ne manque pas d'interpeller les acteurs de la distribution et du e-commerce.

Mais le droit à la portabilité induit également d'importants scénarios de complémentarité entre services. Par exemple le service Yuka, qui scanne les produits alimentaires pour proposer des conseils santé, est déjà dans la poche de millions d'utilisateurs, alors qu'il est pourtant quelque peu rébarbatif, pour le consommateur, de flasher manuellement ses codes-barres en faisant ses courses ou à la maison. **La portabilité du ticket de caisse constituerait un accélérateur au développement de tout un écosystème de services numériques** mêlant coaching diététique, planification des repas, élaboration de recettes et consommation éthique/responsable. Ces services d'aide à la consommation ont besoin pour se développer, d'opérer dans un contexte trans-enseignes pour coller aux modes de consommation actuels.

Le droit à la Portabilité des données peut ainsi devenir le bras armé d'un consommateur cherchant à orienter et maîtriser sa consommation, à la rendre conforme à ses choix de vie.

STÉPHANE CREN :
Stéphane Cren est Head of Innovation, GS1 France, créateur de standards et de communs numériques dans les domaines de la logistique et de l'information produits.

Les acteurs de la distribution traditionnelle :

Comme dans beaucoup d'autres industries, il est essentiel de mieux connaître les attentes individuelles de chaque client ou consommateur. Grâce à une meilleure connaissance client, les marques de retail peuvent réimaginer l'ensemble de la chaîne de création de valeur. Par exemple, ces informations peuvent aider à la conception des produits, à leur assortiment local, à leur bon niveau de stock, au développement et à la mise en place de services adaptées. En d'autres termes, elles peuvent adapter leur promesse client et optimiser leurs opérations. Avec une personnalisation efficace, les clients gagnent du temps et sont alors plus proches des marques. Ils se sentent compris et ainsi une relation de confiance s'instaure ou se renforce. Il y a autant de raisons qui expliquent que les données d'aujourd'hui vont aider à créer le retail de demain.

Le problème majeur pour les distributeurs traditionnels aujourd'hui tient à la difficulté à reconnaître leurs clients et/ou bien les connaître. Il existe une forme d'inégalité d'informations entre les nouveaux écosystèmes puissants (type Amazon) et les entreprises de retail indépendantes plus traditionnelles.

Une interopérabilité simple et redonnant la main aux clients, pourrait à terme venir équilibrer le rapport de force. Les informations utiles et nouvelles que les clients accepteraient de mettre à disposition des enseignes, par la portabilité, pourraient aider les marques à répondre à ces nouveaux enjeux. Il n'existe malheureusement pas de standard d'interopérabilité à date. Avec certaines entreprises de la famille Mulliez, nous sommes en train de développer un système interne qui pourra avoir vocation à s'ouvrir aux clients et donc indirectement à d'autres sociétés.

JULIEN DERVILLE :

Julien Derville anime Valiuz, une plateforme de données multi-entreprises, qui vise à améliorer l'expérience client. Julien est le co-fondateur de ZTP, véhicule d'innovation et d'investissement au service de la performance des entreprises et particulièrement au sein de la famille Mulliez.

e3. Exemples de cas d'usage :

Données portables	Cas d'usage
Historiques d'achat, préférences, habitudes allergies, etc.	je transmets les données de mes achats alimentaires à des services de régime, coach santé, recettes, analyse de mon alimentation (bio, allergènes, sans gluten), etc.
Historiques d'achat	je transmets mes achats habillement vers des plateformes de revente entre particulier (achats mode, achats enfants, etc.)
Historiques d'achat	je transmets mes données de consommation à des services me permettant de calculer mon empreinte carbone ou de mesurer mon impact environnemental
Données fidélité	je transmets mes données fidélité d'une enseigne à une autre pour bénéficier de programmes croisés

f. Gérer ses finances et ses assurances

f1. Les enjeux

Les banques sont certainement l'industrie la plus mûre en ce qui concerne le RGPD et la portabilité. L'exploitation des données est au coeur des métiers de la banque depuis de nombreuses années et, outre la mise en conformité au RGPD, les banques doivent depuis peu se conformer à la directive DSP2[80] qui leur demande d'ouvrir leurs données, notamment aux nouveaux entrants (les startups de la Fintech) en fournissant des moyens d'accéder à leurs données. **Les banques jouent déjà en partie le rôle de tiers de confiance pour leurs clients,** elles gèrent leur argent, sont extrêmement régulées et contrôlées et sont reconnues pour leur capacité à sécuriser leurs systèmes d'information. Elles pourraient largement bénéficier de la portabilité pour proposer de multiples usages à leurs clients :

- standardiser les échanges de données lors d'un changement de banque du client
- simplifier toutes les démarches du client en lui permettant d'importer facilement des données
- assurer plus simplement le KYC réglementaire (Know Your Customer)
- enrichir l'expérience du client et lui proposer de nouveaux usages liés à tous les aspects de sa vie courante (projet d'achat voiture, projet immobilier, etc.)

L'utilisation des données est au coeur de la révolution en cours dans le secteur des assurances. La portabilité permettraient aux assureurs de simplifier la déclaration de sinistres et l'inventaire des biens, ou de suivre les usages afin de proposer des couvertures adaptées (voyage, covoiturage, etc.). Les offres d'assurance reposant également en grande partie sur l'analyse des usages, **les assureurs seraient en mesure de proposer des approches très individualisées,** ce qui bousculerait le modèle mutualiste. Des acteurs importants du secteur ont déjà développé des offres de ce type dans l'assurance automobile, dans le cadre défini par la CNIL[81]. **Le risque potentiel serait de voir certains clients exclus** ou subir d'importantes majorations suite à une analyse détaillée de leurs données. C'est pour cette raison que les autorités de contrôle concernées par la protection des données restent vigilantes.

---

[80] Directive sur les Services de Paiement

[81] https://www.cnil.fr/sites/default/files/atoms/files/pack_vehicules_connectes_web.pdf

f2. Initiatives en cours

Service d'aide à la mobilité bancaire :

Ce service a vocation à assister tout client lors de sa démarche de changement de banque en confiant à sa nouvelle banque le soin de transmettre sa nouvelle domiciliation bancaire auprès des différents organismes prélevant son compte ou réalisant des virements sur ce dernier. Ce service, rendu obligatoire par la loi française, n'a pour autant pas fait l'objet d'implémentations innovantes par les acteurs concernés (les banques) qui y voyaient surtout une contrainte et un coût, plus qu'une opportunité de renforcer sa compétitivité métier.

DSP2 (Directive des Services de paiements) :

La DSP2, entrée en vigueur dans l'ensemble des états membres de l'Union Européenne le 13 Janvier 2018, est une réglementation européenne visant à améliorer la sécurité des utilisateurs de services de paiement et à stimuler l'innovation par une ouverture élargie à la concurrence, en particulier les nouveaux entrants de type startups Fintech.

Concrètement, de nouveaux rôles sont créés (AISP: Account Information Service Provider / PISP: Payment Initiation Service Provider) que des acteurs non limités aux banques traditionnelles peuvent endosser pour proposer de nouveaux services en utilisant les dernières technologies numériques. Les services de finances personnelles tels que l'agrégation de compte ou la gestion de budget sont des exemples de ces nouveaux services.

Un premier cadre de standardisation est fixé au travers des RTS (Regulatory Technical Standards). Ce document, qui se concentre principalement sur la gestion de l'authentification de l'utilisateur et les exigences techniques de communication entre les acteurs, est d'un niveau de détail qui ne permet pas de statuer sur tous les points sur lesquels un effort de standardisation est nécessaire pour atteindre les objectifs fixés. En conséquence, plusieurs standards de spécification détaillée des APIs ont émergé. On peut notamment citer l'Open Banking de OBIE[82], celui du Berlin Group (NextGenDSP2) ou encore celui de la STET.

Au delà de multiples spécifications détaillées, on voit apparaître des problématiques de sécurité et de parcours utilisateur DSP2 sur lesquelles un effort de gouvernance et de standardisation pourrait apporter des éléments de réponse adaptés:

- La protection des données des comptes bancaires repose sur la bonne identification de l'utilisateur. Or la diversité des "identités numériques" (correspondant aux différents comptes d'un utilisateur) d'un utilisateur et leur cloisonnement en terme d'usage ne favorise pas l'émergence d'une identité numérique forte permettant aux différents acteurs DSP2 d'identifier de manière homogène un utilisateur. Pourtant certaines ouvertures existent. On peut notamment citer la plateforme France Connect.
- Le manque de standards d'authentification renforcée amène les acteurs bancaires à développer des moyens d'authentification dont le côté propriétaire nuit à l'expérience utilisateur et donc à son potentiel d'adoption. Par exemple, un utilisateur d'un service d'agrégation de compte client de 3 banques pourra se voir infliger 3 authentifications distinctes (et différentes) tous les 90 jours afin

de pouvoir accéder au service d'agrégation. Là encore, des standards émergent, comme le standard FIDO, encore faut-il que les acteurs de la place l'étudient et aient une position concertée par rapport à l'usage de ce dernier dans leurs services et applications.

Ainsi, la DSP2, en tant que première initiative du secteur promouvant la bonne circulation de certaines données personnelles de l'utilisateur, démontre la nécessité, dans les premiers stades de sa mise en oeuvre, d'une gouvernance et de standards afin de traiter des sujets de place (c'est à dire qui dépassent la stratégie de chaque acteur concerné par la DSP2) et des sujets critiques (sécurité, parcours client) pour atteindre les objectifs fixés (des services bancaires innovants et sécurisés).

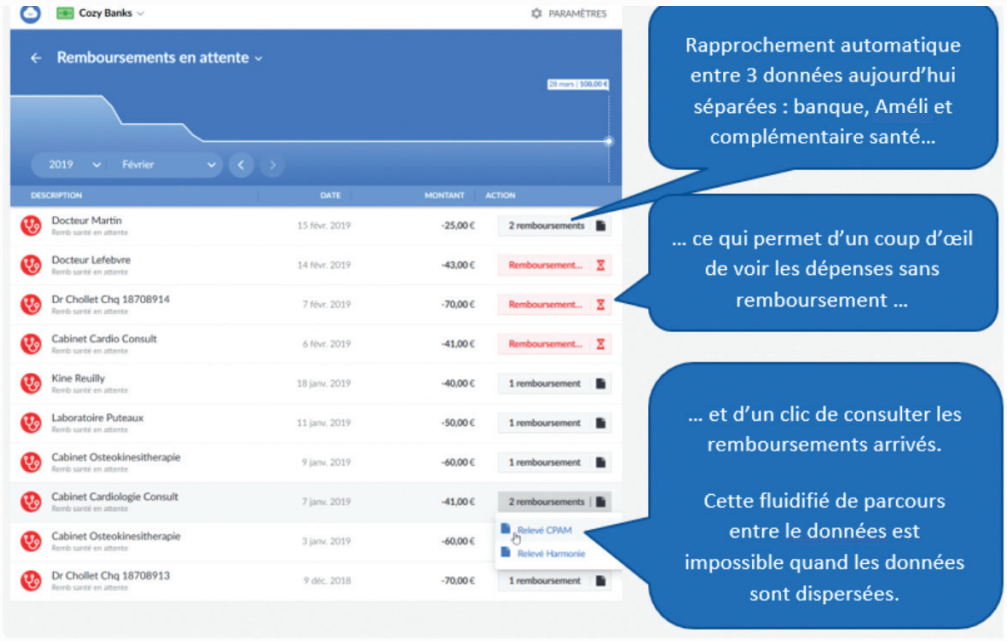
MÉDERIC COLLAS :
Médéric Collas est responsable du pôle innovation sécurité au sein du Centre d'Expertise en Sécurité Métier du groupe BPCE. Il est spécialiste en architecture d'entreprise, industrialisation logicielle, et sécurité métier banque.

[82] Open Banking Implementation Entity

f3. Cas d'usage en cours

Le suivi des remboursements des dépenses de santé Cozy Cloud

Le suivi des remboursements de santé implique généralement la connexion de nombreux sites (caisse primaire d'assurance maladie, assureur de complémentaire santé, et banque), avec 3 mots de passe différents à gérer. Aussi le service de PIMS Cozy Cloud apporte un réel intérêt, en centralisant les flux de données, et la visualisation de celles-ci.



f4. Exemple de cas d'usage

Données portables	Cas d'usage
Factures, garanties	je récupère les factures / garanties de mes commerçants afin d'enrichir mon compte bancaire (affichage plus clair, données plus facile à retrouver).
Factures, garanties	je récupère les données détaillées de mes commerçants pour évaluer mes biens en cas de sinistre ou pour vérifier mon niveau de couverture
Données administratives, identification	je récupère mes données administratives auprès de mon administration pour faciliter mes démarches (KYC, ouverture de compte, demande de prêt)
Données bancaires	je transmets mes données à un service de coach financier ou un agrégateur

g. Gérer son administration

g1. Les enjeux

La portabilité est un aspect clé de la modernisation de systèmes d'information des services publics. Elle permet de simplifier l'ensemble des démarches administratives des citoyens et peut créer de nombreux ponts avec la sphère privée pour permettr la vie des utilisateurs dans leur vie de tous les jours (banque, assurance, voyages, etc.).

Un Etat peut également être légitime à se présenter comme fournisseur d'une identité numérique unifiée auprès de ses citoyens qui pourront alors porter et réutiliser ces identités dans de nombreux services. L'Estonie est en pointe sur cette question où la carte d'identité électronique fournie par l'Etat a été adoptée par la quasi-totalité de la population.

La difficulté pour certains Etats est de **concilier cette démarche novatrice avec des systèmes d'information très hétérogènes et souvent vieillissants.**

Certains Etats n'ont également pas la possibilité de créer une base de données unique pour l'ensemble de leurs services, augmentant la complexité technique de la tâche. Des outils PIMS permettant de centraliser le contrôle des données dans les mains des individus tout en laissant les données décentralisées peuvent représenter une bonne approche pour cette question.

France Connect

L'initiative France Connect, est la plateforme d'identité numérique supportée par l'Etat français pour l'ensemble des services de son administration. La plateforme vise au départ à accélérer la digitalisation du service public en offrant aux citoyens une capacité d'identification/authentification auprès de plusieurs services de l'administration en utilisant un seul compte en ligne (par exemple celui des impôts). France Connect permet à une administration jouant le rôle de fournisseur de services de récupérer une identité certifiée composée de 6 champs (l'identité pivot) auprès d'une autre administration jouant le rôle de fournisseur d'identité via des échanges basés sur le protocole standard Open ID Connect et un enchaînement d'écrans permettant d'informer clairement l'utilisateur final sur le transfert de ses données.

Depuis novembre 2018, et dans le cadre des travaux EIDAS[83], l'usage de France Connect est élargi à certains fournisseurs de services privés qui peuvent bénéficier d'une identité numérique certifiée et, à terme, de mécanismes d'authentification substantiels et/ou élevés de leurs utilisateurs pour leurs services en ligne. Plusieurs acteurs ont testé ou mis en œuvre l'intégration de France Connect dans un objectif de simplification des parcours utilisateurs et de renforcement de la sécurité de leurs services en ligne. A noter que dans le cadre de ces travaux d'ouverture à la sphère privée, l'écran France Connect informant l'utilisateur de tout échange de ses données d'identité numérique entre deux acteurs évolue pour implémenter un écran de consentement permettant à l'utilisateur de fournir un consentement éclairé sur tout transfert à un tiers de ses données d'identité numérique. Au-delà d'assurer la portabilité d'une identité pivot, France Connect permet à un fournisseur de données de partager les données qu'il détient sur un individu à un fournisseur de services, là encore en assurant l'ensemble de la mécanique d'identification/authentification de l'utilisateur final et le recueil de son consentement éclairé sur le transfert. Dans ce dernier le cas, le périmètre des données concernées est donc totalement ouvert et non limité à l'identité pivot. En revanche, l'ouverture actuelle de France Connect à la sphère privée n'intègre pas cette fonctionnalité qui reste à date à l'usage exclusif des administrations et du secteur public.

En synthèse France Connect est un exemple important d'implémentation d'une portabilité de données personnelles. Par ailleurs sa finalité (identification/authentification renforcée des citoyens français auprès d'un écosystème de fournisseurs de services élargi) et sa contribution à la feuille de route européenne en matière de digitalisation (EIDAS) en font un élément très intéressant pour permettre la mise en œuvre d'une portabilité des données personnelles sécurisée et standardisée.

[83] Electronic IDentification, Authentication and trust Services

g3. Exemples de cas d'usage

Données portables	Cas d'usage
Données administratives	je transmets mes données d'un service de l'administration à un autre pour ne plus avoir à ressaisir d'information
Données administratives	je transmets mes données vers des services tiers privés (Banque, services transport/mobilité, assurance, retail, automobile, etc.) pour faciliter mes démarches
Données administratives	je récupère mes données depuis des services tiers privés (Banque, services transport/mobilité, assurance, retail, automobile, etc.) pour faciliter mes démarches

i. Télécommunication

La « Data Portability Cooperation », l'initiative de portabilité des données télécom

Trois grands opérateurs Européens ont annoncé en 2018 travailler à la définition d'un modèle de portabilité des données : l'initiative, appelée « Data Portability Cooperation », vise à analyser l'implémentation de la portabilité des données de manière à créer de la valeur pour l'utilisateur final tout en assurant la protection de sa vie privée. Elle est gérée au sein de la GSM Association et ouverte à l'ensemble des opérateurs qui souhaite la rejoindre. Promue tout particulièrement par Telefónica, Orange et Deutsche Telekom, l'initiative a annoncé lors du Mobile World Congress de février 2019 la publication d'un livre blanc et d'un premier draft de spécification technique (disponible à l'adresse www.dataportabilitycooperation.org).

La Data Portability Cooperation travaille dans une démarche de test et d'apprentissage, la première étape ayant été de produire une vision commune de la portabilité répondant aux besoins du RGPD : la spécification publique propose un premier contour de données du monde télécom (qu'il soit fixe ou mobile) et un format conforme aux standards du marché. Ce format étant extensible, les données personnelles à inclure sont au libre choix de l'opérateur, en fonction de ses capacités techniques, de ses spécificités, etc.

Afin d'étudier les modalités de parcours utilisateur, Orange et Telefónica ont proposé une démonstration pendant le Mobile World Congress, illustrant le transfert de données entre les deux opérateurs. Plusieurs points d'attention sont encore en cours d'étude afin de pouvoir notamment proposer un protocole. Quelques éléments sont particulièrement sensibles : un mécanisme de type « Pull », initié par le client via le responsable cible, pourrait encourager le « phishing », tandis qu'un mécanisme de type « Push », initié via l'espace client du responsable de traitement, complique l'intégration.

Le format proposé est adapté à la fois au mode de téléchargement par l'utilisateur et au mode de transfert entre responsable de traitement. Afin de renforcer la sécurité il est bien entendu possible de proposer une authentification forte à deux facteurs via Mobile Connect, déjà proposé par un grand nombre d'opérateurs mobile.
L'initiative encourage l'ensemble des opérateurs à la rejoindre, mais aussi au-delà de la GSMA que les différents secteurs industriels s'emparent des principes fondateurs et même de la proposition de spécification afin de créer un modèle pérenne de partage sécurisé des données et ainsi faciliter l'innovation et l'émergence de nouveaux services.

Fabien Venries :
Est responsable marketing au Technocentre du groupe Orange. Depuis 2015 il contribue à faciliter l'implémentation de la protection des données auprès des différentes filiales du groupe mais aussi auprès des organismes de normalisations ou des consortiums tels que le TM Forum et des groupes de travail tels que la Fing. En 2018 il lance avec Telefonica et Deutsche Telekom la « Data Portability Cooperation » à la GSM Association.

i. Autres usages

De très nombreux autres usages dans des domaines variés peuvent également être envisagés pour la portabilité :

- La consultation et le partage de contenus multimédias (contenus audios et musicaux, filmographiques, livres numériques, visites de musées et lieux de loisir ...) ;
- La gestion des données des ressources humaines ;
- La maîtrise fine de sa consommation eau / gaz / électricité, avec l'utilisation d'appareils communicants ;
- Les démarches notariales ;
- Le partage de données avec le monde de la recherche sociétale ou commerciale ;

La plupart des usages de la portabilité n'ont pas encore été imaginés.

Conclusion Partie A

Le nouveau droit à la portabilité du RGPD peut devenir le déclencheur d'une transformation radicale de l'économie en offrant aux individus la libre circulation de leurs données personnelles sous leur contrôle. La portabilité promet un marché plus fluide et plus concurrentiel, et elle est dans le même temps vectrice de très nombreuses innovations et de nouveaux usages dans tous les domaines (mobilité, emploi, santé, finance, commerce, éducation, administration, etc.). La portabilité permettra enfin de développer une approche éthique et efficace de la technologie et des services dans le cadre de l'avènement prochain de l'Intelligence artificielle.

Les outils PIMS se posent en facilitateurs de ce nouveau marché. Ils proposent une nouvelle architecture de la donnée plaçant l'individu au centre. Les PIMS offrent du contrôle à l'utilisateur tout en rendant la portabilité accessible économiquement et technologiquement pour toutes les organisations (entreprises, administrations, etc.) qui souhaitent la mettre en oeuvre.

Cependant de nombreux défis technologiques, juridiques, économiques et de design. restent encore à relever. Un travail de coordination d'une ampleur inédite entre tous les acteurs (économiques, institutionnels, utilisateurs, associatifs et académiques) est aujourd'hui nécessaire pour proposer des réponses cohérentes à tous ces défis. La création de standards technologiques et d'une gouvernance adaptée est plus nécessaire que jamais.

Enfin la portabilité, et la circulation des données qui en découle, ne sont pas envisageables si nous ne créons pas un cadre de confiance vis à vis des individus et entre les organisations qui s'échangent des données personnelles. Ce sont les points que nous allons aborder dans la suite de ce document.

B/ REDONNER CONFIANCE AUX INDIVIDUS

Matthias De Bièvre :

Matthias De Bièvre est le fondateur et Président de Visions. Matthias a coordonné la partie B mettant en avant l'état de l'art de la recherche grâce aux travaux de nombreux experts et chercheurs mobilisés pour ce Livre Blanc. Visions édite le logiciel VisionsTrust qui permet aux organisations de facilement gérer les droits des personnes sur leurs données.

Son but est de démarquer les organisations vertueuses par la transparence offerte sur les données personnelles et la simplicité du contrôle. Redonner contrôle à chacun sur ses données personnelles est sa mission et la condition d'une innovation éthique et pérenne. Il s'intéresse et agit pour la mutualisation des données au service de la data science, notamment en éducation. Matthias est également conférencier sur l'éthique dans la data science dans plusieurs universités françaises.

Architectures respectueuses de la vie privée :

Dans cette partie, via deux articles de deux structures privées différentes, nous explorons des nouvelles architectures pour les applications qui utilisent des données personnelles. L'objectif de ces nouvelles architectures techniques est de rendre extrêmement compliqué voir impossible pour l'application d'accéder aux données personnelles sans l'autorisation de la personne concernée.

Différents choix sont abordés :

Ces différentes propositions permettent d'ouvrir une réflexion sur un rééquilibrage des pouvoirs d'accès aux données personnelles et ainsi redonner confiance en redonnant à l'individu le pouvoir de choisir qui a accès à ses données personnelles. La partie suivante se concentrera sur les techniques et outils pour assurer que l'application (ou les applications) soient limitées dans l'utilisation qu'elles peuvent faire des données une fois qu'elles y ont accès.

1. Des nouvelles architectures respectueuses de la vie privée :
a. Cas Qwant

Pour répondre au dilemme : assurer la protection de la vie privée et une personnalisation des services, l'architecture Masq de Qwant propose de stocker les données chez le navigateur du client. Cet article détaille les choix techniques et les limites.

Masq :

Né il y plus de 30 ans, le Web a ouvert la voie à une quantité considérable de connaissances mais a aussi malheureusement permis les nombreuses dérives que l'on connaît aujourd'hui : intrusion dans la vie privée, collecte des données personnelles utilisées à des fins publicitaires, reventes de ces informations à des tiers sans contrôle, vols de données etc... En cause ? l'architecture actuelle du Web, où les serveurs sont au centre de tous les échanges de données et où les entreprises fournissant les services en ligne ont une incitation économique (leur business model) les poussant à accumuler les données et à les analyser en vue, le plus souvent, d'afficher de la publicité ciblée.

A contrario, le respect de la vie privée des utilisateurs est au cœur des valeurs et du projet de Qwant. En leur permettant de reprendre le contrôle sur leur vie numérique, en leur laissant la maîtrise totale de leurs données, Qwant souhaite préserver du mieux possible ses utilisateurs. Pour cela, Qwant évite autant que possible le stockage de données personnelles sur ses serveurs. Toutefois, certains développeurs d'applications web souhaitent pouvoir stocker des données afin d'améliorer l'expérience utilisateur de leurs services, que ce soit des historiques de recherche ou des préférences par exemple.

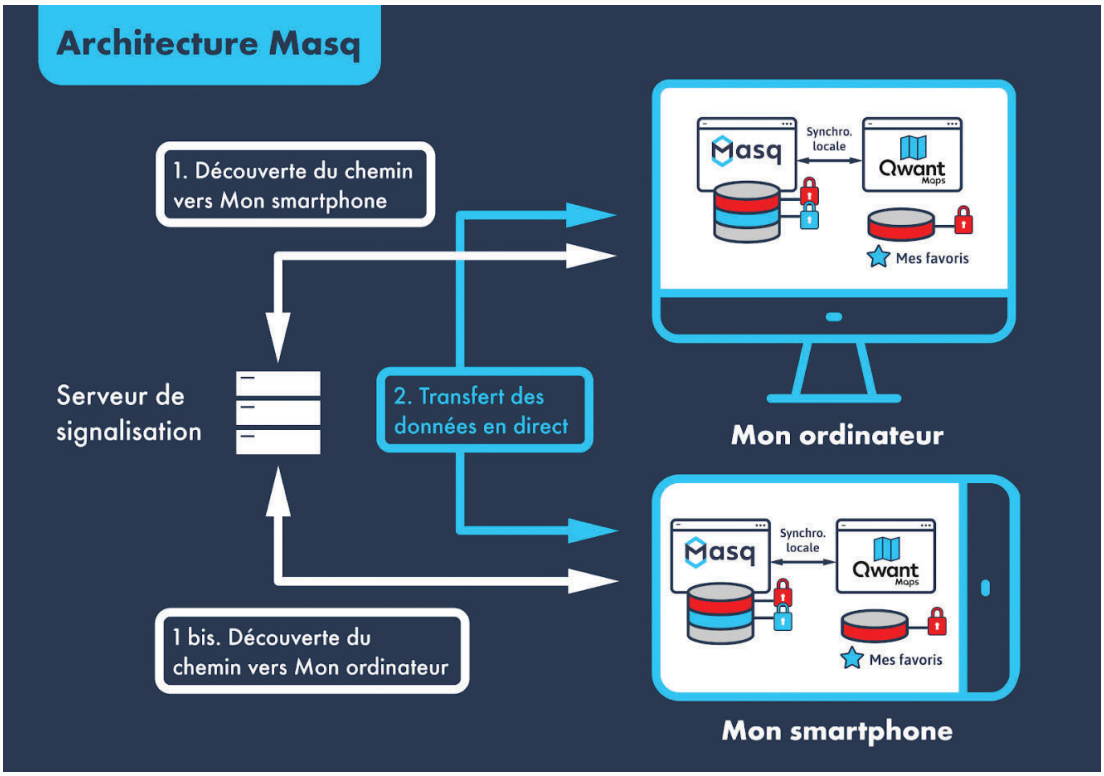
Aujourd'hui, de nombreuses applications utilisent les prétextes d'amélioration de leurs services et/ou de personnalisation de contenu pour justifier la collecte davantage de données, et ainsi établir un profil d'utilisateur toujours plus précis, ce que Qwant se refuse à faire.
Ce principe posé, plusieurs interrogations fondamentales surgissent :
Comment apporter aux utilisateurs un service personnalisé en s'abstenant de toute captation de données personnelles ?
Comment imaginer une solution de stockage de données pour améliorer les services des applications web, en ne stockant aucune donnée personnelle sur des serveurs ? En l'absence de serveur, comment faire en sorte que l'utilisateur puisse retrouver ses données sur différents appareils ?

La solution Masq :

Pour répondre à cette problématique, Qwant a lancé le projet Masq. L'idée est de permettre aux développeurs d'applications web de stocker des données qui ne quitteront pas l'appareil de l'utilisateur. Ainsi, Masq permet au fournisseur de service de s'abstraire de la gestion de compte utilisateur, et propose une interface de programmation pour stocker et récupérer des données de manière sécurisée.

Masq propose d'une part une bibliothèque JavaScript aux développeurs pour intégrer leurs applications avec Masq. D'autre part, l'application Web Masq permet à l'utilisateur de créer son profil, d'autoriser de nouvelles applications, ou de supprimer des données existantes. Elle lui permet également de synchroniser

ses données avec d'autres appareils de manière transparente.



Choix techniques :

Dans un souci de simplicité d'utilisation et d'adoption, Qwant a choisi de proposer l'application Masq sous la forme d'une application Web. Celle-ci est "serverless", il n'y a donc aucune logique serveur. Tout le code s'exécute uniquement sur le navigateur du client. En contrepartie, l'équipe Masq sera limitée par les technologies et interfaces de programmation disponibles sur les différents navigateurs.

Stockages :

Les navigateurs proposent deux interfaces de programmation pour stocker des données appelées "localStorage" et "IndexedDB". Masq utilise IndexedDB qui, contrairement à localStorage, propose une capacité de stockage plus élevée, permettant d'exploiter au minimum plusieurs centaines de mégaoctets.

Par défaut, ces données stockées par les applications web dans les navigateurs peuvent être supprimées si l'espace libre sur le support de stockage devient limité. Il est toutefois possible de demander à l'utilisateur d'autoriser le stockage persistant des données. Masq peut ainsi stocker des données qui ne seront pas supprimées sans action explicite de la part de l'utilisateur.

Sécurité :

Toute nouvelle demande de connexion à Masq par une application doit être confirmée par l'utilisateur ce qui assure, de fait, la protection des données de l'utilisateur.

Grâce à un mot de passe et une gestion robuste des clés de chiffrement, l'intégralité des données est chiffrée. Ainsi, même en cas de vol de l'appareil, un attaquant ne pourra voir le contenu enregistré dans Masq.
En outre, chaque application utilisant la bibliothèque de programmation de Masq peut écrire et lire uniquement dans son propre espace de stockage. Elle n'a pas accès aux données des autres applications. Cependant, l'équipe Masq réfléchit à une solution pour autoriser, sur demande de l'utilisateur, à partager les données d'une application avec une autre.

Synchronisation des données :

Masq permet de synchroniser les données de l'utilisateur entre ses différents appareils. Pour échanger les données sans serveur, il est nécessaire d'établir une connexion directe entre les différentes instances de Masq. Pour ce faire, Masq utilise WebRTC, une technologie qui permet d›établir une communication en temps réel entre deux navigateurs.
Autrement dit, les données sont envoyées de bout en bout sans intermédiaire. Une fois la connexion directe établie, les appareils synchronisent en temps réel les données stockées par Masq (voir les deux étapes sur le schéma d'architecture.

Un projet open source :

Masq est un projet open source qui compte sur des contributions extérieures dans le futur.
Nous utilisons et contribuons à des projets open source :

- hyperdb (https://github.com/mafintosh/hyperdb) est une base de données clé-valeur "scalable", fonctionnant dans un environnement décentralisé. Hyperdb permet d'avoir une même base de données synchronisée sur différents appareils.
- random-access-idb (https://github.com/substack/random-access-idb) est la couche permettant à hyperdb de stocker des données dans le navigateur en utilisant "IndexedDB".
- signalhubws (https://github.com/soyuka/signalhubws) permet à deux appareils de découvrir comment établir une communication en pair à pair.
- webrtc-swarm (https://github.com/mafintosh/webrtc-swarm/) permet de créer un réseau de plusieurs pairs avec WebRTC. Elle est utilisée pour que les différents appareils se synchronisent, mais également pour qu'une application demande l'accès à Masq.

Les limites :

Étant donné qu'aucun serveur ne stocke les données, les appareils sur lesquels Masq est utilisé ne peuvent de facto s'échanger des données seulement lorsqu'ils sont simultanément connectés à internet. On notera que les smartphones sont très souvent en ligne, ce qui fait que le téléphone peut être considéré comme une instance de Masq presque toujours active.

Masq est une solution qui offre au développeur la possibilité de stocker les données des utilisateurs. En revanche, ce dernier reste et restera toujours responsable de la bonne utilisation des données. Masq ne

peut se porter garant du développeur et assurer qu'il n'enverra pas les données stockées de son application vers ses propres serveurs ou des serveurs tiers. Cependant, l'utilisateur conserve le contrôle et peut à tout moment refuser l'utilisation de Masq à une application.

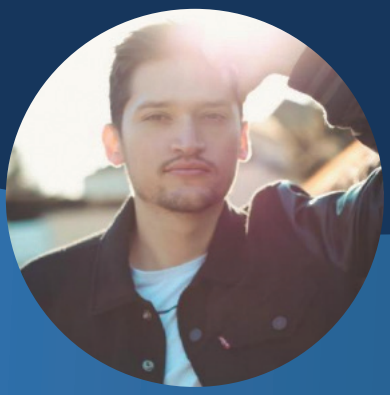
Conclusion :

Pour le développeur, Masq propose une solution de stockage des données de l'utilisateur dans un espace sécurisé et synchronisé sur ses différents appareils. Cela permet de proposer un service personnalisé tout en évitant de manipuler des données sur des serveurs. Il est ainsi possible de déployer des applications statiques, sans aucun serveur, tout en profitant d'une synchronisation de données sur plusieurs appareils. Masq est donc, de facto, totalement aligné avec les standards du RGPD, et l'équipe projet travaille sans compter pour satisfaire tous les usages. Pour conclure, ce projet constitue un premier pas vers un Web décentralisé, qui permet aux utilisateurs de reprendre le contrôle sur leurs données tout en profitant d'une qualité de service similaire aux solutions existantes.

Description :

Développeur autour des technologies React.js et Node.js, passionné des logiciels libres et des technologies peer-to-peer, je travaille chez Qwant sur le projet Masq et sur d'autres projets open source.

Levent Demir :
Docteur en sécurité informatique, je suis passionné par la protection des données. Je travaille parallèlement dans deux domaines en m'appuyant sur des techniques de chiffrement et de cryptographie : le premier concerne la protection de la vie privée des utilisateurs, le second se focalise sur la protection des données de l'entreprise.



Geoffrey Bonnevillle :
Développeur autour des technologies React.js et Node.js, passionné des logiciels libres et des technologies peer-to-peer, je travaille chez Qwant sur le projet Masq et sur d'autres projets open source.

b. proposition Amborella

Dans cet article Amborella détaille sa proposition d'architecture pour assurer contrôle et transparence des flux de données d'objets connectés : le principe consiste à séparer les processus de stockage d'une part et de cryptage d'autre part.

Les premières mises en œuvre du RGPD montrent des signes de complexité dus à l'économie générale de la donnée : la multitude des intervenants et l'autorisation demandée une fois pour toutes sans préciser quelles données sont concernées ni quels traitements leurs sont appliqués rendent illisibles l'usage réellement faits des données personnelles. Il manque, au-delà du RGPD, un outil simple et commun permettant de mettre en œuvre la lettre et l'esprit de la réglementation.

Pourtant, les données personnelles, d'abord connues comme les « traces » que nous laissons lorsque nous consultons un **site web**, puis, plus récemment, comme les « traces » que captent nos **téléphones portables** quand nous les utilisons, nous déplaçons ou prenons des photos, sont en train de prendre une toute autre ampleur avec **le déploiement à grande échelle des objets connectés.**

En effet, ces derniers créent une triple rupture :

- Ils seront **très nombreux**, chacun de nous pourra être environné par plusieurs dizaines d'objets.
- Ils captent nos informations personnelles en dehors même de toute action de notre part, et **en permanence.**
- Les données personnelles qu'ils captent peuvent être extrêmement **sophistiquées** ou **sensibles**, et les objectifs de leurs traitements échapper à la compréhension du commun des mortels.

Cette triple rupture a une conséquence : dans l'état actuel de la réglementation et des outils disponibles, le citoyen ne peut plus prendre conscience de son « **empreinte numérique** » en croissance constante (ie, l'ensemble des données qu'il produit du simple fait qu'il vit), et encore moins la gérer.

Le projet YPYC© (Your Privacy - Your Control) a pour objectif de rendre au citoyen le contrôle permanent sur les données personnelles issues des objets qui l'entourent.

Il arrive à un moment charnière dans nos sociétés numériques, qui voient simultanément le **déploiement massif** de l'Internet des Objets, la **puissance inégalée** des traitements appliqués aux données, et l'emprise des technologies digitales sur la **vie citoyenne**.

1 - **Transparence** : Donner à chaque citoyen en temps réel la liste exhaustive de ses données personnelles susceptibles d'être captées, et pour chacune d'entre elles les acteurs qui y ont accès, le traitement qu'ils leur font subir, et leur finalité.
2 - **Contrôle** : Permettre à chaque citoyen à tout instant de changer la permission qu'il donne à chaque acteur sur chaque jeu de ses données personnelles (y compris fréquence, détail, etc...)

YPYC est donc un outil grand public de contrôle et de commande des données personnelles de chacun. C'est un moteur de la réappropriation de l'empreinte numérique des citoyens par eux-mêmes.

Principe de fonctionnement :

Le principe de base consiste à séparer les processus de **stockage** d'une part et de **cryptage** d'autre part. En d'autres termes, les données personnelles doivent être stockées encryptées, et le moyen de décryptage (la gestion des clés) doit être géré par une entité totalement indépendante de celle qui stocke ces données.

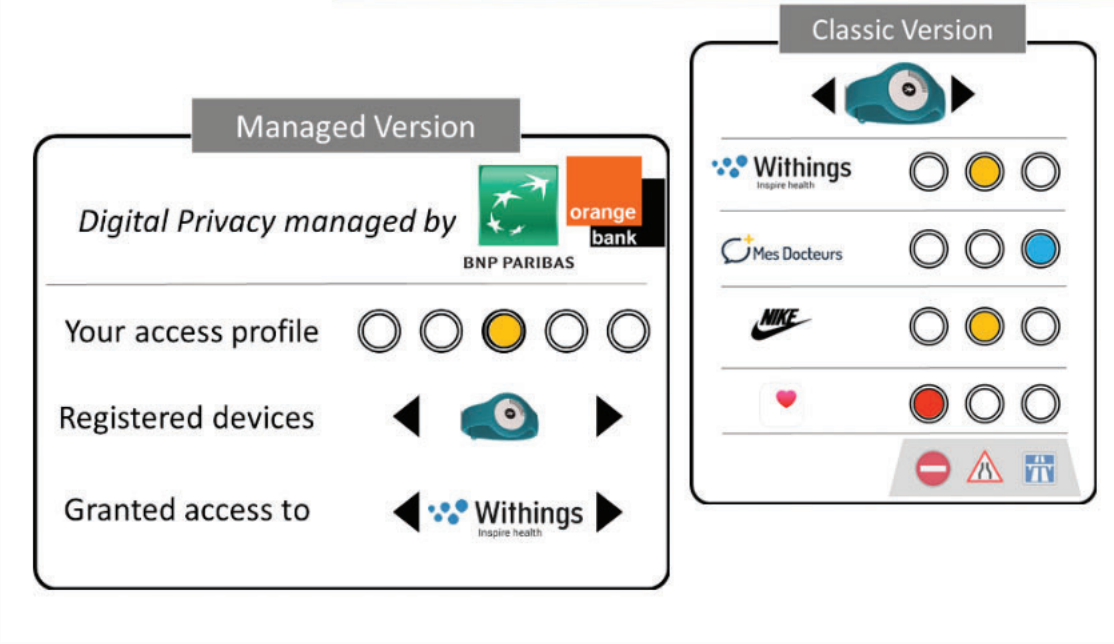
Ainsi, accéder aux données stockées, qu'on en soit l'exploitant ou simplement l'hébergeur, requerra une **autorisation révocable** à tout moment, limitée à un ensemble précis de données, qui sera administrée par un tiers de confiance.

Ces autorisations, requises à chaque accès aux données, donnent lieu à un accusé de réception qui permet de **« tracer » en retour les entreprises utilisatrices** des données avec les informations suivantes :

- Nature exacte de chaque donnée collectée
- Entité légale qui a eu accès à cette donnée
- Déclaration de l'usage qui en est fait
- Date et heure de la collecte

Ces autorisations seront spécifiques pour chaque entité légale utilisatrice : chaque citoyen pourra autoriser spécifiquement telle ou telle société utilisatrice à accéder à telle ou telle partie de ses données. Le tiers de confiance fournira une clé d'accès personnalisée par société utilisatrice qui ne pourra ainsi accéder qu'aux données pour lesquelles elle aura été autorisée par le citoyen.

A chaque instant, le citoyen pourra modifier ces autorisations en fonction de l'usage déclaré par chaque société utilisatrice.



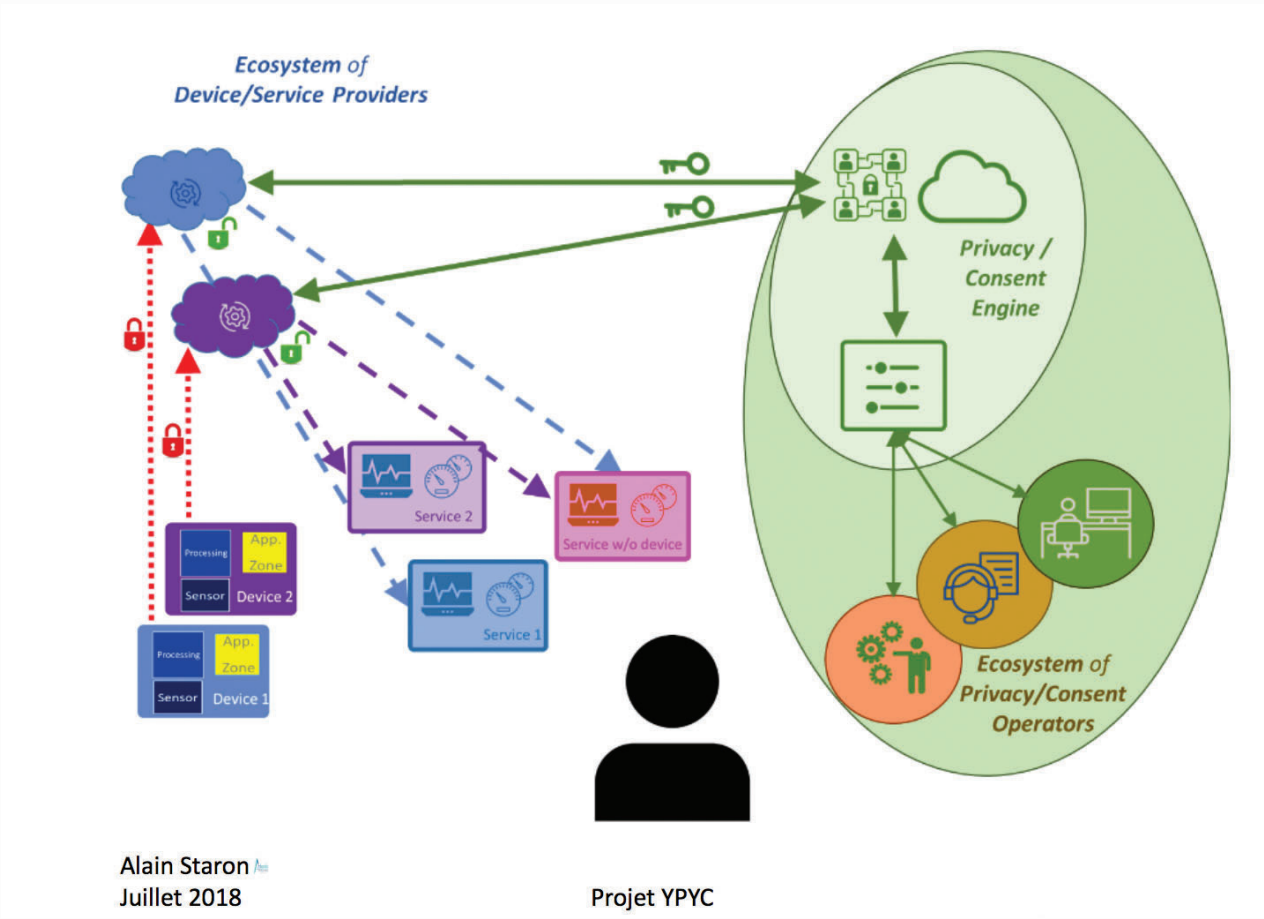
Ecosystème et chaîne de valeur :

Pour le fournisseur d'objet ou de service, YPYC offre la garantie d'un **contrôle des données privées** extérieur à lui-même, ce qui est un avantage compétitif sur les marchés où les citoyens sont sensibles à leurs données privées (typiquement les citoyens européens), voire ceux où la déclinaison d'une **nouvelle réglementation européenne** viserait à séparer les rôles : celui du fournisseur de service et celui de garant de la sécurité des données.

Les services rendus possibles par YPYC pourraient être commercialisés dans chaque pays par des tiers de confiance de type banque, qui s'appuieraient sur la même technologie pour rendre compatibles de nombreux objets. Ils joueraient le rôle **d'opérateurs de consentement** : les citoyens leur feraient confiance pour qu'ils gèrent leurs empreintes numériques.

YPYC est le **moteur de consentement** et se rémunère par une licence très faible sur chaque jeu de données protégé.

Un nouveau marché pourra également s'ouvrir où le citoyen sera rémunéré en échange de l'accès à ses données.



Alain Staron :

Alain a fondé Amborella pour aider à catalyser l'innovation en s'appuyant sur la dynamique des écosystèmes. Il est également membre du board de l'ETSI, et s'appuie sur sa longue expérience de l'innovation quand il était en charge de la transformation digitale du groupe Veolia, du Business Development chez TF1, du Product Management chez Thomson. Les nombreux projets innovants qu'il a mené en entrepreneuriat et en startup, ont donné lieu à deux prix d'innovation et 15 brevets.

Alain est diplômé de l'Ecole Polytechnique, de l'école Nationale supérieure des Télécommunications, et auteur d'une thèse en traitement du signal.

[1] A frictionless future for identity management White paper December 2016 Australia Post

[2] Phygital est un néologisme issu de la contraction des termes « physical » et « digital ».

[3] OpenID

[4] FaceBook Connect..

[5] Google Authenticator

[6] Security Assertion Markup Language

[7] L'objectif de FÆDERATION est de faire en sorte qu'à tout instant -- et pas seulement « dès leur conception » ! -- les applications mobiles de notre vie quotidienne intègrent des fonctions d'authentification forte « sans couture » et des fonctions d'assurance de protection des données auxquelles nos identités sont associées.

[8] ISO/IEC 24760-3:2016

[9] ISO/IEC 24760-3:2016 is applicable to an identity management system where identifiers or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities. Practices for identity management can also be addressed in other standards.

[10] Specialist Task Force 529 - Attribute Based Encryption - Common protocol for data access control for Cloud, Mobile and IoT

[11] Attribute Based Encryption (ABE) is a cryptographic scheme that provides a level of protection similar to ABAC but exclusively leveraging on cryptographic algorithms, without relying on a software based PEP. In practice, ABE mathematically moves the authorisation decision from the functional elements of the access control system (PDP, PEP) to the protected data itself, i.e., the ciphertext, or to the cryptography keys, i.e., the private keys.

[12] https://www.cryptoexperts.com/

[13] Dr Pascal Paillier est également le principal rapporteur d'une période d'études en cours au sein du GT 5 Technologies de la gestion de l'identité et de la protection de la vie privée, dont l'objectif est de normaliser les mécanismes d'authentification d'entité basés sur des attributs.

c. Cas Whaller

Dans cet article, Whaller détaille les choix d'architectures pour permettre à chacun d'être maître de la visibilité de son profil auprès de chaque communauté auquel il appartient.

Ce qui a déclenché la conception de Whaller, c'est la question posée à son fondateur par son beau-frère, lors d'un déjeuner familial. Devait-il autoriser ou non sa fille à utiliser Facebook ? Sans réponse convaincante, Thomas Fauré trouva plutôt l'énergie de développer un nouveau réseau au sujet duquel ce genre de question n'aurait plus lieu d'être posé.

La volonté de Whaller de restituer le contrôle des usages et des données à l'utilisateur est née d'un constat simple. Une technologie est d'abord un outil, et un outil qui ne doit faire que servir celui qui le manipule. Beaucoup de plateformes l'ont aujourd'hui complètement oublié. Les plus utilisées d'entre elles sont précisément celles qui allouent le moins de contrôle à ceux qui les fréquentent. Pire, non seulement ceux-ci y ont perdu toute forme de contrôle, mais ils sont même devenus des sujets d'expérimentation pour les dirigeants de ces plateformes.

L'architecture de Whaller s'est contentée d'épouser les contours de la relation humaine telle que nous la connaissons. Nul ne se présente partout de la même manière. En dépit de l'unité de la personne, nous sommes tous engagés dans une très grande variété de relations les uns avec les autres. Et les communautés à l'abri desquelles naissent, s'épanouissent et parfois s'éteignent ces relations, sont par principe vital étanches les unes par rapport aux autres. L'herméticité conjuguée à la notion de contexte, voilà ce qui garantit que l'utilisateur est bien en situation de contrôle de ses échanges.

Au départ de l'histoire de Whaller, le prisme architectural, c'était la « sphère personnelle » : une somme de relations bilatérales depuis un singleton vers un certain nombre d'autres singletons.

Chaque utilisateur possédait ses propres sphères et se connectait avec d'autres utilisateurs qui le « connectaient » dans leurs propres sphères. Le modèle était logiquement très séduisant, et protecteur. Personne ne pouvait voir dans quelles sphères personnelles il avait été placé par ses contacts. Ainsi une personne pouvait avoir créé une sphère « Amis sans intérêt » et placé des personnes qui de leur côté avaient créé une sphère « Amis ». La relation n'était pas symétrique. Cependant ce modèle séduisant en théorie, et absolument protecteur, posait quelques soucis de compréhension à l'usage puisqu'on pouvait ainsi logiquement voir apparaître dans une conversation des personnes avec lesquelles nous n'étions pas connectés.

Il fallut penser un modèle plus simple, et surtout répondant aux besoins de nos clients qui étaient davantage des organisations que des particuliers. Fût alors créé un modèle appelé « sphères partagées » qui étaient simplement une « synchronisation » de plusieurs sphères personnelles. Les communautés avaient ainsi le même nom, les mêmes administrateurs et restaient pourtant personnelles.

Cela n'était pas suffisant, car rapidement sont apparues les problématiques de maîtrise et de contrôle en dehors des sphères, à un échelon supérieur : les organisations. Une organisation pouvait ainsi posséder plusieurs sphères partagées.

Par la suite, les « sphères personnelles » (« mes amis » par exemple) toujours disponibles furent peu à peu migrées vers ce nouveau modèle de « sphères isolées » et le modèle fut abandonné.

Ainsi Whaller est passé d'un modèle strictement centré sur la personne à un modèle centré sur la communauté. L'utilisateur était dès lors « défini » par son appartenance aux sphères dont il était membre.

Whaller est donc logiquement mais aussi intuitivement passé d'un modèle B2C à un modèle B2B. Dès cet instant, a été fait le choix d'établir que le tiers de confiance, ça n'était plus l'utilisateur en tant que tel, potentiellement exposé aux mauvaises intentions de tel autre ou même et surtout à ses propres défaillances : c'était l'organisation elle-même. Il y a là un parti pris philosophique extrêmement fort qui distingue Whaller de l'ensemble des plateformes existantes. Les réseaux sociaux classiques sont paradoxalement centrés sur l'utilisateur. Ils mettent la focale sur son échelle, mais pas sur ses besoins fondamentaux qui sont des aspirations à la socialisation et au dialogue. Whaller est ainsi radicalement ancré dans la notion de communauté. C'est en cela que Whaller a innové et continue d'innover. Et c'est d'abord dans sa vision initiale de ce qu'est, de ce que doit être une plateforme sociale, que Whaller constitue une proposition originale, dans le sens le plus strict.

La modularité des profils en apporte une preuve supplémentaire. Sur Whaller, vous pouvez attacher un profil différent à chaque réseau auquel vous appartenez. C'est cela, et cela seul qui dote l'utilisateur de la capacité de dire de lui et à d'autres, ce qu'il veut dire de lui, et à d'autres, dans un contexte donné, et pas dans un autre. Le contexte, c'est le « lieu » même, abstrait ou non, de nos échanges. Et il est évident qu'il imprègne ou affecte la nature, la teneur ou la couleur des échanges qu'il abrite. C'est là la garantie de l'étanchéité des flux d'information, des flux de données, et donc de la liberté autant que de la sécurité de chacun. Cela vous autorise à créer des superpositions d'univers sociaux sans aucune forme de transaction entre eux. C'est en cela que nous aimons à dire que Whaller est un méta-réseau.

On touche là à ce qui s'appelle la liberté. D'un point de vue axiologique, une plateforme ne peut pas être neutre. C'est impossible. Elle embarque avec elle des représentations qui informent nolens volens ses utilisateurs. Cela veut dire que si, en amont, ses concepteurs ont compris le pouvoir formidable qui reposait en elle, et qu'ils ont décidé de remettre ce pouvoir à l'utilisateur, cette plateforme peut s'autoriser à dire qu'elle est éthique.

Sur Whaller, l'utilisateur n'a plus besoin de sécuriser chacun de ses profils. Par défaut, par intention, à dessein comme on dirait en bon français (« by design »), c'est la communauté elle-même, sa circonférence, qui l'abrite. Ne retrouve-t-on pas là des règles de communauté très usuelles dans notre vie tangible ?

Prenons l'exemple de Facebook. Sur ce média social, chaque utilisateur est autant émetteur que récipiendaire de données. Sur Whaller, c'est la sphère seule qui forme le lieu de cet échange de flux. Et ce lieu transactionnel, relationnel, possède à lui seul les garanties de sécurité dont auraient dû ailleurs s'assurer individuellement les protagonistes d'une relation. Cela fait peser une responsabilité énorme sur les épaules de nos développeurs qui doivent maintenir et garantir le caractère protecteur de la sphère, puis de l'organisation. Pour employer une image, ils ne vous donnent pas les moyens de revêtir une armure (par le biais de paramètres de sécurité) : ils offrent à votre vie privée la citadelle où elle est en mesure de se déployer dans son commerce avec les autres.

La vision qui a présidé à l'architecture de notre plateforme est tellement inspirée des besoins fondamentaux de toute vie sociale (dans ses opportunités autant que dans ses contraintes) qu'elle convient parfaitement à toutes les formes de réseaux humains.

La méthodologie que nous avons utilisée pour façonner le design de Whaller repose d'abord sur l'observation et à l'écoute de nos utilisateurs, ça a aussi été une méthodologie scientifique de conception sur une page blanche, sans inspiration extérieure. Nous avons prêté notre attention à la manière dont s'étaient développées les premières « sphères personnelles », et les liens qu'elles avaient établis entre elles. Nous les avons « mappées » sous forme de graphes. Beaucoup de ces réseaux s'étaient déployés « en étoile » : de nombreuses relations pointant toutes vers une seule personne. Cela était selon nous la signature d'un réseau mal utilisé, mal compris, pas assez ergonomique et dont l'expérience utilisateurs était à reconsidérer. D'autres réseaux étaient constitués de manière triangulaire. Nous avons pris la décision, avec leurs membres, de commuer ces réseaux « communautaires ». D'une certaine manière, on peut observer dans l'histoire de Whaller ce que tout scientifique relève de son étude la vie : de la cellule à l'organisme complexe, au long d'un cycle de mutagénèse. Pour envisager tous les cas d'usage d'entrée sur un réseau, nous avons codé plus de 2000 tests, qui forment autant de scénarios. Mais l'essentiel réside dans la volonté que nous avons eue de fournir aux mille illustrations de la vie sociale ou collaborative sur Internet un cadre absolument garant de deux biens précieux : la liberté et la sécurité.

Thomas Fauré :

Thomas Fauré a 35 ans, est ingénieur (Centrale Lille). Il y a 7 ans, alors que son beau-frère lui posait la question de savoir s'il devait ou non laisser son fils s'inscrire sur Facebook, Thomas Fauré se mit en tête d'agir plutôt que de commenter. Il coda et développa Whaller : un réseau qui incarne sa vision des réseaux sociaux., et qui redonne aux utilisateurs le contrôle de leurs usages et de leurs données. D'abord ingénieur chez Safran, passionné de code et de biométrie, il rejoint Polyconseil (Groupe Bolloré) en 2011, où il évoqua sa passion d'entreprendre et ses projets jusqu'à convaincre Vincent Bolloré d'investir dans Whaller. L'entreprise est née en 2013. Elle compte aujourd'hui près de 400 000 utilisateurs pour environ 30. 000 réseaux hébergés. Il est l'auteur de "Transmettez !" aux Éditions Baudelaire.

2 - Consentement : Problématiques et standardisation :

La partie précédente abordait par différentes propositions comment limiter l'accès d'un système d'information aux données personnelles d'une personne en fonction des autorisations de cette personne. Cette partie se concentre sur comment limiter l'usage des données personnelles à des utilisations précises et autorisées par la personne, une fois que le système d'information a accès aux données personnelles. Il s'agit donc de garantir le respect automatique et technique du "consentement" au sens du RGPD : en établissant des standards et des règles techniques.

Experts, avocats, ingénieurs, chercheurs abordent ce sujet dans différents articles :

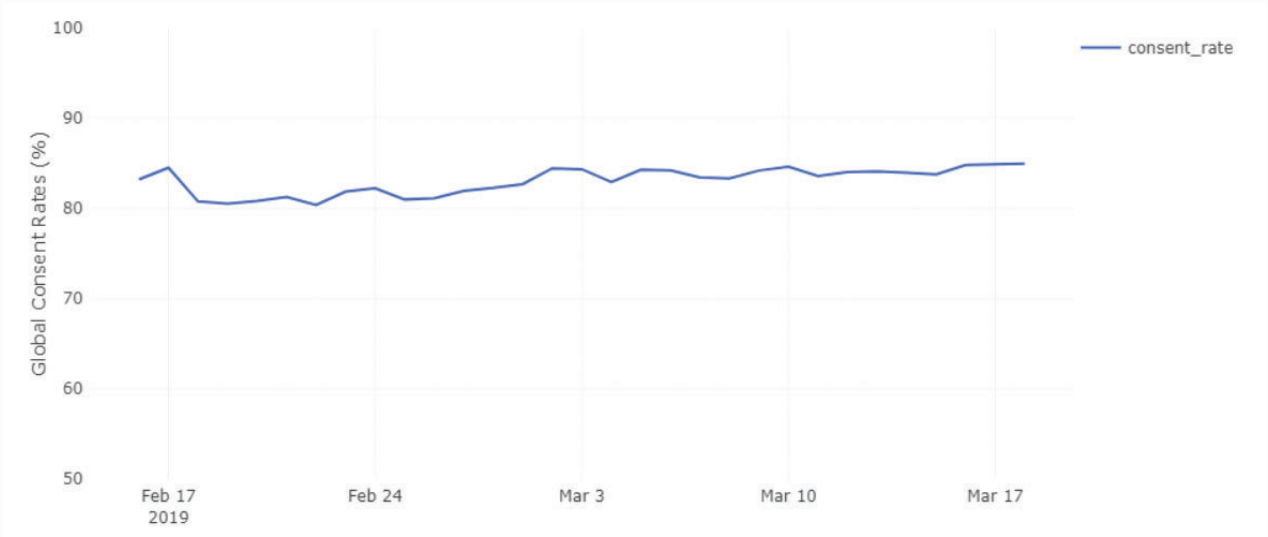
Ces articles donnent des solutions techniques et juridiques pour assurer que les autorisations de la personne sont bien respectées. Les preuves que les autorisations sont bien respectées permettent de susciter la confiance dans l'échange et le partage de données. La prochaine sous-partie sur la confiance se concentrera sur la transparence : une fois que les personnes peuvent contrôler qui a accès à leurs données et pourquoi, comment s'assurer que la personne a un bonne compréhension de ce à quoi elle consent ?

2- Consentement : Problématiques et standardisation

a. Retours d'expérience sur le consentement publicitaire et standards en cours et nouveaux.

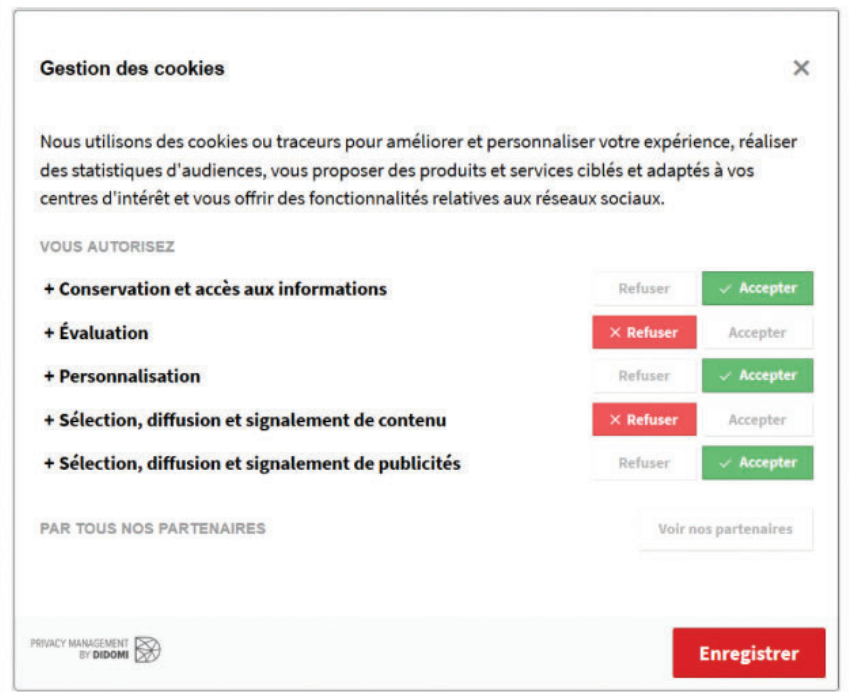
Depuis le 25 mai 2018, de nombreux sites webs et applications mobiles proposent à leurs visiteurs d'indiquer leurs choix de consentement par l'intermédiaire de bannières ou pop-ups apparaissant lors de l'ouverture de la première page. Ce phénomène nouveau est la traduction directe du règlement européen de protection des données (RGPD) dans l'expérience quotidienne des internautes. Constamment sollicités, parfois de façon répétitive ou intrusive, certains internautes développent des consentements réflexes qui posent de nombreuses questions.

Le taux de consentement global observé chez Didomi varie entre 80 et 85%. Il représente le nombre de pages vues par les internautes chez les clients Didomi pour lesquelles les internautes ont au moins donné un consentement. Il reflète la propension naturelle des internautes à consentir en général dans leur navigation, au moins pour les sites qu'ils visitent fréquemment.



Ce taux global est à nuancer fortement car il cache des disparités très importantes avec **des moyennes de consentement variant de 14% à 95%.** Les 2 principaux déterminants du taux de consentement sont le format de collecte (bannière, encart, popup, etc.) et le mode de consentement (clic sur un bouton j'accepte, poursuite de la navigation ou scroll sur la page).

Pour beaucoup de sites webs, l'enjeu est d'optimiser les étapes de consentements de façon à maximiser le taux de consentements. Un bon exemple est le choix fait de procéder à la collecte du consentement en plusieurs étapes avec une première étape offrant un niveau général d'information et permettant de consentir à toutes les finalités en cliquant sur un bouton 'j'accepte' ou d'atteindre une seconde étape en cliquant sur un bouton 'plus d'informations'. Sur cette seconde étape, l'internaute peut effectuer des choix plus granulaires, finalités par finalités, et également s'opposer au traitement de ses données par certains partenaires.

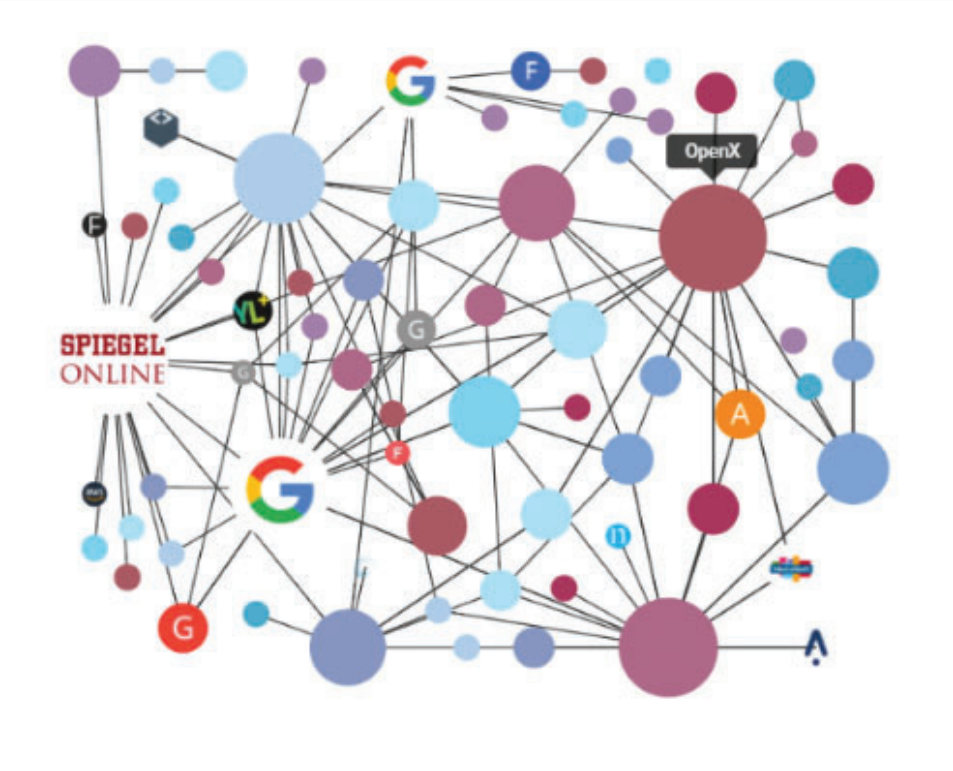


Ce choix d'UX conduit à des taux de consentements très importants car beaucoup d'internautes s'arrêtent à la première étape. Dans les chiffres mesurés pour les éditeurs de médias ayant mis en place cette collecte du consentement en 2 étapes, seuls **1,7% des internautes refusent de manière délibérée tous les consentements au site internet en se rendant sur la seconde étape**. La plupart des internautes n'expriment en réalité pas de choix : ils ne consentent ni ne refusent les finalités. Ce non-choix prend la forme du 'bounce' (= quitter rapidement la page sur laquelle on vient d'atterrir avant toute forme de consentement) ou bien l'internaute ignore simplement la demande de consentement.

En tant que fournisseur de solution de gestion du consentement, Didomi est au cœur des nouvelles problématiques qui se posent aux entreprises. Avec le recul des premiers mois, il se dégage deux grandes catégories de problématiques chez nos clients : celles liées à la conformité, notamment lorsqu'elle implique des arbitrages au détriment du business et les problématiques liées à l'expérience utilisateur, qui affectent de nombreux pans de l'entreprise (marketing, relation client, support, etc.).

Depuis le 25 mai, les entreprises sont **confrontées à des arbitrages compliqués entre conformité et business**. Ce problème est particulièrement pressant pour l'industrie européenne des médias : un site média qui ne recueille pas le consentement des internautes pour la publicité ciblée peut perdre jusqu'à 70% des revenus publicitaires, notamment du fait de la dépendance à certains acteurs comme Google qui s'appuient sur le consentement comme base légale pour leurs traitements de publicité ciblée liés à la donnée. Il existe pour ces acteurs une tension entre leurs intérêts en termes de business (sauvegarder leurs revenus publicitaires) et la mise en conformité avec les principes définissant le consentement dans le

RGPD. Cette tension conduit à des arbitrages entre risque et coût d'opportunité.



Ces défis ont conduit à l'émergence d'un standard porté par l'association International Advertising Board (IAB) Europe : le Transparency and Consent framework (TCF). Cette initiative regroupe tous les intervenants de la chaîne de valeur publicitaire et permet à chacun de collecter et diffuser des consentements de façon normée. Le standard s'articule autour de spécifications techniques et d'une série d'obligations auxquels chaque acteur du standard s'engage. Le standard résout le problème de la traçabilité d'un consentement : chaque acteur s'échange les informations de consentement de la même façon, depuis l'éditeur qui collecte le consentement sur son site web, en passant par les plateformes qui reçoivent les données personnelles de l'internaute pour les traiter, jusqu'à l'annonceur qui bénéficie de ses données pour améliorer la performance de ses investissements publicitaires. Cette approche ouverte a rencontré un grand succès et **aujourd'hui 67% des 100 premiers éditeurs de contenus médias en France sont équipés d'outils de gestion du consentement mettant en place ce standard**. Le standard est encore loin d'être complètement abouti, notamment au regard de certains points de conformité tels que la clarté de l'information des personnes sur les finalités pour lesquels le consentement est collecté, mais présente le mérite d'être pensé pour résoudre concrètement le problème qui se pose à tous les éditeurs qui dépendent des revenus publicitaires pour leur monétisation.

Il est encore très tôt pour tirer des conclusions définitives sur l'usage que les internautes feront des outils de consentement qui sont mis à leur disposition. L'évolution la plus notable qui doit être saluée est **la recherche par tous les acteurs de solutions techniques pragmatiques sur la traçabilité de la donnée personnelle**, notamment autour de la notion de token de consentement. Sous réserve d'une jurisprudence et de directives claires sur la notion de consentement, les internautes pourront bénéficier d'un contrôle effectif sur la circulation de leurs données personnelles sur internet.

Le Consent Web Token :

La question de la standardisation des consentements se pose au-delà des questions liées à l'utilisation de la donnée pour des publicités ciblées. Didomi propose depuis janvier 2018 d'étendre l'idée de token de consentement autour un standard appelé le **Consent Web Token** (CWT). Didomi s'est inspiré du JSON Web Token, qui est le standard dominant sur internet aujourd'hui pour l'authentification d'internautes grâce à un protocole d'échange sécurisé de tokens. L'idée est de permettre l'échange entre différents partis de tokens de consentement dont l'intégrité serait assurée par une signature numérique. L'autorité émettrice du token de consentement signe de façon cryptographique l'évènement de consentement avec toutes ses caractéristiques (date du consentement, expiration, données et finalités consenties, etc.). Ce token est ensuite partagé avec les tiers recevant la donnée personnelle qui peuvent à tout moment vérifier que leur consentement est toujours valide et assurer la traçabilité de ce consentement dans leurs systèmes. Le Consent Web Token est un standard open-source ouvert aux contributions de tous.

Description Didomi :

Didomi est une startup française créée en 2017 et spécialisée dans la gestion du consentement. Les solutions Didomi permettent (i) de collecter auprès des internautes des consentements conforme RGDP sur le web et le mobile, (ii) de les stocker de façon réglementaire et d'en tirer des insights permettant l'optimisation de l'expérience de consentement, (iii) de d'assurer la synchronisation des consentements dans tous les outils utilisés par chez clients pour la publicité, le marketing ou le CRM et (iv) de restituer ces consentements dans un privacy center permettant à un client d'avoir le contrôle sur ses consentements à tout moment. Didomi déploie ses solutions sur plus de 15 000 sites webs et applications mobiles et compte des clients dans 13 pays.

Romain Didomi :
Romain Gauthier est diplômé de l'ESCP Europe et a créé Didomi en 2017 après 7 ans d'expérience dans diverses startups où il a pu développer une expertise dans la création et la vente de solutions logicielles complexes. Didomi est sa deuxième aventure entrepreneuriale après Tactads, startup nantaise créée en 2013 et revendue à une entreprise américaine leader de l'adtech.

2. Consentements au sein d'un écosystème d'échange de données sensibles :

a. Complexité d'assurer le respect des consentements au sein de toute la chaîne et responsabilité du meneur : cas dans la santé

Les objets connectés sont emblématiques de cette multiplication des sources de collecte de la donnée de santé et posent avec encore plus d'acuité la question du respect du consentement de l'individu dans le partage de ses données. Comment le consentement sur la finalité de l'exploitation de ses données de santé, est-il respecté par les différents responsables de traitement ? En d'autres termes, comment peut-on utiliser les outils du RGPD pour redonner à l'individu la maîtrise de l'utilisation de ses données de santé collectées par des objets connectés ?

La M-santé ou santé mobile, terme apparu en 2005 sous la signature du Professeur Robert Istepanian, universitaire londonien, pour désigner « l'utilisation des communications mobiles émergentes en santé publique », regroupe en 2019, les objets connectés et applications de bien-être utilisables via un réseau mobile : smartphone, tablettes numériques. Elle est une composante de la Télésanté, qui elle-même relève de ce qu'on appelle la santé connectée (e-santé), c'est-à-dire l'application des technologies d'information et de communication à l'ensemble des activités en rapport avec la Santé. Cette dernière gère l'information et les données de santé. Elle est considérée comme une science de la mesure alors que la médecine est « l'art de guérir » régie par le serment d'Hippocrate.

Avec l'explosion des objets connectés dans le domaine de la santé, et la « médicalisation » des appareils connectés, ou en tout cas la revendication d'un bénéfice sanitaire, la frontière entre les objets utilisés dans le domaine du bien-être, dans celui de la santé d'une part, et, les dispositifs médicaux réglementés[1], dont la mise sur le marché est subordonnée à un marquage CE préalable qui est sous la responsabilité du fabricant, d'autre part, se brouille.

Les informations collectées par ces objets connectés revêtent un intérêt non seulement pour les professionnels de la santé, mais pour les banques, les assurances, et les data brokers (courtiers en données) en raison de leur richesse informationnelle résultant notamment de leur caractère intrusif. Il existe donc un risque réel de déviance compte tenu de l'importance de l'accès à ces données, par différents acteurs économiques, puissants et organisés.

Tous les objets connectés n'ont pas vocation à rentrer dans les processus de soins. Cependant, compte tenu de la sensibilité des données collectées, il apparaît nécessaire d'appliquer à tous les objets connectés, une obligation d'information claire et loyale et détaillée sur les conditions d'emplois, pour permettre aux utilisateurs de donner un consentement éclairé.

Ces objets connectés collectent des données de santé, considérées comme des données sensibles par le RGPD[2] et dès lors soumises à un régime d'interdiction générale de collecte sauf exception. Elles sont réglementées en France, par la loi informatique et liberté modifiée, par le code de la santé publique, par des lois spécifiques[3]. Le RGPD se superpose aux règles spécifiques régissant les droits du patient dans le contexte de la relation thérapeutique et dans ses relations avec l'équipe de soin. Il va offrir des moyens complémentaires pour préserver ses droits. C'est dans cette logique d'exploitation du RGPD, pour protéger le consentement du patient et de manière plus générale, tout utilisateur d'objet connecté, réglementé ou

non, qu'il convient de réfléchir au moyen le plus approprié pour favoriser le partage des données de santé dans le respect du consentement de l'utilisateur pour instaurer un climat de confiance, une éthique dans la m-santé.

Le RGPD a introduit la privacy by design[4] (art.25§1), méthodologie popularisée au Canada à la fin des années quatre-vingt-dix par A Cavoukian, consistant à intégrer la protection des données personnelles dès la conception des outils de collecte, de traitement et d'exploitation des données en préconisant une approche proactive du responsable de traitement afin de prévenir des risques. Cette approche s'inscrit dans la philosophie de l'adage « code is law » théorisé par L Lessig[5], selon lequel le net est régulé par celui qui écrit le code. Le recours PETs (« privacy-enhancing-technologies[6] ») permet de faire respecter notamment le consentement, en introduisant dans le code informatique, les conditions qui doivent être satisfaites pour autoriser le transfert de données vers un responsable de traitement déterminé. Ces technologies reposent sur le mécanisme des smart contracts, fonctionnant comme toute instruction conditionnelle de type « if-then », si telle condition est vérifiée, alors telle conséquence s'exécute. Le RGPD n'impose pas au fabriquant d'objet connecté de respect le principe de privacy by design, seul l'exploitant en tant que collecteur de données et donc responsable de traitement est soumis à cette obligation. Par cette approche technico-légale mise en œuvre au niveau de la conception, le code n'est plus la loi, mais c'est la loi qui devient le code, dès lors que cette dernière est incorporée au code informatique.

L'autre question est de savoir qui devra mettre en œuvre cette approche ex ante ? En principe, tout responsable de traitement est soumis à l'obligation de privacy by design. Cependant, la mise en œuvre de cette obligation est liée à l'approche par les risques. En effet, l'article 25 §1 du RGPD, conditionne la mise en œuvre de mesures techniques et organisationnelles dès la conception à la prise en compte « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement pour les droits et les libertés des personnes physiques ». Cette évaluation de la gravité et de la proportionnalité des risques pour les droits et libertés des utilisateurs d'objets connectés repose sur le responsable de traitement. Dès lors, en confiant à l'exploitant de l'objet connecté le pouvoir d'adopter ou non des mesures pour faire respecter le consentement de l'utilisateur sur les réutilisations des données de santé, il existe une incertitude sur la mise en œuvre effective de la privacy by design.

L'option la plus adaptée pour réduire les risques de contournement de cette approche ex ante et garantir l'effectivité de sa mise en oeuvre, pourrait être le recours à ce nouvel acteur, intermédiaire qui gère les informations personnelles des utilisateurs (Personal Information Management Systems, PIMS), selon les principes du RGPD. Il permet aux utilisateurs d'objets connectés de reprendre le contrôle de leurs données à caractère personnel, par le recours aux technologies introduisant les principes du RGPD dans le code. Dès lors, le consentement éclairé permettra de transférer les données de santé vers les responsables de traitements récipiendaires autorisés par l'utilisateur, son retrait entraînera une interruption automatique du flux et empêchera le récipiendaire de traiter la donnée, car dans le code le traitement est conditionné à la vérification du consentement.

L'introduction de ce nouvel acteur dans le partage des données de santé, collectées par les objets connectés, pourraient se révéler une option pour garantir le respect du consentement de l'utilisateur dans l'exploitation de ses données de santé et réconcilier l'objectif d'empowerment de l'individu sur ses données garanti par le RGPD et la nécessité de faire circuler la donnée de santé pour améliorer la recherche médicale et les soins

personnalisés.

L'intégration de ce nouvel acteur dans l'écosystème de la donnée de santé collectée par tout objet connecté est une piste à exploiter pour garantir l'effectivité du consentement du patient, de l'utilisateur d'objets connectés, et d'imposer le respect de l'éthique pour créer un environnement de confiance nécessaire au développement de la santé connecté. Cependant, cette intégration ne pourra être effective que si elle est imposée par les acteurs du corps médical à tous les acteurs de la santé connectée[7].

Eleonore Scaramozinno :

Formation

D.E.A Droit économique et fiscal - Panthéon-Assas Paris

Master en Management - ESCP Europe Paris

L.LM en droit européen - Institut d'Etudes Européennes – ULC Bruxelles

Certificat de spécialisation de DPO - CNAM Paris

Expérience

Consultant Direction Générale de la Concurrence Commission européenne (1995-1997)

Avocat Lafarge-Flécheux (1998-2002)

Avocat fondateur Scaraye Avocat (2003-2018)

Avocat fondateur Scaramozzino Avocat Constelletion Partenaires (2019-

[1] Règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

[2] Règlement Général sur la Protection des données personnelles, Règlement (UE) n°2016/679,

[3] Dont notamment, Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite la loi Kouchner, Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, créant le système National des Données de Santé (SNDS)

[4] DEBET (A) : « Les nouveaux instruments de conformité », Dalloz IP/IT, 2016 592

[5] LESSIG (L.): Code is law, On liberty in cyberspace, Harvard magazine, jan.-fév. 2000, adresse : http://harvardmagazine.com/2000/01/code-is-law-html. Pour une traduction française de l'article, v. http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig

[6] DEBET (A), MASSOT (J) et METALLINOS (N), Informatique et libertés. La protection des données à caractère personnel en droit français et européen, Lextenso, coll. Les intégrales, 2015, spéc. nos 55, CE : Etude annuelle 2014, le numérique et les droits fondamentaux, Ed. La documentation française, 2014, spéc. p. 179

[7] Avis 9/2016, avis du CEPD sur les systèmes de gestion des informations personnelles, vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel, 20 octobre 2016.

1. Le consentement est une donnée personnelle :

Le consentement se définit comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. » (Art. 4)
Aux conditions de validité du consentement précisées dans cette définition _ libre, spécifique, éclairé, univoque_ s'ajoutent deux conditions supplémentaires : le consentement doit être démontrable par le responsable de traitement (Art. 7.1) et il doit être révocable par la personne (Art. 7.3). Cela implique d'en conserver les versions et les preuves successives.
En conséquence, un consentement est bien une donnée à caractère personnel en ce qu'il constitue une information se rapportant à une personne physique identifiée ou identifiable, et sa collecte est bien un traitement de données personnelles à part entière, pour lequel il convient donc de prendre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque (Art.32).

2. La collecte des consentements aux traitements de données sensibles doit faire l'objet de mesures appropriées :

Si le consentement à des fins de prospection directe au sens de l'article L34-5 du CPCE revêt un faible risque dans la plupart des cas (attention, cela dépend toutefois des produits ou services visés), les traitements portant sur des catégories particulières de données à caractère personnel (Art. 9) requièrent un soin particulier au moment de la collecte. Le consentement explicite est alors une des principales bases de licéité pour ces traitements. Mais l'accès par un tiers non autorisé à l'existence même de ces consentements peut constituer une fuite de données.
ex : Le fait de savoir qu'une personne a consenti à un ou plusieurs traitements par un service d'oncologie, même sans savoir quelles sont les données personnelles mises en œuvre ni les finalités exactes des traitements, dit quelque chose de cette personne et constitue une information personnelle dont la divulgation pourrait être préjudiciable à la personne concernée.
Pour répondre à ce cas de figure, la société fair&smart met en œuvre un chiffrement fort pour la collecte de ces consentements : les reçus de consentement sont chiffrés dans un espace de stockage dédié au responsable de traitement avec ses propres clés de chiffrement. Le reçu n'est accessible qu'à lui seul. Une source de temps fiable est par ailleurs apportée par un horodatage certifié.

3. Les consentements pour transfert de données à un tiers sont difficiles à mettre en œuvre avec une bonne expérience pour la personne concernée :

C'est un cas pourtant de plus en plus fréquent : on le retrouve notamment dans les écosystèmes d'innovation initiés par les Grands groupes et qui cherchent à animer un réseau de startups réutilisatrices susceptibles d'offrir de nouveaux services à forte valeur ajoutée. C'est aussi le cas de figure de nombreux projets SmartCity ou de projets e-santé.
Quelle est la problématique ?
Un responsable de traitement A propose un service qui réutilise des données personnelles venant d'un responsable de traitement B. A est responsable des traitements impliqués dans son service, pour lesquels

il entend recueillir le consentement de la personne concernée et doit être en mesure de le démontrer. Mais il n'est pas responsable du transfert des données en tant que tel : ce traitement est de la responsabilité de B qui doit lui aussi recueillir le consentement de la personne et être en mesure de le démontrer. Il y a donc deux consentements auprès de deux responsables de traitement bien distincts à collecter.

3 options sont généralement rencontrées :

1. Deux consentements = deux parcours utilisateurs distincts :

La première option est que la personne concernée s'identifie chez B et donne son consentement pour les traitements envisagés, puis s'identifie chez A pour autoriser le transfert à B. Cela implique donc 2 comptes à créer ou 2 authentifications à réaliser, et 2 comptes auxquels il faudra se reconnecter en cas de changement d'avis : si la personne concernée retire son consentement pour les traitements de B, elle devra aussi penser à retirer son consentement pour le transfert effectué par A. C'est indéniablement compliqué pour la personne concernée, difficile à suivre et à maintenir dans la durée, encore plus en cas de multiplication des cas d'usage. **L'expérience utilisateur est sacrifiée à la conformité.**

2. Deux consentements = un seul parcours utilisateur + un contrat :

La deuxième option est que A sous-traite à B la collecte du consentement pour le transfert, ou que B sous-traite à A la collecte des consentements pour ses finalités. Indépendamment du fait que les informations à fournir à la personne doivent être particulièrement claires pour éviter toute confusion, il conviendrait alors pour A et B de contractualiser une relation de sous-traitance pour le traitement « collecte de consentement », avec tout ce que cela comporte (niveaux d'engagement, vérifications, DPA, responsabilités...). D'un point de vue très concret, A pourrait aussi alors avoir accès aux finalités des traitements de B, ce qui peut constituer une communication non souhaitable d'information personnelle au sujet de la personne concernée, ou une information à laquelle A ne souhaitera pas forcément avoir accès pour éviter tout risque de co-responsabilité de traitement.
La bonne expérience utilisateur introduit un risque juridique important.

3. Deux consentements = un seul parcours utilisateur + un tiers de confiance :

La troisième option consiste à faire appel à un même tiers de confiance spécialisé qui sera capable d'exposer le formulaire de collecte de consentement de A puis celui de B à la personne concernée au sein d'un même parcours, pour offrir une bonne expérience à l'utilisateur. Les reçus de consentements sont alors stockés dans des instances dédiées (une pour A, une pour B), chiffrés avec des jeux de clés différents et sans qu'un responsable de traitement accède aux finalités consenties par la personne auprès de l'autre. Une filiation peut aussi être établie entre ces 2 consentements pour qu'une révocation du consentement auprès de B propose automatiquement à la personne concernée la révocation du consentement donné à A. C'est le type d'implémentation proposé par fair&smart.
Le tiers de confiance apporte la bonne expérience utilisateur et la minimisation des risques.

Remarque : Quand la certitude de sa compatibilité avec les droits des personnes aura été clairement établie, une alternative au tiers de confiance pourrait être trouvée dans la mise en œuvre d'une technologie

de type Blockchain.

Conclusions :

1. **Les consentements sont des données personnelles à part entière.** Leur collecte doit faire l'objet de mesures appropriées qu'un tiers de confiance spécialisé peut apporter en offrant la meilleure expérience utilisateur.

2. **Il faut définir des standards** pour garantir l'interopérabilité des consentements dans leur format de consultation comme dans leurs modalités de collecte. C'est une nécessité **pour permettre la fluidité des échanges de données à caractère personnel.**

3. Les consentements font partie des données à restituer à la personne en cas d'exercice de son droit d'accès, notre point de vue est qu'ils doivent aussi rentrer dans le périmètre de la portabilité. **La portabilité des consentements permettrait à la personne concernée de les centraliser** et de les gérer depuis des applications dédiées et sécurisées (type PIMS) **pour avoir une vue réelle sur l'utilisation de ses données et prendre des décisions cohérentes**.

Notes :
Art. 7.1 : 1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
Art. 7.3 : 3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

Xavier Lefevre :
Xavier Lefevre, 42 ans, est diplômé d'HEC. Il est le Président Fondateur de fair&smart qui offre depuis 2016 des solutions Premium de gestion des données personnelles pour les particuliers et les entreprises.
Auparavant, il fut entrepreneur dans la distribution et dans l'édition multimédia puis Directeur de la stratégie et du développement de SSII spécialisées dans la mise en œuvre de l'innovation.

c. Respect des consentements sur toute la chaîne d'échange : standards nécessaires

Cambridge Analytica est une bonne introduction à notre propos : le scandale ne provenait pas du fait qu'on ne pouvait pas gérer l'échange de données (l'utilisateur Facebook peut couper l'échange de ses données vers un tiers) mais du fait que l'acteur principal de l'écosystème – Facebook – n'avait imposé aucun moyen pour assurer un contrôle sur les traitements faits sur les données une fois échangées.

Dans cet article nous rebondissons sur l'article « Respect des consentements sur toute la chaîne d'échange, standards nécessaires » de E. Scaramozinno présent dans ce Livre Blanc et nous aborderons les nécessités de standardisations d'API du consentement pour gérer de façon automatique les consentements le long de toute une chaîne d'échange et de sous-traitance afin de proposer une solution technique aux principes énoncés dans l'article de Scaramozinno.

Nous prenons, pour illustrer notre propos, un cas d'échange de données dans la santé numérique : le cas d'une application de télémédecine (A) échangeant des données avec un Hôpital (H), des sous-traitants (ST) et un objet connecté (OC).

Contexte :

1 - L'e-santé repose sur un grand nombre d'applications et d'objets connectés s'échangeant des données sensibles.
2 - La circulation des données d'un point de vue technique et l'interopérabilité de ces systèmes n'est pas le plus important ou le seul enjeu.
3 - L'enjeu est de pouvoir respecter les consentements et les droits des personnes sur toute la chaîne :
    a. Cet enjeu est d'autant plus important que les données concernées sont sensibles.
4 - Un manquement dans la chaîne d'échange et c'est chaque acteur du réseau qui est atteint légalement et dans sa réputation :
    a. Ce manque de confiance et d'assurance nuit à la volonté des grands acteurs d'échanger des données.
    b. Chaque manquement peut mettre à terme à tout un réseau d'échange au service de l'innovation.

Il ne s'agit donc pas uniquement de pouvoir gérer les flux d'échange de données mais également de s'assurer qu'une fois les données échangées, le système qui les reçoit respecte bien les consentements et droits des personnes sur les données et ne les utilise que pour les traitements autorisés et arrête de les traiter si le consentement est révoqué.

Une bonne gestion du consentement au sein d'un écosystème doit conditionner les flux d'échange de données personnelles entre systèmes d'information (SI) des acteurs mais aussi conditionner les traitements faits au sein d'un SI d'un acteur. Chaque acteur doit donc assurer un certain nombre de procédures pour gérer ses échanges de données mais également ses utilisations de données.

Nous verrons tout d'abord l'intérêt pour un tel écosystème d'utiliser une gestion automatique des consentements passant par un ou plusieurs système(s) de gestion des consentements (SGC) (I) ; ensuite les nécessités de standardisation dans cette gestion du consentement pour garantir une automatisation fluide (II) et finalement nous verrons comment une telle solution de SGC peut-être imposée par le responsable de traitement à ses sous-traitants en utilisant le Règlement Général sur la Protection des Données (RGPD) (III).

1. Intérêt d'utiliser une gestion automatique des consentements dans un écosystème d'échange de données :

Si nous prenons notre exemple ci-dessus de santé numérique et nous pouvons ajouter à ce cas que l'application et l'objet connecté ont deux traitements sur les mêmes données de santé : le premier (T1) est de prévenir l'hôpital en cas d'alerte majeure relative à la santé de la personnes, le second (T2) pour proposer des formules de bien-être en fonction du profil de la personne fondé sur ses données de santé.

Prenons un scénario de consentement : je souhaite à présent révoquer le consentement que j'ai donné à l'hôpital pour échanger mes données avec l'application et je souhaite que A, qui les a elle-même échangées avec ST et OC, n'effectue plus ni T1 ni T2.

Regardons la procédure sans SGC puis avec SGC.

Sans SGC :

1 - Je contacte l'Hôpital qui me demande de confirmer mon identité.
2 - L'hôpital coupe le flux de données vers l'Application et lui envoie un message pour signaler la révocation du consentement pour T1.
3 - L'hôpital doit faire confiance à l'Application pour traiter la demande en interne et envoyer la notification aux tiers (sous-traitants, objets connectés, ...) ainsi que couper les flux vers les tiers et ne continuer pas à traiter la donnée pour T1 même si les flux sont coupés.
4 - L'application doit faire confiance à l'Objet Connecté et aux sous-traitants pour appliquer le retrait du consentement T1 et ne plus traiter les données en conséquence.
5 - Je me connecte sur l'application pour révoquer le consentement pour T2.
6 - Je dois faire confiance que A traite la demande en interne, coupe les flux et envoie la notification pour révoquer le consentement sur T2 à OC et ST
7 - A doit faire confiance à ST et OC d'appliquer le retrait du consentement et ne plus traiter les données.

Cette procédure présente de nombreux inconvénients :

1 - Elle est chronophage.
2 - Elle assure une mauvaise expérience pour la personne.

3 - Elle repose sur la confiance de chaque acteur dans les procédures des autres, uniquement garanties par des clauses contractuelles peu vérifiables.

Avec SGC :

Nous supposons que le SGC apporte une interface de gestion des consentements à la personne.

1 - Je me connecte sur mon interface de gestion des consentements.
2 - Je révoque les consentements sur T1 et sur T2.
3 - Les flux sont automatiquement coupés et tous les acteurs ne peuvent plus traiter la donnée car le traitement est conditionné automatiquement au consentement.

Il apparaît donc clairement que passer par un SGC est beaucoup plus efficace, apporte une meilleure expérience utilisateur et rassure tous les acteurs de la chaîne sur le respect du consentement par les autres car il est assuré techniquement et prouvé.

2. Nécessite de standardisation d'API de SGC :

Pour implémenter le cas « avec SGC », de nombreux acteurs vont devoir interagir avec les consentements pour notamment : les vérifier, les créer, les mettre à jour.

Une standardisation des API (Application Programing Interface) des SGC est donc nécessaire pour éviter un monopole qui présenterait plusieurs inconvénients dont les principaux seraient : un manque de confiance à terme et surtout la dépendance des institutions et de l'économie à cet acteur unique. Les protocoles qui suivent sont ceux que Visions permet d'implémenter grâce à son API VisionsTrust.

- A la création

H envoie les données à A qui les envoie à ST et OC.
Les données sont envoyées sur le consentement de la personne depuis l'interface du SGC. Chaque acteur va avoir pour l'utilisateur un identifiant différent et le SGC doit en créer un pour l'utilisateur également.
Les données doivent donc être à chaque fois envoyées avec le consentement contenant :

- L'identifiant de l'utilisateur dans le SGC.
- L'identifiant de l'organisation qui reçoit les données (A, OC, ST) dans le SGC.
- L'identifiant du traitement dans le SGC.
- L'identifiant de la donnée dans le SGC.
- L'identifiant du responsable de traitement (H) dont proviennent les données.

Dès réception des données, l'organisation qui les reçoit renvoit au SGC de H :

- L'identifiant de l'utilisateur dans le SGC.
- L'identifiant de l'organisation qui reçoit les données (A, OC, ST) dans le SGC.
- L'identifiant du responsable de traitement (H) dont proviennent les données.
- L'identifiant de l'utilisateur qui vient d'être créé dans le SI de l'organisation qui reçoit les données (A, OC, ST).

Il est donc nécessaire de standardiser ce protocole d'échange d'informations et les routes de l'API du SGC sur lesquelles renvoyer l'information, cela permettra au SGC de lier les identifiants de l'utilisateur dans tous les systèmes vers lesquels la donnée a été échangée.

Ce lien sera utile pour permettre au SGC de vérifier les consentements pour chaque utilisateur pour chaque traitement par tous les acteurs.
La nécessité de standardiser les routes facilitera pour A, OC et ST la gestion de plusieurs clients H qui utiliseront des SGC différents.

- A la vérification du consentement

Reprenons notre exemple : A, ST et OC traitent les données pour effectuer T1 et T2.

Avant d'exécuter le traitement il doivent vérifier que le consentement est toujours valable, ils vont donc envoyer une requête sur le SGC comprenant :

- L'identifiant de l'utilisateur chez eux.
- Leur identifiant dans le SGC (reçu lors du premier transfert de données, voir plus haut).
- L'identifiant du responsable de traitement (H) dont proviennent les données (reçu lors du premier transfert de données, voir plus haut).
- L'identifiant du traitement.
- L'identifiant de la/ des données concernées

Grâce au protocole décrit plus haut (A la création), le SGC peut lier l'identifiant de l'utilisateur dans les systèmes traitant la donnée avec l'identifiant chez lui et vérifier si le consentement de cette personne, pour cet acteur sur ce traitement est toujours valable.

L'identifiant du traitement et des données concernées doit être standardisé et partagé par tous les SGC, sinon les A, OC et ST devront s'adapter à chaque terminologie de chaque SGC ce qui alourdirait le processus. Un tel référentiel de traitement peut se faire pour les traitements les plus courants d'une industrie et pour s'adapter aux nouveaux un organisme dédié à la réflexion et création de ces référentiels, tel un consortium, est indispensable à terme.

- Pour l'écosystème

Le rôle du SGC est de modéliser des écosystèmes d'échange de données, en objets liés JSON par exemple. Ces objets liés doivent modéliser la chaîne d'échange et de responsabilité, par exemple à un traitement est rattaché un responsable de traitement (H) auquel sont rattachés des ST, chaque ST a son identifiant, ses traitements, les données concernées.

Nous aurons ainsi des réseaux d'échange et de traitements de données et de la sous-traitance modélisés dans les SGC.
Nous pourrions également à terme imaginer un annuaire des identifiants des responsables de traitements et sous-traitants sur lequel les SGC fonctionneraient plutôt que chaque organisation ait un identifiant différent par SGC.

3 - SGC : la transposition technique des obligations de sous-traitance

Le RGPD définit les obligations respectives des responsables de traitements et des sous-traitants à son Article 28. Pour les définitions de « responsable de traitements » et de « sous-traitant » nous renvoyons à l'article 4 du RGPD.
A l'article 28, paragraphe 1, le RGPD stipule :

« *Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.* »

Ici des « garanties suffisantes quant à la mise en œuvre de mesures techniques [..] de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » peut-être utilisé pour demander à ce que ces garanties suffisantes soient le respect d'un certain nombre de protocoles pour le respect et la vérification du consentement.
A l'article 28, paragraphe 3 alinéa e), le RGPD stipule que le contrat qui lie le responsable de traitement et le sous-traitant garantit que le sous-traitant :

« *tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;* »

Ce passage du RGPD permet d'inclure dans le contrat de sous-traitance l'obligation par le sous-traitant de respecter un certain nombre de protocoles et standards sur la gestion des droits et du consentement.

Conclusion :

Un système de gestion du consentement avec protocoles, API standardisées et référentiels de terminologies permet de transposer techniquement les obligations des responsables de traitement et de sous-traitants vis-à-vis des droits des personnes concernées pour en assurer le respect sur toute la chaîne.

C'est au responsable de traitement d'imposer le respect de ces règles techniques aux sous-traitants. Il apparaît donc bénéfique pour tous les acteurs de la chaîne d'initier un travail de standardisation et de coopération pour définir ces protocoles et API de gestion des droits et des consentements : les responsables de traitement pourront se reposer sur une norme reconnue et légitime, les sous-traitants devront implémenter une fois cette norme pour servir tous leurs clients, les systèmes de gestion du consentement pourront se baser sur cette norme pour garantir une bonne interopérabilité, les personnes concernées se sentiront rassurées et bénéficieront d'une bonne expérience utilisateur.

Matthias De Bièvre :

Matthias De Bièvre est le fondateur et Président de Visions. Matthias a coordonné la partie B mettant en avant l'état de l'art de la recherche grâce aux travaux de nombreux experts et chercheurs mobilisés pour ce Livre Blanc. Visions édite le logiciel VisionsTrust qui permet aux organisations de facilement gérer les droits des personnes sur leurs données.

Son but est de démarquer les organisations vertueuses par la transparence offerte sur les données personnelles et la simplicité du contrôle. Redonner contrôle à chacun sur ses données personnelles est sa mission et la condition d'une innovation éthique et pérenne. Il s'intéresse et agit pour la mutualisation des données au service de la data science, notamment en éducation. Matthias est également conférencier sur l'éthique dans la data science dans plusieurs universités françaises.

c. Vers une Blockchain de consentement ?

Les travaux de la chaire Valeurs et Politiques des Informations Personnelles (VPIP) de l'Institut Mines-Télécom adressent les problématiques du consentement et du principe de responsabilité qui sont au cœur du Règlement Général sur la Protection des Données (RGPD). En effet, un responsable de traitement (RT) doit obtenir le consentement d'une personne physique avant tout traitement de ses données à caractère personnel. De plus, le responsable de traitement (RT) et les sous-traitants (ST) ont obligation de démontrer à tout moment, qu'ils réalisent des traitements sur les données personnelles conformes à l'ensemble des obligations définies par le RGPD, et en particulier conformes aux objectifs convenus avec la personne au moment du consentement.

Deux approches techniques ont été définies et publiées [1, 2, 3] par la chaire VPIP en réponse à ces besoins. D'une part, elles permettent d'adresser le principe de responsabilité en permettant aux RT et ST de conserver une preuve transparente et fiable du recueil de consentement. D'autre part, elles offrent à la personne physique concernée la possibilité de réaliser un audit de façon sécurisée et transparente de sorte (1) à vérifier que les RT et les ST utilisent ses données à caractère personnel conformément aux objectifs initialement convenus, (2) à vérifier si les données ne font pas l'objet de transmissions non consenties entre RTs et STs et (3) à vérifier que le retrait éventuel de son consentement est bien pris en compte dans le système.

Les deux approches conçues reposent toutes deux sur la technologie blockchain[1]. En effet cette technologie offre des garanties de transparence du fait qu'elle assure des propriétés d'authenticité, de disponibilité et d'auditabilité des transactions enregistrées. En contrepartie, ce principe de transparence peut nuire à la vie privée des personnes concernées, dans le sens où certaines données enregistrées dans la blockchain peuvent être identifiantes. Ainsi, l'enjeu consiste à définir une solution d'auditabilité permettant d'enregistrer les consentements des personnes ainsi que tous les traitements effectués sur leurs données, notamment leur transfert d'une organisation (RT, ST) vers une autre, tout en protégeant leur vie privée. Ceci implique de garantir la confidentialité des données à caractère personnel traitées/stockées, et d'empêcher des informations d'être déduites des caractéristiques des transactions enregistrées (types, fréquence...).

1. Une gestion du consentement centrée sur la personne et reposant sur la blockchain :

Dans cette première solution technique proposée [1, 3], la personne concernée est au cœur du dispositif de gestion du consentement. Elle a la responsabilité d'initier un « contrat intelligent » (« smart contract », en anglais) avec chaque RT/ST impliqué dans la collecte et/ou le traitement de ses données à caractère personnel. En effet, le smart contract, sous l'impulsion de la personne concernée, connait les termes du consentement de la personne vis-à-vis de la collecte et l'utilisation de ses données - c'est-à-dire les conditions et finalités des traitements autorisés. Une fois que chaque organisation (RT) a accepté ces termes sous la forme d'une signature électronique, le smart contract enregistre le consentement avalisé par les partis grâce à une transaction, dans la blockchain. Il est ensuite de la responsabilité du RT d'enregistrer chaque traitement sur ces données dans la blockchain. En particulier, s'il décide de transférer des données à un ST, il doit informer la personne concernée de l'intention de transférer ses données personnelles à un tiers et un second smart contract, peut alors être initié entre la personne concernée et le ST sur le même mode

de fonctionnement que le premier.

Pour répondre au besoin de préservation de la vie privée des personnes, la solution respecte les conditions suivantes. Aucune information identifiante n'est inscrite en clair dans la blockchain. Ainsi, aucun lien ne peut être fait, d'une part, entre le contenu des transactions enregistrées dans la blockchain et une certaine personne et, d'autre part, entre deux transactions qui seraient issues d'une même personne. Ce phénomène d'isolation, obtenu par l'utilisation de différents pseudonymes (identifiants inassociables et uniques), permet de préserver la vie privée des utilisateurs.
La solution introduite dans [1] propose deux niveaux d'audit :

- Un audit public basé sur les seules informations disponibles dans la blockchain et qui peut déjà permettre de détecter certaines irrégularités.
- Un audit privé au sein même de l'organisation (RT, ST) qui permet de vérifier la conformité des traitements de données personnelles réalisés en interne par l'organisation au regard des conditions associées aux consentements inscrits dans la blockchain. Cet audit pourrait également être réalisé par une autorité de contrôle.

Un prototype de cette solution de gestion de consentement centrée sur l'utilisateur est disponible en [3] et a été développé par une équipe de Télécom SudParis, Institut Mines Télécom, sur la blockchain publique Ethereum [4].

2. Une gestion du consentement en B2B reposant sur la blockchain :

Cette seconde solution technique [2] vise à contrôler les échanges en B2B, à rendre possible l'audit de ces échanges et à réduire l'intérêt d'échanges directs de données à caractère personnel entre organisations (RT, ST). La solution repose sur une entité appelée « converteur » qui est en charge de traduire des pseudonymes associés à des personnes (en B2B), et ce de manière aveugle. C'est-dire, le converteur participe avec chaque client à la génération d'un pseudonyme unique et inassociable pour chaque fournisseur de service accédé (RT, ST), et ce de manière aveugle ; en d'autres termes, le pseudonyme n'est connu que de la personne et le fournisseur de service ; ni le converteur, ni les autre fournisseurs de services, n'ont connaissance de ce pseudonyme. Ainsi, lors du transfert de données en B2B, les fournisseurs de services doivent passer par l'intermédiaire du converter pour bénéficier de la traduction de pseudonymes. Reste au converter à consigner dans la blockchain tous les échanges B2B et aux fournisseurs à avaliser ces échanges sous la forme de transactions dans la blockchain. Une procédure d'audit peut alors s'appuyer sur les traces laissées dans la blockchain pour vérifier que les transferts de données en B2B sont conformes au RGPD et aux conditions initialement consenties par la personne. La solution [2] respecte la vie privée des personnes du fait que des informations de liaison sont chiffrées en fonction d'un chiffrement multi-niveaux, ce qui permet aux différentes entités/autorités autorisées à accéder uniquement à un sous-ensemble des informations enregistrées.

[1] N. Kaâniche, M. Laurent. A Blockchain-based Data Usage Auditing Architecture with Enhanced Privacy and Availability, IEEE NCA 2017, October 2017
[2] N. Kaâniche, M. Laurent. BDUA : Blockchain-based Data Usage Auditing, IEEE conference on Cloud Computing, San Francisco, CA, USA, 2-7 juillet 2018.
[3] https://github.com/ahmed-mez/consensus-dApp-prototype.
[4] https://www.ethereum.org/

Maryline Laurent :
Dr. Maryline Laurent est professeure en sciences informatiques à Télécom SudParis, Institut Mines-Télécom. Elle dirige l'équipe de recherche R3S du laboratoire CNRS SAMOVAR et est cofondatrice de la chaire Valeurs et politiques des informations personnelles. Elle mène des recherches en sécurité et protection des données personnelles pour des environnements de réseaux.

Nesrine KA NICHE :
Dr. Nesrine Kaâniche est chercheuse en sciences informatiques à Télécom SudParis, et membre de la Chaire Valeurs et politiques des informations personnelles. Elle s'intéresse aux technologies de préservation de la vie privée et à la sécurité dans le cloud. Elle a publié plus de 25 publications dans des revues et conférences majeures.

[1] Pour une meilleure compréhension du fonctionnement de la blockchain et de ses limites, nous invitons le lecteur à se reporter au chapitre 11 du livre no 2 de la Chaire, Signes de confiance : l'impact des labels sur la gestion des données personnelles. https://cvpip.wp.imt.fr/2018/03/19/2018-01-signes-de-confiance-limpact-des-labels-sur-la-gestion-des-donnees-personnelles/

3 - Transparence au service de la confiance et de la conformité et limites

Pour redonner confiance aux individus nous avons vu de façon technique quels seraient les architectures, outils et pratiques pour donner contrôle aux individus sur l'accès au données personnelles et sur l'utilisation faite des données personnelles. Cette partie se concentre sur un aspect fondamental du contrôle sur les données personnelles et donc de la confiance : la transparence. Elle vise à donner des outils, réflexions et méthodologies pour s'assurer que les personnes ont réellement compris l'utilisation faite de leurs données

Différents chercheurs et experts abordent ces sujets :

La confiance est avant tout une relation et dans les applications numériques, la relation entre une personne et une entreprise passe souvent par des interfaces et des expériences utilisateur. Les conceptions de ces interfaces et expériences doivent prendre en compte l'information sur la collecte et l'utilisation des données personnelles pour établir une véritable relation de transparence et d'éthique avec les personnes. Nous devons encourager de méthodologies et règles de conception d'interfaces et expériences à voir le jour tout en étant conscients des limites du "design" seul pour répondre aux enjeux de transparence.

a- Le design et la transparence dans le RGPD : une obligation règlementaire :

a.1 Transparence dans le RGPD

La transparence est mentionnée de façon omniprésente dans le RGPD. Elle est mentionnée transversalement à l'ensemble du règlement en tant que principe, principalement en ce qui concerne la personne concernée et à l'appui des principes du traitement des données et de l'obligation d'information. Le considérant 58, intitulé "Le principe de transparence", introduit des exigences en termes de compréhensibilité. La transparence exige que les utilisateurs, ou même les enfants lorsque cette population vulnérable est impliquée, soient mis en condition de comprendre ce qu'il advient de leurs données.

Les considérants 39 et 60 affinent la transparence en ce qui concerne l'accessibilité, la compréhensibilité et la concision de l'information de la personne concernée en ce qui concerne le traitement des données. Il doit être clairement indiqué : a) que les données sont collectées et traitées et par qui et dans quelle mesure ; b) la finalité du traitement ; c) les risques, les garanties et les droits que le traitement comporte ou peut comporter pour la personne concernée.

La transparence est mentionnée dans d'autres considérants comme une obligation pour les sous-traitants de données, comme un principe de conception de la protection par défaut, comme une qualité à prendre en compte dans la certification et comme un élément de la procédure par laquelle les autorités de contrôle sont désignées (considérants 71, 78, 100 et 121 respectivement). Ces cas sont moins pertinents pour la personne concernée. Elles concernent principalement les responsables du traitement des données, les sous-traitants et les autorités et, pour cette raison, ne seront pas abordées plus en détail dans le présent document.

Là encore, en ce qui concerne les personnes concernées, la transparence apparaît à l'art. 5(1) par principe, ainsi que l'équité et la légalité. Il est inclus en tant qu'objectif éthique dans les codes de conduite dans le cadre de la bonne application du règlement (voir l'art. 40, mais aussi l'article 42, paragraphe 3, et l'article 43, paragraphe 2, où la même notion est soulignée).

Art. 12, intitulée "Transparence de l'information, de la communication et des modalités d'exercice des droits de la personne concernée", traite de la transparence en tant qu'exigence fonctionnelle pour le responsable du traitement lors du traitement des données et définit la qualité des informations que la personne concernée doit recevoir concernant le traitement. L'article 13, paragraphe 2, et l'article 14, paragraphe 2, décrivent plus en détail comment la transparence s'applique à la fourniture d'informations à la personne concernée.

La transparence dans la pratique :

Une telle généralisation des références indique que la transparence joue un rôle assez important dans le règlement. Mais, comme c'est souvent le cas dans les documents juridiques, beaucoup d'efforts sont réservés pour décrire le concept, ses attributs généraux et pour souligner son importance juridique. On en dit beaucoup moins sur la façon de le mettre en œuvre. C'est compréhensible. Le RGPD vise à fournir une protection adéquate et durable indépendamment de la technologie disponible à un moment donné. Ainsi,

même si, dans tous les considérants et articles cités, le règlement qualifie la transparence d'une manière ou d'une autre, il y a une grande marge d'interprétation. Il est difficile de comprendre comment mettre en œuvre la transparence sans une compréhension opérationnelle claire du principe.

Sur le plan pratique, pour avoir une meilleure idée de la façon dont les dispositions du RGPD sont mises en œuvre sur le plan opérationnel, on pourrait se référer à des documents normatifs tels que les normes et les meilleures pratiques. Ils expriment généralement les exigences techniques d'une manière plus claire que dans les documents juridiques.

Les normes et documents similaires sont édités par des comités techniques et n'ont pas besoin d'être soumis aux processus législatifs complexes qui caractérisent plutôt l'élaboration d'un texte législatif. Ils sont ainsi mis à jour plus facilement et plus fréquemment, en adaptant leurs exigences et leurs déclarations à la technologie disponible.

Ils doivent également, comme c'est le cas pour les normes, être certifiés par des autorités désignées. L'activité de certification introduit des mesures reconnues de conformité qui, bien que n'impliquant pas de conformité légale, donnent au moins une présomption de conformité légale. Tout argument dans ce cas doit être étayé par une analyse comparative et interprétative de la corrélation entre les exigences en matière de documents (Bartolini et al 2116). Dans le très rare cas où les normes et les certifications sont endossées par la loi--on parle de normes harmonisées dans ce cas-ci--une conformité aux normes donne aussi une présomption légale de conformité.

En ce qui concerne le RGPD dans son ensemble, il n'existe pas encore aujourd'hui de normes acceptées (et, a fortiori, pas de normes harmonisées) qui traitent directement des dispositions du RGPD, mais beaucoup ont indiqué les normes ISO/IEC comme un moyen viable potentiel de conformité juridique. Les normes de la série 27000, en particulier la norme ISO/IEC 27018 sur la protection des renseignements personnels identifiables et la norme ISO/IEC 29100 sur le cadre de protection de la vie privée, sont pertinentes.

Malheureusement, la situation en matière de transparence est moins marquée. Il n'existe aucune norme qui aborde ce concept. Quelques travaux ont porté sur le respect du principe de transparence du RGPD en dérivant des exigences techniques des articles du règlement. Ils se concentrent sur des aspects spécifiques de ce que l'on croit être des aspects qui contribuent à la transparence. Par exemple, les exigences relatives à la capacité d'intervention, c'est-à-dire l'habilitation des utilisateurs finaux à contrôler le traitement de leurs données personnelles, peuvent être extraites de l'ISO/IEC 29100 (Meis et Heisel, 2017). Les exigences techniques relatives au " droit d'accès ", présentées par le RGPD ainsi que la transparence, peuvent être dégagées du document national sur la protection des données, tel que la loi fédérale allemande sur la protection des données (Bier et al., 2016). Les exigences en matière de transparence peuvent également être suscitées, comme cela a été fait dans (Fischer-Hübner et al., 2014), en examinant les principes de convivialité, en recueillant les avis des ateliers d'experts et en examinant les documents pertinents, tels que le groupe de travail Article 29 sur la protection des données. D'autres documents, tels que le modèle standard allemand de protection des données qui classifie les dispositions de RGPD en termes d'objectifs de protection des données (par exemple, disponibilité, transparence, possibilité d'intervention), peuvent être consultés dans ce processus de déclenchement.

Dans cet exercice de sollicitation, il aide à avoir une vision plus structurée de ce qu'est la transparence.

Une recherche récente sur le sujet suggère que lorsqu'on parle de transparence, deux perspectives doivent être prises en compte (voir Figure, les zones colorées). Une perspective ex ante, pour laquelle la transparence signifie qu'une personne concernée est en mesure d'anticiper ce qu'il adviendra de ses données à caractère personnel, c'est-à-dire d'anticiper les conséquences avant que les données ne soient effectivement divulguées ; une transparence ex post, qui signifie que la personne concernée est en mesure de s'informer sur ce qui est arrivé à ses données personnelles, c'est-à-dire de connaître toute conséquence après la divulgation de celles-ci (Fischer-Hübner et al 2014).

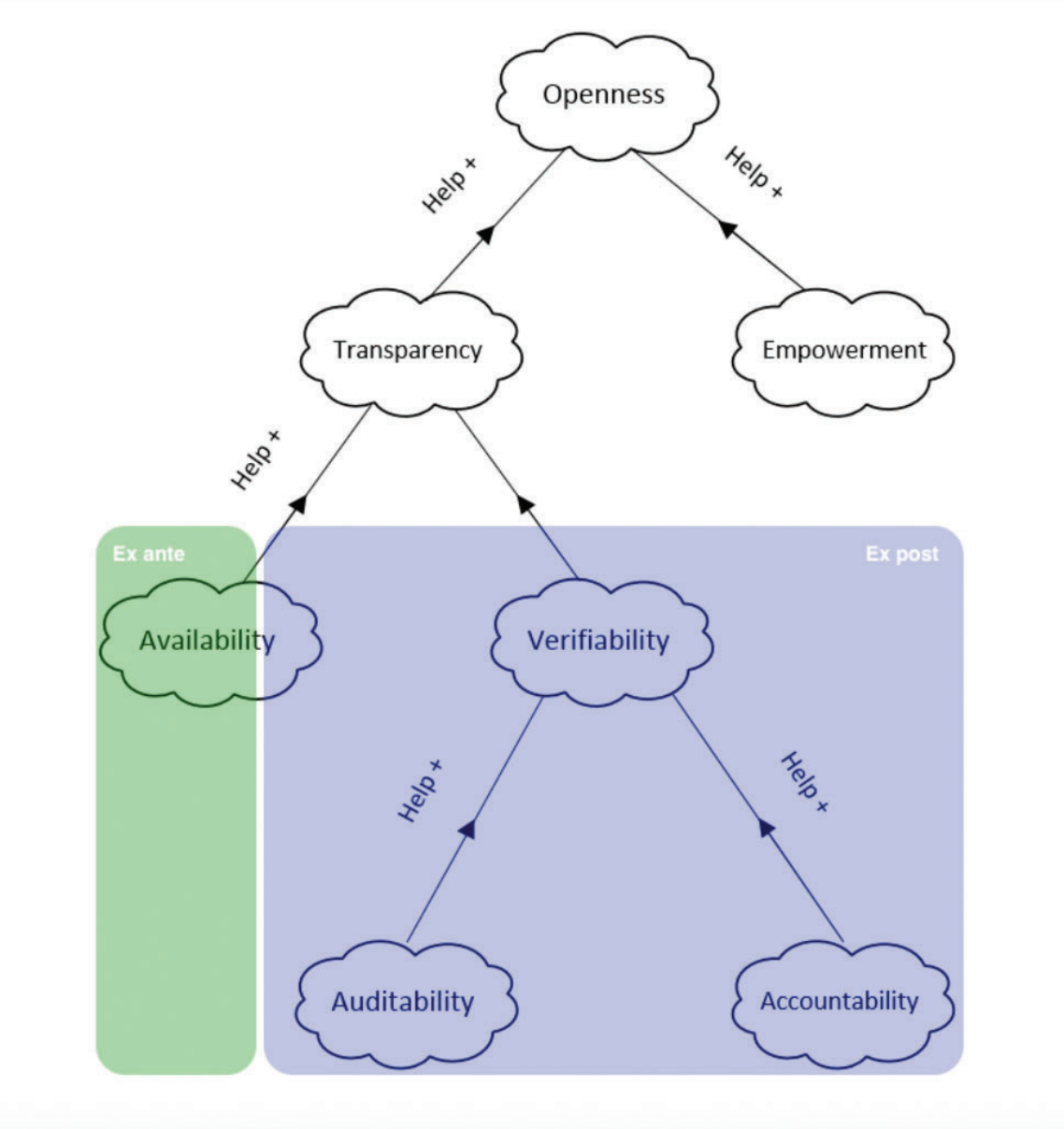
Cette distinction a des conséquences sur les exigences et les moyens techniques de mise en œuvre de la transparence. Une interprétation ex ante reste essentiellement limitée à la question de la fourniture d'informations, un bien que l'on appelle disponibilité. Cette propriété est encore assez abstraite, mais peut être qualifiée par exemple en termes d'accessibilité, de compréhensibilité, d'informativité et de validité de l'information. La liste n'est pas exhaustive. A leur tour, ces qualités peuvent être accompagnées d'attributs mesurables afin qu'une quantification du niveau de cette perspective de transparence devienne possible (Spagnuelo et al., 2017).

Une interprétation ex post va au-delà de la simple mise à disposition d'informations sur ce qui est arrivé aux données d'une personne concernée (par exemple, une atteinte à la protection des données). C'est aussi permettre de vérifier comment le système traite ou a traité les données personnelles. Cette dernière propriété est connue dans la recherche académique sous le nom de vérifiabilité. En général, un système est vérifiable par rapport à une certaine propriété lorsqu'il permet à quelqu'un (variabilité individuelle) ou à quiconque (vérifiabilité universelle) de vérifier que cette propriété est valide lors de l'exécution du système.

La vérifiabilité englobe, en tant que sous-propriétés, la vérifiabilité (lorsque la vérifiabilité fait partie d'une enquête officielle) et la responsabilité (lorsque le système permet également d'attribuer la responsabilité avec une vérification qui révèle une violation).

La distinction ex ante vs ex post conduit à des exigences techniques de transparence variables. Les exigences en matière de transparence ex ante concernent la mise en œuvre d'une solution permettant de mettre en œuvre la disponibilité de l'information et de garantir les différentes modalités selon lesquelles cette disponibilité est réalisée (par exemple, lisibilité, accessibilité, concision, exactitude, portabilité, etc.)

En ce qui concerne le traitement ex post, les exigences techniques devraient également traiter de questions spécifiques concernant la conception du système par rapport au traitement des données. Pour que certaines propositions soient vérifiables, en fait, nous devons mettre en place des mécanismes de collecte, de stockage et de conservation des événements particuliers qui sont nécessaires plus tard au moment de la vérification pour tirer des conclusions valables sur la propriété que nous avons l'intention de vérifier (par exemple, que mon adresse électronique ne soit plus stockée dans la base de données du processeur de données). En gros, nous pouvons dire que le système a besoin d'une boîte noire avec des enregistrements d'événements pour permettre des conclusions solides sur les propriétés à vérifier.



En référence à la Figure 3, nous commentons également une autre distinction importante qui concerne la transparence et l'autonomisation. Bien qu'il n'y ait pas encore de consensus, selon Spagnuelo et al., 2017, l'autonomisation est la capacité de changer quelque chose dans le système, elle est plus forte que la transparence qui consiste plutôt à observer et analyser. Ensemble, la transparence et l'autonomisation contribuent à la notion d'ouverture, conformément au principe de l'initiative open source.

Nous concluons cet excursus sur le sens de la transparence et son applicabilité pratique par la mention d'une technologie particulière qui a émergé comme référence dans la mise en œuvre des mesures de transparence : Outils d'amélioration de la transparence (Transparency Enhancing Technologies - TET).

Les TET sont des applications qu'un utilisateur peut installer pour améliorer le niveau de transparence des

services auxquels il accède également. Il s'agit d'applications autonomes, qui ne sont pas encore prises en compte dans la conception des systèmes, du moins dans la rationalisation du cycle de vie actuel des logiciels, mais qui peuvent certainement être considérées comme une nouvelle technologie logicielle qui mérite notre attention. Les TET concernent à la fois la transparence ex ante et ex post.

Dans l'étude ex ante, nous trouvons les TET classées comme suit : outils d'affirmation utilisés pour révéler et bloquer les traqueurs de services Web ; outils de sensibilisation sur lesquels l'utilisateur peut compter pour mieux comprendre les politiques de confidentialité d'un fournisseur de services comme, par exemple, les outils développés dans le cadre du Usable Privacy Project (Sathyendra et al., 2017) ; et outils de déclaration, similaires aux outils de sensibilisation mais offrant une interactivité, comme par exemple la négociation des politiques sur la vie privée, comme cela a été le cas pour les politiques de la prime vie privée (Fischer-Hübner and Martucci, 2014).

Dans les TET ex post, nous trouvons des outils d'audit qui permettent aux utilisateurs ayant des capacités de lecture spécifiques, par exemple, de connaître les enregistrements originaux et dérivés qu'un sous-traitant possède sur un sujet ; des outils d'intervention, qui offrent en outre un certain niveau d'interaction et de contrôle sur les conditions de collecte et d'utilisation des données ; et des outils de correction qui offrent des fonctionnalités supplémentaires pour exercer activement un contrôle sur la collecte et l'utilisation des données, comme la modification et la suppression de données personnelles enregistrées. On trouvera plus de détails sur l'utilisation des TET et du RGPD dans (Spagnuelo et al., 2019).

Bartolini et al., 2016, A Framework to Reason about the Legal Compliance of Security Standards. C. Bartolini, A. Giurgiu, and G. Lenzini, and L. Robaldo In: Proceedings of the 10th International Workshop on Juris-informatics (JURISIN), 2016.

Spagnuelo et al., 2017, Modelling Metrics for Transparency in Medical Systems.
P. B. D. Spagnuelo; C. Bartolini, and G. Lenzini. In: Proceedings of 14th International Conference on Trust, Privacy and Security in Digital Business (TrustBus), 2017.

Sathyendra et al., 2017. Identifying the provision of choices in privacy policy text. K. M. Sathyendra, S. Wilson, F. Schaub, S. Zimmeck, and N. Sadeh. In: Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing. 2017, pp. 2774–2779

Meis and Heisel 2017, R. Meis and M. Heisel. Computer-Aided Identification and Validation of Intervenability Requirements. In: Information 8.1 (2017), p. 30

Bier et al., 2016, C. Bier, K. Kühne, and J. Beyerer. PrivacyInsight: the next generation privacy dashboard. In: Annual Privacy Forum. Springer. 2016, pp. 135–152.

Fischer-Hübner et al., 2014, S. Fischer-Hübner, J. Angulo, and T. Pulls. How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?. In: Privacy and Identity Management for Emerging Services and Technologies. Vol. 421. Springer Berlin Heidelberg, 2014, pp. 77–92.

Fischer-Hübner and Martucci, 2014. S. Fischer-Hübner and L. A. Martucci. Privacy in social collective intelligence systems. In: Social collective intelligence. Springer, 2014, pp. 105–124

Spagnuelo et al., 2019. P. B. D. Spagnuelo; A. Ferreira, and G. Lenzini. Accomplishing Transparency within the General Data Protection Regulation. In Proceedings of the 5th International Conference on Information System Security and Privacy (ICISSP), 2019

Gabriele Lenzini :

Pr Lenzini est chercheur scientifique Interdisciplinary Centre for Security, Reliability, and Trust (SnT) of the University of Luxembourg l'Université du Luxembourg. Il possède une expertise décennale dans la conception et l'analyse de systèmes numériques sécurisés et privés ; son intérêt plus récent s'étend à des domaines où la sécurité et la protection de la vie privée perdent leur perspective technique et deviennent des concepts interdisciplinaires et socio-techniques.

b. Intégration de la méthode empirique dans la régulation

Il est convenu que la transparence peut diminuer le besoin de confiance des utilisateurs. La question centrale est cependant de savoir comment mettre en œuvre la transparence et l'interprétation des lois afin de répondre aux besoins de la population. Pour différentes mesures réglementaires, nous montrons comment les méthodes d'interaction homme-machine centrées sur l'utilisateur peuvent être intégrées au processus réglementaire et fournir des conseils importants sur les besoins des utilisateurs à l'appui de la gestion de la confidentialité.

1. Protection juridique en cas d'incertitude :

Un régulateur qui cherche à protéger les utilisateurs contre les risques causés par des services et des produits basés sur l'innovation basée sur les données doit se poser, fondamentalement, trois questions :

Premièrement, un tel régulateur doit se demander quels mécanismes de protection il peut exiger dans la loi elle-même et quels sont les éléments que les "destinataires de sa réglementation" (par exemple, les responsables du traitement au sens de l'article 4, paragraphe 7, du RGPD) doivent préciser seuls quand ils interprètent et appliquent la loi. Dans les deux phases, les méthodes de conception empiriques sont très utiles pour s'assurer que les mécanismes de protection à mettre en place sont capables de remplir leur objectif d'amélioration de la protection des utilisateurs des services et des produits. Ainsi, si l'organisme de réglementation exige des mécanismes de protection dans la loi elle-même, par exemple, certaines mesures de transparence, il devrait explorer, tester et évaluer la pertinence de ces mesures, de façon empirique. Si les responsables du traitement des données mettent en œuvre les mesures, ils devraient également vérifier, de manière empirique, si elles répondent effectivement à l'objectif réglementaire.

Deuxièmement, l'organisme de réglementation doit se demander s'il possède suffisamment de connaissances pour être en mesure de préciser tous les mécanismes de protection dans la loi elle-même. Une réglementation aussi détaillée peut s'avérer assez difficile, voire impossible, dans des environnements très innovants, car une "innovation" est, par définition, nouvelle. C'est pourquoi, dans les environnements innovants, les lois sont souvent dépassées lorsqu'elles entrent en vigueur. Pour éviter cette situation, le législateur peut choisir une autre stratégie : Au lieu de déterminer tous les détails par lui-même, un législateur peut aussi se référer à des principes juridiques et à des termes juridiques généraux, et laisser la spécification de ces normes aux destinataires de la réglementation. Par exemple, un responsable de traitement doit ensuite préciser comment mettre en œuvre une obligation générale d'information afin de protéger efficacement les personnes concernées.

Troisièmement, l'organisme de réglementation doit être clair par rapport à ce qu'il veut protéger les utilisateurs. Cela peut sembler évident. Toutefois, comme nous l'avons expliqué précédemment, dans des environnements très innovants, il arrive souvent qu'un régulateur ne sache pas quels risques une innovation future entraînera réellement (et qu'il ne sache pas non plus quels instruments de protection spécifiques sont les mieux adaptés pour protéger les utilisateurs contre un tel risque futur). Par conséquent, le régulateur peut même déléguer l'évaluation de ces risques aux destinataires du règlement. Dans ce cas également, la recherche empirique impliquant de futurs utilisateurs et, par conséquent, leur perception des risques, peut être décisive pour l'efficacité de la protection.

2. Méthodes de conception centrées sur l'utilisateur Amélioration de la protection :

La recherche dans le domaine de l'interaction homme-machine (IHM) place les demandes des utilisateurs au centre de ses recherches. En particulier pour la réglementation devant faire face aux technologies émergentes et évolutives, l'IHM peut fournir un aperçu précoce des besoins des utilisateurs en utilisant un large arsenal de méthodes empiriques de recherche de conception, pour aider essentiellement à accroître l'efficacité des instruments de protection juridique par rapport à un contexte spécifique. Dans ce qui suit, nous montrons comment des méthodes exemplaires d'IHM s'alignent sur les besoins spécifiques des différents processus législatifs décrits au chapitre I et fournissent ainsi une perspective d'utilisateur bien fondée qui informe les régulateurs en tant que destinataires de la réglementation :

Premièrement, sans évaluer le point de vue de l'utilisateur, une réglementation spécifique liée à un objet ou à un service est susceptible d'entrer en conflit avec les demandes des utilisateurs. L'analyse fondée sur des scénarios est une méthode très légère qui permet de découvrir les demandes des utilisateurs en matière de technologie dans le cadre d'un processus législatif. Cela a l'avantage d'être très rapide, mais comme inconvénient que les experts IHM envisageraient les demandes des utilisateurs au lieu d'impliquer réellement les utilisateurs. Une approche fondée sur des méthodes mixtes pourrait fournir des renseignements plus approfondis en permettant d'abord de cerner les besoins de façon exploratoire (p. ex. groupes de discussion, entrevues, ateliers de collaboration ou expériences de rupture), puis de concevoir et d'évaluer les mesures respectives pour répondre aux demandes (évaluation au moyen de prototypes conceptuels, méthodes Wizzard of Oz, sondages). La configuration spécifique décrite ci-dessus fonctionne le mieux dans un contexte et un domaine d'application prédéfinis ou dans une technologie concrète de régulation.

Dans le cas d'une réglementation plutôt générale qui ne vise pas une technologie ou un service particulier, l'IHM peut également éclairer l'application et l'interprétation de la loi. En ce qui concerne des objets ou des services spécifiques, l'IHM peut évaluer les implications des différentes interprétations et recueillir les commentaires des utilisateurs et des autres personnes concernées. En combinant ces impressions avec une marge régulatrice, des solutions de conception peuvent être développées et évaluées de manière itérative avec les utilisateurs, formant ainsi un processus itératif de co-conception.

De plus, l'IHM peut faire des recherches stratégiques sur l'adoption de technologies évolutives et futures pour informer les organismes de réglementation avant même que l'organisme de réglementation ne commence à rédiger une loi. Par exemple, le cadre Living Lab est bien adapté pour cultiver les utilisateurs experts des technologies émergentes en intégrant les prototypes respectifs dans leur vie quotidienne. Les laboratoires vivants permettent d'effectuer des recherches sur l'appropriation des technologies à l'état sauvage sur de plus longues périodes de temps, d'inclure divers intervenants et de co-concevoir en fonction des demandes émergentes. Plutôt que de fournir une expérience en laboratoire limitée à une expérience de premier contact, le cadre Living Labs permet également d'approfondir les cas d'utilisation quotidienne et les problèmes potentiels de confiance et de transparence dans les phases ultérieures de l'utilisation experte. Au sein de Living Labs, la plupart des méthodes peuvent être utilisées pour rechercher des phénomènes spécifiques. l'IHM peut ainsi fournir une évaluation empiriquement fiable de l'impact des

technologies et la traduire en exigences de conception qui, à leur tour, peuvent être reflétées dans des lignes directrices législatives.

3. Concevoir des mesures de transparence dans le cadre du RGPD :

Nous allons maintenant illustrer, dans une troisième étape, comment les considérations précédentes peuvent fonctionner dans la pratique en prenant l'exemple des mesures spécifiques de transparence exigées par l'art. 12-14 et art. 25 du règlement général sur la protection des données (RGPD). Si l'on examine l'approche réglementaire du RGPD, il apparaît clairement que le législateur de l'UE a choisi une stratégie pour relever les défis spécifiques de l'innovation fondée sur les données : Le RGPD ne prévoit pas de dispositions sectorielles spécifiques, mais établit plutôt un cadre intersectoriel composé de principes juridiques et de termes juridiques généraux. L'article 12 sect. 1 qui précise le principe de transparence en vertu de l'article 6 sect. 1 exige des responsables du traitement qu'ils prennent "les mesures appropriées pour fournir toute information (...) sous une forme concise, transparente, intelligible et facilement accessible". Outre la spécification de cette mesure, le législateur de l'UE ne donne que peu d'instructions supplémentaires sur ce qu'il faut faire, mais plutôt sur comment le faire : En mettant en œuvre les mesures appropriées, l'approche de la "protection des données par by design et by default" établie en vertu de l'art. 25 exige que le responsable du traitement le fasse d'une manière qui protège "efficacement" les personnes concernées (c'est-à-dire principalement les utilisateurs de produits et services basés sur des données) contre les risques correspondants. Cela signifie, en ce qui concerne le principe de transparence, que la personne concernée doit être en mesure de comprendre efficacement les risques liés au traitement de ses données. En effet, le législateur ne précise pas lui-même les risques. Toutefois, elle a au moins pensé à la possibilité que le responsable du traitement sollicite, lors de l'évaluation des risques en matière de protection des données, l'avis des personnes concernées ou de leurs représentants sur le traitement envisagé, comme le prévoit l'article 25, point sect. 9 démontre. En effet, tant que le responsable du traitement n'est pas tenu de procéder à une évaluation formalisée des risques en vertu de l'art. 35 RGPD, le responsable du traitement n'est pas tenu, d'un point de vue juridique, d'impliquer les personnes concernées. Cependant, compte tenu de nos considérations précédentes, du point de vue de l'utilisateur, cela est fortement recommandé pour accroître l'acceptation de la technologie.
Dans le souci d'assurer la transparence pour les utilisateurs, c'est-à-dire l'intelligibilité des risques en matière de protection des données liés aux produits ou services axés sur les données, deux aspects sont à l'avant-plan : tout d'abord, il convient d'identifier les risques eux-mêmes tels qu'ils sont perçus par l'utilisateur.
Bien entendu, l'élaboration d'une taxonomie des risques liés à la protection des données qui corresponde au concept de loi sur la protection des données est une tâche majeure pour les juristes et, par conséquent, fait actuellement l'objet de nombreux débats dans le discours juridique. Toutefois, comme on l'a déjà souligné (en se référant à l'article 35, paragraphe 9 du RGPD), ce n'est pas seulement la tâche de l'avocat.

Au contraire, les perceptions des personnes concernées sont également très pertinentes pour une évaluation des risques réussie. Ici, pour mieux comprendre comment les utilisateurs constituent des risques, des méthodes exploratoires comme les entrevues et les groupes de discussion pourraient être utilisées pour déterminer quelles technologies devraient être présentées et discutées.
Une fois les caractéristiques des risques identifiées, la liste pourrait être étendue par le biais de groupes d'experts ou d'autres collectes centrées sur l'utilisateur. En tant que condition préalable à la mise en place de moyens efficaces d'assurer la transparence, il s'agira en premier lieu de s'assurer que les biens et les

objets de protection à communiquer sont correctement compris.
Dans un deuxième temps, il convient d'évaluer les moyens efficaces de communiquer ces risques.

Dans ce cas, le produit ou le service en question devrait déjà être pris en compte lors de la conception de prototypes mettant en œuvre des caractéristiques de transparence basées sur les risques identifiés. Dans l'idéal, le prototype serait évalué de manière quantitative (enquêtes, clics de souris) et qualitative (ux-tests, réflexion à haute voix, entretiens post-tâche) pour évaluer l'efficacité des mesures et commencer une deuxième itération de conception si nécessaire.

Max von Grafenstein :
Max von Grafenstein LL.M. est professeur d'autodétermination numérique à l'Université de Berlin au Career College de l'Université des Arts de Berlin, faisant partie de l'Einstein Center Digital
Future. Il est également co-responsable du programme de recherche " Données, Acteurs, Infrastructures " :
Gouvernance de l'innovation et de la cybersécurité basées sur les données ; à l'Alexander von Humboldt
Institut pour l'Internet et la société (HIIG).

Timo Jakobi :
Timo Jakobi est titulaire d'une maîtrise en interaction informatique. Depuis avril 2012, Timo Jakobi travaille à l'Institut d'informatique économique et des nouveaux médias et à l'Université de Siegen. Dans ses recherches, Timo Jakobi étudie les demandes des utilisateurs concernant la gestion de la vie privée dans l'Internet des objets. En particulier, il cherche à informer le droit du point de vue de l'utilisateur et vice versa, intégrant ainsi les domaines IHM et droit.

c - Le Design au service de la conformité

Depuis 1995, Ann Cavoukian, devenue plus tard Commissaire à l'information et à la vie privée de l'Ontario (CANADA) a proposé la formule et le concept de Privacy by Design, qui au fil du temps a été érigé en principe et repris dans les productions académiques et professionnelles.[1]

Légitimement, le Privacy by Design consiste à appliquer les principes de protection des données dès la conception, concernant le principe de transparence il s'agit donc d'intégrer et d'appliquer la transparence sur les données personnelles et la collecte du consentement dès la conception des interfaces. Cette transparence doit donc faire partie intégrante du produit et est destinée à enrichir agréablement ses fonctionnalités et non être ajoutée à posteriori.
Une information peu claire et/ou accessible ne sera pas jugée conforme, la présence de l'information ne suffit pas : la manière de la présenter compte tout autant.

Dans son Cahier IP[2] de janvier 2019 (Page 10), le laboratoire de la CNIL (LINC) soulignait en ces termes: "Si l'article 25 ne semble pas explicitement s'adresser aux designers, il nous permet cependant de nous intéresser et de pointer le « design de la privacy », la manière dont les différentes techniques du design sont utilisées dans la mise en scène des services pour – et parfois au détriment de – la protection des données des individus, notamment au regard des grands principes que sont la transparence, le consentement et les droits des individus. Une porte d'entrée vers l'association design et régulation".

Certains outils et règles commencent à émerger pour mettre le design au service de la transparence, on peut citer :

Les différents jeux d'icônes existent pour simplifier la compréhension comme celles de l'Association PrivacyTech

La présentation des différentes couches d'information : une information simple et rapide pour tout le monde sur les éléments les plus importants et la possibilité d'aller plus dans le détail pour ceux qui le souhaitent ;

Une information et des demandes de consentement contextuelles : ne pas tout demander en une fois mais demander les consentements lorsque cela est pertinent et nécessaire ;

illustration de l'exemple 3 : Prenons le cas d'une application où l'on peut faire des vidéos en direct à diffuser à son réseau, l'application

---

[1] Ann Cavoukian, Privacy by Design : The 7 Foundational Principles, Information and Privacy Commissioner of Ontario, 2009. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (consulté le 07/12/2018)

[2] Cahier IP de janvier 2018 du laboratoire de la CNIL, le LINC https://linc.cnil.fr/cahier-ip6-la-forme-des-choix

peut demander lorsque la vidéo en direct va commencer si l'utilisateur souhaite activer et afficher la géolocalisation ; plutôt que de le demander à l'installation de l'application. Ceci permet de limiter les actions à l'inscription et d'augmenter les chances d'obtention du consentement, ce qui sert finalement grandement l'application.

Lors d'une collecte de consentement non seulement préciser la finalité du consentement mais également aussi en quoi ces données précisément lui sont utiles et la valeur que va en tirer la personne concernée ;
Utiliser un langage juridique clair, cela implique qu'une personne de 12 ans doit pouvoir comprendre ce qui est énoncé, aussi bien lors des phases de recueil de consentements que dans la politique de confidentialité ;
Comme dans tout bon design : il faut toujours tester ses approches auprès du public et être prêts à changer.

Il est indéniable que tout produit basé sur la donnée personnelle doit mettre le design de ses interfaces et de son expérience au service de la transparence ; non seulement pour être conforme mais également pour acquérir la confiance nécessaire afin de traiter et partager des données personnelles.

Beaucoup de recherche et de règles sur le sujet doivent encore émerger pour répondre à des questions essentielles, par exemple :
Sur les icônes : sont-elles compréhensibles ?
Sur les consentements : quel degré d'information veulent les personnes ? Mettre la durée de conservation des données ou non ?
Sur la transparence : adopter une terminologie commune sur les traitements et les données ?

Dans le sens inverse, il ne faut pas non plus que ce travail sur la présentation et la transparence ne serve de "privacy-washing" à des pratiques organisationnelles peu rigoureuses et une mauvaise gestion des consentements et des droits en général.

Les mesures organisationnelles, techniques et de design doivent s'allier complètement pour respecter efficacement et conformément le principe de Privacy by Design. Enlever donc un de ces trois piliers précités, revient à contredire le principe même.

En définitive, avec le temps, doit émerger une matrice commune ou une modélisation commune des grandes règles du design de manière à rendre fluide la compréhension effective des grands principes de la protection de l'utilisateur connecté. Cette innovation ne saurait être possible sans un large consensus des différents acteurs de l'écosystème. Rappelons que le RGPD à travers le Privacy by design se veut, entre autres, comme un instrument de soft law extraterritorial à destination des éditeurs non européens.

Un nouveau chapitre est donc à dessiner dans lequel Design, Informatique et Juridique s'allieront pour définir les nouveaux schémas du parcours Client dès la conception des offres. Les clés d'un bon design reposent désormais sur la capacité des marques à capitaliser sur les données collectées loyalement. Elles gagneront donc avantageusement en qualité et en réputation ce qu'elles perdront en quantité. A cela, il conviendrait donc d'ajouter la dimension morale qu'implique la simplicité et la clarté dans l'information à délivrer !

Auteurs: Pape Drame (Hub For Health) & Matthias De Bièvre (Visions)

Hub4Health :

L'équipe Hub4Health a rédigé cet article. Hub4Health et son équipe Conformité et Cybersécurité vous accompagne dans la protection de vos données stratégiques ainsi que des données personnelles que vous traitez afin de vous permettre de passer le tournant du numérique en toute sérénité.

2- La transparence de l'éthique comme facteurs de confiance et de performance sur le marché : quelques études et recherches

En 2011, Citigroup, l'un des plus grands établissements bancaires mondiaux, a subi une attaque informatique d'envergure au cours de laquelle les données personnelles de plus de 200 000 clients ont été piratés (noms, emails, numéros de compte). Suite à ce piratage, la valeur boursière de l'action a subi une très forte baisse, avec une perte estimée à près de 860 millions de dollars. Une recherche publiée en 2017 par les universitaires américains Martin, Borah et Palmatier avance que ces pertes auraient été largement moindres (de 16 millions de dollars « seulement »), si sa politique en matière de « data privacy » avait été plus transparente et qu'un contrôle accru sur leurs données personnelles avait été accordé aux clients.

La recherche de Martin, Borah et Palmatier[1] (2017) est ainsi la première à démontrer, à l'appui de données empiriques, un lien entre la politique de l'entreprise en matière de protection des données personnelles et la performance financière de l'entreprise. Ce lien s'explique par le fait qu'un engagement fort de l'entreprise en matière de « data privacy » permet de réduire la vulnérabilité des clients (qu'elle soit réelle, lorsque les risques sont objectivement réduits ou perçue, lorsque le client a le sentiment d'être mieux accompagné / plus en confiance).

Au-delà de la performance financière, avoir des engagements forts en matière de protection des données personnelles est un vecteur de confiance essentiel pour poser le socle de relations durables avec les clients. Si le client se sent vulnérable / ne fait pas confiance à l'entreprise, cela entraîne des conséquences néfastes sur son activité :

- **Les clients peuvent mentir** (Lancelot Miltgen & Smith, 2018[2]). Les rares travaux menés sur ce sujet confirment que le manque de confiance dans l'entreprise sollicitant les données et le souhait de réduire les risques liés à un usage potentiellement détourné des données sont les principaux facteurs expliquant le mensonge (Lancelot Miltgen & Smith, 2018). Ces comportements sont destructeurs de valeur pour l'entreprise, qui collecte ainsi des données erronées. Pour l'entreprise, c'est une double peine : non seulement elle doit engager des ressources (humaines, financières) pour collecter ces données, mais comme celles-ci sont erronées, il lui faut ensuite investir de nouveau pour les nettoyer. L'entreprise pourra par ailleurs baser ses décisions (stratégiques, de communication…) sur des données inexactes, ce qui peut à nouveau représenter un gaspillage des ressources, si ce n'est mettre en péril l'efficacité et le bien fondé de ses décisions.
- **Les clients peuvent résister** (Lancelot, Mimouni et Pez, 2019[3]). Face à la prise de conscience collective des pratiques des entreprises en matière de données personnelles et au danger potentiel que cela représente, les consommateurs entendent reprendre le pouvoir. 88% se disent dérangés par l'exploitation de leurs données personnelles ; 88% aussi se disent inquiets que leur navigation soit enregistrée par des entreprises privées[4]. En réponse, les consommateurs développent des « parades » pour se protéger de ces intrusions. Résultat, le téléchargement de adblocks, sur ordinateur comme sur mobile, ne cesse d'augmenter[5], ce qui représente des pertes de recette publicitaire colossales pour les entreprises.

C'est le signe que les consommateurs ont la volonté de s'équiper de véritables « boucliers » destinés à faire barrage aux pratiques qui entravent, de leur point de vue, leurs principes ou leur liberté. En leur

Virginie Pez-Pérard :

Virginie Pez-Pérard est Maître de Conférences, Habilitée à Diriger des Recherches, à l'Université Paris II – Panthéon-Assas (laboratoire de recherche LARGEPA). Ses thématiques de recherche portent, entre autre, sur l'expérience client. En 2019, elle publie avec ses collègues l'ouvrage « Stratégie Clients Augmentée – La relation client réinventée à l'ère du tout-numérique » (Editions ISTE, in press).

[1] Martin K. D., Borah A. & Palmatier R.W. (2017). Data privacy: effects on customer and firm performance. Journal of Marketing, 81(1), 36-58.

[2] Lancelot-Miltgen C. & Smith J., Falsifying and withholding: exploring individuals' privacy-related decision-making in context, Information and Management, 2018.

[3] Lancelot-Miltgen C., Mimouni-Chaabane A. et Pez V. (2019). Le côté sombre des pratiques de gestion de la relation client à l'ère de la donnée : gérer la résistance et l'intrusion perçue pour des pratiques responsables. In: Stratégie Clients Augmentée, Ed. N'GOALA G., PEZ V. ET PRIM-ALLAZ I. ISTE, chap. 13.

[4] Baromètre Adblocks IAB France/ Ipsos – Novembre 2016, http://www.iabfrance.com/content/presentation-de-la-v2-de-letude-ipsos-realisee-pour-liab-france-sur-les-adblocks.

[5] eMarketer, 2018 Report on AdBlocking https://www.emarketer.com/content/ad-blocking-in-france-2018

Résumé de la contribution :

Cette contribution positionne la transparence des entreprises en matière de données personnelles comme facteur de développement de relations vertueuses avec les clients. Des résultats de recherche font état de liens entre les engagements des entreprises en matière de privacy et leur performance financière. Si le client ne se sent pas en confiance, cela entraîne des conséquences néfastes sur son comportement : il pourrait notamment volontairement transmettre des informations erronées et résister.

3- Principes et cas de transparence :

a. Les icônes comme mécanisme de transparence

Résumé :

Cet article détaillera d'abord les exigences du RGPD en matière d'icônes lisibles par machine destinées à améliorer la transparence des communications relatives à la protection de la vie privée. Ensuite, il donnera un aperçu des initiatives existantes, en mettant l'accent sur les analogies et les différences entre trois études de cas spécifiques : celles de PrivacyTech, de l'Université de Bologne, de l'Institut Weizenbaum. L'article conclut en examinant les potentiels et les limites de l'iconographie pour la protection des données d'un point de vue juridique et psychologique et suggère la voie à suivre pour une efficace mise en œuvre européenne.

1. Introduction :

Le RGPD prévoit l'utilisation d'icônes normalisées et lisibles par machine pour donner aux personnes concernées "d'une manière facilement visible, intelligible et clairement lisible un aperçu significatif du traitement envisagé" (Article 12.7). L'utilisation d'éléments graphiques vise à réduire la quantité excessive d'informations écrites (article 29 WP, 2018), mais aussi à attirer l'attention et à favoriser la compréhension des utilisateurs qui sont habitués à des politique de confidentialité interminables et incompréhensibles. L'appel du RGPD en faveur des éléments graphiques comme moyen de mettre en œuvre le principe de transparence est sans précédent dans la législation de l'UE en matière de protection des données et promet potentiellement de résoudre des problémes connus de longue date sur les politiques de confidentialité qui sont rarement lues et mal comprises (pour plus de précisions sur ce point, V. Legal Design Pattern, p.164). Toutefois, certaines questions restent ouvertes : Comment sélectionner les icônes ? Que doivent représenter les icônes ? Quelle devrait être leur fonction ? Quelles sont les composantes d'une mise en œuvre réussie ? Le présent article présente brièvement certaines initiatives existantes au niveau de l'UE qui tentent de répondre à ces questions.

2. Initiatives antérieures :

Il existe certaines initiatives qui visent à créer une iconographie pour résumer les pratiques en matière de données, bien qu'elles n'aient été ni acceptées ni largement adoptées. En ce qui concerne l'Union Européenne, deux initiatives importantes méritent d'être mentionnées pour motiver la recommandation du RGPD sur les icônes. Le projet européen PrimeLife a notamment mené une première enquête (Graf et al., 2011) qui a abouti à une tentative structurée de créer et d'évaluer un jeu d'icônes pour le domaine de la protection des données de l'UE sur une base factuelle. Un effort différent a été réalisé par la commission LIBE, qui a recommandé d'inclure un tableau contenant six icônes et leur description dans le projet de rapport de 2013 sur la proposition du RGPD (Parlement européen, 2013). Bien que ces icônes aient finalement été abandonnées, on peut trouver des traces de cette proposition dans l'appel à icônes du RGPD.

3. Initiatives en cours :

Dans ce qui suit, afin d'illustrer les différentes approches, trois projets développés par l'éditeur de ce livre blanc et les groupes de recherche des auteurs de cet article sont présentés.

3.1 Privacy Tech :

A l'image des générateurs de licences Creative Commons, la Privacy Tech a lancé une initiative sur des « Privacy Icons » et développé un ensemble d'icônes représentant différents aspects du traitement des données à caractère personnel : catégorie de données à caractère personnel avec les données d'identification, de vie personnelle, de vie professionnelle, d'informations d'ordre économique et financier, de géolocalisation, d'opinions politiques, de données génétiques, de durée de conservation (par exemple pas de conservation, un an de conservation, durée légale de conservation), de partage avec des tiers, politique de sécurité, objectifs de traitement (par exemple commerciaux, marketing), transfert international et modifications de la politique de confidentialité.

L'objectif est de permettre à tout organisme de les utiliser pour afficher de manière graphique son engagement Privacy sur son site ou sa plateforme web correspondant à ses conditions générales d'utilisation étant donné que ces dernières sont rarement lues.

Ce travail est le résultat du Privacy Hackhaton du 16 mars 2017 regroupant une centaines d'expert de Privacy et de plusieurs ateliers pour la mise en œuvre afin réaliser ce qui a été envisagé.

https://www.privacytech.fr/privacy-icons/

3.2 DaPIS : le Data Protection Icon Set de l'Université de Bologna :

Le CIRSFID (Université de Bologne, IT, www.cissfid.unibo.it), en collaboration avec l'Académie des Beaux-Arts de Bologne et la Società Italiana Informatica Giuridica (SIIG), a développé DaPIS, un ensemble d'icônes de protection des données représentant : (1) les opérations de traitement des données et les données traitées (par exemple, données rendues anonymes, données cryptées), (2) les finalités du traitement (par exemple, à des fins commerciales, scientifiques), (3) les bases juridiques du traitement (par exemple, obligation légale, consentement), (4) les agents et rôles (par exemple, personne concernée, contrôleur des données, autorité de contrôle), (5) les droits de l'intéressé (par exemple, droits d'accès, droit à l'effacement et à la portabilité).

Le DaPIS peut être visionné à l'adresse suivante : http://gdprbydesign.cirsfid.unibo.it/dapis-2/.

Rossi 2019 et Rossi, Palmirani 2019 décrivent les recherches liées au design du jeu d'icône.

3.2.1. Fonction : icônes d'accompagnement

Les icônes DaPIS ont été conçues comme des icônes d'accompagnement, c'est-à-dire des " symboles graphiques qui représentent le sens ou la fonction de l'élément textuel qu'ils accompagnent " (p. 26,

Haapio & Passera, à venir, traduit par l'éditeur). Ils aident les lecteurs à rechercher et à trouver rapidement l'information pertinente, surtout dans les textes longs et indifférenciés comme les politiques de protection de la vie privée, et appuient la mémorisation. Ils peuvent également mettre en évidence et communiquer rapidement les aspects clés des pratiques d'une organisation en matière de protection de la vie privée, et peuvent donc être utilisés dans les consentements.

3.2.2. Sélection des concepts :

Les concepts DaPIS ont été sélectionnés conformément à l'Art. 13-14 RGPD et ont été intégrés à d'autres concepts importants, formalisés dans le PrOnto de l'ontologie computationnelle (Palmirani, et al., 2018). Le fondement ontologique a joué un rôle déterminant dans la création d'un ensemble d'icônes lisibles par machine (tel que fourni par le RGPD), à savoir un langage iconique dont les éléments ont des significations interprétables par ordinateur qui sont explicitement et officiellement définies dans l'ontologie. Grâce au balisage XML des expressions linguistiques des documents, les applications peuvent récupérer et afficher de manière semi-automatique les icônes codées dans l'ontologie à proximité des morceaux de texte pertinents dans le document.

3.2.3. Conception participative :

DaPIS a été créé grâce à la conception participative, c'est-à-dire une "méthodologie de conception dans laquelle les futurs utilisateurs d'un design participent en tant que co-designers au processus de conception" (p. 41, Van der Velden & Mörtberg 2015, traduit par l'éditeur). Une série d'ateliers s'est tenue entre juillet 2017 et juillet 2018 (à l'Université de Stanford et à l'Université de Bologne) et a impliqué différents acteurs : un groupe hétérogène de graphistes, avocats et juristes, informaticiens, professionnels de la communication, profanes intéressés et représentants du monde des affaires. Cela a permis d'exprimer les différentes valeurs et priorités des parties prenantes susceptibles d'être affectées par le jeu d'icônes, tout en évitant de négliger un aspect fondamental de la conception des icônes juridiques. Les ateliers ont suivi le processus de design (juridique) proposé par M. Hagan (n.d.), qui comprend une série d'étapes par lesquelles les participants élaborent, testent et affinent une ou plusieurs solutions à des problèmes spécifiques dans un cycle itératif. Ainsi, DaPIS a évolué au fil du temps, d'une version prototype à la version réelle, pour refléter les retours d'expérience recueillis lors des ateliers et des phases d'évaluation.

3.2.4. Évaluation

L'évaluation de DaPIS s'est déroulée en trois phases successives au fur et à mesure de l'évolution du jeu d'icônes. Au total, 42 participants d'origines, d'horizons professionnels et d'âges différents ont été recrutés et ont été invités à noter et commenter les icônes produites lors des ateliers, en fonction de leur lisibilité et de leur compréhensibilité. Les commentaires recueillis ont permis d'affiner les icônes existantes, d'écarter les icônes peu prometteuses et d'en proposer de nouvelles, plus prometteuses.

3.3 Une approche fondée sur les risques : Le Privacy Icon Project du Weizenbaum Institute for the Networked Society

Le groupe de recherche interdisciplinaire " Data as a Means of Payment " de l'Institut Weizenbaum vise

à développer des icônes de protection de la vie privée qui soutiennent le processus décisionnel des utilisateurs vers un consentement plus autodéterminé et éclairé. D'un point de vue psychologique, un changement dans la manière dont les conséquences négatives possibles des aspects informatiques sont communiquées aux utilisateurs pourrait atténuer certains des problèmes les plus courants, par exemple l'asymétrie d'information ou certaines limitations cognitives. Par conséquent, le groupe de recherche prévoit de développer un ensemble d'icônes qui permet de visualiser les aspects liés au traitement des données tout en communiquant indirectement leur niveau de risque inhérent.

3.3.1 Sélection des concepts :

Les risques liés au traitement des données seront évalués au moyen d'une analyse qualitative multiméthodologique des risques. L'objectif principal de la première phase est d'élaborer un catalogue complet des risques fondé sur le concept de risques associés au traitement des données du RGPD par le biais d'une analyse systématique et qualitative du contenu du RGPD par des avocats ainsi que d'un enrichissement de la liste par des entretiens avec des experts. Un classement ultérieur des aspects du traitement des données en fonction de leurs risques inhérents, basé sur des critères prédéfinis, par des experts et un échantillon représentatif d'utilisateurs, déterminera les aspects finaux du traitement des données qui devront être visualisés. Après ce processus de sélection, les icônes seront conçues, testées, évaluées et révisées à différents stades du processus de développement selon des méthodes mixtes en fonction de leur utilisation prévue.

3.3.2 Fonctionnement :

La fonction principale des icônes est de transmettre du sens tout en préservant les ressources cognitives des utilisateurs et en augmentant leur attention, leur conscience et leur motivation dans le traitement des données.

– Effort cognitif : Les icônes de protection de la vie privée fondées sur le risque peuvent faciliter et accélérer la compréhension des aspects liés au traitement des données et de leurs risques inhérents, ce qui exige moins de ressources cognitives (Stenberg, 2006) pour inclure non seulement les " avantages " mais aussi les " coûts " possibles (= conséquences négatives) dans le processus décisionnel.

– Attention : Les utilisateurs se concentrent sur leur objectif principal, par exemple l'acquisition d'un produit ou d'un service numérique, mais dans la plupart des cas, pas sur la protection des données. Pour déplacer les processus attentionnels de la tâche principale vers les questions de protection des données, nous avons besoin de stimuli externes très importants (attention ascendante).

– Motivation : Fournir aux utilisateurs des informations sur les aspects liés au traitement des données et leurs risques inhérents peut les motiver à adopter un comportement plus protecteur comme l'indique la théorie de la motivation de protection (Boss, Galletta, Lowry, Moody & Polak, 2015).

– Prise de conscience : Un jeu d'icônes normalisé et fondé sur les risques peut accroître la volonté de s'engager dans le traitement des données et la sensibilisation à ses aspects en raison de l'exposition et de la confrontation constantes. Toutefois, la culture numérique pour apprendre les aspects liés au traitement des données, pour favoriser la compétence décisionnelle et pour sensibiliser l'opinion est d'une grande importance et doit être un complément indispensable.

4. Potentiels et défis :

4.1 Potentiels :

Si nous comparons les mots aux images, il a été prouvé que les images ont un avantage en termes de reconnaissance plus rapide et de rappel de mémoire moins difficile - un effet connu sous le nom de supériorité d'image (Paivio, 1971). Par rapport au texte brut, des icônes bien conçues et normalisées facilitent la compréhension et l'accessibilité, attirent l'attention, économisent les ressources cognitives et surmontent les barrières linguistiques et tiennent compte des différences culturelles. En outre, la mise en œuvre d'un jeu d'icônes normalisé crée une comparabilité entre les sites Web, ce qui peut accroître la sensibilisation des utilisateurs à leurs choix. Comme l'ont démontré les expériences, les renseignements sur la protection de la vie privée qui sont saillants et faciles d'accès et à comprendre pendant la prise de décision suscitent davantage de comportements protecteurs (surtout dans le contexte du commerce électronique ; Tsai, Egelman, Cranor et Acquisti, 2011).

4.2 Défis à relever :

L'utilisation fréquente et généralisée d'icônes standardisées comporte le risque d'effets d'accoutumance. Cependant, certains mécanismes comme les variations polymorphes ou la présentation d'icônes saillantes pourraient contrecarrer l'accoutumance. De plus, les limites d'attention et de mémoire de travail doivent être prises en compte en ce qui concerne le nombre d'icônes qui doivent être affichées. Un jeu d'icônes normalisé ne pourra pas tenir compte des différences interindividuelles de besoins et de préférences, comme cela pourrait être fait avec les outils de gestion de la vie privée.

5. Conclusion :

Le but premier et véritable des icônes est de refléter l'information qui est très pertinente pour les utilisateurs et de communiquer la signification d'une manière rapide et sans effort. Elles doivent être considérées comme un ajout à la politique de protection de la vie privée complète : elles représentent le premier niveau d'attention d'une architecture d'information descendante, qui inclut la politique de protection de la vie privée complète comme dernier sous-niveau. La sélection, la conception, la mise en œuvre et l'acceptation des icônes par les utilisateurs sont cruciales et, comme le montrent déjà les trois projets présentés, il existe différentes approches. Un échange de connaissances entre les initiatives existantes favoriserait la mise au point d'une approche fondée sur des données probantes, débouchant sur un ensemble significatif d'icônes qui pourraient être proposées comme normes ou au moins comme meilleures pratiques et mises en œuvre au niveau communautaire.

Article 29 Working Party. "Guidelines on Transparency under Regulation 2016/679, 17/EN WP260", 2018.

European Parliament. Committee on Civil Liberties, Justice and Home Affairs "Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [COM(2012)0011 - C7-0025/2012 - 2012/0011 (COD)] ", 2013, Annex 1.

Boss, Scott, et al. "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors." MIS Quarterly (MISQ) 39.4 (2015): 837-864.
Graf, Cornelia, et al. "Final HCI research report." Primelife Project Deliverable D 4 (2011).

Haapio, Helena and Stefania Passera. "Contracts as interfaces: Exploring visual representation patterns in contract design". In R.A. Dolin M. J. Katz and M. Bommarito, editors, Legal Informatics. UK: Cambridge University Press, Forthcoming.

Hagan, Margaret. "Design Process for Lawyers" In M. Hagan, Law by Design, n.d. Available at: http://www.lawbydesign.co/en/home/ (Last accessed: March 14, 2019).

Palmirani, Monica, et al. "A Methodological Framework to Design a Machine-Readable Privacy Icon Set." Data Protection/LegalTech Proceedings of the 21st International Legal Informatics Symposium IRIS18, 2018.

Palmirani, Monica, et al. "Legal Ontology for Modelling RGPD Concepts and Norms." Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference. Vol. 313. IOS Press, 2018.

Paivio, Allan. Imagery and Verbal Processes. Holt, Rinehart & Winston, 1971.

Palmirani, Monica, and Fabio Vitali. "Akoma-Ntoso for legal documents." Legislative XML for the semantic Web. Springer, Dordrecht, 2011. 75-100.

Rossi, Arianna, and Palmirani, Monica. "A visualization approach for adaptive consent in the European data protection framework." 2017 Conference for E-Democracy and Open Government (CeDEM). IEEE, 2017.

Rossi, Arianna and Palmirani, Monica. " DAPIS an ontology-based Data Protection Icon Set". Knowledge of the law in the Big Data Age, edited by G.Peruginelli and S.Faro, Ios Press, forthcoming.

Rossi, Arianna "Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts". Alma Mater Studiorum Università di Bologna. Dottorato di Ricerca in Law, Science and Technology, 30 Ciclo, 2019.

Tsai, Janice Y., et al. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." Information Systems Research, vol. 22, no. 2, June 2011, pp. 254–268. EBSCOhost, doi:10.1287/isre.1090.0260.

Stenberg, Georg. "Conceptual and Perceptual Factors in the Picture Superiority Effect." European Journal of Cognitive Psychology, vol. 18, no. 6, Nov. 2006, pp. 813–847. EBSCOhost, doi:10.1080/09541440500412361.

Van der Velden, Maja, and Christina Mörtberg. "Participatory design and design for values." Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains (2015): 41-66.

Arianna Rossi :

Arianna Rossi est chercheuse au centre interdisciplinaire SnT de l'Université du Luxembourg. Ses sujets de recherches comprennent la conception juridique, l'iconographie et la communication visuelle des aspects liés à la protection des données, à la vie privée et à la sécurité. Elle est co-fondatrice de la Legal Design Alliance et co-auteure d'un manifeste relatif au Legal Design.

Marie Schirmbeck :

Marie Schirmbeck (MSc Psychologie) est associée de recherche à l'Institut Weizenbaum pour la société en réseau à Berlin. Auparavant, elle a travaillé comme analyste en conversion. Ses recherches portent sur les processus dynamiques cognitifs et émotionnels-motivationnels qui sous-tendent la divulgation souvent étendue de données personnelles par les individus et les conséquences individuelles et sociétales de ce comportement.

Modèles de “Legal Design” pour la transparence de l’information dans les informations liées à la vie privée :

Résumé :

Les divulgations obligatoires liées au traitement des données présentent de nombreux problèmes bien documentés. Après avoir brièvement exposé les problèmes, nous présentons les modèles de “Legal Design” comme une solution possible offrant de multiples moyens efficaces pour favoriser la transparence de l’information sur les pratiques en matière de données.

1. Obstacles à l’efficacité des avis sur la protection de la vie privée :

L’article 12 du RGPD fixe un ensemble d’obligations de transparence pour les responsables de traitement, qui prennent les mesures appropriées pour fournir aux personnes concernées certaines informations spécifiques sur le traitement des données (énumérées aux articles 13 et 14 du RGPD) “sous une forme concise, transparente, intelligible et facilement accessible, dans un langage clair et compréhensible”.

La recherche et la pratique nous montrent que les méthodes traditionnelles d’information des personnes concernées ne fonctionnent pas. Les raisons en sont multiples et comprennent les suivantes :

Problème	Brève description	Référence
Illisibilité due aux petits caractères	La petite taille des caractères, certaines familles de caractères et le manque d'interlignes peuvent dissuader les utilisateurs de lire la politique de confidentialité, les décourager rapidement ou affecter l'intelligibilité du texte.	Rello et al. 2016 BEUC, 2017
Complexité linguistique	Le langage employé dans les avis de confidentialité peut être si complexe qu'il dépasse la compréhension de l'utilisateur moyen d'Internet.	Fabian et al., 2017; Jensen & Potts 2004
L'imprécision des termes	Une utilisation extensive d'expressions vagues telles que "Nous pouvons collecter des informations sur vous" et "nous divulguons certaines données personnelles à des tiers" peut laisser le lecteur perplexe quant à leur signification.	Pollach, 2004 Reidenberg, 2016
Mur de texte	Les politiques de protection de la vie privée peuvent être affichées sous la forme d'un "mur de texte" qui est "impénétrable" à l'œil humain en raison de l'absence de hiérarchie de l'information et d'organisation visuelle significative (p. ex. paragraphes, titres, variété des tailles de police). Par conséquent, il est difficile de naviguer dans le document et de trouver de l'information.	Passera, 2015 EDPS, 2015
Manque de connaissance	La plupart des utilisateurs n'ont pas les connaissances et l'expérience nécessaires pour comprendre et évaluer les conséquences de leurs comportements de divulgation de données.	Solove, 2013

Manque d'adaptation à l'auditoire	Les avis de confidentialité sont souvent rédigés "par des avocats pour des avocats", au lieu de tenir compte de leur public cible. Souvent, l'envoi d'avis vise simplement à satisfaire à l'exigence légale de divulgation obligatoire, au lieu d'informer efficacement les personnes concernées de la collecte et du traitement de leurs données à caractère personnel.	Berger-Walliser et al., 2011, p. 56 ; Robinson et al., 2009
Mauvais moment	Le choix du moment est une dimension cruciale pour l'efficacité des avis : s'ils sont affichés à un moment inopportun (par exemple lors de l'exécution d'une tâche différente), les utilisateurs peuvent les percevoir comme une nuisance et les ignorer.	Obar & Oeldorf-Hirsch, 2016 ; Schaub et al., 2015 ; WP29, 2018
Longueur excessive	Les chartes de confidentialité ont tendance à être extrêmement longs et nécessitent beaucoup de temps pour être lus (p. ex. 30 min environ pour une politique de confidentialité moyenne). Cependant, au lieu d'accroître la compréhension, une information excessive peut entraîner une surcharge d'information et décourager les utilisateurs de la lire.	Obar & Oeldorf-Hirsch, 2016 ; Calo, 2011
Comparabilité difficile	En raison de l'absence de formats structurés normalisés, il est difficile de comparer des renseignements semblables d'une politique de protection de la vie privée à l'autre.	Kelley et al. 2010
Fatigue de l'attention	La rareté de l'attention empêche les utilisateurs d'analyser soigneusement le nombre de notification qu'ils reçoivent. Les utilisateurs peuvent choisir de ne pas consulter la politique de confidentialité d'un service parce qu'ils supposent que le coût en temps (c.-à-d. le coût de transaction) ne serait pas compensé par les avantages de la lecture. Dans ce cas, choisir de ne pas lire est un choix délibéré.	Hartzog, 2018 ; Zuiderveen Borgesius, 2013

Le "Legal Design" est un nouveau domaine émergent de recherche et de pratique, une approche interdisciplinaire qui applique une conception centrée sur l'être humain pour prévenir ou résoudre des problèmes juridiques. Il offre un certain nombre de moyens prometteurs pour surmonter ces obstacles afin de mettre en œuvre le principe de transparence d'une manière centrée sur l'utilisateur, conformément aux orientations proposées par le WP29, 2018. Dans cette contribution, nous proposons des modèles de conception juridique pour soutenir la mise en œuvre effective du principe de transparence dans le cadre du RGPD.

2. Surmonter les obstacles : Modèles de Legal Design

Les modèles de conception sont des modèles réutilisables d'une solution à un problème courant (Haapio & Passera, à paraître). Entre autres choses, ils aident à sélectionner et à décrire les meilleures pratiques et les normes sur les solutions réalisables pour un problème donné ; et proposent une lingua franca pour partager les connaissances et l'innovation sur des défis similaires dans tous les domaines (Haapio et Hagan, 2016).

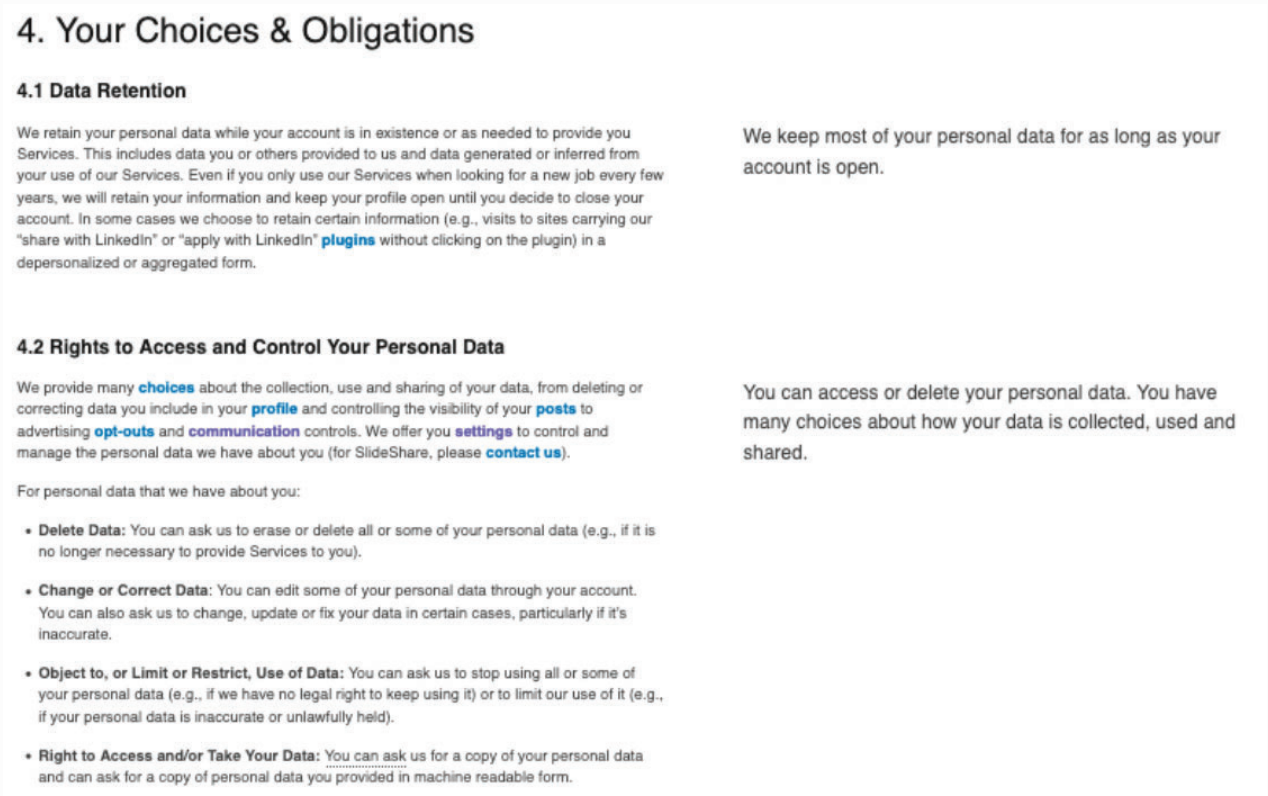
Dans ce qui suit, nous présentons un résumé des modèles de conception de l'information juridique qui sont destinés à résoudre les obstacles communs à la communication liés au traitement des données.

2.1 Exemple à titre d'illustration :

Donner un exemple en langage clair et simple pour clarifier les termes juridiques et techniques ou pour rendre les énoncés abstraits plus tangibles.
Problèmes : Complexité de la langue ; imprécision des termes ; manque d'adaptation l'auditoire ; manque de connaissance.
Exemple : "Ce sont les principales raisons pour lesquelles nous recueillons et utilisons des données sur nos utilisateurs ; Pour vous montrer l'actualité qui est pertinente pour vous et pour améliorer votre expérience sur notre site ; Pour fournir les services auxquels vous vous inscrivez, tels que les abonnements; Pour effectuer des analyses marketing et vous envoyer des communications lorsque nous avons votre permission, ou lorsque la loi le permet ; Pour nous permettre de montrer de la publicité sur nos sites".

2.2 Résumés :

Placez des résumés rédigés en langage clair et simple sur les informations essentielles, soit à côté de la clause originale de la politique de confidentialité, soit au début de celle-ci. Les résumés offrent différents niveaux de profondeur de l'information et répondent donc simultanément aux besoins de ceux qui ne veulent saisir que la teneur de la politique de confidentialité et de ceux qui veulent être informés en profondeur.
Problèmes : Petits caractères ; complexité de la langue ; imprécision des termes ; mur de texte ; longueur excessive ; mauvais moment ; manque de connaissance ; fatigue de l'attention.
Exemple : Image 1



4. Your Choices & Obligations

4.1 Data Retention

We retain your personal data while your account is in existence or as needed to provide you Services. This includes data you or others provided to us and data generated or inferred from your use of our Services. Even if you only use our Services when looking for a new job every few years, we will retain your information and keep your profile open until you decide to close your account. In some cases we choose to retain certain information (e.g., visits to sites carrying our "share with LinkedIn" or "apply with LinkedIn" **plugins** without clicking on the plugin) in a depersonalized or aggregated form.

We keep most of your personal data for as long as your account is open.

4.2 Rights to Access and Control Your Personal Data

We provide many **choices** about the collection, use and sharing of your data, from deleting or correcting data you include in your **profile** and controlling the visibility of your **posts** to advertising **opt-outs** and **communication** controls. We offer you **settings** to control and manage the personal data we have about you (for SlideShare, please **contact us**).

For personal data that we have about you:

- **Delete Data:** You can ask us to erase or delete all or some of your personal data (e.g., if it is no longer necessary to provide Services to you).
- **Change or Correct Data:** You can edit some of your personal data through your account. You can also ask us to change, update or fix your data in certain cases, particularly if it's inaccurate.
- **Object to, or Limit or Restrict, Use of Data:** You can ask us to stop using all or some of your personal data (e.g., if we have no legal right to keep using it) or to limit our use of it (e.g., if your personal data is inaccurate or unlawfully held).
- **Right to Access and/or Take Your Data:** You can ask us for a copy of your personal data and can ask for a copy of personal data you provided in machine readable form.

You can access or delete your personal data. You have many choices about how your data is collected, used and shared.

Img 1. Un exemple de la politique de confidentialité de LinkedIn, montrant des résumés à côté des clauses verbeuses originales. L'exemple montre également l'organisation du texte et des sujets dans une structure cohérente et visuellement différenciée.

2.3 Commande et étiquettes :

Organiser la politique de confidentialité d'une manière significative: chaque sujet est couvert dans une section spécifique qui est étiquetée avec une rubrique cohérente et informative pour soutenir la navigation dans les documents et la recherche d'informations.
Problèmes : Petits caractères ; mur de texte ; comparabilité difficile.
Exemple : Image 3 et Image 1.

2.4 Table des matières :

Fournir une table des matières qui donne un aperçu des sujets couverts dans la politique de confidentialité et un système de navigation rapide vers la section pertinente du document. Placez le menu soit au début de la page, soit dans une boîte flottante sur le côté. Cette structure est particulièrement utile pour un affichage efficace sur de petits écrans.
Problèmes : Mur de texte ; comparabilité difficile.
Exemple : Image 2.

TABLE OF CONTENTS

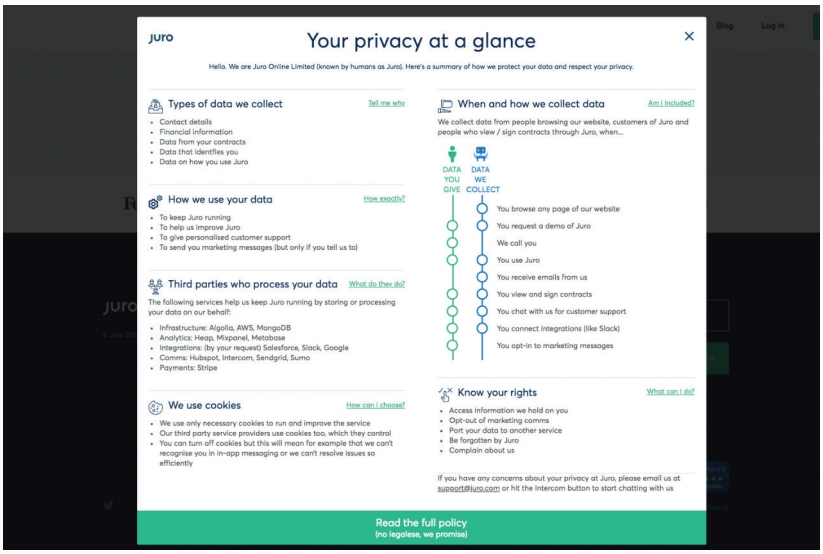
Img. 2 : une table des matières navigable placée au début de la politique de confidentialité. Le tableau fournit également une brève explication de ce que le lecteur peut s'attendre à trouver dans chaque section. Extrait de la politique de confidentialité du National Geographic.

2.5 Information à tiroir :

Distribuez l'information sur des couches séparées, de sorte que les utilisateurs puissent avoir un aperçu du contenu de la politique de confidentialité dès la première couche, tandis qu'ils peuvent explorer les détails contenus dans des couches supplémentaires sur demande.

Problèmes : Mur de texte ; longueur excessive ; manque d'adaptation à l'auditoire ; mauvais moment ; manque de connaissance.

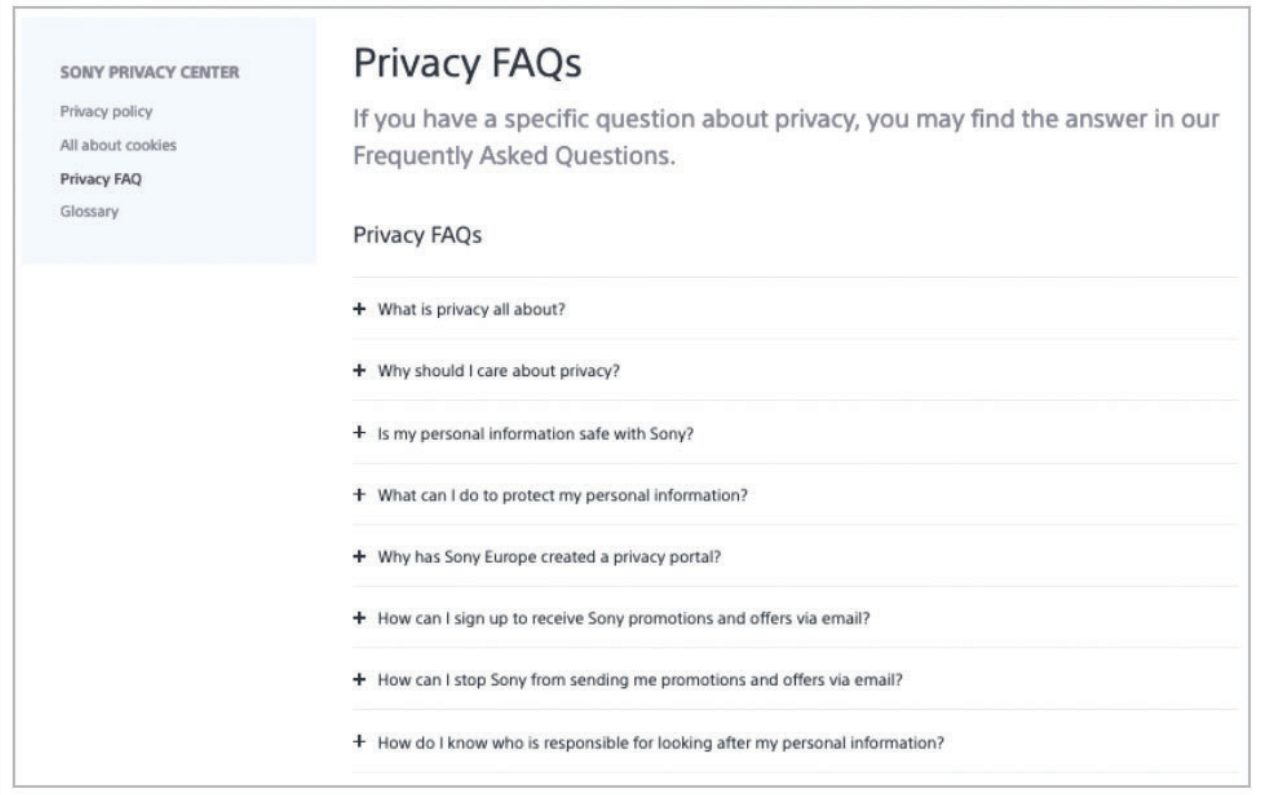
Exemple : Voir Image 3.



La première couche de la politique de confidentialité de Juro, affichée lorsque l'utilisateur arrive sur la page principale (https://juro.com/). Les liens à côté de chaque section fournissent des paragraphes extensibles, tandis que le lien en bas renvoie à la politique de confidentialité complète. Cet exemple montre également une implémentation possible d'icônes indicatifs et d'une chronologie indiquant l'heure de la collecte des données personnelles.
Redessiné par Stefania Passera.

2.6 Questions fréquentes :

Fournir des explications simplifiées et faciles à consulter sur les questions les plus fréquemment posées et sur les pratiques les plus pertinentes en matière de données.
Problèmes : Complexité de la langue, imprécision des termes, longueur excessive, manque d'adaptation à l'auditoire, mauvais moment, manque de connaissance, comparabilité difficile.
Exemple : Image 4.



La FAQ de Sony sur la protection de la vie privée, avec des questions d'ordre général sur la protection de la vie privée, mais aussi des tutoriels "comment faire...".

2.7 Icônes d'accompagnement :

Inclure des icônes dans la politique de confidentialité pour indiquer visuellement où se trouve un élément d'information. Utilisez des icônes en combinaison avec du texte dans un avis en couches pour offrir un aperçu rapide de son contenu. Les icônes peuvent soutenir la recherche d'informations dans de longs documents et la mémorisation.
Problèmes : Mur de texte ; comparabilité difficile.
Exemple : Image 3 et Image 5.

Hello! We are the International Association of Contract and Commercial Managers Inc, but we are usually referred to as IACCM. There are three companies that form IACCM and this Privacy Policy applies to all three:

Our US Parent Company: International Association of Contract and Commercial Managers Inc
Our UK Service Company: IACCM EMEA Limited
Our Australia Service Company: IACCM Pty Limited

IACCM is committed to protecting your privacy and we include this commitment in our Code of Conduct. We have prepared this Policy to describe to you our practices regarding the Personal Data we collect from you, how we protect it and respect your privacy. If you have any questions about this Policy, then please contact info@iaccm.com.

Types of Data We Collect

IACCM collects Personal Data and Anonymous Data from you when you visit our site, use or participate in our services or when you send us information or communications.

"Personal Data" means data that allows someone to identify or contact you, including, for example, your name, address, telephone number, e-mail address, as well as any information about you that is associated with or linked to any of the foregoing data.

"Anonymous Data" means data that is not associated with or linked to your Personal Data; Anonymous Data does not permit the identification of individual persons.

Sometimes you provide us with data and sometimes data about you is collected automatically.

Below we describe when and how we collect data.

Img. 5. Politique de confidentialité de l'IACCM.

2.8 Chronologie :

Afficher sur une ligne de temps une série d'étapes, de processus ou d'événements dans un ordre logique ou chronologique qui a un sens pour l'utilisateur, car il reflète sa perception du temps. Les échéanciers rendent l'information plus tangible et plus saillante, et donnent un aperçu de ce qui est prévu à l'avenir.
Problèmes : Termes vagues, mur de texte, manque de connaissance.
Exemples : Voir Image 6..

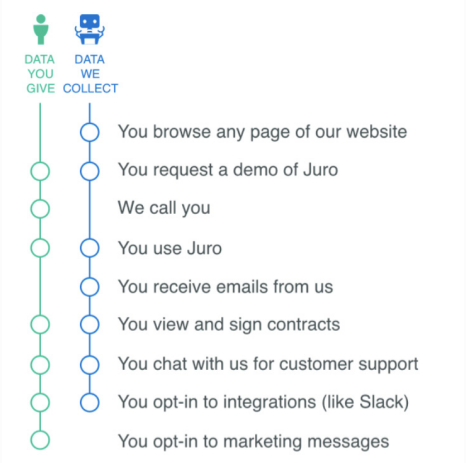


Image 6 .La chronologie de la collecte des données de Juro, telle que présentée dans sa politique de confidentialité.
Redessiné par Stefania Passera.

2.9 Cartoons :

Les bandes dessinées peuvent attirer et retenir l'attention et souligner certains aspects de la politique de confidentialité. Ils intègrent des informations textuelles et non textuelles et utilisent généralement un style de conversation qui peut susciter la curiosité des jeunes ou des personnes moins alphabétisées.
Problème : Complexité de la langue ; imprécision des termes ; mur de texte ; manque d'adaptation à l'auditoire ; manque de connaissance.
Exemples : Image 7.

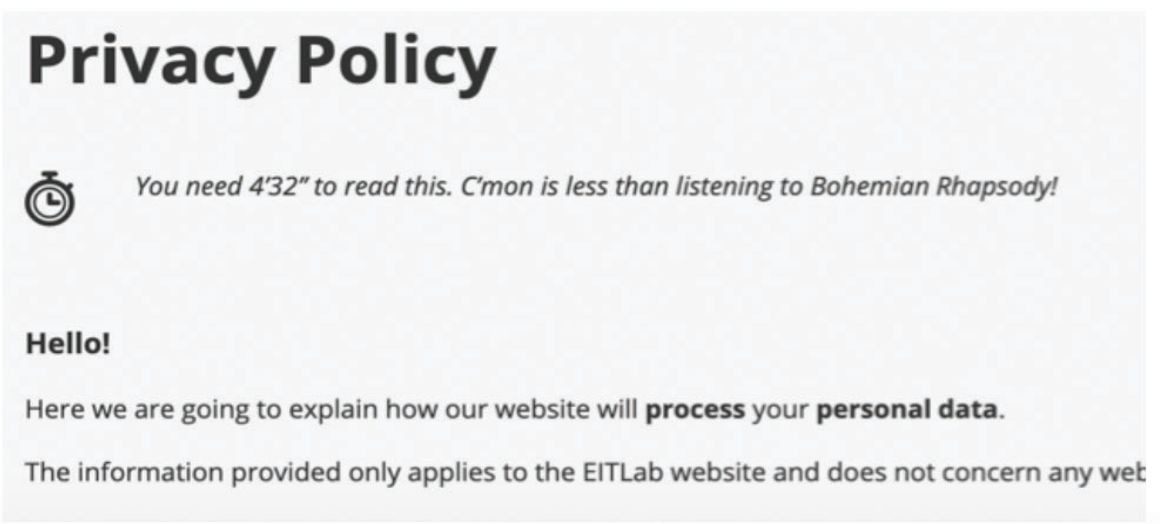
Img. 7 : L'entreprise de mobilité vénitienne AVM affiche des parties cruciales de sa politique de confidentialité (par exemple, les droits des personnes concernées) à travers des bandes dessinées, qui sont périodiquement diffusées sur leurs médias sociaux et sur leur site web. Les personnages sont représentés dans les décors de la ville de Venise et parlent le dialecte local, qui est la langue quotidienne de nombreux habitants vénitiens. Les bandes dessinées se terminent toujours par une touche d'humour. Dessins de Maurizio Boscarol.

2.10 Vidéo :

Utilisez une courte vidéo pour donner un aperçu de la politique de confidentialité ou pour vous concentrer sur des points précis, en combinaison avec la version textuelle. Une vidéo peut attirer l'attention des utilisateurs et être perçue comme étant moins chronophage que la lecture du document. Elle peut également être entendu par les personnes malvoyantes et les personnes ayant un faible niveau d'alphabétisation.
Problème : Complexité de la langue ; manque d'adaptation de l'auditoire ; manque de connaissance.
Exemples : La politique de confidentialité d'Easyjet ; la politique de confidentialité du Guardian ; la politique de confidentialité de Google.

2.11 Estimation du temps de lecture :

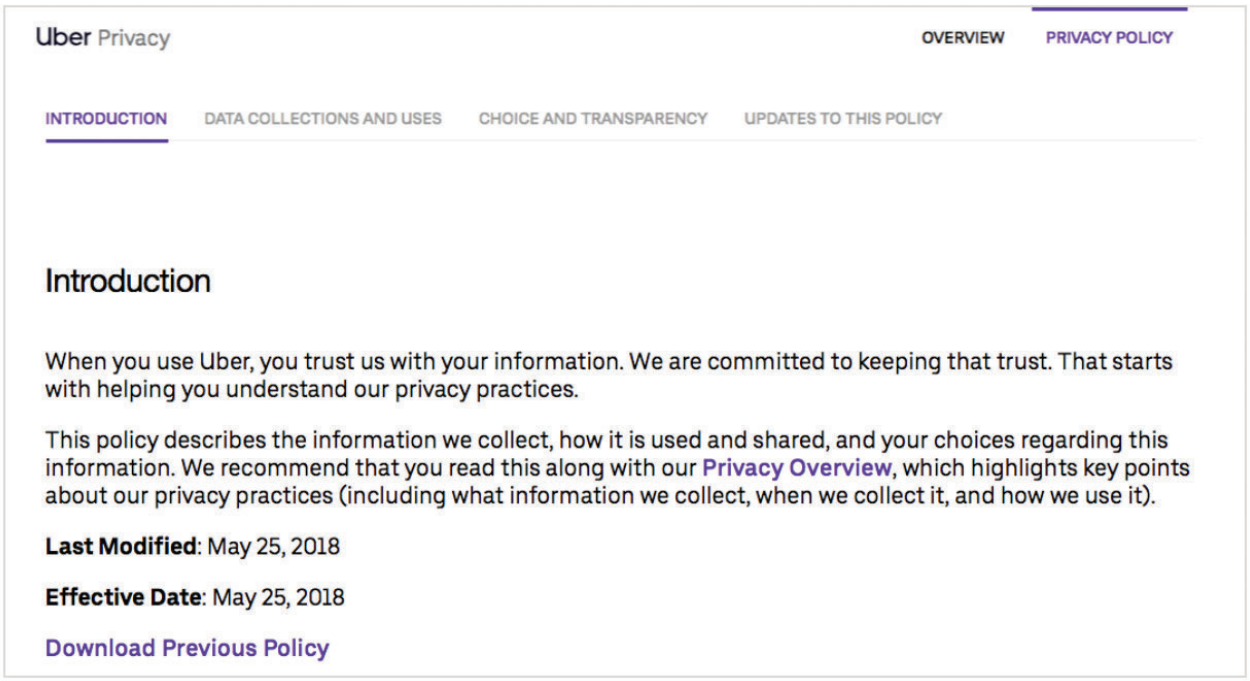
Donnez une estimation du temps nécessaire pour lire la politique de confidentialité, afin que les utilisateurs puissent avoir des attentes réalistes quant à l'effort attendu, ce qui pourrait accroître leur motivation à lire.
Problème : Longueur excessive.
Exemples : Image 8.

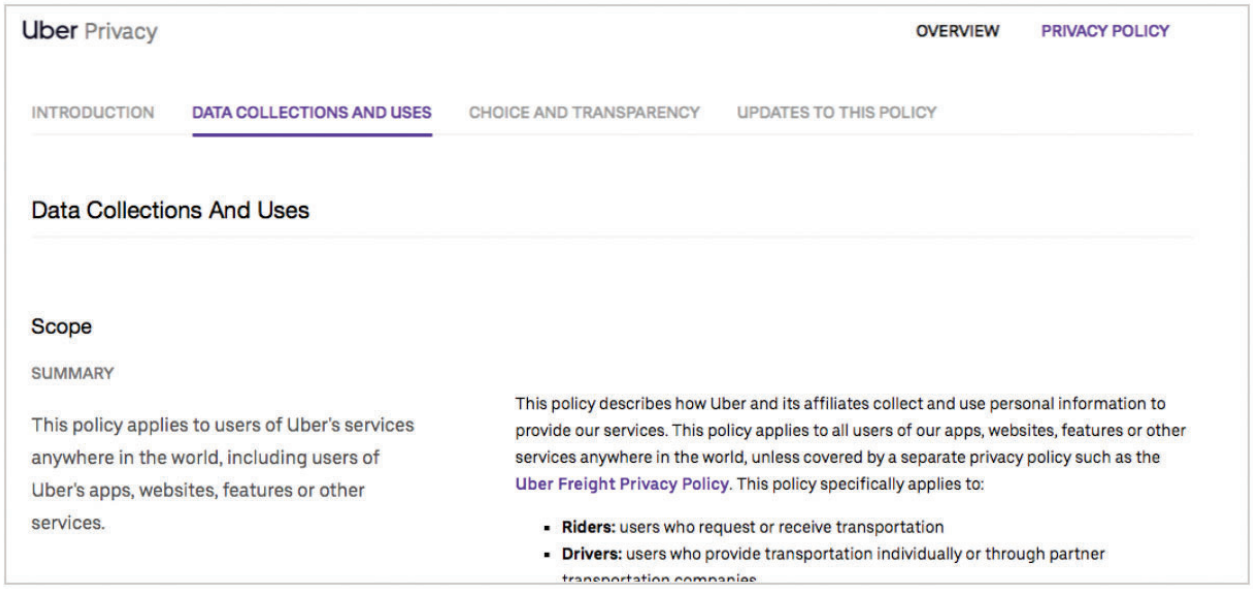


Img 8 : Une estimation initiale du temps de lecture de la politique de confidentialité de l'EITLab, conçue par Rossana Ducato.

2.12 Mécanisme de progression de l'utilisateur :

Afficher un mécanisme (p. ex. une barre de progression) montrant les progrès du lecteur à travers la politique de confidentialité, ce qui pourrait soutenir sa motivation à lire. Les progrès peuvent également fournir une orientation aux utilisateurs, en leur suggérant où ils se trouvent, les sections qu'ils ont déjà lues et celles qui vont suivre.
Problème : Longueur excessive.
Exemples : Image 9.





Img.9. Uber présente un menu navigable affichant les principales sections de la politique de confidentialité (Introduction - collecte et utilisation des données - choix et transparence - mise à jour de cette politique). L'utilisateur peut cliquer dessus et sauter au contenu sélectionné (modèle : table des matières), mais le menu met aussi automatiquement en surbrillance dans une couleur différente la section du document lorsque l'utilisateur fait défiler la page Web. C'est une façon de représenter le mécanisme de progrès.

2.13 Expérience de jeu :

Présenter les termes de confidentialité dans un environnement de jeu, et éventuellement récompenser les utilisateurs (par exemple en termes de points), en explorant la politique de confidentialité, renforçant ainsi leur motivation à lire.
Problème : Mur de texte ; manque d'adaptation à l'auditoire ; fatigue de l'attention.
Exemples : Image 10.

Img. 10. Deux captures d'écran de PrivacyVille montrant les implémentations du mécanisme de progrès à travers la politique de confidentialité de Zinga. Le document a été conçu comme une expérience de jeu qui récompense les utilisateurs qui terminent les tâches.

2.14 Chatbot :

Développer un agent conversationnel (p. ex. un chatbot) qui peut interagir avec les utilisateurs et répondre à leurs questions sur les pratiques relatives aux données sous forme orale ou écrite et en temps réel.
Problème : Complexité de la langue ; imprécision des termes ; longueur excessive ; manque d'adaptation à l'auditoire ; manque de connaissance ; fatigue de l'attention.
Exemple : Image 11.

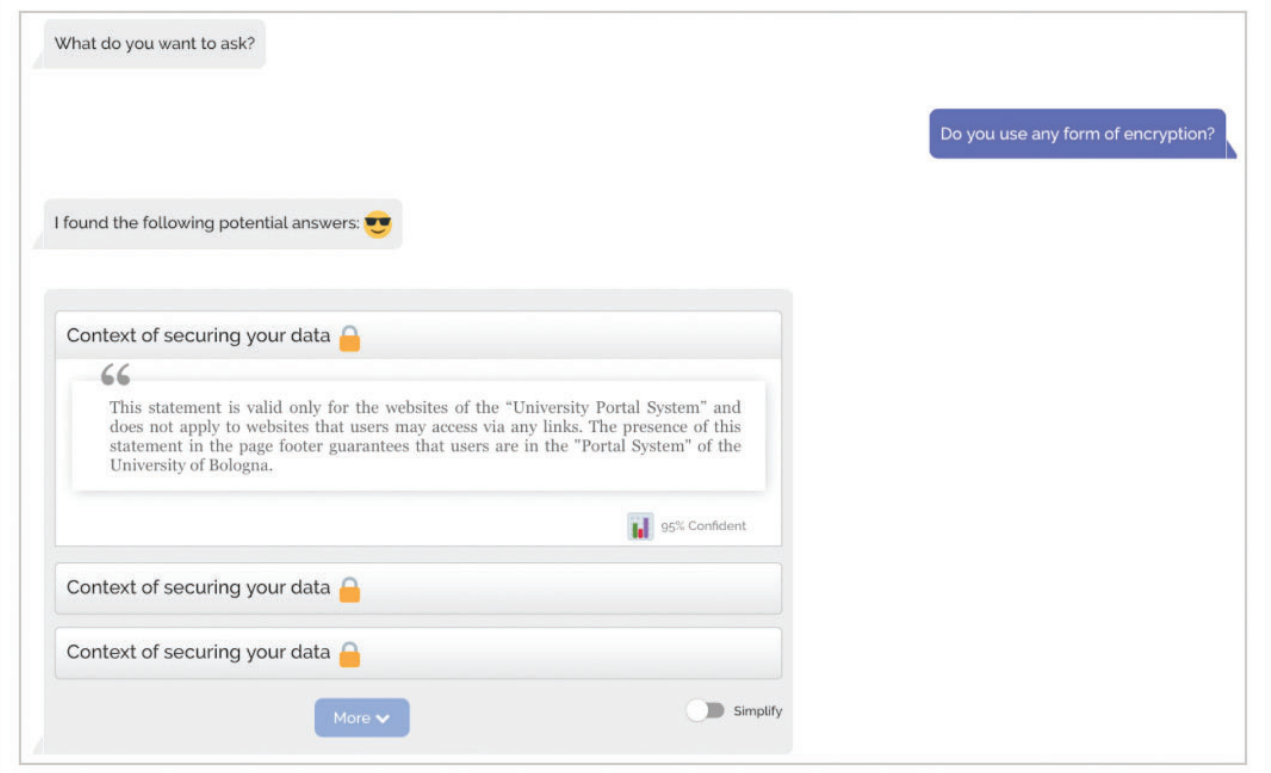


Image 11. Une capture d'écran de l'interaction possible avec PriBot, un chatbot en interface avec un système d'intelligence artificielle qui peut analyser toute politique de confidentialité présente sur le web et répondre à des questions prédéfinies. Cette image montre également qu'un chatbot peut transmettre le ton de la voix en utilisant un ton conversationnel et des émoticônes. Le pourcentage indique la confiance du système à l'égard de la réponse récupérée.

3. Conclusion :

Il existe déjà un certain nombre de solutions aux problèmes de communication documentés adressés aux personnes concernées. Les modèles de conception juridique offrent un moyen de les explorer, de les réutiliser et de les partager. Nous invitons les praticiens et toutes les personnes qui conçoivent des politiques de confidentialité à contribuer: nos prochaines étapes seront d'élargir notre collection et de la transformer en une bibliothèque de modèles consultable et navigable.

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. Digital privacy: theory, technologies and practices, 18, 363-377.

Article 29 Working Party (2018). Guidelines on Transparency under Regulation 2016/679, 17/EN WP260.

Berger-Walliser, G., Bird, R. C., & Haapio, H. (2011). Promoting business success through contract visualization. JL Bus. & Ethics, 17, 55.

BEUC (2017), Fitness Check of EU Consumer Law. Additional BEUC Policy Demands, https://www.beuc.eu/publications/beuc-x-2017-040_csc_fitness_check_of_consumer_law_policy_recommendations.pdf

Calo, R. (2011). Against notice skepticism in privacy (and elsewhere). Notre Dame L. Rev., 87, 1027.

Ducato, R., Hagan, M., Haapio, H., Palmirani, M., Passera, S., and Rossi, A. Legal Design Manifesto v1, available at https://www.legaldesignalliance.org/ (last accessed on 12 March 2019).

Elshout, M., Elsen, M., Leenheer, J., Loos, M., & Luzak, J. (2016). Study on Consumers' Attitudes Towards Terms Conditions (T&Cs) Final Report, https://ssrn.com/abstract=2847546

European Data Protection Supervisor (2015). Opinion 4/2015 Towards a New Digital Ethics.

Fabian, B., Ermakova, T., & Lentz, T. (2017). Large-scale readability analysis of privacy policies. In Proceedings of the International Conference on Web Intelligence (pp. 18-25). ACM.

Haapio, H. and Hagan, M., (2016). Design patterns for contracts. In Networks. Proceedings of the 19th International Legal Informatics Symposium IRIS (pp. 381-388).

Haapio, H. and Passera, S. (forthcoming). Contracts as Interfaces: Exploring Visual Representation Patterns In Contract Design, Legal Informatics, D. M. Katz, M. Bommarito and R. Dolin (eds), Cambridge University Press, forthcoming.

Haapio, H., Hagan, M., Palmirani, M., & Rossi, A. (2018). Legal design patterns for privacy. In Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS (pp. 445-450).

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 531-548).

Hartzog, W. (2018). Privacy's blueprint: the battle to control the design of new technologies. Harvard University Press.

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478). ACM.

Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing privacy notices: an online study of the nutrition label approach. In Proceedings of the SIGCHI Conference on Human factors in Computing

Systems (pp. 1573-1582). ACM.

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 1-20.
Passera, S. (2015). Beyond the wall of text: How information design can make contracts user-friendly. In Design, User Experience, and Usability: Users and Interactions, vol. 9187, Lecture Notes in Computer Science, A. Marcus (ed.), Cham, Springer (p. 341–52).

Pollach, Irene. (2005) "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62, no. 3.
Reidenberg, J. R., Bhatia, J., Breaux, T. D., & Norton, T. B. (2016). Ambiguity in privacy policies and the impact of regulation. The Journal of Legal Studies, 45(S2), S163-S190.

Rello, L., Pielot, M., & Marcos, M. C. (2016, May). Make it big!: The effect of font size and line spacing on online readability. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 3637-3648). ACM.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of EU data protection directive: summary. Information Commissioner's Office.

Rossi, A., Ducato, R., Haapio, H. & Passera, S. (forthcoming), "When Design Met Law: Design Patterns for Information Transparency.". Droit de la consommation - Consumentenredit : DCCR, 10 122-123.

Rossi, A. (2019). Legal Design for the General Data Protection Regulation. A Methodology for the Visualization and Communication of Legal Concepts. Alma Mater Studiorum Università di Bologna. Dottorato di Ricerca in Law, Science and Technology, 31 Ciclo.

Rossi, A., Ducato, R., Haapio, H., Passera, S., & Palmirani, M. (2019, February). Legal Design Patterns: Towards A New Language for Legal Information Design. In Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS (pp. 517-526).

Rossi, A., Ducato, R., Haapio, H., Passera, S., & Palmirani, M. (2019). Legal Design Patterns: Towards A New Language for Legal Information Design. In Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS (pp. 517-526).

Solove, D. J. (2012). Privacy self-management and the consent dilemma. Harv. L. Rev., 126, 1880.

Waller, R., Waller, J., Haapio, H., Crag, G., & Morrisseau, S. (2016). Cooperation through clarity: Designing simplified contracts. Journal of Strategic Contracting and Negotiation, 2(1-2), 48-68.

Zuiderveen Borgesius, F. (2013). Consent to Behavioural Targeting in European Law-What Are the Policy Implications of Insights from Behavioural Economics?. Amsterdam Law School Research Paper 2013-43

Auteurs :

Arianna Rossi (CIRSFID, Université de Bologne / SnT, Université du Luxembourg), Rossana Ducato (UCLouvain / Université Saint-Louis - Bruxelles), Helena Haapio (Université de Vaasa / Lexpert), Stefania Passera (Helsinki University / Passera Design), Monica Palmirani (CIRSFID, Université de Bologne).

c. Méthodologies et cas de conception d'interfaces

c1. Cinq recommendations pour une bonne expérience utilisateur dans les PIMS

Résumé :

De plus en plus, les appareils grand public étendent leurs fonctionnalités grâce à des applications tierces. Cependant, les utilisateurs ne sont pas à l'aise avec la gestion des permissions et des paramètres de confidentialité et ont besoin du soutien d'outils de gestion de la confidentialité (PIMS) appropriés et bien conçus pour accomplir ces tâches. Cet article présente cinq recommandations de conception issues de recherches axées sur l'amélioration de l'expérience de l'utilisateur des appareils de PIMS pour téléphones intelligents. Celles-ci le sont : (1) établir un équilibre entre la protection de la vie privée et l'expérience de l'utilisateur ; (2) fournir des renseignements utiles sur la protection de la vie privée ; (3) tenir compte des émotions désagréables suscitées par l'interaction avec ces outils ; (4) tenir compte des attentes, attitudes et croyances des utilisateurs ; (5) intégrer l'information et éviter le jargon technique. Il est en outre avancé que, bien que les recommandations ci-dessus découlent de recherches sur les TPM pour smartphones, elles peuvent également être utiles aux concepteurs travaillant sur les TPM dans différents contextes technologiques exigeant que les utilisateurs gèrent l'accès à des informations sensibles par des applications tierces.

Apprentissages clés :

- Les utilisateurs doivent être pris en charge dans la gestion des permissions des applications tierces.
- Cinq recommandations générales sont proposées pour l'amélioration de la conception des outils de gestion de la protection de la vie privée.
- D'autres recherches pourraient s'appuyer sur les conclusions du rapport pour étendre davantage les recommandations formulées.

Introduction :

De nombreux appareils et services que nous utilisons tous les jours sont également des plates-formes d'applications tierces (applications), comme les smartphones, les navigateurs Web, les appareils portables, les téléviseurs intelligents et les assistants vocaux, pour n'en citer que quelques-uns. Pour permettre aux applications tierces de fournir leurs services, des plates-formes telles qu'Android ou iOS partagent les informations des utilisateurs via une interface de programmation d'applications (API), qui permet aux développeurs d'accéder aux bibliothèques de codes et aux ensembles de données. Du point de vue des utilisateurs, cela signifie qu'ils sont tenus de donner leur consentement à une liste complexe et souvent imprécise de politiques de protection de la vie privée, ainsi que de gérer une gamme d'autorisations pour accorder ou refuser l'accès à des renseignements sensibles. Il s'agit d'une tâche qui n'est ni facile ni prioritaire pour les utilisateurs qui souhaitent accéder au service et qui ne sont généralement pas conscients des menaces potentielles concernant leur vie privée (Balebako et al., 2013 ; Balebako et Cranor, 2014 ; Whitten et Tygar, 1999).

Par conséquent, sans un soutien approprié, les utilisateurs ont peu de possibilités de prendre des décisions

en matière de confidentialité dans leur propre intérêt lorsqu'ils configurent ou révisent les paramètres de confidentialité des applications.

Dans le contexte du présent article, l'expression Outil de gestion de la protection de la vie privée (PIMS) décrira un type de technologie d'amélioration de la protection de la vie privée visant à sensibiliser les utilisateurs et à les aider à équilibrer les compromis qui sous-tendent l'utilisation de dispositifs qui étendent leurs fonctionnalités grâce à des applications tiers, comme dans le cas des smartphones.

Le but de cet article est de présenter cinq recommandations de conception pour aider les concepteurs à faire face à la complexité de la conception des PIMS. Ces recommandations sont basées sur les résultats d'une recherche doctorale (Carelli, 2019 (en cours de révision)) qui s'est concentrée sur l'amélioration de l'efficacité et de l'expérience utilisateur des PMT pour les applications smartphone. De tels dispositifs offrent un excellent moyen de cibler la recherche sur les PIMS en raison (1) de la disponibilité de millions d'applications tierces accessibles aux utilisateurs, souvent sans frais initiaux (Statista, 2018) et (2) du large éventail de données sensibles pour la vie privée qui fuient les applications à des fins marketing (Zang et al., 2015). En outre, (3) les systèmes d'exploitation initialement conçus pour les smartphones sont de plus en plus intégrés dans des technologies différentes, comme dans le cas des systèmes basés sur Android utilisés dans les dispositifs portables et les voitures. Les recommandations fournies dans cet article peuvent donc également être utiles aux concepteurs de PIMS pour d'autres technologies. De plus, les observations présentées dans le présent article corroborent les conclusions d'autres études qui ont porté sur la possibilité d'utiliser des extensions de navigateur pour améliorer la protection de la vie privée, comme celles de Leon et al (2012), Mathur et al (2018) et Schaub et al (2016).

La recherche de doctorat comportait un certain nombre d'études empiriques. Dans le premier cas, des questions de conception et des entrevues en profondeur ont été utilisées pour comprendre l'expérience de neuf participants qui ont installé une application de gestion de la vie privée sur leur téléphone et l'ont utilisée pendant deux semaines. Dans la deuxième étude, les résultats de l'étude sur les utilisateurs ont d'abord été triangulés avec ceux d'autres études pertinentes, puis élaborés sous forme de recommandations de conception initiales. Enfin, dans la troisième étude, ces recommandations ont été évaluées en collaboration avec cinq experts de l'expérience utilisateur et de la protection de la vie privée mobile de l'industrie et du milieu universitaire.

Pour améliorer l'efficacité et l'expérience de l'utilisateur d'une TGP, les résultats de la recherche suggèrent que les concepteurs (1) aident les utilisateurs à atteindre un équilibre entre les niveaux souhaités de protection de la vie privée et l'expérience de l'utilisateur ; (2) fournissent des renseignements significatifs sur la vie privée en faisant correspondre les modèles mentaux et les attentes des utilisateurs et (3) atténuent les émotions négatives suscitées par ces renseignements ; (4) prennent en considération les attentes, attitudes et convictions des utilisateurs au moment de la conception ; (5) fournissent une information de base et évitent le jargon technique. Chacune de ces recommandations est examinée plus en détail ci-dessous.

Équilibrer la confidentialité et l'expérience de l'utilisateur :

Faciliter la gestion des permissions et des paramètres de confidentialité est la fonctionnalité de base de tout PIMS. Les recherches existantes montrent que les utilisateurs sont prêts à échanger leur vie privée pour préserver les fonctionnalités de leurs applications et services préférés, même lorsqu'ils sont conscients des menaces potentielles pour la vie privée (Balebako et al., 2013 ; Shklovski et al., 2014). Une telle préférence des utilisateurs implique un compromis entre la protection de la vie privée et l'expérience de l'utilisateur. Par conséquent, la conception d'un PIMS devrait reposer sur la prémisse que les utilisateurs sont prêts à protéger leur vie privée tant qu'elle n'exige pas le sacrifice des fonctionnalités souhaitées de leur téléphone intelligent. Sur la base de cette prémisse, le PIMS devrait donc équilibrer les tâches les plus appropriées pour améliorer la protection de la vie privée avec les fonctionnalités souhaitées par les utilisateurs. Le fait de ne pas donner la priorité à cette caractéristique dans la conception du PIMS, et donc d'empêcher l'utilisation d'applications et de services pertinents, est susceptible de donner l'impression que le PMT est inefficace ou inutile. Par exemple, un utilisateur qui utilise une application de navigation nécessitant l'accès à des données de localisation ne devrait pas être avisé de désactiver cette autorisation, même si l'application est susceptible de partager cette information avec des annonceurs. Au lieu de cela, il devrait informer l'utilisateur du problème, tout en lui conseillant également de ne pas accorder l'accès aux informations de contact lorsqu'elles ne sont pas strictement liées à la fonctionnalité de base.

Pour indiquer explicitement quelles permissions peuvent être désactivées sans affecter la fonctionnalité principale de l'application, le PIMS doit inévitablement identifier les applications pertinentes pour les utilisateurs, les fonctionnalités qui contribuent à l'expérience utilisateur et la raison pour laquelle un service ou une application a demandé à accéder aux ressources du téléphone. Ce n'est manifestement pas une tâche insignifiante. Dans le contexte des smartphones, on peut actuellement noter un flux croissant de contributions à la recherche sur le cadre technologique pour inférer le but de l'accès aux données par les applications et fournir des recommandations ciblées aux utilisateurs (Agarwal et Hall, 2013 ; Chitkara et al, 2017 ; Lin et al, 2012 ; Liu et al., 2016). Cela donne à penser qu'une technologie plus mature sera probablement disponible dans un avenir proche, ce qui aurait des implications positives pour différents secteurs technologiques. La prise de décision automatique grâce à l'apprentissage automatique est une façon prometteuse d'alléger le fardeau de la gestion de la vie privée. Un certain nombre d'études ont étudié et fourni des solutions techniques pour mettre en œuvre les décisions prises par le système (Liu et al., 2016 ; Tsai et al., 2017 ; Wijesekera et al., 2015). Cependant, les recherches empiriques menées dans le cadre de la recherche doctorale avec les utilisateurs ont révélé des divergences d'opinion sur les niveaux d'intervention souhaités du PIMS et donc sur la volonté de contrôler le degré d'autonomie qu'ils souhaitent déléguer à cet outil. Par conséquent, les concepteurs devraient également réfléchir à la manière de sensibiliser les utilisateurs avant de permettre au PIMS de prendre des décisions automatiques en leur nom.

Fournir des renseignements utiles sur la protection de la vie privée :

Fournir des informations significatives et exploitables sur la protection de la vie privée est une condition essentielle pour un PIMS. Pour ce faire, il est important de tenir compte du fait que les personnes vivent différemment la protection de la vie privée, car elles ont des modèles mentaux qui diffèrent de ceux des concepteurs et des spécialistes de la protection de la vie privée (Dunphy et al., 2014). Les résultats de l'étude sur les utilisateurs ont montré que les participants perçoivent la transparence comme des couches

qui se chevauchent et que les répercussions sur la protection de la vie privée d'éventuelles utilisations abusives de leurs données personnelles sont les plus importantes. Ainsi, dans la mesure du possible, le PIMS devrait informer l'utilisateur (1) des implications potentielles pour sa vie privée et (2) des types de données recueillies et partagées avec des services tiers, de manière simple et directe. Cependant, chercher à améliorer la transparence et la compréhension en informant l'utilisateur des informations partagées avec une application tierce pourrait ne pas suffire, car il est probable que les conséquences potentielles pour la vie privée, le cas échéant, ne seraient pas entièrement comprises et pourraient même favoriser l'incompréhension et l'incertitude.

Une approche largement utilisée pour informer les utilisateurs des menaces potentielles pour la vie privée consiste à leur fournir un classement des menaces potentielles (Kelley et al., 2010 ; Liccardi et al., 2014 ; Lin et al., 2012). Il ne doit pas s'agir d'un résumé statique du caractère potentiellement invasif d'une application, mais plutôt d'une boucle de rétroaction, par exemple en montrant un niveau de menace réduit en réponse à la gestion par un utilisateur d'une tâche de confidentialité, ce qui favorise la compréhension et rassure. De plus, la justification utilisée pour classer les applications en fonction de leur niveau de menaces devrait être facilement accessible et rendue explicite par l'intermédiaire du PIMS.

Tenir compte des émotions des utilisateurs :

Lorsqu'ils sont exposés à de l'information sur la violation de la vie privée, les utilisateurs peuvent éprouver un mélange de sentiments qui comprennent l'anxiété, une étrangeté générale associée à la recherche sur la protection de la vie privée en combinaison avec l'émotion viscérale de l'" effroi " (Tene et Polonetsky, 2013 ; Thierer, 2013). Par ailleurs, des recherches antérieures ont montré que la nervosité peut être provoquée par des stimuli visuels fournis, par exemple, par l'interface (Zhang et Xu, 2016). Cependant, tirer indistinctement parti d'un tel sentiment comme stratégie de persuasion pourrait être contre-productif, car cela pourrait évoquer des sensations d'impuissance, et par conséquent de scepticisme, par rapport à l'avantage d'utiliser un PIMS. Il est donc probable qu'une telle stratégie soit plus efficace lorsqu'il s'agit de trouver une solution claire et réalisable pour rétablir un meilleur niveau de vie privée. Par exemple, lorsque le TGP détecte qu'une autorisation spécifique est une source potentielle de menaces à la vie privée, le TGP peut insister sur le risque de ne pas prendre de mesures. Cependant, il y a certainement des cas où, malgré le risque pour la vie privée des utilisateurs, le PMT ne peut offrir des solutions pratiques et réalisables. Par exemple, comme le soulignent Zang et ses collaborateurs (2015), les applications mobiles recueillent un ensemble plus large de données comportementales sur les utilisateurs sans leur offrir de contrôle ni de conseils appropriés. Dans de tels cas, le fait de susciter l'effroi est susceptible de renforcer l'acceptation passive de l'atteinte à la vie privée telle que rapportée dans Shklovski et al (2014).

Répondre aux attentes, aux attitudes et aux croyances des utilisateurs :

Les utilisateurs ont des attentes, des attitudes et des croyances à l'égard de la technologie qui peuvent influer sur leur intention d'adopter (Davis, 1989 ; Oinas-Kukkonen et Harjumaa, 2009 ; Wright et McCarthy, 2010). Ceci est également valable dans le cas des PIMS. Par exemple, comme les menaces à la vie privée et les outils pour les atténuer sont complexes, les utilisateurs peuvent attribuer à tort au PIMS des propriétés qui dépassent ses capacités techniques, ce qui suscite le scepticisme et la méfiance lorsque les utilisateurs réalisent que leurs attentes ne sont pas à la hauteur. Par conséquent, les concepteurs devraient prendre

soin d'informer les utilisateurs des capacités et des avantages réels de l'outil afin de réduire l'impact négatif potentiel des idées fausses sur les menaces à la vie privée et les fausses attentes à l'égard des résultats de l'outil. Cet objectif peut être atteint en adaptant le contenu ciblé et en améliorant la phase d'intégration.

En outre, il faut tenir compte des différents niveaux d'expertise des utilisateurs ainsi que de leurs divers besoins qui les amènent à avoir des attentes différentes quant aux avantages de l'utilisation d'un PIMS. Par exemple, un utilisateur technologiquement averti peut s'attendre à obtenir des informations plus détaillées sur l'outil et à pouvoir bloquer certaines fonctions dans des conditions spécifiques. Par conséquent, pour répondre aux besoins des utilisateurs avancés, le PIMS devrait donner accès à des outils avancés qui nécessitent une meilleure compréhension de la technologie à mettre en place. Au contraire, il serait approprié de cacher ce type d'informations détaillées aux utilisateurs moins enclins sur le plan technique.

Recommandations supplémentaires pour les utilisateurs non experts :

La phase d'acquisition est un élément important de l'expérience utilisateur, car elle offre des informations pertinentes sur les principales fonctionnalités et avantages de l'outil (Cascaes Cardoso, 2017 ; Fraser et al., 2016). Tout au long de cette phase, le PIMS devrait à la fois présenter et proposer des suggestions sur les principales fonctionnalités et avantages du PIMS. Par exemple, le PIMS devrait mettre en évidence les applications qui doivent être examinées en premier lieu, en expliquant, dans un langage simple et humain, la raison d'être du classement de la gravité des menaces et en suggérant comment et quand utiliser les caractéristiques pertinentes des outils. Un autre aspect de la phase d'intégration concerne le renforcement de l'engagement et de l'intérêt des utilisateurs à l'égard du PMT, ainsi que les questions de confidentialité liées aux smartphones et aux applications. Par conséquent, les utilisateurs auraient avantage à recevoir un contenu personnalisé pour accroître l'intérêt et la compréhension de l'outil.

En outre, il est important d'éviter l'utilisation de jargon technique dans la communication avec les utilisateurs. Le PMT devrait plutôt informer les utilisateurs sur les questions de protection de la vie privée, les solutions possibles et les limites inhérentes à la gestion de la vie privée dans les termes les plus simples, car le niveau d'alphabétisation concernant les technologies renforçant la protection de la vie privée peut varier considérablement pour l'utilisateur moyen par rapport à ceux qui sont plus " experts en technologie " (Mozilla Internet Citizen, 2017).

En plus des recommandations ci-dessus, il est important d'évaluer continuellement, dans le contexte, la façon dont le PIMS est utilisé et donc de prêter attention à tout problème potentiel qui pourrait survenir lors de son utilisation. Les concepteurs, en particulier, devraient porter une attention particulière aux problèmes cognitifs potentiels qui peuvent découler de l'utilisation d'un PIMS afin de minimiser le risque de perdre son efficacité dans l'adoption à long terme. Pour ces raisons, l'évaluation de la façon dont ces outils sont utilisés dans leur contexte, pour détecter et opposer l'émergence de tels biais, il est essentiel d'améliorer l'efficacité de l'outil et l'expérience utilisateur.

Conclusion

Afin d'informer les concepteurs des différentes technologies qui exigent des utilisateurs qu'ils prennent des décisions complexes en matière de protection de la vie privée, le présent article présente les résultats d'une recherche doctorale axée sur les outils de gestion de la vie privée pour les téléphones intelligents.

Elle a proposé cinq grands domaines d'intervention pour les concepteurs qui visent à améliorer l'efficacité et l'expérience des utilisateurs des PIMS.

Les travaux futurs pourraient s'inspirer de ces idées pour faire rapport sur l'utilisation des recommandations pour des études de cas spécifiques. En outre, d'autres recherches pourraient élargir les résultats actuels afin d'inclure des domaines de conception qui ne sont pas couverts dans le présent article. Par exemple, d'autres recherches pourraient porter sur la manière de fournir aux utilisateurs des recommandations sur mesure afin de souligner l'arbitrage entre la protection de la vie privée et la fonctionnalité, sur la manière de visualiser des informations approfondies sur la protection de la vie privée qui ne submergent pas les utilisateurs et sur la manière de renforcer la confiance envers le PIMS.

Alessandro CARELLI :
Alessandro CARELLI est candidat au doctorat à la Loughborough Design School (Royaume-Uni), où il a effectué une recherche à l'intersection de la vie privée et de l'expérience utilisateur. En tant qu'UX et Service Designer chez Digital Entity (Milan, Italie), il aide les organisations mondiales à répondre aux besoins et aux objectifs commerciaux de leurs utilisateurs.

c.2 Transparence et consentement : un cadre éthique pour l'exploitationdes données personnelles

Introduction :

Dans leur article « The dynamics of big data and human rights: the case of scientific research » - paru dans la revue "The ethical impact of data science" de la Royal Academy qui définit pour la première fois le concept de "Data Ethics" - Effy Vayena et John Tasioulas pointent le fait que l'éthique est souvent une juste balance entre plusieurs principes : dans le cas du Big Data, le principe de l'Article 12 de la Déclaration Universelle des Droits de l'Homme (droit à la vie privée) et de l'Article 27 (droit de participer au progrès scientifique). Il s'agit donc de balancer une dignité individuelle avec l'intérêt collectif. Les auteurs signalent également que cette balance ne doit pas être un jeu à somme nulle : un principe ne doit pas être respecté au détriment d'un autre, les deux doivent se compléter et toute avancée dans l'application de l'un doit s'accompagner d'une avancée dans l'accomplissement de l'autre.

L'éthique n'est donc pas l'application catégorique et sans conditions d'un principe mais le barycentre entre différents principes convenus qui s'équilibrent. L'éthique dans la collecte et l'utilisation de données personnelles constitue donc l'équilibre entre les principes guidant la protection de l'individu et de sa vie privée et l'intérêt d'exploiter ces données personnelles par une organisation.

Nous pouvons alors nous demander sur quelles bases définir des règles concrètes de protection de l'individu et comment les appliquer effectivement dans un contexte d'exploitation de données pour que ces règles de protection s'équilibrent avec l'intérêt de l'exploitation.

Cet article vise à démontrer par les faits la pertinence de cet équilibre et les moyens de l'appliquer par l'implémentation de VisionsTrust (outil de transparence, de gestion des droits et du consentement de Visions) au sein du réseau social professionnel jollyclick.

1. Protection des données personnelles : les principes que VisionsTrust applique :

Visions est une entreprise qui permet aux organisations d'appliquer de façon technique les principes de protection des données personnelles – notamment les principes de transparence et de consentement inclus dans le Règlement Général sur la Protection des Données – au sein de systèmes d'information et d'applications pour garantir une éthique de leur exploitation de données personnelles.

1.1 Principes de transparence :

Le RGPD accorde une grande place à la transparence, il ne suffit pas que l'information soit présente pour être conforme mais la manière dont elle est présentée compte tout autant.

Le RGPD ne définissant pas la manière dont on applique la transparence [Lenzini, 2019], Visions s'est tournée vers d'autres principes pour appliquer cette transparence : le legal design [Rossi et al, 2019] tout comme l'expérimentation [Von Grafensetein, 2019] permettent de donner des cadres et règles pour s'assurer de la compréhension des personnes de la collecte et de l'utilisation de leurs données.

Les principaux principes de legal design permis par VisionsTrust sont : une politique de confidentialité claire et concise [Rossi et al, 2019], l'utilisation d'icônes [Rossi et al, 2019], une information à tiroir [Rossi et al, 2019], une information contextuelle [Rossi 2019], une explication des bénéfices et risques liés au partage d'une donnée [Rossi 2019].

Voici plus précisément comment cela se traduit au sein d'une application et de ses interfaces :

Règles de transparence :

1 - L'information est en « langage juridique clair » et accompagnée d'icônes
2 - L'information est présente à différents moments :

a. Au préalable :

a.1 Avant tout échange de données la personne a accès en langage juridique clair et avec icônes à une information comprenant :

a.1.1 Les traitements effectués sur les données personnelles et une description.

a1.2 La nature des données pour chaque traitement

a.1.3 Le sous-traitants vers lesquels les données sont échangées et la finalité de la sous-traitance

a.1.4 Les mesures de sécurité appliquées par l'organisation

a.1.5 Le contact du DPO

b. Contextuelle :

b.1 A chaque collecte de données, la liste des finalités de l'utilisation de la donnée est disponible.

b.2 A chaque traitement, la liste des données utilisées pour effectuer le traitement est disponible.

b.2.1 Si des consentements sont liés au traitement, la personne peut les gérer de manière contextuelle depuis la bulle d'information.

b.2.2 Pour les consentements une explication spécifique est donnée pour expliquer pourquoi cette donnée est demandée.

c. A la demande :

c.1 A tout moment l'utilisateur peut retrouver toute l'information et gérer ses consentements et droits depuis son « Privacy Dashboard » dans les paramètres par exemple.

c.2 Cette interface liste les traitements et leurs descriptions, les données associées et leurs descriptions et permet aux gens d'exercer leurs droits automatiquement :

c.2.1 Suppression.

c.2.2 Accès

c.2.3 Consentements

c.2.4 Opposition

c.2.5 Portabilité

Au-delà de l'application du legal design, l'efficacité de la transparence doit également être mesurée et testée pour être certains que la transparence soit adaptée au public [Von Grafensetein, 2019 ; Roda, 2019].
Ainsi Visions organise des focus groups sur le public cible pour évaluer : le degré de compréhension, le temps de compréhension et l'intérêt pour la plateforme. Ces focus groups sont toujours organisés avant le lancement des nouvelles interfaces et les résultats permettent d'itérer sur l'implémentation des principes de transparence.
Visions initie également un partenariat avec le Security and Trust Lab pour faire de la recherche quantitative et qualitative sur les facteurs de compréhension et de confiance lorsqu'il s'agit de partager des données personnelles.

Les règles que VisionsTrust permet d'appliquer découlent du principe de transparence dans le RGPD et de la recherche faite sur le sujet pour s'assurer que la transparence soit réellement comprise et serve ainsi l'individu tout en rendant clair l'intérêt de l'exploitation de ses données.

1.2 Principes de contrôle :

Le RGPD offre un certain nombre de droits aux personnes sur leurs données et impose l'utilisation du consentement dans certains cas.

Lorsqu'une personne veut exercer un droit (suppression, accès, portabilité, rectification, opposition) ; le responsable de traitement doit informer la personne de la procédure à suivre puis dispose de 30 jours pour l'informer de la suite donnée à la demande.

Les règles de transparence permises par VisionsTrust permettent d'appliquer l'obligation de transparence sur le consentement qui doit être présenté dans une « forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ».
L'utilisateur peut à différents moments donner ou retirer son consentement pour une donnée et un traitement précis et ce consentement est alors automatiquement respecté par le responsable de traitement. Ceci répondant à au fait qu' « il est aussi simple de retirer que de donner son consentement ».

De la même manière, la personne peut facilement exercer ses droits et elle sera automatiquement informée de la politique de l'entreprise sur le sujet (suppression, accès, portabilité, rectification).

Ici nous appliquons techniquement les obligations du RGPD et un principe issu de la « data ethic » : puisque la collecte et l'utilisation des données se fait de façon automatique et sans grand effort de la part de la personne, retirer une autorisation ou supprimer une donnée doit être de la même simplicité [Vayena et Tasioulas, 2016].

Règles de contrôle :

1. L'exercice des droits (suppression, accès, portabilité, opposition) est automatique, depuis le Privacy Dashboard.
2. Consentement :
    a. Chaque consentement est accompagné d'une description spécifique indiquant ce que le traitement de la donnée concernée va apporter à l'utilisateur.
    b. Les consentements sont automatiquement respectés et stockés pour pouvoir être prouvés.
3. Chaque partage de données vers d'autres personnes ou d'autres organisations doit faire l'objet d'un consentement.

Les règles de contrôle permettent à l'individu de paramétrer l'utilisation de ses données et d'exercer un contrôle direct et automatique sur leur exploitation, tout en l'information des bénéfices ou manques liés à l'exploitation ou à la non exploitation des données.

1.3 Évolution et vérification des règles :

Les règles sont amenées à évoluer et à être légitimées par la recherche académique faite sur le sujet, par les usages et également par la recherche spécifique menée avec le Security and Trust Lab du Luxembourg. Le but de cette recherche est de déceler le niveau d'information et de contrôle que les utilisateurs souhaitent avoir sur leurs données pour être en situation de compréhension et de confiance suffisante pour partager des données personnelles.

VisionsTrust permet d'implémenter ces règles. La véracité des informations présentes sont assurées par un audit initial légal, procédural et technique et par des audits réguliers au moins bi-annuels. Le respect des consentements et des exercices de droits est assuré par l'implémentation de VisionsTrust, par les audits réguliers et part des informations concernant la fréquence de vérification des consentements faits par un service sur les serveurs de Visions.

VisionsTrust permet donc à un système de respecter ces règles et principes de transparence et de contrôle sur les données personnelles. Ces principes de protection peuvent alors s'allier aux principes d'exploitation des données personnelles de l'organisation pour ensemble former une éthique qui permet une utilisation pérenne des données personnelles, démarquant l'organisation et lui permettant ainsi de collecter et d'accéder à davantage de données.

Nous sommes persuadés que l'application de telles règles aboutit sur davantage de consentements, nous menons à cette fin une expérience avec jollyclick décrite ci-dessous.

2. Application des règles au sein de jollyclick

2.1 Nature de l'exploitation des données et intérêt pour jollyclick d'implémenter VisionsTrust :

jollyclick est un cas pilote qui correspond parfaitement au problème éthique tel que nous le posons, à savoir un ensemble de règles qui se complètent et se limitent pour former un équilibre de conduite. En l'occurrence, le réseau social utilise les données personnelles pour apprendre à connaître ses utilisateurs afin de leur suggérer du contenu pertinent en fonction de leur projet professionnel, personnaliser leur parcours sur le service, data visualiser leur activité sur le service et du besoin de transformer des données personnelles en fonctionnalités de ciblage anonymes à des fins commerciales. L'entreprise jollyclick a besoin d'itérer son service, de l'améliorer mais aussi de monétiser les données à caractère personnel de ses utilisateurs car, comme beaucoup de plateformes, leur valeur réside dans leur position d'entremetteur de la donnée. Cependant, à l'inverse des pratiques générales, en collaboration avec Visions, jollyclick exerce toutes ces activités de collecte et d'analyse des données de façon activement transparente et, dans certains cas, conformément aux consentements accordés ou non par les utilisateurs.

En intégrant VisionsTrust, jollyclick peut ainsi demander à ses utilisateurs à pouvoir utiliser leurs données personnelles aux fins exposées tout en garantissant à ces derniers le refus et la révocabilité de leur accord par un tiers de confiance. En effet, de nombreuses applications numériques, en dépit de leur bonne volonté, se contentent d'autoévaluer et d'autocontrôler le niveau de transparence de leur gestion des données à caractère personnel fournies par les utilisateurs. Ces procédés ont fini de démontrer leur insuffisance au détriment des utilisateurs qui désormais, après les multiples scandales relatifs à de la mauvaise gestion des données personnelles impliquant Facebook, Google, LinkedIn et d'autres, connaissent une crise de confiance vis-à-vis des plateformes qu'ils utilisent.

jollyclick a fait appel à Visions non seulement pour se démarquer en matière de gestion éthique et transparente des données de ses utilisateurs, mais aussi pour restaurer un climat de confiance dans la relation U2S (User-to-Service) qui in fine – jollyclick et Visions vont mener, avec le Security and Transparency Lab de l'Université du Luxembourg un projet de recherche expérimentale à cette fin – devrait aboutir à une circulation des données plus fluide et plus stable.

C'est la convergence des principes guidant l'utilisation de données de jollyclick avec les principes de transparence et de contrôle implémentés par VisionsTrust qui détermine le degré et le type de transparence et de contrôle à offrir aux utilisateurs et donc l'éthique dans la collecte et l'utilisation des données. A présent, nous allons détailler les méthodes et les fonctionnalités implémentées et expérimentées sur le service jollyclick en connexion avec l'API de VisionsTrust.

2.2 Implémentation de VisionsTrust dans jollyclick :

Avant toute collecte de données :

Une interface respectant les principes de legal design est disponible à l'inscription d'une personne sur jollyclick, pour facilement avoir une vue d'ensemble sur l'utilisation qui sera faite des données personnelles. Cela vient répondre au fait que les CGUs qui contractualisent la relation entre l'utilisateur et la plateforme sont rarement lues : ici les termes du contrat sur l'utilisation des données personnelles sont plus clairs.

https://visionstrust.com/information/jollyclick

Pendant la collecte et le traitement :

A chaque collecte de donnée par jollyclick, la personne peut savoir à quelles fins elle sera utilisée.

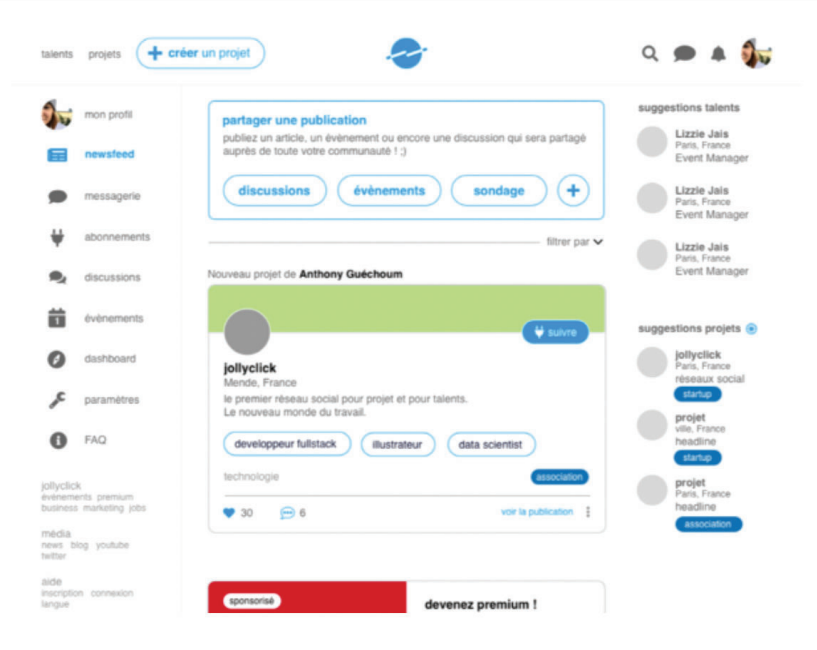
Exemple : si jollyclick demande à l'utilisateur ses centres d'intérêts, celui-ci peut savoir immédiatement et

facilement dans quels objectifs les données « centres d'intérêts » seront utilisés.

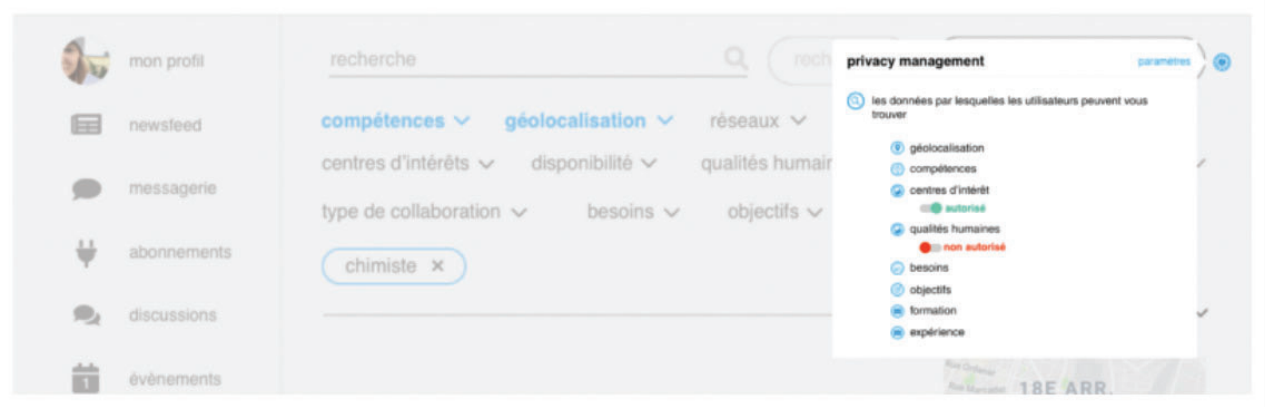
Il s'agit pour le service d'être directement et non indirectement transparent et informatif. Il s'agit d'être proactif, non réactif. Cette approche donne un premier gage de confiance à l'utilisateur, le rassurant dans l'échange de données : surtout dans les premières interactions avec la plateforme, il peut être inquiétant d'échanger un grand nombre de données. Une démarche proactive permet de montrer à l'utilisateur que ses émotions et sa vie privée sont prises en compte et anticipées par la plateforme. Egalement, ce devoir de transparence oblige les concepteurs de la plateforme à réfléchir à chaque utilisation de donnée, sachant que cette utilisation sera rendue claire.

De la même manière, lorsqu'un traitement est effectué l'utilisateur peut savoir sur la base de quelles données ce traitement est effectué et gérer ses autorisations, ainsi que s'informer sur la raison de l'utilisation des données pour ce traitement.

Exemple : parce que le réseau social jollyclick met en relation des personnes et des projets (matching), l'utilisateur peut donc **savoir sur la base de quelles données le matching est calculé** et ainsi gérer toutes les autorisations relatives.



Exemple : parce que le réseau social jollyclick permet aux utilisateurs de chercher d'autres utilisateurs sur la base de différents critères (search), l'utilisateur peut donc **savoir sur la base de quelles données il peut être retrouvé** et ainsi gérer toutes les autorisations relatives.



Cette information et ce contrôle contextuels rassurent l'utilisateur et s'inscrivent dans un rapport S2U (Service-to-User) respectueux : **apporter la bonne informatio**n au bon moment.

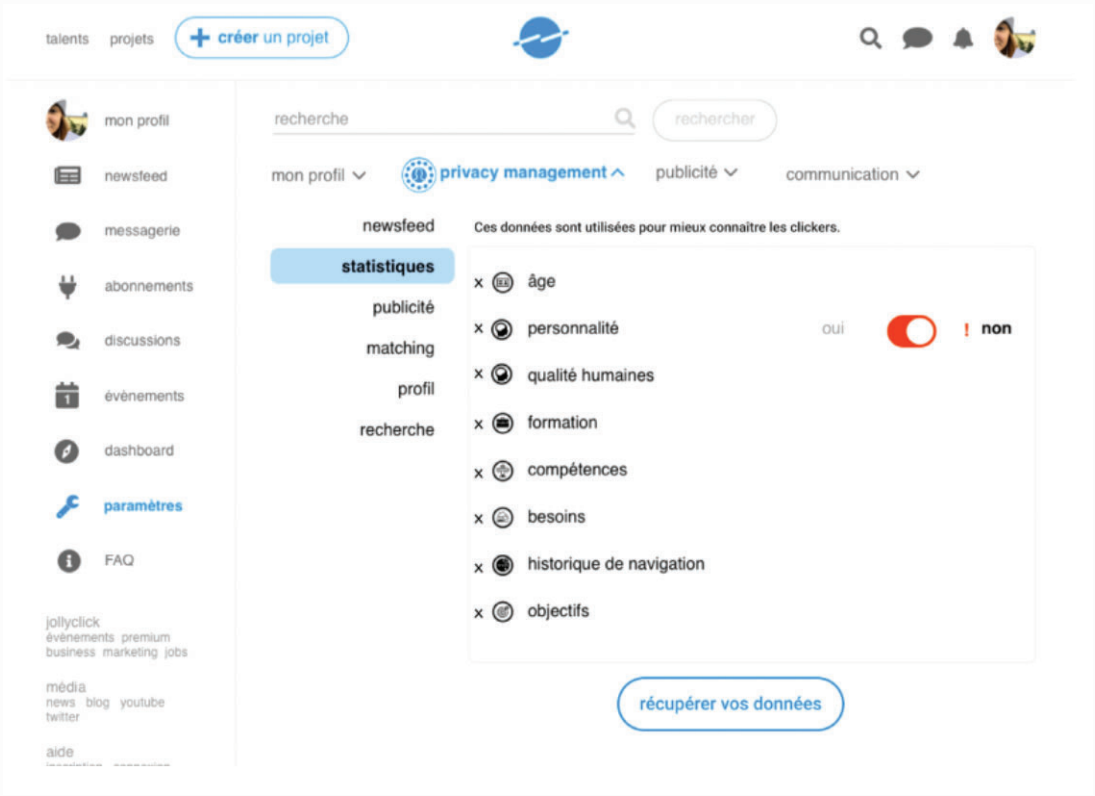
Une demande de consentement en contexte permet également de ne pas sur-solliciter l'utilisateur dès l'inscription. La plupart des plateformes aujourd'hui demandent les autorisations à l'inscription de l'utilisateur, cela pose différents problèmes vis-à-vis de la transparence et de la compréhension de l'utilisateur :

1 - Devoir répondre à beaucoup de demandes lors de l'accès à un service ne garantit pas des choix réfléchis de la part de l'utilisateur.
2 - Devoir répondre à des autorisations avant de connaître le service, ne permet pas un consentement « éclairé ».

A tout moment :

Il est important et agréable d'offrir une information et un contrôle contextuels mais tout aussi important de les offrir à la demande, à tout moment de façon simple et centralisée.

L'intégration dans jollyclick offre une **interface de gestion centrale (Privacy Management dashboard)** dans les paramètres depuis laquelle les utilisateurs peuvent exercer tous leurs droits en direct et gérer leurs préférences de manière intuitive.



Ils peuvent retrouver toutes les informations relatives à chaque traitement, gérer leurs consentements, mais aussi **supprimer ou récupérer leurs données.**
Pour chaque suppression ou récupération de donnée, l'utilisateur reçoit une notification sur le site et une confirmation par courriel.

Consentements : règles de contrôle

Vous avez dû le remarquer, l'utilisateur ne peut pas autoriser ou désactiver toutes les données mais seulement deux : "personnalité" et "centres d'intérêts".

Nous avons là implémenté une première règle de confiance et d'éthique : **donner contrôle sur ce qui se rapproche des données sensibles**.

Les données sensibles sont : donnée de santé, opinions politiques et philosophiques, orientation religieuse, origine ethnique, orientation sexuelle, appartenance syndicale.

"Personnalité", qui est le résultat d'un test, se rapproche d'une **donnée de santé**.
"Centres d'Intérêts" peut se rapprocher des **opinions politique, religieuse et/ou philosophique.**

jollyclick est un réseau social professionnel qui met en relation des personnes qui ont des compétences et des personnes qui ont des projets. **Par conséquent, toutes les données professionnelles sont indispensables à son fonctionnement et légitimement récupérables. Sans elles, jollyclick ne rend plus le service auquel s'attend l'utilisateur, ce qui contredit ces principes. L'utilisation des données indispensables alliées aux principes de transparence rend leur exploitation acceptable.**

S'agissant des données "personnalité" et "centres d'intérêts", leur nécessité est moins importante bien qu'elles permettent de meilleures recommandations. C'est ici une application de la « social preferability » qui est l'objectif que toute initiative de « data ethic » se doit d'atteindre [Floridi, 2016].

Nous menons en ce moment une expérimentation pour déceler si les principes de transparence et de contrôle entraînent plus ou moins de consentements de la part des utilisateurs sur les données « personnalité » et « centres d'intérêts ».

Notre conviction, qui sera validée ou altérée suite aux résultats de notre recherche, dit qu'en raison du système de gestion fluide et de la transparence apportée, les utilisateurs confieront d'autant mieux au service leurs données personnelles en accordant les autorisations demandées par celui-ci.

C. Données publiques et données au service de la recherche :

Les utilisateurs contrôlent ce qui s'affiche publiquement que ce soit dans le newsfeed ou sur leur profil, indépendamment de la donnée. En effet, ne pas afficher ses compétences ne contredit pas la promesse de jollyclick de mettre en lien les personnes sur la base de complémentarité : la donnée « Compétence » peut-être utilisée par le matching mais offrir ce contrôle permet d'offrir aux personnes contrôle sur la visibilité publique de leurs données.

Visions étant partenaire du « Projet Lyli » - unissant 14 universités et 27 collèges du Conseil Départemental du Val d'Oise pour apporter une meilleure orientation au lycéens – qui va intégrer VisionsTrust dans son outil numérique d'orientation à destination des lycéens ; jollyclick pourra échanger des données avec cet outil pour fournir davantage de données à la recherche en orientation. Ces échanges se feront toujours sur le consentement des personnes, même si les données sont anonymisées. Cela participe d'une règle éthique de transparence qui dépasse les règles nécessaires à la conformité mais qui participe à instaurer une relation de confiance.
Une telle collaboration entre jollyclick et le Projet Lyli, nous permettrait également de mener une première recherche sur l'influence des principes de transparence et de contrôle sur la volonté des utilisateurs de partager des données avec des tiers.

Conclusion :

L'éthique est le respect d'un ensemble de principes qui guident l'action.

L'éthique dans l'utilisation des données personnelles doit veiller à appliquer à l'exploitation des données personnelles des principes de protection des données personnelles. Le contrôle et la transparence sur les données est un moyen de respecter ces principes de protection et de permettre leur application.

VisionsTrust - en se fondant sur le RGPD, l'état de l'art de la recherche en legal design, en data ethic et en interaction homme-machine - permet d'appliquer des principes et règles de transparence et de protection des données aux principes d'exploitation des données de l'entreprise. Cette alliance des principes de protection et d'exploitation permet de garantir un cadre éthique qui guide et démarque l'organisation dans son utilisation des données personnelles. Ainsi l'organisation peut créer une relation de confiance avec

ses utilisateurs pour demander davantage de données, en échanger avec des partenaires et exploiter les données personnelles de manière pérenne. Le choix des règles appliquées doit faire l'objet de recherche et d'itération pour s'assurer que l'application des principes de transparence et de contrôle sert toujours le but : la compréhension des personnes sur l'utilisation de leurs données afin de créer un climat de confiance propice à leur exploitation éthique.

Le degré de contrôle offert aux personnes sur leurs données n'est pas donc uniquement un enjeu technique. Il est surtout une réflexion éthique sur comment assurer le respect des personnes et le respect des valeurs et de la mission de l'organisation. En informant clairement sur cette mission, sa façon d'utiliser les données à cette fin et en offrant un paramétrage sur les données qui ne sont pas indispensables à la réalisation de la mission, jollyclick allie le respect de l'individu et de sa vie privée avec le respect de son but social.

L'application de l'éthique dans l'utilisation des données est un procédé subtil qui doit partir des valeurs, principes et objectifs de l'organisation pour se conjuguer avec le respect des individus, par notamment la transparence et un contrôle pertinent offert sur leurs données personnelles.

Pour arriver à ce point d'équilibre il est nécessaire de bien poser les valeurs de l'organisation et de les rendre transparentes, en appliquant le legal design et en testant les interfaces et leur réception auprès du public cible. L'éthique et le contrôle sur les données est donc une problématique humaine plus que technique.

(1) Vayenas et Tasioulas, « The dynamics of big data and human rights: the case of scientific research », Philosophical Transactions of the Royal Society, 375, 2084, 28/12/2016

(2) Lenzini, « Transparency in the RGPD », ce livre Blanc, 2019

(3) Rossi et al, "Legal Design Patterns, ce Livre Blanc, 2019

(4) Von Grafenstein, « Integrating the User Perspective in the Regulation", ce Livre Blanc, 2019

(5) Floridi, « What is data ethics ?", Philosophical Transactions of the Royal Society, 375, 2084, 28/12/2016

Matthias De Bièvre :

Matthias De Bièvre est le fondateur et Président de Visions. Matthias a coordonné la partie B mettant en avant l'état de l'art de la recherche grâce aux travaux de nombreux experts et chercheurs mobilisés pour ce Livre Blanc. Visions édite le logiciel VisionsTrust qui permet aux organisations de facilement gérer les droits des personnes sur leurs données.

Son but est de démarquer les organisations vertueuses par la transparence offerte sur les données personnelles et la simplicité du contrôle. Redonner contrôle à chacun sur ses données personnelles est sa mission et la condition d'une innovation éthique et pérenne. Il s'intéresse et agit pour la mutualisation des données au service de la data science, notamment en éducation. Matthias est également conférencier sur l'éthique dans la data science dans plusieurs universités françaises.

“le son des objets intelligents. la conception sonore en tant que technologie permettant la protection de la vie privée.”

Le présent article examine certains défis que pose la mise en œuvre d’innovations en matière de conception sonore comme les technologies renforçant la protection de la vie privée (Privacy Enhancing Technologies - PET).
Les signaux sonores peuvent en effet représenter une forme de notification conforme aux règles du RGPD en matière de notification et au principe de transparence en ce qui concerne le traitement des données à caractère personnel. La pertinence du son des dispositifs interactifs en tant qu’outil de protection de nos données personnelles a rarement été explorée dans la littérature académique.

1. Le son comme élément clé de l’expérience utilisateur et comme outil de transmission de données :

Les métiers en constante évolution de l’UID (concepteur d’interface utilisateur) et de l’UXD (concepteur d’expérience utilisateur) se sont jusqu’à présent moins concentrés sur les sons, les interfaces utilisateur visuelles étant encore prédominantes de nos jours. Les écrans sur les comprimés, les montres et les appareils portables nous permettent de visualiser nos actions sur l’appareil, ce qui rend souvent inutile un feedback sous la forme d’une confirmation audible de ces actions. Cependant, nous nous dirigeons vers une ère où les assistants virtuels et un certain nombre d’objets interactifs occuperont nos vies personnelles et où le son deviendra un élément fondamental dans notre interaction avec les objets intelligents. Les tâches de conception sonore vont donc devenir, dans un avenir proche, une étape essentielle dans le processus de conception d’objets intelligents et de machines intelligentes.
Nous savons déjà que le son peut être utilisé à la fois pour transmettre des données et pour permettre à l’utilisateur de percevoir des données. “Sonification” est le terme utilisé pour désigner l’utilisation d’un son non vocal pour transmettre des informations ou pour permettre de percevoir des données. La technologie innovante Chirp™ est un bon exemple de la façon dont le son peut être utilisé pour transmettre des données. Le son est en effet omnidirectionnel et peut être transmis à partir d’une source pour voyager dans toutes les directions à partir de sa source. Cela le rend particulièrement adapté à la transmission de données dans une configuration de réseau “un à plusieurs” vers des dispositifs qui peuvent ne pas avoir d’interaction ou d’association préalable. Par contre, le deuxième aspect, celui de l’utilisation de l’audio non vocal pour percevoir les données, est quelque chose de plus consolidé et de plus répandu. Les signaux sonores sont présents dans plusieurs appareils ou applications que nous utilisons déjà largement, en particulier dans ceux dont l’interface utilisateur est moins visuelle. Dans de tels appareils et applications, une confirmation sonore des actions de l’utilisateur est souvent disponible. Par exemple dans l’application mobile Gmail™ un son nous confirme que l’e-mail a été envoyé.
La perception auditive présente plusieurs avantages en termes de résolution temporelle, spatiale, d’amplitude et de fréquence qui font du son un outil alternatif ou complémentaire aux techniques de visualisation. Dans cette perspective, les tâches de conception sonore visent donc en premier lieu à étendre l’utilité du produit, en fournissant à l’utilisateur une plus grande valeur en termes d’utilité et d’efficacité. Lorsqu’ils conçoivent les sons d’applications Web, les concepteurs sonores doivent tenir compte de plusieurs facteurs. Tout d’abord, chaque son est conçu en tenant compte de son positionnement dans

le flux des actions disponibles pour l'utilisateur. Deuxièmement, les signaux auditifs doivent être conçus et mis en œuvre dans les applications de manière à pouvoir être rapidement associés par l'utilisateur à chaque action à laquelle ils se rapportent. Enfin, chaque signal sonore doit être conçu par rapport aux autres : cela signifie que si chaque son doit pouvoir être suffisamment distingué des autres signaux, il doit en même temps bien s'intégrer à l'autre de la même application.
Les concepteurs finissent par créer une sorte de palette sonore qui se distingue pour chaque application.

2. Le son comme une marque et comme une marque de fabrique. L'entreprise "identité sonore" :

La "palette" de sons choisis par les concepteurs pour une certaine application ou un certain dispositif a également un lien clair avec la marque de l'entreprise qui distribue l'application ou le dispositif. Les concepteurs sonores devront donc tenir compte des besoins du "sonic branding" afin de créer et de consolider une identité sonore qui permette de distinguer toutes les applications d'une certaine entreprise de celles d'un concurrent différent.
Comme nous le savons tous, un son peut être enregistré comme marque de commerce tant qu'il est distinctif. La plupart des offices de brevets et de marques dans le monde acceptent le dépôt de marques sonores. L'Office italien des brevets et des marques (UIBM), par exemple, accepte le dépôt de marques sonores conformément à l'article 7 du décret législatif 30/2005, mais à condition qu'il puisse être représenté sous forme graphique en cas de dépôt papier. En revanche, en déposant une demande en ligne, il est possible de télécharger un fichier qui reproduit le son.
Jusqu'à présent, les sons qui ont déjà été enregistrés en tant que marques étaient des sons contenus dans des slogans publicitaires. Toutefois, la protection de l'identité sonore relative à l'application globale ou à la "palette sonore" du dispositif est plus susceptible d'être couverte par les législations nationales sur la concurrence déloyale. En Italie, par exemple, l'identité sonore peut être protégée par les règles contre l'imitation servile de l'article 2598, paragraphe 1, du Code civil.

3. Le son comme PET (Technologie d'amélioration de la protection de la vie privée) :

Les signaux sonores d'appareils intelligents ou interactifs peuvent également contribuer à protéger nos données personnelles. Une telle perspective a rarement été explorée dans la littérature.
L'un des problèmes les plus problématiques avec les appareils IOT est le risque que les utilisateurs n'aient pas le contrôle sur le flux automatique de données généré par les appareils utilisés. Un appareil peut en effet être activé sans que l'utilisateur soit correctement informé de son activation. De plus, une communication entre les différents objets intelligents utilisés peut être établie automatiquement. Il peut également arriver que, en raison de l'absence de normes dans le format des données, l'utilisateur ne soit pas au courant des activités continues de collecte de données par ces dispositifs. En outre, les dispositifs IOT peuvent collecter des données auprès de tiers (autres que le propriétaire) qui n'ont pas donné leur consentement et qui n'ont peut-être même pas remarqué qu'ils se trouvent dans la zone de détection d'un dispositif IOT.
Le groupe de travail sur l'article 29 a déjà examiné ces préoccupations dans un avis publié en 2014 (avis 8/2014), au titre des directives 95/46/CE et 2002/58/CE (avant l'entrée en vigueur du RGPD). Dans ce document, le groupe de travail n'a pas couvert tous les domaines d'application possibles de l'IOT (tels que les secteurs des machines industrielles et des villes intelligentes) mais a plutôt limité son analyse aux

appareils IOT déjà largement utilisés par les consommateurs européens, tels que les appareils domotiques et les appareils portables (comme les bracelets pour mesurer les performances sportives ou les montres à puce).

Dans l'avis susmentionné, le GT29 a précisé que les fabricants de dispositifs, de plates-formes et d'applications IOT doivent traiter ces risques à un stade précoce, c'est-à-dire pendant la phase de conception des dispositifs, afin de garantir la protection des données personnelles tout au long du cycle de vie des données. Il s'agit essentiellement d'un énoncé du principe de la prise en compte du respect de la vie privée dès la conception, qui a ensuite été explicitement inclus en tant qu'exigence légale par le règlement général européen sur la protection des données (RGPD), qui entrera en vigueur en mai 2018. Le principe du respect de la vie privée dès la conception exige que les fabricants de dispositifs ou les développeurs d'applications ou de plates-formes Web intègrent le respect de la vie privée et la sécurité dans la conception du noyau fonctionnel du dispositif ou de l'architecture de la plateforme Web ou des applications. Ces recommandations restent valables bien que le règlement relatif à la protection de la vie privée dans le secteur des communications électroniques, qui traite plus spécifiquement du traitement des données dans de tels contextes, ne soit pas encore approuvé.

En particulier, le principe du respect de la vie privée dès la conception exige que les utilisateurs aient un contrôle total sur le flux des données détectées et collectées par les dispositifs intelligents. Plus précisément, les fabricants et les développeurs sont invités à s'assurer que (1) le dispositif ne s'active pas automatiquement, mais à la suite d'une action de l'utilisateur ; (2) un signal informe l'utilisateur que le dispositif est actif et qu'il collecte des données ; (3) l'utilisateur est informé du type de capteurs et du type de données collectées ; (4) il peut accéder et éventuellement exporter ses données dans les formats de données les plus utilisés et de façon structurée ; (5) il peut toujours modifier ou supprimer les données avant leur transmission au fabricant ou leur publication sur la plateforme Web.

Les trois premières exigences de la liste ci-dessus représentent une mise en œuvre pratique du principe plus général de transparence énoncé dans le RGPD, comme dans la directive précédente de 1995. (Pour en savoir plus sur le principe de transparence et les obligations de notification, voir M.L. Manis, "The Processing Of Personal Data In The Context Of Scientific Research. The New Regime Under The Eu-RGPD", Biolaw Journal-N.03/2017, disponible sur http://www.biodiritto.org/ojs/index.php?journal=biolaw&page=article&op=view&path%5b%5d=259)

L'avis du WP29 n'a pas précisé si les "signaux appropriés" destinés à l'utilisateur et aux tiers (qui se trouvent dans la zone de détection des dispositifs IOT) doivent être visuels ou sonores. Toutefois, en plus des cas d'utilisateurs aveugles ou malvoyants, il existe plusieurs scénarios où un signal visuel peut ne pas être suffisant. Par conséquent, les signaux audio (en plus des fonctions mentionnées au paragraphe précédent) peuvent également contribuer à respecter les exigences de la législation en matière de protection de la vie privée et, en particulier, les règles relatives à la notification, au consentement et au principe de la transparence. cet effet, les signaux audio peuvent également être considérés comme des technologies renforçant la protection de la vie privée (PET).

Par conséquent, nous devons nous attendre à un développement considérable du secteur de la conception sonore en Europe, en raison également des règles plus strictes en matière de respect de la vie privée dès la conception définies par le RGPD et du développement croissant du secteur des TES.

4. Comment trouver un équilibre entre la normalisation et la nécessité d'une identité solide ?

L'une des conséquences naturelles de l'application des principes de la vie privée par défaut et de la vie privée par conception sera la tendance à la normalisation des technologies renforçant la protection de la vie privée. Et les TEP représentées par des signaux sonores ne seront pas exclues d'une telle tendance. Les signaux doivent être facilement reconnaissables et doivent être normalisés pour pouvoir remplir leur fonction.

Pensons à un système d'éclairage intelligent installé dans un quartier résidentiel. Dans le cas où les résidents décident de se connecter à la même plateforme, qui contrôle l'éclairage, à d'autres applications qui permettent la détection du passage ou à d'autres services de vidéosurveillance qui collectent des informations sensibles, un signal sonore doit informer les tiers de cette activité de collecte de données (les tiers étant des non-résidents qui n'ont pas donné leur consentement et ne se trouvent pas dans un lieu privé).

Pour remplir sa fonction de "notification", le signal audio doit être reconnaissable et doit donc être conforme aux normes du marché ou aux normes technologiques appropriées. Le RGPD établit que, lors du choix des technologies appropriées pour la collecte et le traitement des données, les responsables du traitement des données tiendront compte (en plus des coûts de mise en œuvre) de l'état de l'art (article 25) et, conformément à la nouvelle approche fondée sur le risque introduite par le RGPD, ils devront choisir des technologies renforçant la protection des données qui ont acquis une maturité suffisante pour être considérées comme adaptées à cet objectif. (Pour les évaluations de la maturité des PET, voir les travaux de l'agence Enisa https://www.enisa.europa.eu). Pour une analyse de l'approche dite fondée sur le risque dans le cadre du RGPD, voir M.L.Manis, extrait de https://marialuisamanis.nova100.ilsole24ore.com/2017/11/17/risk-based-approach-under-the-RGPD-can-a-strong-harm-based-approach-apply-to-bio-banking/

Par conséquent, les concepteurs sonores devront bientôt s'efforcer de trouver un équilibre entre le besoin d'une " identité sonore " (qui différencie les produits de l'entreprise des produits concurrents sur le marché) et le besoin opposé d'une normalisation des signaux audio requise par la réglementation sur la protection de la vie privée.

Auteur : Maria Luisa Manis

Cet article est une traduction autorisée d'un billet de blog publié à l'origine en italien le 27.11.17.

4- Limits of design

a. La “privacy literacy”, condition indispensable de la réussite du design

Les limites de la transparence par le design : Insuffisant à lui seul pour relever le défi de la protection des données :

Les résultats de la recherche en sciences du comportement sont d’une grande valeur pour les politiques réglementaires et non réglementaires visant à modifier les comportements. L’un des principaux objectifs devrait être d’élaborer des stratégies et de trouver des solutions pour soutenir au mieux et aider les utilisateurs à prendre des décisions en matière de protection de la vie privée afin de permettre et de renforcer un comportement respectueux de la vie privée dans un environnement numérique de plus en plus complexe. Cela comprend les aspects de design, comme les visualisations ou les outils d’aide à la protection de la vie privée, qui favorisent la transparence et, en bout de ligne, pourraient améliorer l’autodétermination et le contrôle des utilisateurs. Cependant, le processus de design est confronté à de nombreux défis liés au contexte et à la technologie qui doivent être pris en compte dans la prise de décision humaine.

Les sections qui suivent abordent certains de ces défis à l’aide de l’exemple des icônes de protection de la vie privée et concluent par les limites d design et l’importance de la synergie qui en résulte entre le design et l’éducation.

Les défis du design :

Les décisions relatives à la protection de la vie privée sont le plus souvent prises dans des conditions incertaines, par exemple des renseignements incomplets, des conséquences inconnues et des probabilités d’événements indésirables, ce qui peut entraîner des comportements moins réfléchis, moins rationnels et moins délibérés en matière de protection de la vie privée. Il est important de noter que même si les utilisateurs disposaient d’une information globale, leur capacité à la traiter serait encore limitée en raison de leur rationalité limitée (Simon, 1989). Ces limitations cognitives conduisent souvent les utilisateurs à s’appuyer sur des raccourcis mentaux, appelés heuristiques (Tversky & Kahneman 1974), qui n’impliquent pas autant de réflexion et d’effort cognitif (Dinev, McConnell & Smith, 2015). L’heuristique peut conduire à des décisions efficaces et acceptables (Gigerenzer, Hartwig & Pachur, 2011), mais elle peut aussi conduire à des erreurs systématiques de jugement, appelées biais cognitifs (Tversky & Kahneman 1974). Les nudges, couvrant “ tout aspect de l’architecture de choix qui modifie le comportement des gens d’une manière prévisible sans interdire aucune option “ (Thaler & Sunstein, 2008, p.6), s’appuient sur des heuristiques et des biais. Les concepteurs peuvent utiliser certaines heuristiques et biais pour inciter les utilisateurs à adopter un comportement plus respectueux de la vie privée. De plus, le design peut contrecarrer spécifiquement les préjugés qui pourraient mener à des comportements moins protecteurs de la vie privée (Ly, Mazar, Zhao et Soman, 2013). Le temps et les préférences en matière de risques en sont des exemples. La plupart du temps, les utilisateurs recherchent une satisfaction immédiate, ignorant ainsi les conséquences négatives potentielles afin, par exemple, d’utiliser un service ou d’acquérir une marchandise immédiatement (Zuiderveen Borgesius, 2015). Ce préjugé en faveur d’une satisfaction immédiate s’accentue souvent lorsque les conséquences négatives sont inconnues, non mentionnées ou négligées dans les politiques de protection de la vie privée. ea design peut intervenir activement contre ces problèmes

d'information incomplète et asymétrique en offrant aux utilisateurs des indicateurs de protection de la vie privée qui sont facilement accessibles, opportuns dans le temps, pertinents et compréhensibles. De tels indicateurs pourraient être des icônes de protection de la vie privée. Dans le même temps, il faut tenir compte des limites de la capacité de traitement de l'information humaine, en particulier en ce qui concerne l'abondance de l'information (voir les études sur la surcharge d'information par Eppler & Mengis, 2004 ; Roetzel, 2018) qui affecte la mémoire de travail et les processus attentionnels. En conséquence, des solutions doivent être trouvées pour déterminer comment et dans quelle mesure les informations doivent être présentées aux utilisateurs afin d'obtenir des comportements de protection de la vie privée. Dans le cas des icônes de confidentialité, cela signifie que le nombre d'icônes présentées doit être bien pensé. Les mécanismes d'attention sélectionnent les informations pertinentes pour un traitement ultérieur et suppriment les informations non pertinentes. L'être humain peut soit diriger volontairement son attention visuelle en raison d'attentes et d'objectifs (de haut en bas), soit attirer automatiquement son attention sur lui par des stimuli externes et saillants (de bas en haut) (Katsuki & Constantinidis, 2013). Dans un environnement en ligne, les utilisateurs semblent se concentrer sur leur objectif premier (attention descendante), par exemple l'acquisition d'un produit ou d'un service numérique, mais surtout pas sur la protection des données. Pour déplacer les processus attentionnels de la tâche principale vers les questions de protection des données, des stimuli externes très importants sont nécessaires (attention ascendante). Il faut donc veiller à ce que les utilisateurs ne soient pas submergés par un trop grand nombre d'icônes et qu'ils soient en mesure d'accorder leur attention. De plus, la capacité de la mémoire de travail visuelle est limitée. La mémoire de travail visuelle, définie comme "[...] la maintenance active de l'information visuelle pour répondre aux besoins des tâches en cours " (Luck & Vogel, 2013, p. 392) joue un rôle décisif dans la prise de décision. Entre autres facteurs, les utilisateurs doivent décider si les aspects liés au traitement des données sont conformes à leurs attentes et préférences ou s'ils l'emportent sur les avantages de l'arbitrage. Cependant, la capacité humaine est limitée et le dépassement d'un certain seuil dépendant du contexte entraîne un déclin du traitement de l'information. Comme on peut le constater, l'étendue de l'information présentée a une influence considérable sur la prise de décisions en matière de protection de la vie privée. Dans l'exemple des icônes de protection de la vie privée, la présentation d'un trop grand nombre d'icônes pourrait entraîner une surcharge d'information qui a des effets préjudiciables sur le transfert d'information prévu.

Un autre défi auquel il faut prêter attention est l'habituation des utilisateurs aux mécanismes de transparence, tels que les icônes de protection de la vie privée. Des études empiriques issues de la recherche sur la sécurité font état d'une diminution de l'attention visuelle des utilisateurs en raison de l'exposition répétée à des messages d'avertissement normalisés (Kim et Wogalter, 2009). Cependant, certains mécanismes peuvent être appliqués pour lutter contre les effets d'accoutumance, tels que les variations polymorphes du dessin, par exemple les variations de couleur, les accents, les mots indicateurs, les contrastes ou les frontières (Anderson, Jenkins, Vance, Kirwan & Eargle, 2016).

De plus, les interventions universelles comme les icônes de la protection de la vie privée ne peuvent tenir compte des différences interindividuelles, comme les traits de personnalité (Egelman et Peer, 2015), les différents niveaux de connaissances et de conscience préexistants, les préférences, les normes sociales (Acquisti, John et Loewenstein, 2012) et les influences culturelles et générationnelles (Miltgen et Peyrat-Guillard, 2014) - facteurs qui influencent également les décisions concernant la vie privée. Les outils personnalisés d'aide à la protection de la vie privée peuvent certainement expliquer ces différences

interindividuelles, mais très probablement au détriment de l'autonomie des utilisateurs et de la transparence du processus décisionnel.

Combattre les facteurs situationnels qui tiennent compte des différences intraindividuelles est un défi de taille, sinon un défi qui dépasse le cadre du design. Un exemple serait l'heuristique d'effet qui décrit comment le fait d'être de bonne humeur peut entraîner une sous-estimation des risques et une surestimation des bénéfices (Finucane, Alhakami, Slovic & Johnson, 2000). De plus, lorsque les utilisateurs sont épuisés cognitivement, ils s'appuient davantage sur l'heuristique automatique qui n'implique pas autant de délibération et d'effort cognitif (Dinev, McConnell & Smith, 2015). Les facteurs situationnels ne peuvent être traités qu'en partie par des mécanismes et des technologies préventifs tels que les retards décisionnels (Wang et al., 2011, 2013), les systèmes d'alerte ou de rétroaction (Acquisti et al., 2017) qui peuvent permettre aux utilisateurs d'entreprendre un traitement plus délibéré de l'information.

Comme on peut le constater, la prise de décision humaine est influencée par un ensemble complexe de facteurs dont certains posent d'énormes défis en matière de design.

Limites du design :

Même le design la plus réfléchie et la plus responsabilisante pour l'utilisateur a ses limites pour ce qui est de faciliter les comportements respectueux de la vie privée. Le paradoxe du contrôle (Brandimarte, Acquisti et Loewenstein, 2013), qui décrit la constatation selon laquelle les gens divulguent plus d'information s'ils croient avoir le contrôle, illustre le mieux cette situation. Par conséquent, l'amélioration du contrôle des utilisateurs par le biais des principes de design ne va pas nécessairement de pair avec la promotion du comportement des utilisateurs en matière de protection de la vie privée. Compte tenu des contraintes cognitives et temporelles des utilisateurs dans les environnements numériques, une modification de l'architecture de choix par le design peut les aider à adopter un comportement plus respectueux de la vie privée. Afin d'obtenir des changements de comportement à long terme, des approches éducatives sont nécessaires comme complément important aux principes de design. Il ne suffit pas de développer des systèmes visant à soutenir et à protéger la vie privée des utilisateurs en ligne si ceux-ci n'ont pas les connaissances de base sur l'existence et la fonctionnalité de ces systèmes (Acquisti et al., 2017) ainsi que sur la notion de protection des données (Vasalou, Oostveen, Bowers & Beale, 2015). Comme indiqué précédemment, le fait de détourner l'attention de la tâche principale vers les questions de protection des données, par exemple dans les situations d'autorisation, constitue déjà un obstacle. Si l'on a surmonté cet obstacle grâce à un design bien réfléchie de l'interface utilisateur, on se heurte au problème que l'utilisateur doit être motivé pour traiter le problème et reconnaître le besoin. Les gens doivent être non seulement extrinsèquement mais aussi intrinsèquement motivés à s'engager dans des technologies et des mécanismes de protection de la vie privée (Vasalou, Oostveen, Bowers & Beale, 2015), ce qui peut être réalisé par la formation et l'éducation. L'effet positif de l'amélioration des compétences des utilisateurs ou de la transmission de nouvelles compétences (par ex. l'alphabétisation au risque ou la gestion des incertitudes) sur la prise de décision est étudié dans l'approche "boost" (Grüne-Yanoff & Hertwig, 2016 ; Hertwig & Grüne-Yanoff, 2017), qui est basée sur le programme simple de recherche heuristique (Gigerenzer, Hertwig & Pachur, 2011). Tant l'approche de l'impulsion que l'éducation scolaire représentent des points de contact essentiels pour parvenir à des changements de comportement à long terme.

L'importance d'accroître l'engagement et la culture numérique des utilisateurs doit également être prise en compte dans l'élaboration et le design d'outils personnalisés d'aide à la protection de la vie privée. Tant que l'on ne peut pas supposer que les utilisateurs possèdent au moins quelques connaissances de base sur le concept de protection des données, il n'est pas possible de garantir que les outils de protection de la vie privée basés sur l'apprentissage automatique permettront de prédire les véritables choix des utilisateurs, car on peut se demander si ces prévisions sont réellement fondées sur leurs préférences en matière de protection des données ou plutôt sur leur nescience de ce concept.

Conclusion :

Le monde numérique devient de plus en plus complexe alors que la capacité humaine de traitement de l'information reste limitée. Les modifications de design, la protection de la vie privée par défaut et la protection de la vie privée dès la conception peuvent aider et guider les utilisateurs dans leur comportement en matière de protection de la vie privée dans des environnements numériques complexes, ce qui souligne la pertinence et l'importance de faire constamment progresser le design et la technologie des interfaces utilisateur. Le défi consiste à élaborer des outils, des principes et des politiques de design qui appuient et aident les utilisateurs à prendre des décisions respectueuses de la vie privée tout en préservant l'autodétermination, le contrôle et la liberté de choix. La littératie en matière de protection de la vie privée est la clé de voûte d'une prise de décision éclairée et délibérée et doit être en synergie avec les principes de design visant à préserver la vie privée pour relever le défi de la protection des données.

La complexité et le chevauchement des compétences dans ce domaine de recherche exigent un échange de connaissances interdisciplinaire et multisectoriel afin de déterminer des interventions efficaces et de suivre le rythme des progrès technologiques qui s'accompagnent toujours de questions de protection des données.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). L'impact des normes relatives sur la propension à divulguer. Journal of Marketing Research, 49(2), 160-174. https://doi.org/10.1509/jmr.09.0215

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. & Wilson, S. (2017). Nudges pour la confidentialité et la sécurité : Comprendre et aider les choix des utilisateurs en ligne. ACM Comput. Surv. 50(3).

Anderson, B. B., Jenkins, J. L., Vance, A., Kirwan, C. B., & Eargle, D. (2016). Votre mémoire travaille contre vous : Comment le suivi oculaire et la mémoire expliquent l'accoutumance aux avertissements de sécurité. Decision Support Systems, 92, 3-13.

Brandimarte, L., Acquisti, A. et Loewenstein, G. (2013). Des confidences mal placées : La vie privée et le paradoxe du contrôle. Social Psychological and Personality Science, 4(3), 340-347.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informer la recherche sur la protection de la vie privée par le biais des systèmes d'information, de la psychologie et de l'économie comportementale : Sortir du cadre

"APCO". Information Systems Research, 26(4), 639-655.

Egelman, S. & Peer, E. (2015). Le mythe de l'utilisateur moyen : améliorer les systèmes de confidentialité et de sécurité par l'individualisation. Dans les Actes de l'Atelier 2015 sur les nouveaux paradigmes de sécurité (NSPW'15). ACM, New York, NY, USA, 16-28.

Eppler, M., & Mengis, J. (2004). Le concept de surcharge d'information : Une revue de la littérature des sciences de l'organisation, de la comptabilité, du marketing, des systèmes d'information de gestion et des disciplines connexes. Société de l'information, 20(5), 325-344.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). Ils affectent l'heuristique dans les jugements des risques et des bénéfices. Journal of Behavioral Decision Making, 13(1), 1-17.

Grüne-Yanoff, T., & Hertwig, R. (2016). Coup de pouce ou coup de pouce : Dans quelle mesure les politiques et les théories sont-elles cohérentes ? Esprits et machines, 26, 149-183. doi:10.1007/s11023-015-9367-9

Katsuki, F. et Constantinidis, C. (2014). Attention du bas vers le haut et du haut vers le bas : Différents processus et systèmes neuronaux qui se chevauchent. The Neuroscientist, 20(5), 509-521.

Kim, S. et Wogalter, M. S. (2009). Habituation, déshabituation et effets de rétablissement dans les avertissements visuels. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 53(20), 1612-1616. https://doi.org/10.1177/154193120905302015

Luck, S. J., et Vogel, E. K. (2013). Capacité de la mémoire de travail visuelle : De la psychophysique et de la neurobiologie aux différences individuelles. Trends in Cognitive Sciences, 17(8), 391-400.

Ly, K., Mazar, N., Zhao, M. et Soman, D. A. (2013). Guide du praticien sur les coups de poing. SSRN Electronic Journal, 1-28.

Miltgen, C.L. et Peyrat-Guillard, D. (2014). Cultural and Generational Influences on Privacy Concerns : a Qualitative Study in Seven European Countries. European Journal of Information Systems 23(2), 103-125.

Gigerenzer, G., Hertwig, R. et Pachur, T. (2011). Heuristique : Les fondements du comportement adaptatif. (G. Gigerenzer, R. Hertwig, & T. Pachur, Eds.). New York, NY : Oxford University Press.

Hertwig, R. et Grüne-Yanoff, T. (2017). Des coups de pouce et des coups de pouce : Orienter ou habiliter les bonnes décisions. Perspectives on Psychological Science, 12(6), 973-986.

Roetzel, P.G. (2018). Surcharge d'information à l'ère de l'information : une revue de la littérature sur l'administration des affaires, la psychologie des affaires et les disciplines connexes avec une approche bibliométrique et l'élaboration de cadres. Business Research, p. 1-44.

Ryan, R. M., & Deci, E. L. (2000). Motivations intrinsèques et extrinsèques : Définitions classiques et nouvelles orientations. Contemporary Educational Psychology, 25(1), 54-67.

Simon, H. A. (1989). Le scientifique comme solutionneur de problèmes. Dans D. Klahr & K. Kotovsky (dir. publ.), Complex information processing : L'impact de Herbert A. Simon. (pp. 375-398). Hillsdale, NJ : Lawrence Erlbaum Associates, Inc.

Thaler, R. H., & Sunstein, C. R. (2008). Nudge : Améliorer les décisions concernant la santé, la richesse et le bonheur. New Haven, CT : Yale University Press.

Tversky, A. et Kahneman, D. (1974). Jugement dans l'incertitude : Heuristique et biais. Science, 185(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

Vasalou, A., Oostveen, A.-M., Bowers, C., & Beale, R. (2015). Comprendre l'engagement dans le domaine de la protection de la vie privée par la recherche en design. Journal of the Association for Information Science & Technology, 66(6), 1263-1273.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G., & Cranor, L.F. (2011). J'ai regretté la minute où j'ai insisté sur le partage : une étude qualitative des regrets sur Facebook. Dans les Actes du Septième Symposium sur la protection de la vie privée et la sécurité utilisables (SOUPS'11). ACM, New York, NY, USA.

Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A., Cranor, L.F. (2013). Nudges sur la protection de la vie privée dans les médias sociaux : Une étude exploratoire sur Facebook. In : Actes de la 22e Conférence internationale sur le World Wide Web. pp. 763-770. ACM.

Zuiderveen Borgesius, F.J. (2015). Consentement éclairé : Nous pouvons faire mieux pour défendre la vie privée. IEEE Security and Privacy, 13(2), 103-107.

Marie Schirmbeck :

Marie Schirmbeck (MSc Psychologie) est associée de recherche à l'Institut Weizenbaum pour la société en réseau à Berlin. Auparavant, elle a travaillé comme analyste en conversion. Ses recherches portent sur les processus dynamiques cognitifs et émotionnels-motivationnels qui sous-tendent la divulgation souvent étendue de données personnelles par les individus et les conséquences individuelles et sociétales de ce comportement.

C/ LA CERTIFICATION PRIVACY TECH

Autobiographie :

Alessandro FIORENTINO est responsable de l'offre Informatique et Libertés du Cabinet Infhotep et Vice-Président de l'association Privacy Tech.

Alessandro FIORENTINO a débuté sa carrière en tant qu'analyste-programmeur, il a par la suite assumé la fonction d'architecte des systèmes d'information au sein d'un grand groupe de courtiers en gestion de patrimoine.

Titulaire d'un Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP), il a soutenu une thèse professionnelle relative à la mise en œuvre du Privacy by Design.

Nommé "Ambassadeur du Privacy by Design", le 22 mai 2013 par l'Office du Commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada, le promoteur du PbD.

Cette reconnaissance importante motivée par la contribution d'Alessandro FIORENTINO à la promotion du Privacy by Design souligne son savoir-faire et sa proactivité dans la recherche des solutions novatrices juridiques applicables au domaine des NTIC.

Il travaille sur plusieurs projets d'innovation et de prospective liés au concept, assure aujourd'hui l'unité d'enseignement Privacy by Design au sein du Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP) et l'unité d'enseignement Méthodologies du DPO au sein du Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Mines-Telecom Business School.

Introduction :

L'entrée en application du Règlement Général sur la Protection des Données le 25 mai 2018, a donné naissance à une myriade de vocation pour la protection des données à caractère personnel. En effet de nombreux opportunistes s'improvisent sur ce marché, et des "apprentis-experts RGPD" fleurissent sur le web surfant sur l'épée de Damoclès que représentent les nouvelles sanctions en proposant du conseil, de la formation ou encore des solutions logiciels miracles pour se mettre en conformité.

Giovanni Buttarelli s'est d'ailleurs exprimé sur le sujet récemment en mettant en garde sur le choix des conseils. Pour la Privacy Tech, cette mise en garde est également pertinente dans le choix des outils.
Une multitude de solutions pour accompagner la conformité des organismes sont présentes sur le marché. Des logiciels proposés par des gros éditeurs experts du RGPD pour l'occasion, des outils de sécurité déclinés depuis avant-hier pour faire de la protection des données, des outils à l'origine dédiés aux Correspondants Informatique et Libertés relookés ou encore des nouvelles solutions plus ou moins bien nées.

Pour un Responsable de traitement, il est difficile de faire la part des choses au milieu de tout cela, ces derniers sont très méfiants dans le choix des outils dédiés à ce sujet et nous pouvons les comprendre. Forcé de constater qu'au vu de ce contexte, il est souvent très compliqué pour les « start-up » passionnées d'atteindre la signature du contrat. En effet pour ces derniers la mise en concurrence est rude et les périodes d'avant-vente ou de réponse aux appels-offres sont chronophages et coûteuses pour ces jeunes entreprises.

Ces différentes phases représentent souvent des frontières infranchissables pour ces petits acteurs souvent plus compétents sur le sujet que les gros éditeurs de logiciels plus habitués à montrer patte blanche lors des démarches précontractuelles dans des dédales de grilles d'évaluations toujours plus importantes.

Pour la PRIVACY TECH stimuler l'excellence française en matière de « Privacy » est un objectif à atteindre. Alors voilà la question que beaucoup d'entre-nous ont eu en tête durant ces derniers mois. Comment permettre à cet écosystème français de passer ces frontières en fluidifiant leurs négociations et assurer un facteur confiance à la hauteur des attentes des organisme de toutes tailles.

La seule réponse à cette question est la certification.

21 mars 2019
Alessandro FIORENTINO
Vice-Président de la Privacy TECH
Responsable de l'offre Informatique et Libertés du Cabinet Infhotep
Ambassadeur du Privacy by Design

Démarche méthodologique :

Afin d'avoir une vision sur les différents types de solutions sur le marché nous avons participé à l'organisation de la Trust&Privacy Night 2018 en collaboration avec U Change (créateur des Trust&Privacy Day 2016 et 2017), SNCF développement et K&L Gates. La Trust&Privacy Night regroupa le 25 avril 2018, 350 professionnels directement concernés par la mise en conformité RGPD, startups, PME, ETI et grandes entreprises.

Cet événement nous a permis de tester une démarche de labellisation des meilleures solutions PrivacyTech. Toutes les startups sélectionnées ont présenté en quelques minutes leurs solutions avec un focus sur leur capacité à apporter une solution concrète dans le cadre de l'application du Règlement Général sur la Protection des Données.

À la suite de cet événement, le bureau de l'association s'est réuni pour acter le projet de créer un référentiel de certification afin d'initier un travail de certification avec l'AFNOR comme l'une des initiatives du programme Privacy Tech 2018-2019.

Lors de la Trust&Privacy Night, nous avons pu constater que cinq familles de solutions étaient présentes. Nous nous sommes donc donnés comme objectif d'élaborer un référentiel d'exigences unique avec critères valables en fonction des catégories de solution.

Les cinq catégories de solution :

Les différentes catégories de solution sont les suivantes :

Catégorie 1 :

Data Protection Management Asset : cette catégorie regroupe toutes les solutions logicielles qui permettent à un organisme de répondre à un ou plusieurs principes fondamentaux assurant la licéité des traitements (Droit d'information, garanties de l'exercice des droits, gestion des consentements etc..).

Catégorie 2 :

Data Protection Management Solution : cette catégorie regroupe toutes les solutions logicielles qui permettent à un organisme de répondre à ses obligations documentaires (Registre, PIA, registre d'exercice des droits, journal des violations).

Catégorie 3 :

Data Processor Compliant Solution : cette catégorie regroupe toutes les solutions logicielles mises à disposition par un organisme qui a vocation à endosser un rôle de sous-traitant au sens du RGPD (solution logicielle RH, solution logicielle CRM, solution logicielle d'archivage, plateforme de gestion d'évènements, plateforme de routage courriel ...).

Catégorie 4 :

Personal Data Management : cette catégorie regroupe toutes les solutions logicielles tournées sur l'individu qui renforcent l'autodétermination informationnelle par la maîtrise et le contrôle par l'utilisateur sur ses données personnelles.

Catégorie 5 :

GAFA Alternative : cette catégorie regroupe toutes les solutions à destination de personnes physiques répondant à des besoins aujourd'hui majoritairement couverts par les GAFA
(Moteur de recherche, Messagerie électronique, Réseau social...)

Critères de la certification PRIVACY TECH :

Ces critères visent à certifier les cinq catégories de solution. Les critères à couvrir dépendent de la catégorie à laquelle appartient la solution qui candidate à cette certification.

1. Conditions préalables à remplir par l'organisme candidat présentant une solution à la certification :

Exigence 1.1 :

Pour pouvoir accéder à la phase d'évaluation, l'organisme candidat remplit toutes les conditions préalables suivantes :
Justifier de la désignation d'un délégué à la protection des données (DPO) par l'organisme.
Justifier de l'adhésion à l'association PRIVACY TECH ou s'engager à régler les droits d'utilisation du logo PRIVACY TECH correspondant à la catégorie de la solution directement à l'organisme de certification équivalent à 50% d'une adhésion en fonction de la tarification en vigueur et à respecter la charte Privacy Tech.

Éléments d'auditabilité :

Téléversement du récépissé de désignation auprès de la CNIL.
Téléversement de l'attestation émise par Privacy Tech ou de l'attestation d'engagement signée de la charte d'utilisation du logo PRIVACY TECH correspondant à la catégorie de la solution.

L'exigence 1.1 est imposée aux cinq catégories.

2. Exigences liées à l'organisme

Exigence 2.1 :

L'organisme possède une politique ou des règles internes en matière de protection des données.

Eléments d'auditabilité :

Téléversement de la politique de confidentialité internes à l'organisme.

L'exigence 2.1 est imposée aux cinq catégories.

Exigence 2.2 :

L'organisme met en œuvre des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement que sa solution logicielle assure.

Eléments d'auditabilité :

Téléversement d'un Plan d'Assurance Sécurité (PAS) lié à la solution

L'exigence 2.2 est imposée aux cinq catégories.

Exigence 2.3 :

L'organisme met en œuvre des mesures de protection des données dès la conception et/ou par défaut adaptées aux risques et à la nature des opérations de traitement que sa solution logicielle assure telles que le chiffrement ou un système assurant le principe de minimisation sur les différents points de collecte que la solution logicielle peut assurer.

Eléments d'auditabilité :

Téléversement d'une déclaration du DPO qui acte le fait qu'une réelle étude sur le principe de minimisation a été conduite sur l'ensemble des interfaces ou des points de collecte de la solution.
Téléversement de ladite étude.

L'exigence 2.3 est imposée aux cinq catégories.

Exigence 2.4 :

L'organisme tient à jour le registre des activités de traitement ainsi que la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données pour les traitements que sa solution logicielle assure à ses clients.

Eléments d'auditabilité :

Téléversement des fiches de traitement liées à la solution pour répondre aux exigences de l'article 30.2

L'exigence 2.4 est imposée aux trois premières catégories.

Exigence 2.5 :

L'organisme respecte le cadre juridique relatif à la sous-traitance en matière de traitement de données à caractère personnel et a fortiori l'ensemble des obligations de l'article 28 du Règlement Général sur la Protection des Données (RGPD).

Eléments d'auditabilité :

Téléversement des clauses contractuelles de sous-traitance.

L'exigence 2.5 est imposée aux trois premières catégories.

Exigence 2.6 :

L'organisme informe de ses clients ou utilisateurs les instruments juridiques susceptibles d'être utilisés si des transferts de données hors Union européenne existent dans un ou plusieurs des processus qu'il assure.

Eléments d'auditabilité :

Téléversement des mentions d'information avec l'url de ces dernières.

L'exigence 2.6 est imposée aux cinq catégories.

Exigence 2.7 :

L'organisme sait accompagner ses clients en matière d'analyse d'impact relative à la protection des données (en particulier si l'un ou plusieurs processus d'un traitement de données à caractère personnel sont assurés par le biais de la solution évaluée). Il est en mesure d'assurer la reddition de comptes nécessaire pour les différentes mesures techniques et organisationnelles qu'il assure pour ses clients dans le cadre de la solution logicielle.

Eléments d'auditabilité :

Téléversement d'un PIA lié à la solution.

L'exigence 2.7 est imposée aux trois premières catégories.

Exigence 2.8 :

L'organisme informe de toutes vulnérabilités détectées dans sa solution logicielle susceptible d'engendrer une violation de données personnelles nécessitant une notification à l'autorité de contrôle et/ou une communication aux personnes concernées.

Eléments d'auditabilité :

Téléversement de l'engagement contracté avec le Responsable de traitement.
Téléversement de la procédure formalisée liée à ce type d'événement
Téléversement des « printscreen » des interfaces dédiées à la journalisation de ces évènements (uniquement pour la seconde catégorie)

L'exigence 2.8 est imposée aux cinq catégories.

Exigence 2.9 :

L'organisme autorise la réalisation d'audit, par une tierce partie, en matière de protection des données à la demande et aux frais de ses clients.

Eléments d'auditabilité :

Téléversement de l'engagement contracté avec le Responsable de traitement.

L'exigence 2.9 est imposée aux trois premières catégories.

3. Exigences liées à la solution :

Exigence 3.1 :

Un guide d'utilisation de la solution est mis à disposition des clientS de l'organisme et mis à jour à chaque évolution.

Éléments d'auditabilité :

Téléversement du guide d'utilisation de la solution.

L'exigence 3.1 est imposée aux trois premières catégories.

Exigence 3.2 :

La solution permet d'assurer la traçabilité des actions exécutées, notamment à l'aide de tableaux de bord ou d'outils de suivi.

Éléments d'auditabilité :

Téléversement d'un « printscreen » de l'interface permettant d'assurer la piste d'audit.
Téléversement d'une extraction anonymisée d'un cas client.
Téléversement d'un compte d'accès à un plateforme de démo pour que l'auditeur puisse vérifier

L'exigence 3.2 est imposée aux cinq catégories.

Exigence 3.3 :

L'organisme candidat assure une mise à disposition régulière des dernières versions des sources (non obfusquées) de la solution auprès d'un tiers de confiance qui pourra être sollicité en cas besoin (par exemple pour assurer une continuité d'activité en cas de difficultés de l'éditeur).

Éléments d'auditabilité :

Téléversement d'une preuve de dépôt liée à la dernière version actuellement en production auprès d'un tiers de confiance.

L'exigence 3.3 est imposée aux trois premières catégories.

Exigence 3.4 :

La solution sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données et sait accompagner son exécution.

Éléments d'auditabilité :

Téléversement du « printscreen » d'évolution des éléments déclencheurs.

L'exigence 3.4 est imposée à la seconde catégorie.

Exigence 3.5 :

La solution embarque un dispositif d'effacement paramétrable en production en fonction des durées de conservation des différents traitements assurer par la solution.

Éléments d'auditabilité :

Téléversement du « printscreen » de l'interface dédiée.

L'exigence 3.5 est imposée aux cinq catégories.

Exigence 3.6 :

La solution assure le droit à la réversibilité de toutes les données traitées, ainsi que l'effacement des données à la suite d'un traitement de réversibilité.

Éléments d'auditabilité :

Téléversement d'exemple d'export réutilisable de tous les traitements liés (xml, json, csv, xls).
Téléversement d'un certificat d'engagement d'effacement type.

L'exigence 3.6 est imposée 3 premières catégories.

Exigence 3.7 :

La solution dispose d'une interface permettant d'assurer les différents droits des personnes, à destination du DPO pour la catégorie 2, à destination des personnes concernées pour les autres catégories.
(Exigence imposée aux cinq catégories)

Éléments d'auditabilité :

Téléversement d'un « printscreen » de l'interface permettant d'assurer cette fonctionnalité.
Mise à disposition d'un compte accès à une plateforme de démo pour la seconde catégorie uniquement.
Mise à disposition d'un accès à l'espace dédié informant de la procédure à suivre pour toutes les catégories hormis la seconde.

L'exigence 3.7 est imposée aux cinq catégories.

4. Conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH :

Exigence 4.1 :

L'organisme certifié s'engage à respecter les conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH figurant en Annexe 1 du présent référentiel en la signant et en adressant la version signée à l'organisme de certification.

Annexe 1 : Conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH conformément au référentiel de certification de solutions PRIVACY TECH :

Préambule :

Les présentes conditions générales constituent une déclaration expresse des valeurs, principes et règles qui doivent guider la conduite des organismes certifiés conformément au référentiel de certification des solutions PRIVACY TECH dans leurs relations avec leurs clients, leurs usagers, leurs prestataires, leurs fournisseurs, les institutions publiques ou privées et le public en général.

Les conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH regroupent des engagements concernant l'intégrité, la confidentialité et la transparence que tout organisme candidat à la certification doit prendre en compte dans son activité.

Article 1 – Champ d'application :

Les valeurs, principes et règles figurant dans cette charte doivent être appliqués par les organismes candidats à la certification. Les organismes habilités à certifier sont désignés en assemblée générale de la PRIVACY TECH. (Accréditation COFRAC sur la norme ISO 17021 pour la certification ISO 27001)

Article 2 – Principes généraux :

L'organisme candidat doit exercer son activité conformément aux principes suivants :

Intégrité, en respectant la réglementation en vigueur, notamment s'agissant des services qu'il fournit et en s'abstenant de toute activité illégale. L'organisme candidat ne doit pas communiquer sur sa certification PRIVACY TECH pour d'autres solutions que celles ayant fait l'objet de l'évaluation et dont la certification lui a été délivrée. Il doit faire un usage loyal et intègre de la certification et conforme à la charte de l'association PRIVACY TECH.

Rigueur, en poursuivant l'objectif de proposer une solution constamment à jour en termes de conformité à la réglementation en vigueur et sans imposer un surcoût tarifaire lié à cet objectif.

Transparence, en informant de manière claire, précise et suffisante ses clients de :

toute évolution de l'organisme vis-à-vis des compétences certifiées (par exemple : l'organisme ne remplit plus les conditions de la certification) ;
toute évolution de la solution (par exemple : par la présentation d'une feuille de route constamment à jour concernant le développement d'une nouvelle fonctionnalité non étudiée par l'organisme certificateur) ;
toute évolution susceptible de nuire au maintien de la certification notamment tout changement de statut de l'organisme (par exemple, fusion-acquisition, fusion-absorption).

Confidentialité, en respectant et assurant la protection et la confidentialité des informations auxquelles il peut avoir accès en tant qu'éditeur ou fournisseur de services, en protégeant le droit à la vie privée de toutes les personnes concernées. De telles informations ne sauraient être utilisées pour un avantage concurrentiel et ne sauraient être communiquées ou divulguées à des tiers non autorisés.

Article 3 – Relations avec les clients ou les usagers :

Dans ses relations avec ses clients ou ses usagers, l'organisme candidat :
Doit informer du contenu de la présente charte.
Doit s'abstenir d'exercer une activité promotionnelle (publicité, matériel d'information, etc.) qui pourrait conduire ses clients ou prospects à une interprétation inexacte de la signification de la certification de PRIVACY TECH sur la base du référentiel concernant la catégorie sur laquelle la certification lui a été délivrée.
Doit mettre à la disposition de ses clients un formulaire à compléter en cas de plainte ou de réclamation portant sur ses services fournis en tant qu'éditeur ou fournisseur de services. Ce formulaire sera adressé à l'organisme concerné par la plainte ou la réclamation et à l'organisme de certification.

Article 4 – Collaboration avec les organismes de certification :

L'organisme collabore aux actions de supervision nécessaires au maintien et au renouvellement de la certification. Il informe l'organisme de certification de toute situation nouvelle susceptible d'affecter sa certification, notamment concernant l'identité de l'organisme, ses effectifs, son organisation, son activité, son système de management, ses services, les personnes ayant pouvoir de décision ou leur(s) représentant(s). La Privacy Tech peut évaluer l'incidence de ces modifications sur le maintien de la certification.

L'organisme candidat collabore également avec l'organisme de certification concernant toute demande relative à une violation alléguée de la présente charte et pour résoudre toute plainte ou réclamation.

A cette fin, l'organisme candidat tient un registre de toutes les plaintes et réclamations à son encontre concernant les activités exercées dans le champ de la certification de la solution concernée et donne accès à ce registre à l'organisme de certification.

Dans les 15 jours ouvrés suivant la réception de la plainte ou de la réclamation, l'organisme certifié adresse une notification écrite et la copie de la plainte ou de la réclamation à l'organisme de certification qui pourra mener un audit circonstancié exceptionnel.

Article 5 – Acceptation et interprétation des conditions générales :

L'organisme certifié doit comprendre le contenu des présentes conditions et s'engager à la respecter en la signant. Toute question qu'il pourrait avoir sur l'interprétation et l'application de ces conditions doit être adressée à l'organisme de certification qui est en charge de l'interpréter en cas de question et d'en assurer le respect.

Article 6 – Non-respect des conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH :

Le non-respect de l'un des principes, valeurs ou règles des présentes conditions générales d'obtention et de maintien de la certification de solutions PRIVACY TECH peut conduire à l'ouverture d'un examen et le cas échéant, à l'adoption de sanctions relatives au maintien, à la suspension, retrait ou à la réduction du périmètre de certification.

D / DES STANDARDS ET UNE GOUVERNANCE POUR LES DONNEES

Olivier Dion :
Est le président fondateur de Onecub qu'il a créée en 2011 afin de redonner la maîtrise de leurs données aux individus. Onecub est un outil de portabilité des données personnelles, permettant à ses utilisateurs de faire circuler leurs données tout en gardant le contrôle, et aux entreprises de mettre en oeuvre un droit à la portabilité innovant. Depuis plusieurs années Olivier est un membre actif des communautés Open Data et Self Data en Europe comme aux Etats-Unis.

L'étude sur les standards et la gouvernance présentée dans cette partie du document a été réalisée grâce au concours des différents collectifs européens pour la protection des données et le Self Data (MyData Global, FING, Stiftung Datenschutz, Ctrl-Shift) ainsi que grâce à Microsoft pour le projet DTP et au projet Solid.

Depuis plus d'une décennie, plusieurs initiatives tantôt portées par des gouvernements, tantôt par des innovateurs, ont proposé sous diverses formes des moyens de redonner aux individus la maîtrise et l'usage de leurs données personnelles. Parmi elles, on peut citer **le projet américain du VRM (Vendor Relationship Management), concept fondateur proposé par l'université Harvard** (Berkman Center for Internet and Society). Fondé par Doc Searls, le projet VRM a posé les bases de l'écosystème en développant une communauté pour **permettre aux individus la gestion de leurs données personnelles** via des outils dédiés. Aux Etats-Unis toujours, dès 2010, les initiatives de Blue Button et Green Button, développées sous l'administration Obama, visaient à restituer leurs données de santé et d'énergie aux individus. En 2011 le projet MiData porté par le gouvernement du Royaume-Uni prônait et expérimentait "l'empowerment" des individus grâce à leurs données.

Le RGPD (Règlement Général sur la Protection des Données) joue aujourd'hui le rôle de catalyseur pour l'écosystème de la donnée personnelle et propose un cadre juridique fort. Né en Europe mais de portée mondiale, le RGPD est le socle sur lequel peut s'appuyer la libre circulation des données sous le contrôle des individus en créant un cadre de confiance harmonisé entre tous les acteurs de l'écosystème, individus et organisations, et en incitant les organisations, pour la plupart réfractaires jusqu'ici, à ouvrir leurs données aux individus. **Cependant le RGPD n'est pas suffisant en soi** et il est maintenant temps d'aller plus loin en proposant des outils et des standards technologiques reprenant ses principes et règles.

Depuis plusieurs années et encore plus depuis l'adoption du RGPD, nous assistons à un véritable boom d'initiatives autour de la donnée personnelle, non seulement en Europe et aux Etats-Unis mais aussi dans le reste du monde. Ces initiatives ne sont pas encore toutes matures, mais leur potentiel est réel et elles devraient se structurer rapidement.

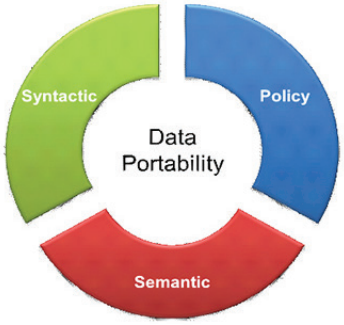
1 - Des initiatives majeures de standardisation

a. Data Transfer Project DTP

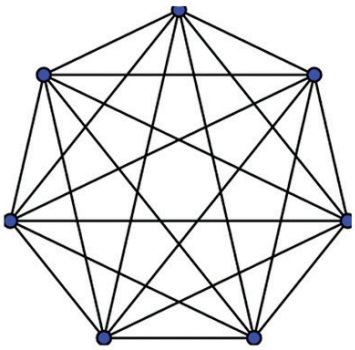
Lancé en 2018, le Data Transfer Project ou DTP est un projet open source de standardisation de abilité porté par Google, Microsoft, Facebook et Twitter. Le projet vise à proposer une rme pour permettre aux individus de déplacer leurs données d'une plateforme à une autre, sans avoir besoin de télécharger ces dernières.

Un standard portabilité pour les géants du Web :

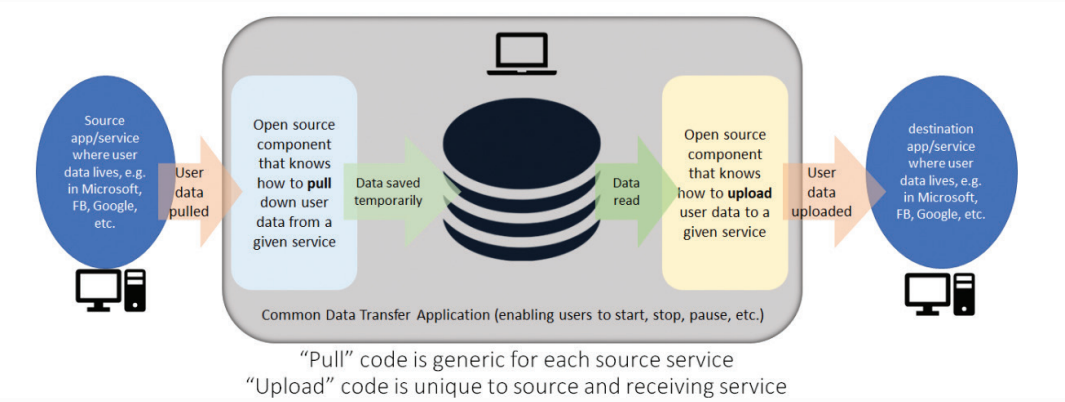
" La Portabilité des données n'est pas triviale ! "



On pourrait aller au-delà de la portabilité des données de base pour rendre possible un transfert direct et automatisé des données entre une source et un service destinataire. Cela nécessite un travail supplémentaire et une coordination entre les prestataires. En effet, le nombre de scénarios de transfert direct de données pourrait être très important et chaque scénario nécessite une coordination entre les fournisseurs. Le transfert direct des données exige que deux fournisseurs conçoivent, construisent et testent ensemble. Pour N fournisseurs, il existe N*(N-1)/2 projets de ce type. Il y a évidemment un problème d'échelle. C'est pourquoi nous pensons qu'un projet open source serait l'approche la plus pragmatique.



Un tel projet open source permettrait à différents fournisseurs de services de se regrouper. Chaque scénario impliquant un transfert direct de données utilisateur nécessiterait la construction d'une paire d'adaptateurs personnalisés. Chaque adaptateur invoquera les API existantes exposées par le fournisseur de services respectif pour télécharger ou transférer les données. Le projet DTP a construit un composant d'exécution commun pour héberger ces adaptateurs. Ce composant commun offre une bibliothèque de capacités dont la plupart des adaptateurs ont besoin. Ce processus offre également la possibilité d'héberger des transferts de longue durée (certains transferts de données peuvent prendre des heures, voire des jours, par exemple le transfert de 5 ans d'emails). De telles tâches de longue durée devraient pouvoir être interrompues ou reprises, de sorte que le processus commun offre également de telles capacités. De cette façon, les développeurs d'adaptateurs peuvent se concentrer uniquement sur l'envoi ou la réception de données à destination ou en provenance des fournisseurs de services.



"Pull" code is generic for each source service
"Upload" code is unique to source and receiving service

Transfert de service à l'initiative de l'utilisateur :

- Un utilisateur décide de passer d'un fournisseur de services à un autre et souhaite importer ses données dans le nouveau service.
- Y compris (mais sans s'y limiter) les contacts, photos, tâches, courriels et données dérivées.

Activation du service partenaire :

- Sur la base du consentement de l'utilisateur, un fournisseur de services partage des données spécifiques une seule fois avec un autre fournisseur pour accomplir une tâche.
- Par exemple, les données de localisation et de distance de conduite sont partagées d'un service de cartographie à une compagnie d'assurance afin de fournir une soumission précise.

Pour chaque paire de transferts source/destination, il y a une paire de composants open source. Les fournisseurs "sources" sont encouragés à "amorcer" le référentiel open source en fournissant des éléments de référence montrant comment les données peuvent être extraites ou publiées de ou vers leurs services. Les applications communes hébergeant les composants fournissent le temps d'exécution et l'interface utilisateur permettant aux utilisateurs de lancer des demandes de transfert de données.

Le code source du projet est sur GitHub (répertoire de logiciels libres) et est ouvert à la participation de tous. Le succès d'un tel projet open source dépend du niveau de participation. L'espoir est donc d'attirer non seulement les grands fournisseurs, mais aussi les PME et les petits acteurs de tous les secteurs de l'industrie qui stockent des données sur les consommateurs comme les banques, les télécommunications, l'assurance, etc.

Babak Jahromi :
Est architecte standard chez Microsoft. Il aide à développer des solutions technologiques globales pour Microsoft, qui peuvent ensuite devenir des normes internationales ou de solutions open source.

b. Solid

Créé en 2015, le projet Solid « vise à changer radicalement le mode de fonctionnement actuel des applications Web, pour aboutir à une véritable propriété des données et à une confidentialité améliorée »

Une nouvelle architecture pour le Web par son inventeur Tim Berners-Lee :

Solid est un écosystème qui redéfinit la relation entre les personnes, les applications/services et les données. Les données sont découplées des applications, de sorte que les gens peuvent passer d'une application à l'autre de façon transparente et qu'une personne peut lire dans une application ce qu'une autre personne a créé dans une autre application.

En fin de compte, Solid est une question de choix : nous choisirons où nous stockons nos données, à qui nous donnons accès à quelles parties de nos données, quels services nous voulons en plus, et comment nous payons pour cela. De nos jours, nous sommes plutôt obligés d'accepter des services que nous ne pouvons pas personnaliser. Par exemple, Facebook nous montre un flux d'actualité mettant en vedette nos amis, payé par la publicité - mais seulement si nous stockons nos données personnelles sur Facebook. Nous ne pouvons pas voir les messages Twitter d'autres personnes (à moins qu'elles ne choisissent de copier leurs données sur Facebook également). Ces pratiques sont courantes, car pratiquement toutes les applications Web avec lesquelles nous interagissons se comportent de cette façon.

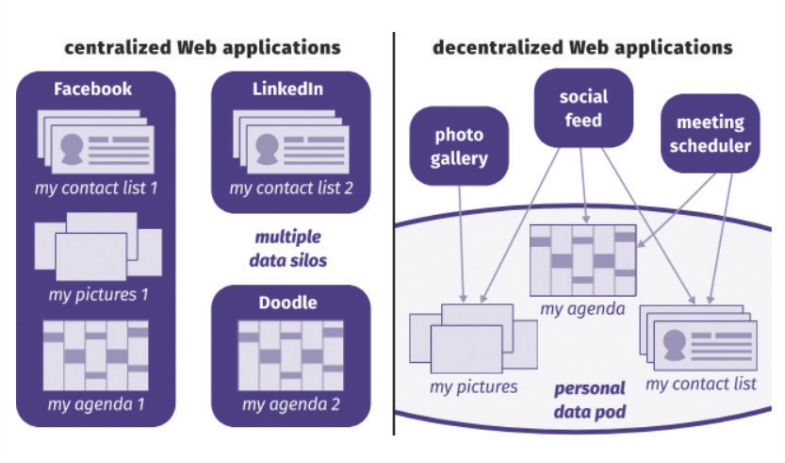
Le principe de la décentralisation proposé par Solid, est de permettre aux individus de choisir où ils stockent leurs données. Au lieu d'avoir à choisir entre une poignée de fournisseurs comme Google ou Facebook, dans un monde décentralisé, il y aura de nombreuses options parmi lesquelles choisir et nous serons libres de créer les nôtres. Cette idée nous ramène à la vision originale du Web, où n'importe qui a son propre site Web ou blog et y publie ses idées, plutôt que dans un seul flux appartenant à une seule entreprise. Dans une certaine mesure, nous avons déjà ce choix : depuis sa création, l'architecture décentralisée du Web a permis à chacun de disposer de son propre espace. Cependant, nous voulons la commodité du flux unique sans le contrôle central qui l'accompagne actuellement. Nous voulons continuer à bénéficier des mêmes types de services qui ne sont aujourd'hui disponibles que sur des plateformes centralisées.

La plateforme Solid introduit le concept de " pod " de données personnelles. Un pod de données est un simple emplacement de stockage de données sur un serveur, équipé d'un contrôle d'accès hautement granulaire, permettant à chacun de décider exactement quelles personnes et applications peuvent accéder à quelles parties de leurs données. Les applications deviennent les clients de ces serveurs, en s'approvisionnant en données à partir de plusieurs blocs de données. Solid envisage à terme un monde avec plusieurs modules de données par personne : un à la maison pour les données personnelles, un au bureau pour les dossiers de travail sensibles, un à l'école pour le suivi du matériel scolaire, etc. Dans un réseau social entièrement décentralisé, chaque partie d'une interaction - qui serait maintenant stockée dans son intégralité sur Facebook - pourrait résider dans différents modules de données.

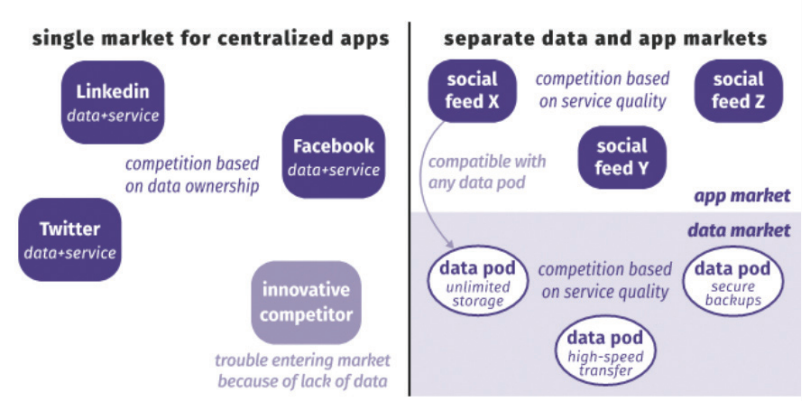
En rompant le couplage étroit entre les données et les applications, la décentralisation remet en question et modifie la nature même d'une application. Fondamentalement, l'avantage concurrentiel de plusieurs des

plates-formes centralisées populaires d'aujourd'hui est leur silo de données et le fait que leur service dépend entièrement de l'accès à ces données. Du point de vue conceptuel, le service offert par Facebook, Twitter et LinkedIn est assez simple et pourrait être facilement reproduit par d'autres. Pourtant, l'une des principales raisons pour lesquelles les gens apprécient les services de ces plateformes, c'est à cause de leurs données : Facebook est attrayant parce que les données de nos amis sont là, Twitter a tous les tweets et messages directs du monde, et LinkedIn contient notre réseau professionnel. En fait, ces plateformes sont devenues inséparables de leurs données : nous utilisons "Facebook" pour désigner à la fois l'application et les données qui la pilotent. Le résultat est que presque toutes les applications Web essaient aujourd'hui de vous demander de plus en plus de données, ce qui conduit à des données suspendues sur des profils en doublon et incohérents que nous ne pouvons plus gérer. Et bien sûr, cela s'accompagne d'importantes préoccupations en matière de protection de la vie privée.

Dans cet écosystème, les flux d'amis de Facebook deviennent une vue de votre liste de contacts dans votre pod de données, combinée avec les derniers messages que vos contacts ont postés dans leurs pods de données. Les services décentralisés de LinkedIn et du calendrier en ligne Doodle pourraient avoir accès à votre carnet d'adresses, de sorte que votre liste de collègues serait toujours synchronisée pour les demandes de réunion (car il n'y aurait en fait qu'une seule liste au lieu de plusieurs). Doodle et Facebook pourraient tous deux avoir accès à votre agenda, où Doodle pourrait seulement voir quand vous êtes disponible, et Facebook pourrait seulement ajouter des événements. Tout changement dans une vue se reflèterait directement dans une autre parce qu'elles partageraient la même mémoire.



Il est important de noter que cette séparation des données et des services crée des marchés distincts pour les données et les applications. Chacune d'entre elles a ses propres forces concurrentielles qui stimulent la créativité et l'innovation à un rythme plus élevé, puisque la capacité de fournir un service ne dépend plus de la propriété des données.



La clé d'un écosystème sain est l'indépendance de ces deux marchés, réalisée grâce à une relation sans engatgement entre les applications et les données. Puisqu'il n'existe actuellement aucune séparation de ce genre, les nouvelles plateformes d'applications novatrices ont de la difficulté à émerger parce qu'elles n'ont pas les données - et les plateformes existantes manquent d'incitatifs pour innover, car elles possèdent déjà des données. Cet argument de concurrence est très semblable au débat sur la neutralité du Net, qui vise à maintenir la séparation des marchés du contenu et de la connectivité. En effet, nous pouvons considérer une approche totalement décentralisée comme un moyen de réaliser la neutralité de plateforme, où les applications et les solutions de stockage deviennent interchangeables, tout comme les sites Web et les fournisseurs Internet.

La dernière question est de savoir comment accéder à ces services qui ont un coût. Là encore, les utilisateurs auront le choix. Les offres groupées telles que Facebook et Twitter n'offrent pas cette possibilité et se rémunèrent notamment grâce à la publicité. Dans un monde décentralisé, nous pouvons choisir nos fournisseurs de données et d'applications de manière indépendante, et décider pour chacun comment nous sommes prêts à payer. La mauvaise nouvelle, c'est que cela signifie que tout ne sera pas "gratuit" comme aujourd'hui. Toutefois, une concurrence accrue - sur deux marchés distincts - devrait conduire à des prix équitables. Et si nous voulons vraiment des options gratuites, nous pourrions même imaginer de payer avec nos données personnelles. C'est bien sûr la manière dont les médias sociaux sont implicitement pris en charge aujourd'hui, mais la principale différence sera que nous déciderons quelles données peuvent être utilisées à des fins publicitaires et lesquelles ne le peuvent pas. Cela prouve une fois de plus qu'à la base, la décentralisation commence par la reprise du contrôle de nos données, en tant que source d'une nouvelle génération d'applications Web innovantes.

Ruben Verborgh :
est professeur de technologie du Web sémantique à l'Université de Gand et participe au groupe de recherche d'Information Décentralisée de la CSAIL au MIT. Ruben est Solid advocate, l'écosystème d'applications qui permet aux individus de conserver leurs données.

c. Les standards IPEN

Le terme privacy-by-design ou « respect de la vie privée par construction » a été proposé par Ann Cavoukian au début des années 90 pour inciter à prendre en compte la préoccupation du respect de la vie privée au niveau de l'ingénierie des applications. Mais cette ingénierie doit faire face aujourd'hui à plusieurs défis.

Le défi de la mise en place d'écosystèmes vertueux

Les opérations concernant la circulation des données personnelles mettent en jeu un écosystème complexe. Il comprend les parties prenantes qui vont produire, partager les données, mettre à disposition des applications, ou fournir des solutions et technologies. Il comprend les parties prenantes qui vont vérifier la conformité des applications, ou piloter la gestion des incidents (p.ex. une fuite des données personnelles). Il comprend finalement les citoyens qui souhaitent pouvoir contrôler le devenir de leurs données personnelles.

L'enjeu est la coordination et de gouvernance de ces parties prenantes dans un environnement géographique qui peut dépasser le cadre d'une juridiction nationale.

La conception des écosystèmes est une préoccupation majeure d'ingénierie. En matière de choix d'architecture on pourra citer les approches centrées utilisateur (ou personal data ecosystem) où l'on inverse le modèle d'interaction : l'approche classique où une organisation commerciale gère la liste de ses utilisateurs individuels est remplacée par une approche où l'utilisateur gère et contrôle les organisations commerciales qui accèdent à ses données personnelles.

Le défi d'une ingénierie globale au service de la création d'écosystèmes vertueux

Une ingénierie globale doit être mise en place qui doit répondre aux exigences suivantes :

· la prise en compte de tout le cycle de vie de la donnée personnelle, y compris pour la gestion des brèches et pour la préparation à l'éventualité de ces brèches. Elle doit également comporter la mise en place d'une approche d'amélioration continue, qui sera l'objet de la nouvelle norme ISO 31700 en cours de définition.[1]

· la prise en compte d'une coordination au niveau de l'écosystème, c'est-à-dire au niveau des interactions entre les parties prenantes d'une chaîne de traitement et d'échange de donnée. Ceci fera en particulier l'objet de la nouvelle norme ISO 23751 en cours de définition[2]

· l'intégration dans les pratiques d'ingénierie, y compris au niveau de la formation des développeurs. Ceci a fait l'objet de la norme ISO/IEC 27550 qui sera publiée sous peu[3].

La mise en place de normes

Un ensemble de normes est disponible ou en cours d'élaboration, soit à l'ISO soit dans le cadre de groupe de travail commun ISO/IEC. On pourra citer les catégories suivantes de normes:

· les normes posant les principes ;
· les normes portant sur les mécanismes ;
· les normes permettant aux organisations de construire des solutions respectueuses ;
· les normes portant sur l'enjeu des écosystèmes.

La table ci-dessous donne la liste des normes publiées ou en cours de développement.

Catégorie	Référence	Description	Disponibilité
Principes	ISO 37100	Consumer protection : privacy-by-design for consumer goods and services	En cours
	ISO/IEC 29100	Privacy framework	Publié (accès libre)
Mécanismes	ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	Publié
	ISO/IEC 29184	Online privacy notices and consent	En cours
Pratique au niveau de l'organisation	ISO/IEC 27550	Privacy engineering for system life cycle processes	Publiable sous peu
	ISO/IEC 27552	Privacy information management -- requirements and guidelines	Publiable sous peu
	ISO/IEC 27555	Establishing a PII deletion concept in organisations	En cours
	ISO/IEC 27556	User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	En cours
	ISO/IEC 29134	Privacy impact assessment guidelines	Publié
	ISO/IEC 29151	Code of practice for PII protection	Publié
	ISO/IEC 29190	Privacy capability assessment model	Publié
Pratique au niveau de l'écosystème	ISO/IEC 20547-4	Big data security and privacy	En cours
	ISO/IEC 27030	Security and privacy guidelines for IoT	En cours
	ISO/IEC 27570	Privacy guidelines for smart cities	En cours
	ISO/IEC 23751	Data sharing agreements	En cours

Vers une communauté Française d'ingénierie sous l'égide d'IPEN

Le contrôleur Européen de la protection des données EDPS a lancé en 2016 le réseau d'ingénierie de la vie privée sur Internet IPEN (Internet Privacy Engineering Network)[4]. Cette initiative vise à regrouper les développeurs et les spécialistes de la protection des données ayant une expérience technique dans différents domaines afin d'initier et de soutenir les projets qui doivent assurer le respect de la vie privée par construction. Nous proposons de créer le sous-groupe Français d'IPEN.

---

[1] Consumer protection : privacy-by-design for consumer goods and services
[2] Data sharing agreement
[3] Privacy engineering for life cycle processes
[4] https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_fr

Antonio Kung :
Antonio est cofondateur de Trialog. Avec une expérience de plus de 30 ans dans le domaine des systèmes Cyber physiques et de l'internet des objets, il apporte expertise et savoir-faire dans les domaines de l'architecture, l'interopérabilité ou la sécurité et protection des données. Il a été coordinateur de multiples projets collaboratifs en France, en Europe et à l'international dans ces domaines. Grâce à cette expérience il est à même d'appréhender les facteurs culturels dans la gestion de projets. Il est actif sur la standardisation sur l'internet des objets, la sécurité et protection des données, notamment l'éditeur des standards ISO/IEC 27550, 27030, 27570, 21823-3. En 2018, il devient associé principal de Trialog et en assure la présidence.

2 - Un mouvement international en marche - le Self Data

Au delà des initiatives de standardisation technologique pure, un mouvement mondial porté par de multiples communautés, associations et innovateurs est en marche depuis plusieurs années : le Self Data. Le Self Data souhaite redonner aux individus la maîtrise de leurs données. Nous présentons ici 4 branches de ce mouvement portées par MyData (Finlande & Global), La FING et son projet MesInfos (France), Stiftung Datenschutz (Allemagne) et Ctrl-Shift (Angleterre).

a. MyData (Finlande & Global)

MyData est une vision alternative pour une meilleure société numérique grâce à une utilisation éthique et humaine des données personnelles. L'idée de base de MyData est que nous, vous et moi, devrions avoir le contrôle sur les données recueillies à notre sujet. Seules des approches éthiques saines à l'égard des données personnelles et de leur gestion peuvent être véritablement durables.

Le courant de pensée MyData est apparue en Finlande en 2012. En 2018, ce mouvement est devenu une association comptant plus de 500 membres dont plus de 70 organisations, la MAIF, le Ministère finlandais des transports et des communications et l'Université d'Edimbourg.

Le modèle MyData :

Le modèle MyData combine les droits des individus et des normes élevées de protection des données avec l'amélioration de la disponibilité des données et leur utilisation pour différents types d'avantages pour les entreprises ou d'autres acteurs. Le modèle favorise une gestion des données personnelles centrée sur l'être humain, ce qui signifie que la personne au sujet de laquelle les données sont recueillies conserve le contrôle sur qui peut accéder à ces données ou les utiliser. Ce modèle contraste avec le modèle chinois, où le gouvernement contrôle les données personnelles de ses citoyens, et avec le modèle de la Silicon Valley, où les grandes sociétés multinationales contrôlent les données personnelles des citoyens.

Le mouvement et la communauté MyData

Le mouvement MyData trouve ses racines dans la communauté des données ouvertes (Open data). En 2012, un groupe de personnes s'est réuni pour réfléchir à la relation entre les données ouvertes et les données personnelles. En 2014, le ministère finlandais des transports et des communications a publié un livre blanc décrivant une approche humaine de la gestion des données personnelles, qui a ensuite été traduit en anglais sous le nom de "MyData : A Nordic Model for Personal Data Management". Depuis la publication de la traduction anglaise, un mouvement international a commencé à se former. En 2015, la Commission européenne a organisé une table ronde pour les acteurs européens du secteur des PIMS ("Personal Information Management Systems"). En 2016, la première conférence MyData a été organisée et la communauté qui avait commencé à se regrouper autour du concept MyData a pris conscience d'elle-même. En 2017, la communauté a produit une Déclaration qui expose les principes et les objectifs du mouvement. Plus récemment, en 2018, la communauté s'est organisée en une association domiciliée à Helsinki, en Finlande.

MyData Organisation mondiale

L'établissement de MyData Global en tant qu'association en 2018 marque une nouvelle étape dans le mouvement vers une gestion des données personnelles centrée sur l'humain. L'objectif de l'organisation, tel qu'il est inscrit dans ses statuts, est de "donner plus de pouvoir aux individus en améliorant leur droit à l'autodétermination concernant leurs données personnelles". Le paradigme centré sur l'être humain vise une société numérique équitable, durable et prospère, où le partage des données personnelles est basé sur la confiance ainsi que sur une relation équilibrée et équitable entre les individus et les organisations." Au sein de l'association, le droit de vote est réparti à parts égales entre les catégories de membres individuels et les catégories de membres organisationnels. L'organisation compte actuellement 20 pôles locaux officiels et groupes thématiques qui constituent le lieu d'activité du mouvement. L'organisation centrale joue le rôle de facilitateur et de point de liaison entre les centres, les groupes, les organisations et les membres individuels, et de facilitateur du travail local en vue de la réalisation des objectifs de la Déclaration MyData.

La déclaration MyData :

Le mouvement MyData cherche à effectuer les trois changements suivants dans le paradigme actuel de l'économie et de l'échange des données :

- Premièrement, nous devons passer de droits purement formels à des droits réellement applicables ;
- Deuxièmement, nous devons passer de la protection des données à l'autonomisation grâce aux données ;
- Et troisièmement, nous devons rechercher une transition d'écosystèmes fermés à des écosystèmes ouverts.

Afin d'effectuer ces changements, le mouvement MyData s'est engagé à respecter les six principes suivants :

- la gestion des données personnelles centrée sur l'être humain,
- l'individu comme point de connexion pour les données le concernant,
- l'autonomisation individuelle,
- la portabilité et la réutilisation des données,
- la transparence et la responsabilité,
- et l'interopérabilité.

Viivi Lähteenoja :
Est responsable des programmes de MyData Global, poste qu'elle a occupé pendant deux ans au sein du mouvement MyData. Elle est également chercheur en éthique des données et se concentre sur les données personnelles avec une formation en éthique classique.

b. Mes Infos - FING (France)

Depuis 19 ans, la Fing aide les entreprises, les institutions et les territoires à anticiper les mutations liées aux technologies et à leurs usages. Elle a construit un nouveau genre de think tank, dont les productions sont largement reconnues en Europe et ailleurs.

MesInfos, un projet porté par la Fing :

Au sein du projet MesInfos, la Fing a tenté d'ouvrir des perspectives et de proposer une alternative - devenue beaucoup plus réelle, depuis l'entrée en vigueur du RGPD en mai 2018, et l'apparition du "droit à la portabilité[1]" : **la piste du Self Data, à savoir la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins**. Que se passerait-il si, demain, les organisations partageaient les données personnelles qu'elles détiennent avec les individus qu'elles concernent, pour qu'ils en fassent ce qui a du sens pour eux ? Quels usages, quelles connaissances, quels services, quels risques aussi, pourraient émerger si les individus disposaient, non seulement du contrôle, mais de l'usage de leurs données : leurs finances, leurs achats, leurs déplacements, leurs communications et leurs relations en ligne, leur navigation web, leur consommation d'énergie, etc. ? En bref, et si les individus devenaient maîtres et utilisateurs de leurs données ?

Depuis 2012, la Fing - avec ses partenaires - explore, veille, expérimente. Elle collabore avec ses homologues internationaux et a permis le développement de l'ONG internationale MyData Global. Elle produit de la connaissance sur les usages, l'architecture et les défis d'un changement de paradigme : passer d'une économie de la donnée à sens unique (les entreprises collectent et traitent les données, les personnes essaient de contrôler ce que d'autres font de leurs données) à une économie où la valeur d'usage des données est partagée entre les individus et les organisations. Il s'agit de mettre fin à l'asymétrie entre individus et entreprises concernant la collecte et l'utilisation des données Self data, devenir le maître de ses données : "si j'ai une information sur vous, vous l'avez aussi. Et vous en faites ce qui a du sens pour vous !"

Retours d'expériences :

Deux expérimentations ont permis de tester le Self Data à grande échelle. La plus récente, le "Pilote MesInfos", a été un bac à sable pour le droit à la portabilité, une sorte de "portabilité avant la portabilité". Ce projet a réuni de nombreux partenaires pour explorer ensemble la notion de Self Data : permettre aux individus de devenir maîtres de leurs données en les récupérant depuis le système d'information des organisations avec lesquelles ils sont en relation, en les stockant dans des espaces sécurisés (PIMS) où ils peuvent administrer leurs données et surtout en tirant de celles-ci une valeur d'usage grâce à des services tiers.

Les enseignements issus de ces expérimentations (300 testeurs en 2013 pour 8 mois d'expérimentation / 2000 testeurs pour le pilote MesInfos entre 2016 et 2018) soulignent que le scénario Self Data est riche en promesse d'usages et en création de valeur pour les organisations, les individus et l'écosystème d'innovation, mais que son implémentation reste encore trop confidentielle et longue. Si juridiquement, le droit à la portabilité est une grande avancée et que le potentiel d'usage des données personnelles partagées est immense, peu d'organisations implémentent réellement le partage des données aux individus. Des systèmes d'information parfois vieux et construits pour garder les données, pas pour les partager, un écosystème d'innovation peu habitué à ce nouveau paradigme, des outils complexes pour des individus nécessitant une médiation importante, constituent quelques uns des obstacles à surmonter pour faire du droit à la portabilité (et donc du Self Data) une réalité et une opportunité.

Perspectives :

Au cours des dernières années, la Fing a documenté de nombreux cas d'usage autour des données personnelles partagées. Elle a également défini les grandes actions à mettre en place pour aller vers un droit à la portabilité réellement mobilisateur et créateur de nouveaux usages afin de créer un "Monde de Self Data" :

- Faire des villes, de l'acteur public local l'impulseur privilégié de ces dynamiques (voir le projet "Self Data Territorial")
- Sensibiliser les détenteurs de données
- Outiller la médiation et l'appropriation citoyenne
- Favoriser l'union des PIMS (Personal Information Management Systems)
- Instaurer une clause Self data
- Générer des retours d'usage : expérimenter et échanger
- Mobiliser : construire les conditions d'un droit à la portabilité citoyen
- Labelliser et rassurer
- Soutenir financièrement le marché du Self Data
- RGPD : dépasser la mise en conformité
- Réfléchir et agir mondialement : le réseau MyData.

[1] Le projet MesInfos est d'ailleurs cité par le G29 comme l'un des projets innovant qui permettent de démontrer le potentiel d'innovation du droit à la portabilité.

Sarah Medjek :
Est chargée de projet à la Fing et doctorante à l'université Paris-Nanterre. Ses recherches portent sur l'appropriation des données personnelles et des outils permettant leur gestion par les individus, ainsi que sur les questions de privacy et de confiance. Depuis novembre 2018 elle est également présidente du conseil d'administration de MyData Global.

Sarah Medjek :
Depuis plusieurs années, au sein de l'association Fing, Think Tank de référence sur le numérique, Manon Molins participe à la production d'idées et à leur diffusion dans un environnement international, au pilotage d'expérimentations et à l'accompagnement d'acteurs publics et privés sur les transformations induites par le numérique et les technologies.

c. Stiftung Datenschutz (Allemagne)

La Fondation pour la Protection des Données a été fondée en 2013 par le gouvernement de la République fédérale d'Allemagne. L'organisation est indépendante et a pour mission de promouvoir la protection des données. Il offre une plateforme de discussion sur les questions de politique des données et fournit des informations sur la mise en œuvre du droit de la protection des données dans la pratique. La Fondation se considère comme une interface entre la politique, les autorités de régulation, les entreprises, la science et la société.

En 2017, la Fondation a examiné les possibilités de mettre en pratique le droit à la portabilité des données. Le projet propose des suggestions pour définir et organiser correctement la portabilité des données : comment interpréter de manière étroite ou large le concept de fourniture de données, comment le transfert d'un ensemble de données d'un fournisseur à un autre peut être réalisé et quelles mesures doivent être prises par les entreprises concernées en ce qui concerne l'exercice de ce droit.

Recommandations de la Fondation :

Objectifs :

Le règlement devrait être mis en œuvre conformément à son objectif initial - l'amélioration de la confidentialité des données ("autodétermination informationnelle") pour les consommateurs. Il s'agit avant tout des possibilités de contrôle de la transmission des données à caractère personnel. L'efficacité du règlement doit être observée dans la pratique. Il s'agira, par exemple, d'enquêtes quant à la mobilisation effective des utilisateurs pour la portabilité des données. Les résultats devraient être pris en compte dans l'évaluation de l'applicabilité du règlement général de l'UE sur la protection des données, et, le cas échéant, amener des précisions ou clarifications sur les points identifiés.

Il serait intéressant de promouvoir la mobilisation la plus large de ce nouveau droit, par des campagnes d'information sur sa portée et ses possibilités (par exemple, par les autorités nationales chargées de la protection des données ou par des plates-formes d'information). Ces campagnes d'information devrait viser autant les consommateurs que les acteurs de l'écosystème (détenteurs, réutilisateurs, développeurs ...).

Détermination du champ d'application :

La détermination du champ d'application devrait se concentrer sur les avantages pour le consommateur afin d'accroître l'acceptation et le succès du nouveau droit. La définition des "données fournies" devrait être fondée sur l'esprit et l'objet du règlement. Outre la déclaration du Groupe de travail de l'article 29, les autorités de régulation devraient préciser ce que l'on entend par "données fournies" et donner des exemples pour les catégories de données incluses sous ce terme. La question de savoir si le champ d'application pourrait inclure les données d'inventaire ainsi que les données d'utilisation doit être tranchée en fonction de chaque cas individuel et du service concerné.

Il convient d'examiner dans quels cas le transfert de données d'utilisation "fournies" à un autre fournisseur de services soutiendrait effectivement les droits de contrôle de la personne concernée. Quant au format des données et à l'interopérabilité demandée, les questions de droit de la concurrence doivent être prises en compte. Il convient d'examiner dans quelle mesure des critères doivent être développés afin d'obtenir une perspective cohérente dans toute l'Europe ainsi qu'un résultat différencié en ce qui concerne le droit de la concurrence et le droit de la protection des données. Il convient d'éviter les problèmes de concurrence en ce qui concerne les accords sur les méthodes de transfert de données. L'objectif de protection de la réglementation, à savoir faciliter le passage d'un fournisseur à un autre, doit être réalisé de manière efficace.

Toutes les parties concernées devraient toujours garantir la transparence lorsque le droit à la portabilité des données est exercé. Les personnes concernées ne devraient pas perdre la trace des responsables du traitement et des droits d'effacement auxquels elles ont droit. Ils doivent connaître toutes les informations relatives au traitement effectué par l'ancien et le nouveau responsable du traitement. En ce qui concerne la demande " lorsque cela est techniquement possible ", il convient de décider si des critères objectifs peuvent être élaborés ou si les capacités individuelles du responsable du traitement concerné (norme subjective) sont prises comme base. Il est également important de s'efforcer d'obtenir une harmonisation et une interprétation cohérente à travers toute l'Europe dans l'interprétation de l'art. 20 du RGPD.

Stratégies de mise en oeuvre :

Il est recommandé d'élaborer des approches d'autorégulation régulée" établissant un cadre sous la supervision de l'Etat dans lequel les autorités de régulation, les ONG ainsi que les entreprises développent des stratégies de mise en œuvre et des normes pour la portabilité des données. Pour une définition et une organisation efficaces de la portabilité des données et de la mise en conformité juridique, les entreprises et les industries qui seront particulièrement concernées devraient être associées aux processus de consultation formelle des autorités réglementaires :

En cas de transfert d'ensembles de données sectorielles au sein d'une catégorie de contrôleurs et lorsqu'il existe déjà des solutions de portabilité interne au sein de l'industrie, une procédure sectorielle est recommandée.

Les approches de solutions basées sur les PIMS semblent très prometteuses pour les cas d'applications intersectorielles. Afin de permettre une meilleure orientation, les organismes responsables devraient s'efforcer d'élaborer des règles de conduite pour la mise en œuvre pratique de la portabilité.

Frederick Richter :
Est le directeur de la Fondation pour la protection des données allemande. Il a été consultant et délégué à la protection des données de la Fédération des industries allemandes (BDI) puis consultant au Bundestag allemand sur le droit d'auteur et la politique des réseaux.

d. Ctrl-Shift (Royaume-Uni)

Ctrl-Shift est un cabinet de conseil en innovation de données personnelles, qui aide les organisations du monde entier à saisir les opportunités de croissance des données personnelles en créant des solutions stratégiques, durables et pratiques qui apportent une nouvelle valeur ajoutée dans la vie des personnes.

Pourquoi les données personnelles sont importantes ?

Les données personnelles sont depuis longtemps reconnues comme un moteur majeur de la croissance de nos économies numériques. Alimentée par l'omniprésence des appareils numériques personnels et, de plus en plus, par l'Internet des objets, la croissance des données personnelles est explosive. La portée et l'ampleur de cette révolution des données personnelles signifient que l'utilisation intelligente des données peut offrir de nouvelles possibilités sans précédent de croissance commerciale, de valeur pour les consommateurs et de bien public dans une économie numérique en évolution rapide.

Où en sommes-nous aujourd'hui ?

Jusqu'à présent, toutefois, la majeure partie des données à caractère personnel a été enfermée dans des silos organisationnels où seule une seule organisation peut avoir accès aux données, ce qui limite la portée de l'utilisation des données. En gardant jalousement les données, les entreprises ont appris à considérer l'accès exclusif aux données personnelles qu'elles collectent comme un atout stratégique clé et une source d'avantage concurrentiel.

Depuis l'entrée en vigueur du RGPD, la portabilité des données personnelles est devenue une obligation légale en Europe. Cela signifie que toutes les organisations détenant des données à caractère personnel sont tenues de fournir, sur demande, une copie électronique des données à la personne concernée. Le fait de pouvoir récupérer ainsi des données à caractère personnel est un droit de l'homme et, avec un accès libre basé sur le consentement, constitue une étape essentielle vers la réalisation de niveaux entièrement nouveaux d'innovation, de productivité et de concurrence.

En consacrant les droits de l'individu en matière de portabilité des données personnelles, le RGPD a créé une base juridique solide pour une utilisation économique et sociale plus large des données personnelles. Pour autant, le texte ne suffit pas et il faut désormais créer les structures permettant le partage sûr et facile des données personnelles. De plus, l'absence d'un environnement sécurisé pour le partage des données ouvre la porte à de nouveaux risques majeurs.

Dans l'état actuel des choses, il n'existe aucun mécanisme de protection des utilisateurs qui souhaitent exercer leurs nouveaux droits à la portabilité des données personnelles. Le RGPD ne fait pas non plus grand-chose pour protéger les responsables du traitement des données lorsque la portabilité des données ne fonctionne pas correctement ou fait l'objet d'abus. En l'absence d'un environnement sûr et sécurisé pour le partage des données à caractère personnel, les nouveaux droits que les personnes ont sur leurs données présentent de sérieux risques tant pour elles que pour les organisations avec lesquelles elles interagissent.

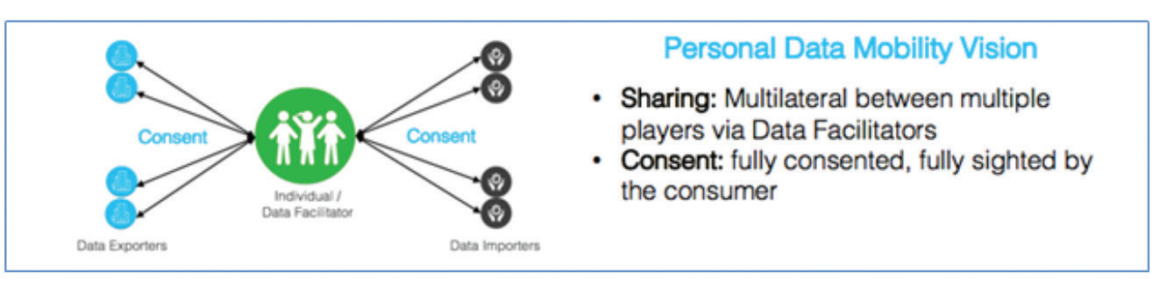
Les problèmes récents de Cambridge Analytica illustrent clairement le genre de problèmes qui peuvent survenir lorsque les utilisateurs " transfèrent " leurs données d'une entreprise à une autre sans avoir une compréhension claire de l'objectif du traitement et de ses conséquences.

En outre, le manque de savoir-faire et de compréhension du marché numérique créent également des risques et une appréciation limitée de la valeur qu'ont les données personnelles des utilisateurs.

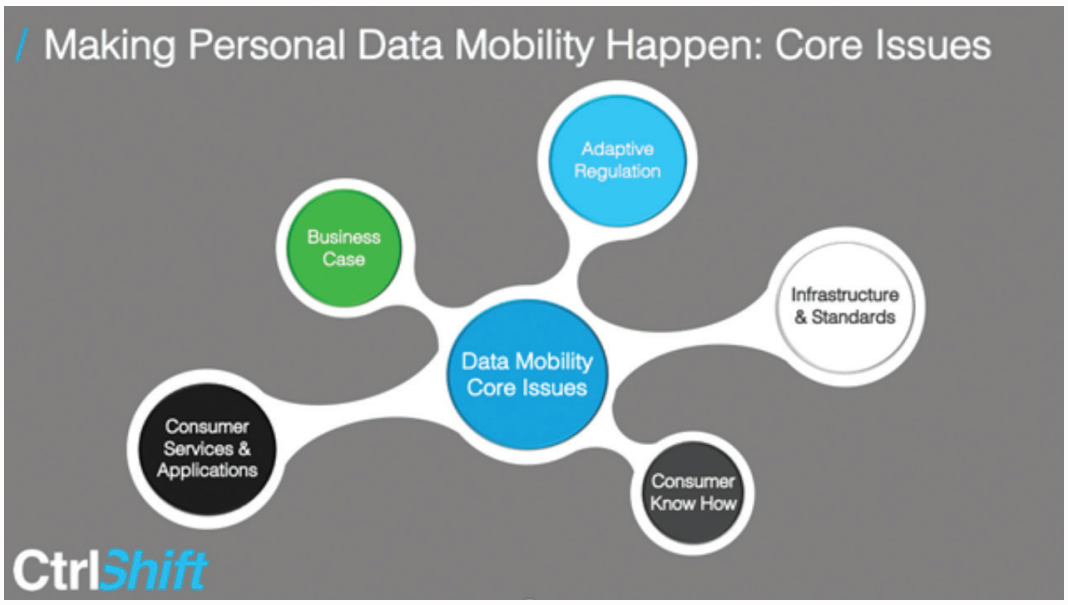
En raison de la faible demande des consommateurs, il est difficile pour les organisations d'élaborer des analyses de rentabilité convaincantes pour de nouveaux services innovants, d'autant plus que ces analyses de rentabilité doivent aujourd'hui surmonter les obstacles créés par l'absence d'infrastructures et de normes.

Que faisons-nous à partir de maintenant ?

Une récente étude globale Ctrl-Shift sur la circulation des données ("L'opportunité de croissance de la portabilité des données personnelles pour l'économie britannique", commandée par le gouvernement britannique), se concentre sur une vision de la circulation des données personnelles qui va au-delà de la portabilité des données telle que spécifiée par le RGPD - pour libérer le plus grand potentiel économique des données personnelles.



L'étude Ctrl-Shift a, pour la première fois, codifié les principaux enjeux et défis de la circulation des données personnelles, notamment les normes et infrastructures, les nouveaux services et applications, le savoir-faire des consommateurs, l'élaboration d'une analyse de rentabilité et la réglementation adaptative.



Dans ce contexte, de nombreuses initiatives ont été prises pour améliorer la portabilité des données personnelles, pour débloquer et simplifier l'accès sécurisé aux données personnelles et pour leur utilisation dans diverses applications.

Parmi les initiatives clés, citons MIDATA au Royaume-Uni, les services de gestion des données personnelles et les services de gestion des informations personnelles au niveau mondial, Mesinfos en France, PSD2 dans l'UE et Blue Button et Green Button aux États-Unis. Cependant, aucune d'entre elles ne crée des solutions complètes et évolutives et le développement n'est pas coordonné.

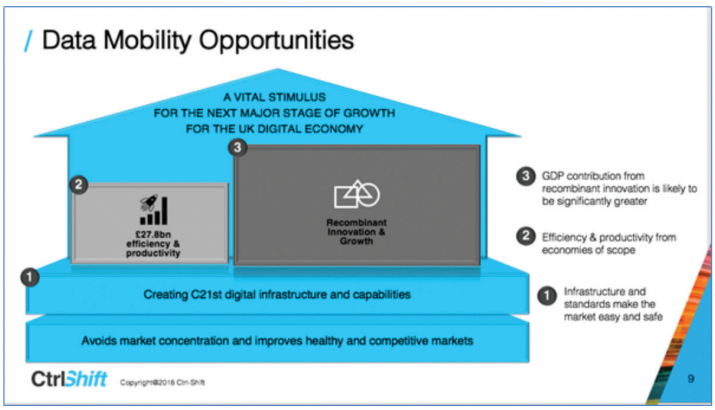
Quelles sont les opportunités ?

La circulation des données personnelles a le potentiel de créer des bénéfices tant pour les individus que pour les organisations. Ce faisant, elle peut apporter une contribution majeure à l'économie et à la société du XXIe siècle.

Les caractéristiques recombinantes et non rivales des données (la capacité de les recombiner sans limite et de ne jamais les " consommer ", même lorsqu'elles sont utilisées par de nombreuses parties) distinguent fortement les actifs de données des actifs physiques en fonction de leur potentiel de création de valeur continue. Là où la richesse et le volume des données augmentent, cette opportunité de valeur est multipliée. Avec l'augmentation exponentielle de la quantité de données personnelles, le marché numérique connaît une opportunité de valeur sans précédent.

Une étude économique réalisée par London Economics, commandée par Ctrl-Shift, met en évidence de nombreuses opportunités offertes par la circulation des données. Permettre un partage plus équitable de la valeur, éviter la concentration des données et de la valeur et permettre la création de marchés concurrentiels sains qui soutiennent et encouragent l'innovation et la croissance, notamment grâce à l'intelligence artificielle et au machine learning.

L'étude a également mis en lumière les possibilités offertes par la création d'infrastructures et de normes telles que l'interopérabilité, l'accès aux données, les modèles de responsabilité, les mécanismes de consentement, les certificats numériques et les données sûres.



La circulation des données peut profiter à tous. Pour les individus, cette autonomisation permettra d'accéder à une plus grande part de valeur dans l'économie numérique de demain. Pour les entreprises, la circulation des données personnelles ouvrira la porte à de nouveaux services tirant parti de l'innovation recombinante et de relations clients plus solides qui favorisent l'efficacité, la productivité et de nouveaux revenus. Pour la société, la circulation des données offre des avantages encore plus importants, par exemple en améliorant l'efficacité dans l'utilisation des ressources et des infrastructures, les résultats sanitaires et le renforcement des communautés.

Prochaines étapes :

Il est clair que le gouvernement a un rôle à jouer pour s'assurer que le marché est à la fois sûr et simple. Le régulateur doit élaborer des normes et soutenir le développement de l'infrastructure. Toutefois, il s'agit d'un marché en évolution rapide, et son développement exige une compréhension commune des enjeux et une collaboration entre les législateurs, les organismes de réglementation, les entreprises et les organisations technologiques. En tant que tel, le rapport appelle à la création d'une entité de coordination de la circulation des données personnelles.

Ctrl-Shift a créé l'Environnement de test de circulation des données Ctrl-Shift. L'Environnement de test est le fruit d'une collaboration entre de grandes organisations de la banque de détail, des médias, de l'énergie, des médias sociaux et des télécommunications. Ensemble, les participants s'engagent à tester les capacités et à identifier les leviers nécessaires pour soutenir le développement d'une vision partagée de la circulation des données.

De plus, l'Environnement de test comprend des observateurs de l'ICO, du DCMS, du Centre for Data Ethics and Innovation, de Consumers International et du Web Sciences Institute de l'Université de Southampton, permettant à toutes les parties de comprendre les opportunités et les limites.

L'objectif principal de l'Environnement de test Ctrl-Shift pour la circulation des données est de mieux comprendre comment la mobilité des données peut être activée par les capacités actuelles et d'identifier les développements supplémentaires nécessaires pour fournir les données réelles et sûres qui permettront aux individus de partager leurs données personnelles et de créer de la valeur. Les premiers résultats seront publiés en mai 2019.

Liz Brandt :
est co-fondatrice et PDG de Ctrl-Shift. Elle a 25 ans dexpérience dans le conseil dans de nombreux secteurs. Elle a également fondé plusieurs sociétés. Depuis son lancement, Ctrl-Shift a été à l'avant-garde de la compréhension, l'explication et la mise en forme de l'économie des données personnelles.

3 - Une nouvelle infrastructure pour le Web

a. Un besoin de standards

L'adoption d'un standard global et unique pour la portabilité et la protection des données aurait un impact majeur sur l'économie digitale et donc sur l'ensemble de l'économie et de la société. Le standard pourrait remettre l'humain aux commandes de sa vie en ligne et lui permettre de profiter pleinement des bénéfices des nouvelles technologies sans avoir à faire de compromis avec la protection de sa vie privée.

Les acteurs de l'écosystème, y compris gouvernementaux, devront convenir d'un standard unique et global, à la fois technique et juridique, qui permettra :

- **aux individus de faire circuler leurs données en toute confiance** et de la manière la plus simple possible.
- **aux organisations de limiter les coûts** à la mise en place et de **se décharger d'une responsabilité qui relève plus naturellement des autorités représentative de l'ensemble de la population, que d'entreprises technologiques**, aussi puissantes soit-elles.

b. Les limites des initiatives actuelles

Comme nous l'avons vu, **les initiatives de standardisations pour la circulation et la protection des données sont très nombreuses** et, dopées par le RGPD, elles sont en plein boom. Cette explosion démontre le besoin pressant de trouver des solutions communes. Cependant **la pluralité des initiatives limite grandement leur impact et leurs chances de réussite.**

Les initiatives de standardisations sont aujourd'hu**i trop locales** et leur **périmètre est trop souvent trop restreint,** limité à un faible nombre d'expertises ou d'acteurs qui fonctionnent en vase clos ou n'arrivent pas à atteindre la masse critique nécessaire pour se diffuser à tous les marchés.

La portabilité et la protection des données sont par nature des sujets faisant appel à des expertises très variées :

- Juridique
- Technique
- Design
- Business
- Politique
- Stratégie
- Données non personnelles
- Etc.

Vu la complexité du sujet, il est regrettable de constater que **des initiatives nationales redondantes s'inspirent grandement les unes des autres sans se coordonner.**

Certaines initiatives sont purement sectorielles (finance, santé, automobile, télécom, etc.) ou regroupent même **parfois un nombre très limité d'acteurs** dans des consortiums fermés. Pourtant la circulation des données implique la possibilité de transférer des données d'un service à un autre, y compris dans des industries distinctes. La protection des données doit passer par des pratiques et standards communs, tous secteurs et acteurs confondus.

c. Standards technologiques pour la circulation des données

Pour permettre une meilleure circulation des données personnelles basée sur le droit à la portabilité, le standard proposé devra prendre en compte toutes les aspects du sujet.

Récapitulatif des besoins de standardisation issus de la partie A de ce document :

- Les questions d'interopérabilité technique (protocoles d'échange, authentification, API et modèles des détenteurs et réutilisateurs, etc.) ;
- La question des formats de données (données non-personnelles, Open Data, catalogue de données de référence, etc.) ;
- Les modèles de revenus (gérés de manière transparente) ;
- Le framework légal pour la circulation des données ;
- La gestion des consentements ;
- La communication auprès des utilisateurs (iconographies, etc.) ;
- La confiance entre les responsables de traitement pour l'échange de données avec un mécanisme d'évaluation approprié ;
- Le rôle des PIMS ;
- Etc.

Suite à la mise en place d'un tel standard, de nouvelles problématiques devraient rapidement apparaître et être prises en compte de manière très évolutive et itérative.

Il sera également nécessaire de fixer les terminologies et définitions (ex : les types de PIMS) afin de simplifier la communication entre tous les acteurs de l'écosystème.

d. Standard technologiques pour la protection des données

Pour permettre une protection réelle et efficace des données personnelles sous le contrôle de l'individu, différents standards et bonnes pratiques doivent être développés et imposés :

Récapitulatif des besoins de standardisation et d'uniformatisation issus de la partie B de ce document :

- Standardisation des consentements pour permettre leur portabilité ;
- Standardisation des API de création, mise à jour et vérification du consentement ;
- Standardisation des icônes de vie privée ;
- Frameworks d'information et de transparence sur les finalités du traitement ;
- Bonnes pratiques de conception d'interface d'information et de collecte du consentement ;
- Bonnes pratiques de validation de la transparence par tests utilisateurs et itération ;
- Terminologies partagées dans chaque secteur pour les traitements récurrents ;
- Registres d'identifiants de responsables de traitement et de sous-traitants.

Sur la problématique du respect des droits des personnes, certains éléments peuvent être standardisés, d'autres - notamment sur la compréhension de la transparence - devront s'appuyer sur des bonnes pratiques et des mesures d'efficacité constantes.

e. Standard pour assurer la confiance pour la protection des données

Une multitude de solutions pour accompagner la conformité des organismes sont présentes sur le marché.

Pour un responsable de traitement, il est difficile de faire la part des choses au milieu de tout cela, ces derniers sont très méfiants dans le choix des outils dédiés à ce sujet et nous pouvons les comprendre.

Force est de constater qu'au vu de ce contexte, il est souvent très compliqué pour les « start-up » passionnées d'atteindre la signature du contrat. En effet pour ces derniers la mise en concurrence est rude et les périodes d'avant-vente ou de réponse aux appels-offres sont chronophages et coûteuses pour ces jeunes entreprises.

Pour la PRIVACY TECH stimuler l'excellence française en matière de « Privacy » est un objectif à atteindre. L'objectif a donc été de lancer une initiative pour fluidifier ce marché en assurant un facteur confiance à la hauteur des attentes des organismes de toutes tailles par la création d'une certification Privacy Tech en partenariat avec l'AFNOR.

Ce besoin de confiance est omniprésent dès que l'on touche à la donnée. Des solutions pilotes débuteront le processus de certification début mai.

Nous espérons que cette certification ouvrira la voie vers une initiative européenne ou internationale.

4 - Une gouvernance pour les données personnelles ?

a. Un besoin de gouvernance

Aujourd'hui il n'existe pas d'instance susceptible de proposer un standard unique et global pour la portabilité et la protection des données. La tâche est immense et le niveau de coopération et de coordination attendu est sans précédent. Sans effort de coordination, nous risquons de recréer des silos disjoints : certains pays auront leurs règles propres et certains acteurs proposeront des mécanismes spécifiques, difficilement compatibles entre eux. Or les données personnelles n'ont pas de frontières et ne se bornent pas à un usage ou à un nombre limité d'acteurs.

Les premiers standards comme le DTP ou Solid vont dans la bonne direction en tentant de briser les silos. Cependant **le sujet des données personnelles n'est désormais plus un sujet technologique, il est devenu l'un des plus importants sujets de société du XXIe siècle et doit donc être traité de manière plus large avec une implication de toutes les parties prenantes, y compris les gouvernements et instances de régulation.** Le RGPD a fixé un cadre législatif qui pourrait harmoniser les pratiques, nous devons maintenant poursuivre dans cette voie et l'étendre à la technologie et aux autres domaines de manière cohérente et intégrée.

Les GAFAM, souvent pris pour cible, à raison, par les régulateurs, pourraient tirer profit d'une harmonisation globale des pratiques qui leur permettrait d'offrir davantage de confiance à leurs utilisateurs, en laissant la main sur certaines questions, pour lesquels ils ne sont pas légitimes, à un organe de gouvernance supérieur et plus représentatif.

Cette globalisation des pratiques va aussi dans le sens d'une plus grande égalité entre les utilisateurs mondiaux. **Pour être légitime, cette harmonisation doit émaner d'un organe de gouvernance indépendant à même de créer un consensus accepté par le plus grand nombre.**

b. Un organe de gouvernance

“Nous, la communauté des acteurs de la donnée personnelle, appelons à la création d’un nouvel organe de gouvernance des standards de la circulation et de la protection des données personnelles. “

Missions de l’organe de gouvernance :

Ce nouvel organe aurait pour mission de proposer :

- Des standards technologiques de portabilité et de protection des données personnelles en ligne avec les principes du RGPD,
- Des terminologies,
- Des bonnes pratiques,

Validés par les experts de chaque domaine et applicables directement par les acteurs du marché ou indirectement via des facilitateurs de type PIMS.

Il devrait être indépendant et coordonner tous les acteurs de l’écosystème pour promouvoir une nouvelle donne de l’économie numérique centrée sur l’Humain.

Ce nouvel organe produirait des recommandations, à l’instar du W3C et/ou des certifications.

Par ailleurs, il pourrait avoir comme missions secondaires de proposer :

- Un état des lieux sectoriel (assurances, banque, distribution, constructeur automobile, fabricant de produits de santé, marketing ...) et intersectoriels, des cas d’usage identifiés pour la portabilité ;
- Des études de cas d’usages à développer (prospectifs) ;
- Des retours d’expériences des utilisateurs (en mode observatoire) ;
- Des modèles économiques « éthiques » ;
- Des moyens d’évaluation des pratiques des organisations (certifications, labels) ;
- La détection de nouvelles problématiques.

Relations de l’organe de gouvernance avec les acteurs de l’écosystème :

L’organe de gouvernance devrait agir de manière concertée avec différents types d’acteurs :

- **avec les gouvernements et régulateurs :** assurer l’intégration des régulations dans les standards, permettre le contrôle et le suivi des pratiques (contrôle des finalités, etc.) et proposer en retour des recommandations et amendements permettant de faire avancer la régulation “au rythme des technologies” (réglementation adaptative) ;
- **avec le monde académique :** les standards doivent se fonder sur l’état de l’art de la recherche et leur mode de création doit suivre des méthodologie reconnues ;
- **avec les acteurs économiques :** proposer des standards technologiquement et économiquement viable basés sur le consensus et prendre en compte les retours du marché pour faire évoluer les standards ;

- avec les individus / utilisateurs : prendre en compte les attentes et besoins pour la construction des standards, les finalités, les pratiques et prendre en compte les retours d'expérience ;
- avec les PIMS : proposer des standards utilisables par les PIMS et encadrer leur rôle, les autoriser et les contrôler ;
- avec les communautés de données non personnelles : proposer des standards cohérents avec ceux proposés pour les données non personnelles ;
- avec les autres organismes de standardisation : assurer la cohérence.

Création et financement :

Les communautés du Self Data, par les valeurs qu'elles véhiculent, leur réseau et leur expérience, semblent représenter un cadre adapté pour la création et la diffusion des standards.

L'organe de gouvernance pourrait être financé par une multiplicité d'acteurs impliqués. La variété des sources de revenu et la transparence auront leur importance pour garantir l'indépendance et la confiance dans la gouvernance.

Proposition de principes de fonctionnement :

L'organe de gouvernance pourrait être constitué de la manière suivante :

- **Un board :** élu par la communauté et en charge de la coordination générale interne et les relations de contrôle / coordination avec les entités externes (gouvernements, régulateurs, PIMS, entreprises, utilisateurs, autres organes de standardisation, etc.).
- **Des workgroups :** composés d'experts et traitant de problématiques transverses (éthique, portabilité, consentement, transparence, design, formats, protocoles de communication/ authentication, framework juridique, blockchain, prospective, observatoire des cas d'usage, tests utilisateurs, conformité RGPD, etc.)
- **Des hub sectoriels :** composés de représentants d'entreprises regroupés par secteur (banque, assurance, santé, administration, énergie, éducation, commerce, etc.) et en charge de questions propres à l'industrie (formats de données et régulations spécifiques, etc.)

Les principes de base pourraient être les suivants :

- Le board constitue les workgroups et les hubs sectoriels
- Le board émet des recommandations générales avec l'appui des workgroups et des entités externes (gouvernements, régulateurs, utilisateurs, etc.)
- Les hubs sectoriels émettent des recommandations spécifiques propres à leur industrie en s'appuyant sur les recommandations générales et avec le soutien des workgroups
- Les workgroups assurent la cohérence dans les pratiques et les recommandations spécifiques des différents workgroups
- Le board valide la conformité des recommandations spécifiques et les publie.

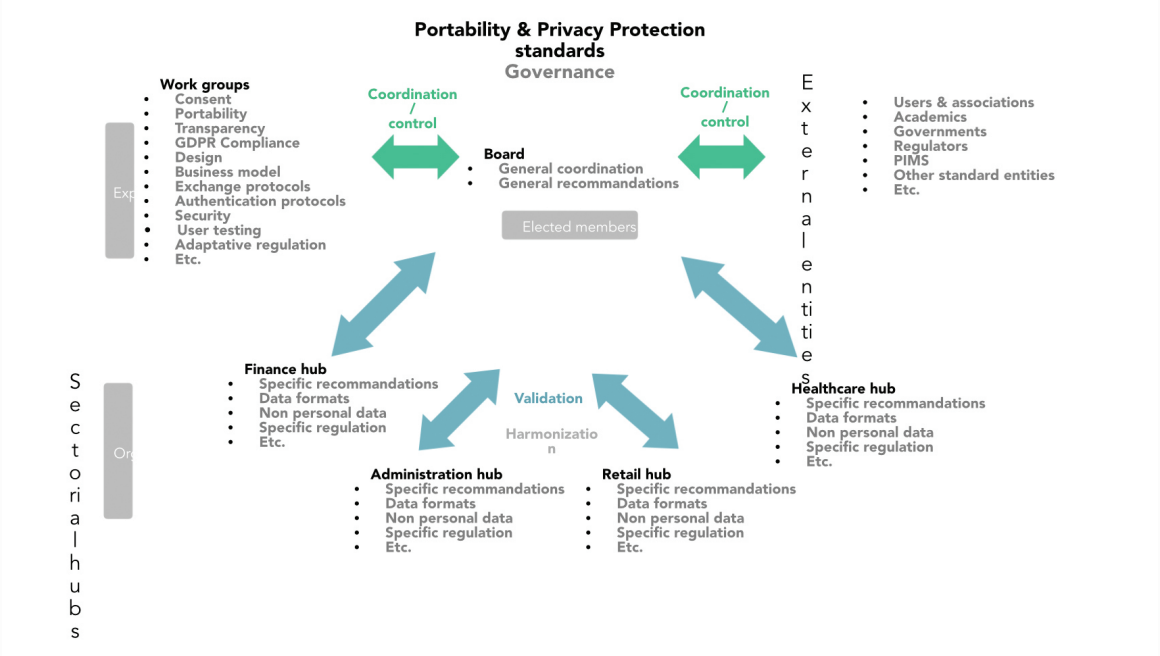


Schéma de fonctionnement de l'organe de gouvernance proposé

Prochaines étapes :

Si les principales parties prenantes sont d'accord, une phase concertée, ouverte et collaborative de design détaillé de la gouvernance pourra commencer et mener enfin vers la construction concrète de standards ouverts et accessibles à tous.

Conclusion

La libre circulation des données personnelles sous le contrôle des individus est à même de transformer radicalement nos économies et notre rapport au digital. Il s'agit de rétablir la confiance entre tous les acteurs économiques, en remettant l'humain au centre, et d'ouvrir la voie à une nouvelle époque d'innovation qui aura su tirer les leçons des erreurs du passé.

Le Règlement Général sur la Protection des Données est une innovation majeure pour le monde par les valeurs qu'il diffuse. Le droit à la portabilité, le consentement, le privacy by design, etc. sont les principes fondateurs d'une nouvelle économie basée sur la confiance, et pour une fois la loi a devancé l'innovation technologique en ce sens. Les plus grands acteurs du numérique commencent à s'accorder sur le fait que nous avons besoin d'un cadre commun pour harmoniser les pratiques à l'échelle mondiale et recréer la confiance.

Un an après la mise en application du RGPD, nous devons désormais passer à la phase 2 en traduisant ces nouveaux principes en outils et standards technologiques qui pourront rendre concrètes les valeurs du règlement. Un nouveau mode de gouvernance associant gouvernants, individus et acteurs économiques et technologiques, est donc à imaginer pour créer ces standards et faire en sorte qu'ils s'accordent de manière évolutive avec le cadre réglementaire. A un moment de notre histoire où l'Intelligence Artificielle pourrait nous amener à redéfinir notre place dans la société, il est primordiale que la technologie serve l'intérêt général, l'humain doit désormais être au coeur de toutes nos innovations et ces standards doivent être les garants techniques du respect de l'article 1 de la Loi Informatique et Libertés.

"L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi."

L'EQUIPE PRIVACYTECH :

Alessandro FIORENTINO est responsable de l'offre Informatique et Libertés du Cabinet Infhotep et Vice-Président de l'association Privacy Tech.
Titulaire d'un Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP), il a soutenu une thèse professionnelle relative à la mise en œuvre du Privacy by Design.
Nommé "Ambassadeur du Privacy by Design", le 22 mai 2013 par l'Office du Commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada, le promoteur du PbD.
Il assure aujourd'hui l'unité d'enseignement Privacy by Design au sein du Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP) et l'unité d'enseignement Méthodologies du DPO au sein du Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Mines-Telecom Business School.
fondé plusieurs sociétés.

Anaïs PERSON est Chef de projet et DPO de la Legal Tech Seraphin.legal, Anaïs Person est Déléguée à la Protection des Données (DPD/DPO) de plusieurs organismes et dispense des formations en Droit numérique et Droit des données personnelles. Juriste numérique, elle est spécialisée dans les droits de la Propriété Intellectuelle et des Affaires Numériques.
En parallèle de ces activités, Anaïs Person est enseignant vacataire auprès de l'Institut Droit et Santé de l'Université Paris Descartes, où elle effectue une thèse de doctorat sur l'évolution des assurances santé à l'heure du pilotage par la robotique et l'intelligence artificielle.

David BESSOT est passionné par l'impact du numérique sur la société et les organisations, David Bessot accompagne les dirigeants et les parties prenantes à gagner en compétence, pérenniser les outils et protéger les données. Cofondateur du cabinet Infhotep.com et de l'association privacytech.fr, il est diplômé de l'Universite paris 8

Matthias DE BIEVRE est le fondateur et Président de Visions. Matthias a coordonné la partie B mettant en avant l'état de l'art de la recherche grâce aux travaux de nombreux experts et chercheurs mobilisés pour ce Livre Blanc. Visions édite le logiciel VisionsTrust qui permet aux organisations de facilement gérer les droits des personnes sur leurs données.

Son but est de démarquer les organisations vertueuses par la transparence offerte sur les données personnelles et la simplicité du contrôle. Redonner contrôle à chacun sur ses données personnelles est sa mission et la condition d'une innovation éthique et pérenne. Il s'intéresse et agit pour la mutualisation des données au service de la data science, notamment en éducation. Matthias est également conférencier sur l'éthique dans la data science dans plusieurs universités françaises.

Olivier DION est le président fondateur de Onecub qu'il a créée en 2011 afin de redonner la maîtrise de leurs données aux individus. Onecub est un outil de portabilité des données personnelles, permettant à ses utilisateurs de faire circuler leurs données tout en gardant le contrôle, et aux entreprises de mettre en oeuvre un droit à la portabilité innovant. Depuis plusieurs années Olivier est un membre actif des communautés Open Data et Self Data en Europe comme aux Etats-Unis.

Patrick TIEV est consultant en protection des données à caractère personnel chez Infhotep.
Juriste de formation, Patrick a choisi de se spécialiser, par passion, en droit du numérique et plus précisément dans le droit des données personnelles.

Il a débuté comme juriste auditeur dans la protection des données personnelles et la cybersécurité. Il s'est ensuite naturellement tourné vers le conseil et est également un membre actif de la Privacy Tech.

Thierry ROBY est titulaire d'une maîtrise en droit privé (obtenu à Paris XIII), et diplômé d'un mastère spécialisé en management et protection des données personnelles, obtenu à l'ISEP, il a soutenu une thèse sur l'autodétermination informationnelle.
Il a travaillé 10 ans dans le secteur des assurances, auprès d'un grand groupe, et est maintenant consultant dans la gouvernance des activités de traitement de données personnelles, et conseille responsable de traitements, et sous-traitants.

Thomas SAINT-AUBIN est enseignant-chercheur en Droit numérique, Thomas Saint-Aubin est le CEO de la Legal Tech Seraphin.legal, qui accompagne les professionnels du droit dans leur transformation digitale et préfigure le juriste de demain, augmenté par la technologie et l'interprofessionnalité. DPO de plusieurs organismes, Thomas Saint-Aubin a fondé la Privacy Tech en 2016 pour recenser, promouvoir et co-développer des solutions juridico-techniques au service de la protection de la vie privée sur Internet. Également expert en propriété intellectuelle, il est aussi CEO de la Legal Tech About Innovation, une solution intelligente et collaborative qui accompagne les créateurs dans le cycle de vie de leur portefeuille de propriété intellectuelle.

CE LIVRE BLANC A ETE DESIGNE PAR L'AGENCE MAKE :

www.agencemake.com

Make, 33 avenue de Wagram, 75017, Paris


PRIVACY
TECH