The Positive Way

WAVESTONE

VIE PRIVÉE À L'ÈRE DU NUMÉRIQUE

DU BIG DATA AU SMART DATA

The Positive Way

WAVESTONE

www.wavestone.com

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Le contexte actuel d'hyper-connectivité associé à l'émergence de nouvelles technologies telles que le data mining, les objets connectés ou encore l'intelligence artificielle, conduit à une véritable **révolution de la donnée**. Celle-ci représente plus que jamais un levier de transformation numérique et **sa valorisation devient un enjeu stratégique et prioritaire pour les organisations.**

Jusqu'à présent, l'approche favorisée a été la récolte massive et systématique des données personnelles. Les organisations sont ainsi parvenues à constituer d'importantes bases de données mettant à profit l'ensemble de notre écosystème personnel et professionnel connecté. Mais depuis peu, le paysage réglementaire sur le sujet du respect de la vie privée évolue. En découle une prise de conscience inédite des citoyens et une crise de confiance en devenir.

Les organisations sont prévenues : après des années d'acceptation, les citoyens, conscients de leurs droits, veulent récupérer la maîtrise de leurs données pour ne les confier qu'aux tiers choisis.

La révolution de la donnée ne se fera donc pas sans confiance. Pour les organisations, la perdre c'est prendre le risque de la non adoption de leurs nouveaux services digitaux. Il convient donc de s'adapter et se poser de nouvelles questions : comment concilier valorisation de la donnée, respect de la vie privée des citoyens et conformité à la réglementation ? **Comment passer d'une approche « *big data* » à une approche « *smart data* » ?** Un équilibre est à trouver. Certains verront dans la situation globale une vraie opportunité de faire du respect de la vie privée un atout. **Et vous, comment allez-vous tirer parti de cette révolution ? Quels nouveaux usages allez-vous développer et comment ?**

GÉRÔME BILLOIS- Partner

AUTEURS

Raphaël BRUN

Raphaël est Senior Manager au sein de la practice Cybersécurité & Confiance numérique avec une expertise développée depuis plusieurs années en matière de protection des données personnelles. Il pilote des programmes de mise en conformité dans de nombreux secteurs (grande distribution, transport, assurance, ...) et accompagne la mise en conformité de plusieurs projets règlementaires auprès de l'état (valorisation des données de santé, fraude dans les transports). Raphaël a également travaillé à la conception de processus de gestion des crises cyber et à la conduite d'exercices de crise.

raphael.brun@wavestone.com

Damien LACHIVER

Damien est Manager au sein de la practice Cybersécurité & Confiance Numérique avec une expertise en protection des données et en gestion de crise cybersécurité. Il pilote notamment des programmes de mise en conformité au règlement européen RGDP et des projets de simulation de crise cybersécurité.

damien.lachiver@wavestone.com

Adèle COUDERT

Adèle est consultante au sein de la practice Financial Services. Elle intervient sur des projets de protection des données personnelles et des programmes de mise en conformité au règlement européen RGPD.

adele.coudert@wavestone.com

Débora DI GIACOMO

Débora est Senior Manager au sein de l'équipe Services Européens. Elle possède une expérience solide en stratégie IT et business, notamment dans le domaine des institutions Européennes. Elle travaille sur des sujets tels que la digitalisation des services publics, l'interopérabilité, l'évaluation de l'impact des politiques Européennes, des analyses coût-avantages et des études de faisabilité.

debora.digiacomo@wavestone.com

Anaïs ETIENNE

Anaïs est consultante au sein de la practice Cybersécurité & Confiance Numérique. Au travers de ses missions et notamment de programmes de mise en conformité RGPD pour de grands comptes, elle a développé une expertise dans la protection de données à caractère personnel et la gestion des risques.

anais.etienne@wavestone.com

Nous tenons à remercier chaleureusement Gwendal Le Grand, Tristan Nitot et Benjamin André de nous avoir accordé trois entretiens venus enrichir cette publication. Nous remercions également Pascal Vidal et Nick Prescot pour leur contribution ainsi que tous les consultants Wavestone dont les retours d'expérience ont rendu possible l'élaboration de ce document.

SOMMAIRE

LES CITOYENS EN ALERTE SUR LA PROTECTION DE LEUR VIE PRIVÉE NUMÉRIQUE

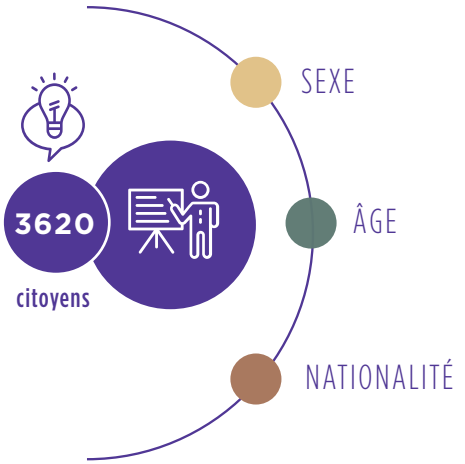
UNE SECONDE ENQUÊTE INTERNATIONALE

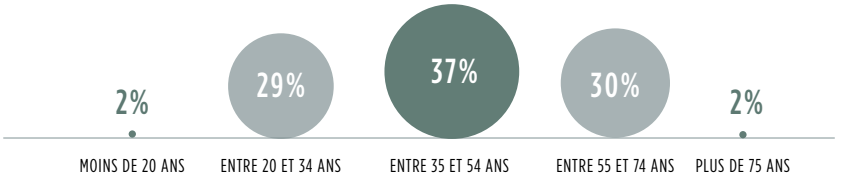
Wavestone commandite régulièrement des sondages auprès des citoyens afin de mesurer les tendances en matière de vie privée.

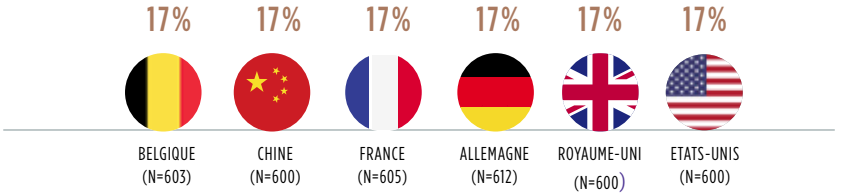
Un premier sondage a fait l'objet d'une étude « la vie privée à l'ère du numérique », publiée en 2016. Les observations de cette étude ont été mises en relief par un second sondage, mené en octobre 2018. Cela nous a notamment permis de mesurer l'impact de l'entrée en vigueur du RGPD sur la sensibilité des citoyens vis-à-vis du respect de leur vie privée.

Cette seconde enquête a été menée auprès de 3 620 citoyens originaires de six pays à travers le monde : Belgique, Chine, France, Allemagne, Royaume-Uni, Etats-Unis. Ces pays ont été sélectionnés dans le but de représenter les éventuelles disparités sur la perception de la vie privée dans les pays concernés en fonction de leur situation socio-économique mais aussi de leur cadre réglementaire local. Les répondants à l'étude sont répartis de manière homogène selon leur sexe et leur tranche d'âge. Il n'y a ainsi pas de sur-représentation de la tranche de 20 à 34 ans, qui pourrait avoir une plus grande sensibilité aux problématiques de protection de la vie privée.

Statistiques du sondage







UNE PRISE DE CONSCIENCE DES CITOYENS INÉDITE

Une prise de conscience globale de la population

94% des sondés déclarent **être préoccupés par le respect de leur vie privée soit une augmentation de 19% en deux ans**

Une prise de conscience inédite ! Les résultats de notre enquête tendent à démontrer que la vie privée est devenue **un sujet de préoccupation mondial**, **et pas seulement Européen**, et que les attentes qui en découlent sont similaires sur tous les continents. En définitive, nous constatons généralement peu, voire pas de différence entre les statistiques des différents pays. Cette sensibilité à la vie privée prend de l'importance d'année en année et devrait s'inscrire dans la durée, portée notamment par le durcissement et la multiplication des règlementations.

Pour les citoyens, la protection de la vie privée est liée avant tout à la maîtrise de leur vie numérique

2/3 Pour 2/3 des citoyens, **le respect de la vie privée est assimilable au respect de la vie privée sur le net**

Dans notre étude de 2016, nous soulignions l'évolution du sens de la « vie privée » avec l'émergence du numérique. Historiquement, le respect de la vie privée était intimement lié à la notion de liberté : liberté de préserver une forme d'anonymat dans ses activités et de disposer d'une capacité à s'isoler pour protéger ses intérêts. Aujourd'hui, face à une collecte toujours plus massive de données à caractère personnel sous toutes ses formes, les citoyens associent clairement **la protection de leur vie privée avec la maîtrise de leurs données**.

Comme en 2016, les citoyens ont d'abord défini le respect de la vie privée comme le fait de contrôler « qui obtient des informations sur moi ».

Avant même de savoir quelles données sont collectées et pour quels usages, **la protection de la vie privée est avant tout associée à la capacité donnée de choisir les tiers qui collectent et manipulent leurs informations**

En définitive, les individus sont prêts à partager leurs données personnelles à des tiers mais cela a un prix : celui de la confiance.

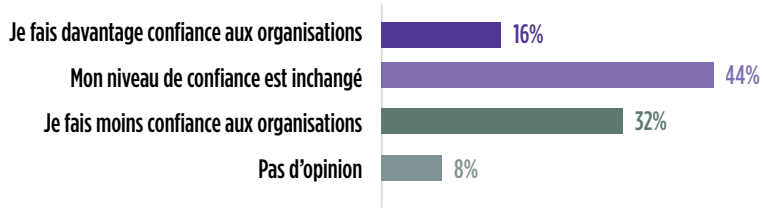
UNE CONFIANCE ENVERS LES TIERS QUI DÉCROÎT…

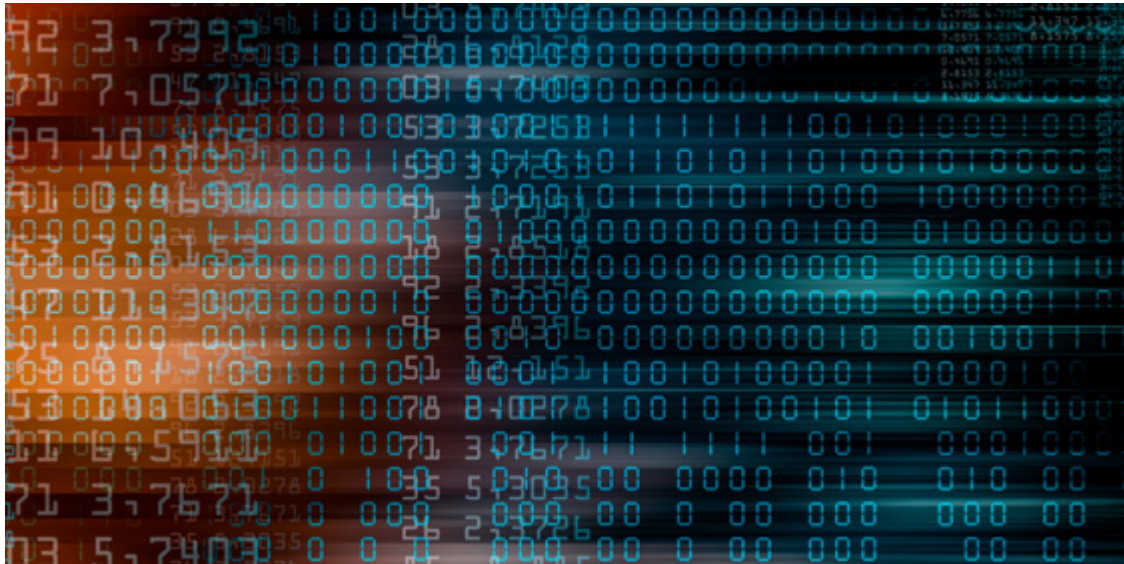
Une baisse générale dans le niveau de confiance envers les tiers

Cette baisse de confiance accordée aux tiers peut très bien s'expliquer par la multiplication des violations de données, ou a minima par le relais médiatique qu'elles rencontrent, comme ce fut le cas pour les scandales Facebook/Cambridge Analytica et Equifax.

32% de la population mondiale considère que **son niveau de confiance envers les tiers sur le sujet de la protection de leur vie privée a diminué depuis l'année dernière**

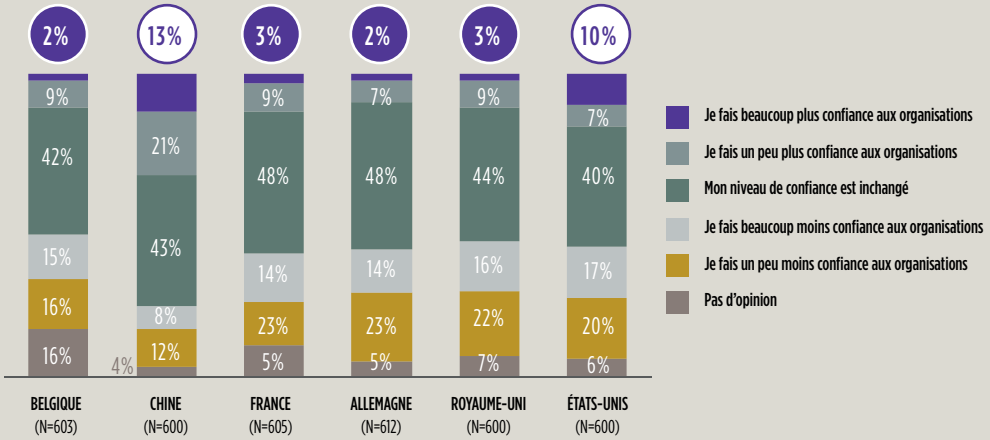
Pensez-vous que votre niveau de confiance envers les organisations a changé au cours de cette dernière année en ce qui concerne l'utilisation de vos données ?





Le RGPD a provoqué une crise de confiance en Europe !
Du fait de la complexité renvoyée, des annonces de fuites maintenant publiques et des scandales associés, les citoyens sont méfiants.

Pensez-vous que votre niveau de confiance envers les organisations a changé au cours de cette dernière année en ce qui concerne l'utilisation de vos données ?



Notre étude dresse un bilan particulièrement surprenant pour les pays Européens. Malgré l'entrée en vigueur du RGPD, une règlementation supposée leur redonner confiance, et les efforts fournis par les organisations pour s'y conformer, 68% de nos sondés Européens ne perçoivent aucun changement sur la maîtrise de leurs données. Pire encore, certains ont même le sentiment d'avoir moins de maîtrise sur leurs données. Cette crise de confiance traduit une forme de prise de conscience des enjeux autour de la protection de leurs données : ils sont mieux sensibilisés au sujet notamment grâce à la médiatisation du RGDP, aux efforts d'évangélisation des autorités de contrôle, voire même de leur propre organisation. Ce chiffre peut traduire également une mauvaise compréhension des efforts fournis par les organisations ou une méfiance de plus en plus développée envers celles qu'ils voient comme des « boîtes noires » traitant leurs données. Les quelques campagnes de renouvellement de consentement et les différentes communications autour du RGPD n'auront pas suffi et ceci à juste titre : la confiance prend du temps à se bâtir.

Un quart des citoyens sont des « *privacy absolutists* » : quel que soit l'usage fait de leurs données, ils y sont défavorables

Autre constat issu de notre sondage, quel que soit l'usage fait des données, les proportions de sondés prêts ou pas au partage de leurs données ne varient que très peu. En conséquence, l'usage des données n'est probablement pas le cœur du sujet. L'analyse des résultats du sondage (comme illustré sur le graphique ci-dessous) nous permet de distinguer aisément trois natures de comportements vis-à-vis des données.

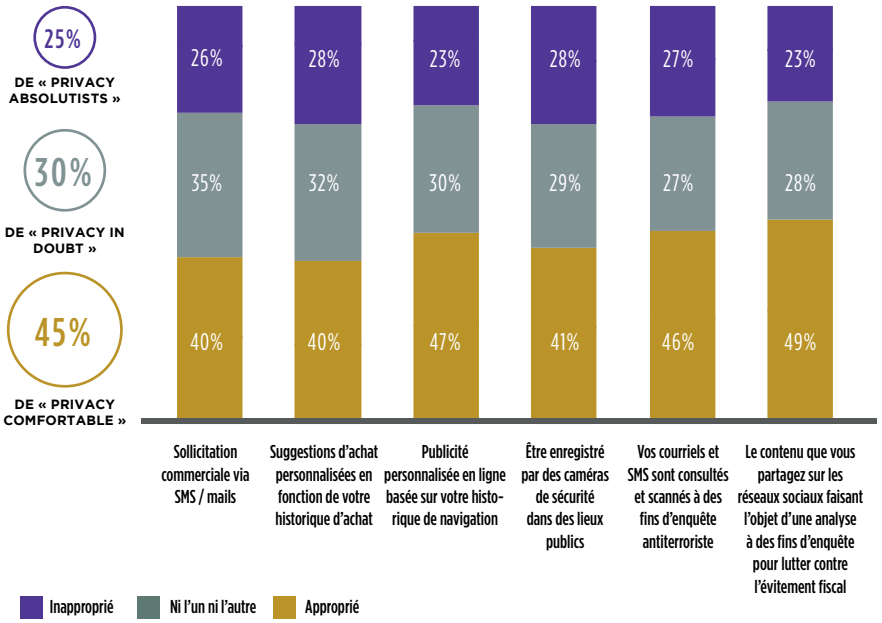
- **45% de la population peut être qualifiée de « *privacy comfortable* »**. Elle est favorable au partage de ses données. Cette catégorie n'a pas attendu l'entrée en vigueur du RGPD ou de nouvelles actions de communication de la part des organisations pour accepter les nouveaux usages digitaux et le partage de ses données comme contrepartie pour y avoir accès.

- **30% de la population peut être qualifiée de « *privacy in doubt* »**. Cette catégorie comprend l'intérêt du partage de ses données pour accéder à un service. Cependant, elle a besoin d'un cadre clair lui permettant d'accorder sa confiance au tiers à qui elle les confie. Une conformité au RGPD, accompagnée d'une communication claire et transparente peut constituer ce cadre et ainsi la convaincre de partager ses données.

- **25% de la population peut être qualifiée de « *privacy absolutists* »**. Cette catégorie est particulièrement réfractaire au partage de ses données. Contrairement à la catégorie

précédente, une conformité à la règlementation ne sera pas suffisante pour la convaincre. Il faudra donc réfléchir à d'autres moyens de créer la confiance. Le vrai challenge pour les organisations sera alors de limiter la progression de cette troisième catégorie voire même de trouver les leviers pour la convaincre de souscrire à des services digitaux consommateurs de données. Quelques pistes seront proposées dans la troisième partie de cette étude.

Veuillez évaluer la pertinence de l'utilisation de vos données personnelles dans les situations suivantes :



Un irritant persiste : la sollicitation commerciale non désirée

1/3 de nos sondés déclarent **avoir déjà demandé à une organisation de cesser de leur envoyer de la communication**

Malgré le peu d'importance accordée à l'usage fait des données confiées, l'un d'entre eux continue néanmoins à irriter les citoyens : la sollicitation commerciale non désirée. Historiquement, les équipes marketing ont eu tendance à collecter un maximum de données de contact pour avoir le plus de chance d'envoyer le bon email à la bonne personne. Néanmoins, cette pratique a une conséquence majeure : un agacement certain des individus sollicités de manière répétée.

Cela se traduit concrètement dans les chiffres : un tiers de nos sondés déclarent avoir déjà demandé à une organisation de cesser de leur envoyer de la communication. Il s'agit d'ailleurs l'exercice de droit le plus demandé. L'autorité de contrôle française confirme ces chiffres et indique que 21% des plaintes réceptionnées portent sur la prospection commerciale, avec une hausse importante de plaintes concernant la prospection par SMS. **Vu de l'individu, cette forte sollicitation à mauvais escient a pour impact direct la détérioration de la relation de confiance avec le tiers concerné, conséquence identifiée en première position par nos sondés.**

Il y a un donc un véritable enjeu à construire des bases de données marketing qualitatives qui ne soient pas uniquement centrées sur l'appétence de la personne pour le contenu transmis. En investissant dans la protection de la vie privée, les organisations pourront se concentrer sur **un marketing personnalisé et plus efficace**. Le recours à la collecte systématique d'un consentement clair et éclairé tel que préconisé par le RGPD constitue une première piste pour minimiser les plaintes et la perte de confiance. Pour aller plus loin, proposer une personnalisation plus fine de la relation commerciale, par exemple en collectant des consentements même lorsque le RGPD ne le requiert pas ou en permettant un paramétrage plus fin de la « pression relationnelle » exercée, est un levier intéressant pour garder ou établir le lien de confiance avec les individus. L'idée est de véritablement susciter son intérêt, établir un dialogue avec ses destinataires pour construire une relation sur la durée.

… QUI SE MATÉRIALISE PAR UNE POSTURE DES CITOYENS PLUS OFFENSIVE POUR PROTÉGER LEUR VIE PRIVÉE

1/2 de nos sondés déclare **avoir déjà exercé ses droits dans l'année passée**

Au-delà d'une simple prise de conscience, les citoyens adoptent une posture offensive pour protéger leur vie privée. Les citoyens n'acceptent plus l'intrusion des organisations dans leur vie privée et ainsi sont moins enclins à accepter la collecte

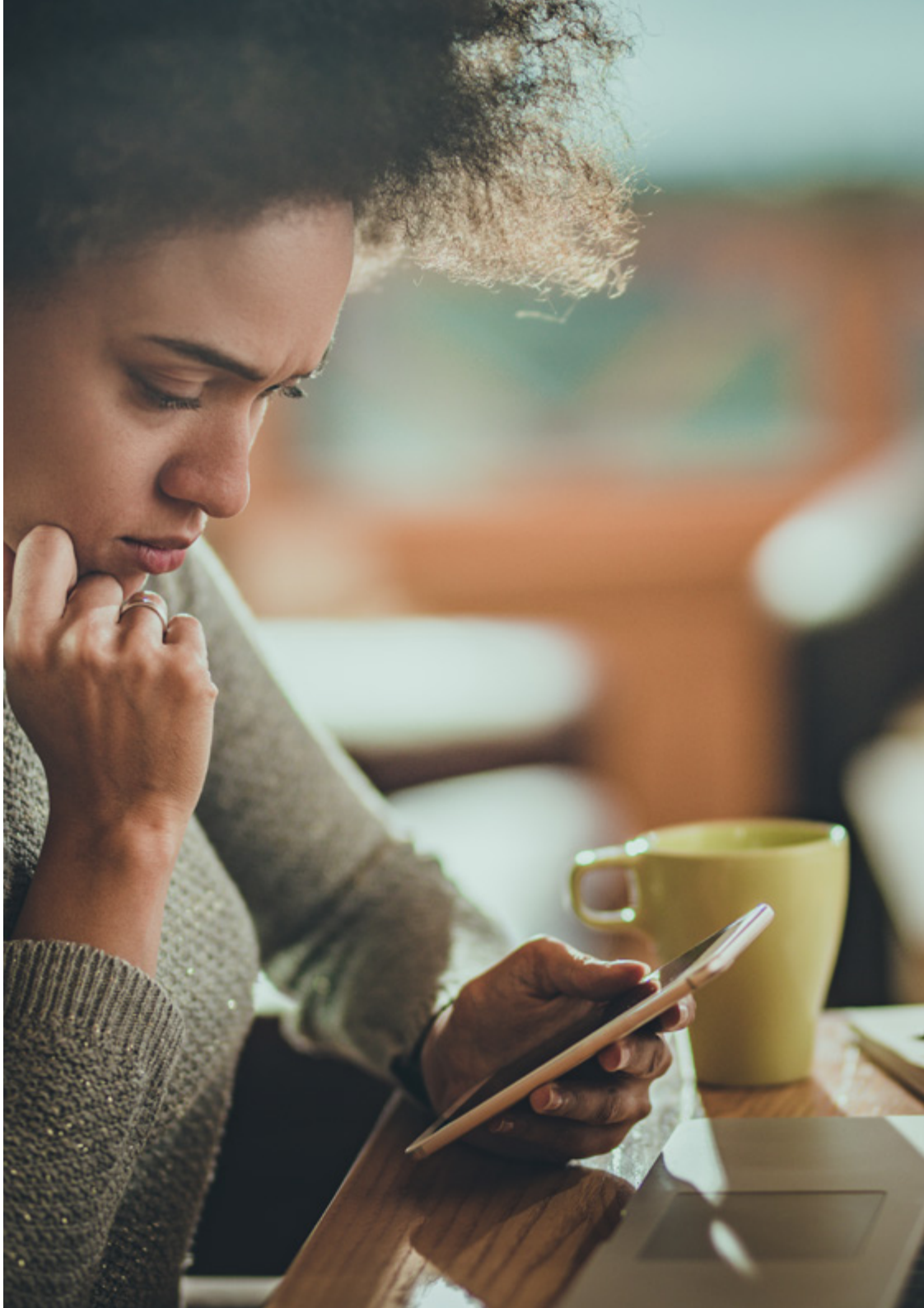
massive de leurs données. Pour pallier des années d'acceptation, **certains d'entre eux ont pris les devants et cherchent à en récupérer la maîtrise avec les moyens qu'ils ont à disposition** et notamment ceux que leur donne le RGPD. Très concrètement, ils n'hésitent pas à **faire valoir leurs droits**, et même à **avoir recours à des plaintes collectives** lorsque le cadre règlementaire dans lequel ils évoluent le leur permet.

Face à la crainte de dépeupler leurs bases de données clients, à date seulement 15% des organisations ont fait le choix de mener des campagnes de renouvellement des consentements. Les citoyens ont donc tiré parti du renforcement de la réglementation pour retirer spontanément leur accord à la réalisation de certains traitements voire pour demander la suppression pure et simple de l'intégralité de leurs données. Plus d'un sondé sur deux déclare avoir déjà exercé ses droits dans l'année passée : une nette augmentation des demandes qui se constate également sur le terrain du côté des organisations. Lorsqu'ils ne sont pas satisfaits de la réponse à leur demande en termes de délais ou de qualité, les citoyens n'hésitent pas non plus à saisir les autorités.

Pour gagner en force de frappe et rationnaliser les coûts, les consommateurs se regroupent et mettent en place des **plaintes collectives**. Ils sont pour cela **accompagnés par des associations de consommateurs** (les plus connues étant NOYB, Privacy International, La Quadrature du Net) qui se positionnent comme les défenseurs des droits des citoyens sur leurs données. Ces associations n'hésitent pas à s'attaquer aux géants du numérique comme Google, Amazon, Facebook, LinkedIn, etc. Pour mettre en évidence les dérives et sensibiliser le grand public, Privacy International organise également annuellement un concours nommé « les *Big Brother Awards* » pointant les pires atteintes à la vie privée et aux libertés des citoyens.

> « En 2018, la CNIL [Commission Nationale de l'Informatique et des Libertés française] a réceptionné un total de 11077 plaintes sur l'année, soit une augmentation de 32% par rapport à l'année précédente.»
>
> *GWENDAL LE GRAND, Directeur des technologies et de l'innovation CNIL*

Clairement, les citoyens et associations de consommateurs commencent à véritablement se saisir du sujet. Et c'est un véritable risque pour les organisations ! Leurs nouveaux services digitaux pourraient ne pas être adoptés par le grand public en absence d'un bon niveau de confiance des utilisateurs. La preuve : 26% de nos sondés ont arrêté d'utiliser certains services afin de protéger leur intimité numérique et de garder la maîtrise de leurs données. Dès lors, il est impératif de répondre présent en s'attachant à construire ou reconstruire des relations sur des bases saines.



UNE RESPONSABILISATION DES ORGANISATIONS À L'ÉCHELLE MONDIALE

LE RGPD, L'OCCASION POUR LES ORGANISATIONS HORS EUROPE D'ANTICIPER UNE ÉVOLUTION DE LA RÈGLEMENTATION DANS LEUR PAYS

La protection de la vie privée est devenue un sujet à l'échelle internationale. En 2016, notre rapport présentait un panorama des cadres juridiques de protection des données à caractère personnel et soulignait une véritable évolution ces dernières années. Depuis l'entrée de la notion de vie numérique dans les textes législatifs, les règlementations se sont multipliées. **L'Union Européenne s'est positionnée comme une locomotive de cette tendance avec le RGPD, mais les autres pays ne sont pas en reste** et nous assistons à une structuration globale des règlementations autour des données à caractère personnel.

Le RGPD s'applique à toutes les organisations établies sur le territoire de l'Union Européenne ou dont l'activité cible directement des résidents Européens. Dès lors, il impose naturellement une appropriation de ses concepts et exigences du sujet au-delà des frontières de l'Europe. Et le caractère transfrontalier se démontre rapidement puisque c'est une entreprise américaine qui a fait l'objet de la plus grosse sanction. Google a en effet écopé d'une amende de 50 millions d'euros de la part de l'autorité française de contrôle en janvier 2019 à la suite d'une plainte collective de ses citoyens. L'agence de contrôle française fait part d'une coopération européenne autour de cette sanction pour déterminer les principes à mettre en œuvre dans ce cadre.

C'est aussi l'occasion pour les organisations qui ne sont pas directement concernées à date d'anticiper une potentielle évolution de la règlementation au sein de leur pays. D'une part, parce que le numérique n'a pas de frontière, la protection de la vie privée exige un cadre mondial harmonisé. D'autre part, parce qu'il existe une véritable demande en la matière, autant au niveau des citoyens (notre sondage le prouve), qu'au niveau des organisations elles-mêmes. A titre d'exemple, le patron d'Apple, Tim Cook, a fait l'apologie du RGPD en début d'année dans le cadre d'une tribune dédiée pour Time Magazine[1] en demandant notamment la mise en place d'une règlementation similaire pour les Etats-Unis.

Gwendal Le Grand confie d'ores et déjà collaborer avec des autorités internationales sur les sujets de la vie privée : « d'autres autorités cherchent, dans la vague du RGPD, à se doter également de lois nationales ou régionales ». Dans son bilan annuel, la CNIL indique aussi se rapprocher avec ses homologues d'Asie (APPA) pour « échanger sur l'impact du RGPD dans cette région, réfléchir sur les perspectives de coopération et le partage d'expertise ». Le but ? « Réussir la diplomatie de la donnée tant en Europe, avec nos homologues du CEPD [Comité Européen de Protection des Données], comme sur le plan international » précise Gwendal Legrand.

Aujourd'hui, tout indique que le RGPD est en passe de devenir **LA référence mondiale en termes de cadre règlementaire de protection de données à caractère personnel.**

1. http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/

LE RGPD, UN PREMIER PAS VERS UN NUMÉRIQUE DE CONFIANCE ?

GWENDAL LE GRAND, Directeur des technologies et de l'innovation, CNIL [Commission Nationale de l'Informatique et des Libertés]

LE RGPD A-T-IL PERMIS LA PRISE DE CONSCIENCE ESCOMPTÉE ?

Le RGPD est entré en application le 25 mai 2018 et c'est un texte que tout le monde s'est approprié : les organisations, les particuliers et les autorités de protection des données. Les citoyens ont tiré parti de leurs droits et les ont davantage exercés auprès des organisations. En résulte une augmentation significative du nombre de plaintes : si on regarde les chiffres, la CNIL a reçu 11077 plaintes sur l'année dernière, soit une augmentation de 32% par rapport à l'année précédente.

QUELS SONT LES SUJETS QUI SUSCITENT LE PLUS DE PLAINTES ?

À date, les plaintes reçues par la CNIL restent assez « traditionnelles ». Elles sont surtout liées à la volonté de maitrise des données à disposition en ligne (déréférencement, suppressions de contenu sur des blogs, des sites de presse ou des réseaux sociaux etc.). On réceptionne aussi beaucoup de plaintes liées à la prospection commerciale et aux questions RH. Sur ce dernier point, ce sont en particulier les activités de surveillance qui font l'objet de plaintes : surveillance au travail, surveillance d'activité ou vidéosurveillance. On constate également l'émergence de plaintes collectives. Ce sont notamment des plaintes des associations la quadrature du net et NOYB (menée par Max Schrems) qui ont donné lieu récemment à la plus grosse sanction prononcée à ce jour par la CNIL.

ET À L'INTERNATIONAL, QUEL BILAN ?

Le but est de réussir la diplomatie de la donnée avec nos homologues au niveau CEPD, groupe des CNIL européennes, comme sur le plan international. On discute avec un certain nombre d'états ou de régions du monde, qui, dans la vague du RGPD, cherchent à se doter également de lois nationales ou régionales. Nous avons notamment travaillé avec des partenaires asiatiques, avec les Etats-Unis et dans le cadre de la convention 108 du conseil de l'Europe. Ce sont des travaux qui sont bien évidemment amenés à se poursuivre.

AU NIVEAU DES CONTRÔLES ET SANCTIONS, QUEL BILAN ET QUELLES PERSPECTIVES ?

Côte chiffres, l'année dernière environ 300 contrôles ont été effectués (en ligne, sur place ou sur pièces) et on dénombre 11 sanctions en France.
On le sait, le pouvoir de sanction des autorités a sensiblement augmenté avec le RGPD. Pendant très longtemps la sanction maximale que la CNIL pouvait infliger s'élevait à 150 K . Ce montant est passé à 3M avec la loi pour une République Numérique en 2016. Il s'élève maintenant à 20M ou 4% du CA mondial. Il faut garder à l'esprit qu'une procédure de sanction prend du temps : une part des contrôles aboutit à une mise en demeure. La procédure de sanction est généralement engagée lorsque l'organisme ne s'est pas mis en conformité à l'issue du délai imparti par la mise en demeure. Cette procédure implique elle-même le respect du contradictoire, de manière à ce que l'organisme incriminé puisse se défendre. Les autorités activent progressivement, au fur et à mesure que les procédures de contrôle se déroulent, les nouveaux plafonds permis par le RGPD.
En ce qui concerne les contrôles à venir, trois thématiques seront particulièrement concernées en 2019 : les droits des personnes, les sous-traitants et les données des mineurs.

INNOVATION ET RGPD, UN MARIAGE POSSIBLE ?

Le pari du législateur européen est de concilier innovation et droits des personnes, en définissant le cadre pour une innovation responsable.
En outre, notre site (linc.cnil.fr) traite de ces questions des nouvelles technologies en adhérence avec la protection de la vie privée. Nous y publions régulièrement des dossiers sur des thématiques nouvelles : les assistants personnels, la blockchain, le design des interfaces, le partage de données etc.
La CNIL investit également dans l'accompagnement de startups. Nous sommes déjà présents dans les lieux comme station F, nous y proposons des ateliers sur le thème de la protection de la vie privée. Cela nous a permis de rencontrer plus de 400 représentants de startups sur l'année 2018. Dans ce cadre, nous leur expliquons les fondamentaux de la loi mais veillons surtout à répondre à leurs interrogations propres. Cela leur permet ensuite de développer leurs activités en respectant le cadre fixé par le RGPD. Pour continuer à les accompagner, nous venons également de mettre en place une rubrique dédiée sur le site https://www.cnil.fr.

ROYAUME-UNI ET VIE PRIVÉE, QUELLES PERSPECTIVES ?

NICK PRESCOT, expert Cybersécurité & Confiance Numérique, Wavestone, Royaume-Uni

LA PROTECTION DE LA VIE PRIVÉE EST-ELLE UNE PRIORITÉ POUR LES ORGANISATIONS BRITANNIQUES DEPUIS LA CRÉATION DU RGPD ?

Pour de nombreuses organisations britanniques, l'impact du RGPD a été important car il n'a pas seulement été abordé comme un nouveau standard intra-européen de protection des données personnelles. En raison des liens étroits entre le Royaume-Uni et les Etats-Unis, il a été vu comme une norme mondiale (de nombreux sièges sociaux Europe/Afrique/Moyen-Orient d'organisations internationales sont établis au Royaume-Uni). Les organisations ont donc investi dans la mise en conformité au RGPD, et elles continuent à travailler pour faire en sorte que celle-ci soit maintenue dans le temps !

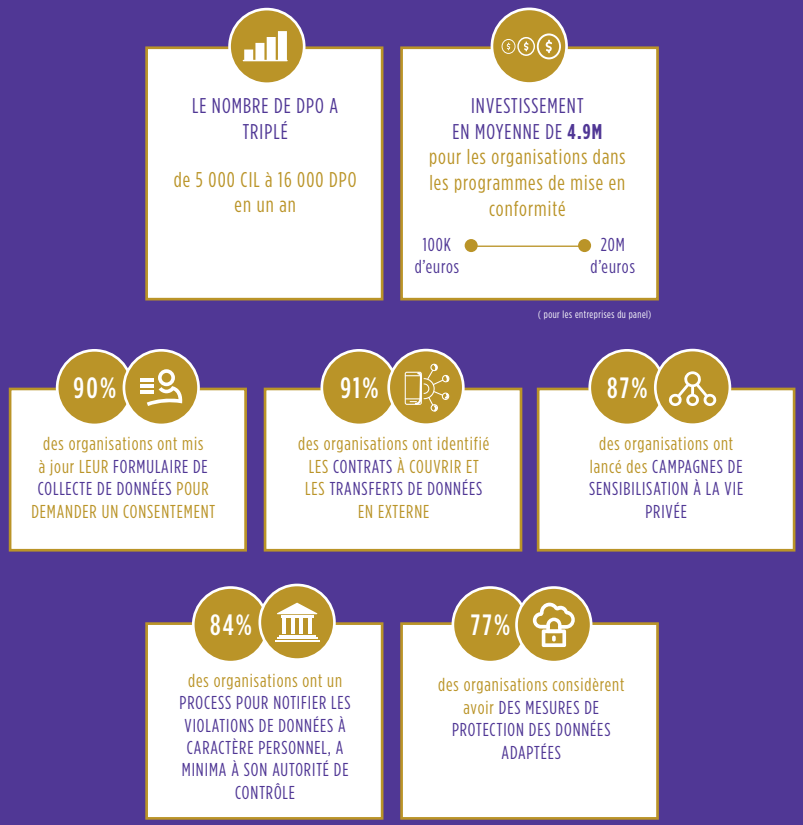
LA MENACE DU BREXIT A-T-ELLE UNE INFLUENCE SUR LES EFFORTS DÉPLOYÉS POUR SE CONFORMER AU RGPD ?

Le Brexit, reporté au 31 octobre 2019, ne remet pas en cause la mise en œuvre des principes du RGPD au Royaume-Uni, puisqu'il a été décliné localement dans la loi britannique de 2018 sur la protection des données. Cette législation va même plus loin puisque certaines infractions liées à la manipulation ou la violation de données personnelles relèvent d'infractions pénales. La principale préoccupation concerne l'éventuel statut de «pays tiers» du Royaume-Uni après sa sortie de l'UE qui réclamerait la mise en place d'un nouvel accord sur le traitement des données. Cela aurait été coûteux à mettre en œuvre dans le cas d'un Brexit sans accord mais cette hypothèse ne semble pas se réaliser. A partir du moment où le Parlement britannique ratifie un accord de retrait, il devrait y avoir une période de transition jusqu'en décembre 2020 pendant laquelle la situation actuelle perdurerait. Après cette date, il sera nécessaire de mettre en place un nouvel accord sur le traitement des données.

QUELLES SONT LES PERSPECTIVES POUR LES MOIS À VENIR EN MATIÈRE DE VIE PRIVÉE ?

La confidentialité des données à caractère personnel est devenue un concept de plus en plus important pour la génération des 18-25 ans au Royaume-Uni. Les scandales récents comme la fuite de 500 millions de comptes Facebook et le scandale Cambridge Analytica ont rendu cette génération beaucoup plus consciente des données qu'elle partage en ligne. Cette tendance est récente car la société commence progressivement à prendre conscience des données détenues par des entreprises tierces mais aussi des efforts qu'elles font pour les protéger. Par ailleurs, les suites de la fuite de données qui a touché British Airways en décembre 2018 vont être particulièrement scrutées car elles sont amenées à faire jurisprudence, en particulier le montant de l'amende infligée par l'ICO (*n.d.l.r. Information Commissioner's Office, l'autorité de contrôle britannique*). Il sera intéressant de voir si British Airways écope d' une amende de 2% du chiffre d'affaire mondial comme toutes les organisations le craignent !

DES EFFORTS IMPORTANTS MENÉS PAR LES ENTREPRISES POUR SE CONFORMER AU RGPD



Présentation du benchmark réalisé auprès de 24 organisations de différents secteurs 6 mois après l'entrée en vigueur du RGPD

Afin d'apprécier les travaux menés par les organisations au regard du respect de la vie privée, Wavestone a mené un état des lieux auprès de 24 de ses clients français et internationaux. Pour ce faire, nous avons capitalisé sur les données de nos accompagnements de programme menés tant sur le périmètre Français qu'international. Le but ? Estimer le niveau de conformité global des organisations au RGPD et mettre en lumière les principaux enjeux et les tendances à venir sur la base de notre expérience. Les chiffres qui suivent sont tirés de ce benchmark.

À DATE, UNE CONFORMITÉ GLOBALE POUR LES ORGANISATIONS DU PANEL MAIS DES DÉFIS À VENIR POUR PÉRENNISER LA DÉMARCHE…

Les chiffres le prouvent : les organisations du panel se sont saisies du sujet et ont fait des efforts afin de se mettre en conformité. L'un des effets positifs de ces investissements est une meilleure compréhension de la donnée au sein de leur organisation. Si le niveau de conformité atteint est globalement satisfaisant, deux points de vigilance sont à souligner :

Il faut traiter pleinement la mise en conformité du volet RH

30% des interrogés déclarent même que **la prise en compte de la protection de leur vie privée pourrait constituer le critère principal de choix de leur employeur**

Sur le terrain, nous constatons que les organisations ont souvent pris le parti de concentrer leurs efforts sur les données des clients plutôt que sur les données des employés. Deux raisons à cela : ne pas altérer durablement la relation de confiance établie avec les clients mais également prioriser la conformité « visible » pour ne pas attirer l'attention des autorités de contrôle. Paradoxalement, il est intéressant de noter que, contrairement à ce que l'on observe du côté des clients, la confiance envers son employeur en ce qui concerne l'utilisation de ses données personnelles semble avoir progressé (même faiblement) ces dernières années. Ceci peut notamment s'expliquer par l'attention historique que les organisations ont attaché à la protection des données de leurs collaborateurs, notamment dans le cadre de l'application du droit du travail ou de la gestion des relations sociales. Les attentes en termes de protection des données étaient donc généralement déjà respectées avant l'arrivée du RGPD, et le niveau de maturité sur le sujet des filières RH déjà élevé.

Si l'approche initiale choisie peut donc sembler pragmatique, en particulier pour les organisations B2C, il convient néanmoins de ne pas négliger les données des salariés. **La confiance croissante ne signifie pas pour autant que l'attente des salariés soit moins importante vis-à-vis de leur employeur**. Nous retrouvons en effet des proportions similaires d'interrogés pour lesquels la protection des données est importante au sein même de leur organisation que ce que l'on voit vis-à-vis des organisations tierces.

Il est crucial de maintenir et renforcer la relation de confiance avec ses employés pour les organisations. Ceci est d'autant plus vrai que les données manipulées par l'employeur peuvent être sensibles et donc qu'une violation de données des employés peut sérieusement entacher la réputation d'une organisation. Dans le futur, une confiance bien établie pourra également faciliter l'introduction de nouvelles technologies par les filières RH dans leurs processus (analyse prédictive des carrières, pilotage de l'activité, etc.).

Il faut assurer la pérennité de la démarche au-delà des programmes

Les processus mis en place au sein des organisations (réponse aux demandes d'exercice des droits, méthodologie *privacy-by-design*, réalisation d'AIPD…) restent encore souvent manuels, il s'agit maintenant de les **industrialiser, les optimiser et les pérenniser** pour s'assurer que les efforts fournis pour se mettre en conformité ne seront pas perdus sur la durée. La date butoir du 25 mai 2018 passée, il s'agit maintenant de mettre en place une **conformité durable** mais aussi de tirer parti plus largement des efforts produits dans le cadre des programmes de mise en conformité. Cela implique de répondre à un certain nombre de challenges.

> « Le RGPD exige la mise en place d'une conformité dite dynamique : il nécessite la réévaluation régulière des mesures de sécurité pour tout ce qui touche à la protection des données à caractère personnel. Nous passons d'une logique de conformité à un instant T à un logique d'amélioration continue »
>
> *GWENDAL LE GRAND,*
> *Directeur des technologies et de l'innovation CNIL*

…REPENSER LE SYSTÈME D'INFORMATION AUTOUR DE LA DONNÉE

L'entrée en vigueur du RGPD a mis le doigt sur un point de douleur des organisations dites « historiques » : une non maîtrise globale de leur système d'information.

Là où les organisations du digital ont fait de la maîtrise de la donnée et de sa valorisation le cœur de leur valeur ajoutée, les questions basiques du RGPD posent des problèmes fondamentaux aux autres organisations : Quelles données sont collectées ? Où sont-elles stockées ? Quels traitements sont effectués sur ces données ? Combien de compte(s) est-ce qu'un client unique possède réellement ? Sommes-nous en capacité de garantir le bon effacement des données ? Comment redonner aux individus la main sur leurs données ? Le manque de maîtrise du SI dans sa globalité induit de vraies difficultés pour les acteurs historiques.

Plusieurs constats sur le terrain :

- **L'architecture du système d'information est orientée service ou calquée sur l'organisation interne et ne permet donc pas une approche globale centrée sur la donnée**. De ce fait naît un manque de cohérence mais aussi une perte dans la valorisation potentielle de la donnée au service du client. À titre d'illustration, 55% des organisations de notre panel sont contraintes de gérer le consentement par silo et ne peuvent donc pas garantir une complète maîtrise de son utilisation.
- **La transformation digitale et l'évolution rapide des usages ont poussé les organisations à ouvrir leur système d'information** à des partenaires, à intégrer rapidement de nouvelles technologies, à développer des logiciels pour répondre à de nouveaux besoins métier **sans prioriser la prise en compte de la cohérence globale de l'architecture**. En conséquence directe, le cycle de vie complet de la donnée n'est pas maîtrisé, ce qui complexifie la mise en conformité industrialisée au RGPD.
- **Très concrètement, dans la plupart des organisations, il est techniquement impossible d'automatiser la suppression des données** à terme de leur durée de conservation ou à la demande, soit pour des contraintes technologiques, soit pour une difficulté à mesurer l'impact global d'une telle suppression. En conséquence, il est complexe de mettre en œuvre un processus efficace de traitement des demandes d'exercice de droit ou d'en garantir le résultat. Par extension, il est complexe de traiter les nouveaux droits issus du RGPD en particulier la portabilité et la limitation.

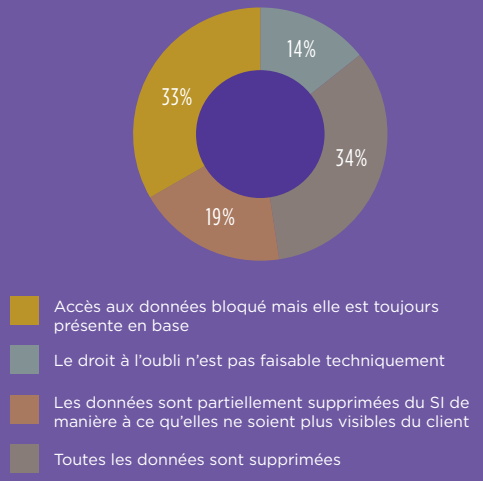
FOCUS SUR LES DIFFICULTÉS RENCONTRÉES DANS LE TRAITEMENT DES DEMANDES D'EXERCICE DE DROITS

Respecter les délais de réponse à une demande d'exercice de droit peut s'avérer plus compliqué qu'anticipé pour certaines organisations. Notre benchmark met en évidence un écart de maîtrise entre les droits classiques et les nouveaux droits du RGPD. Ainsi, les droits classiques incluant le droit de modification et le droit d'accès sont considérés comme maîtrisés pour plus de 3 entreprises sur 4. À l'inverse, le droit d'opposition et les nouveaux droits tels que le droit à l'effacement, à la limitation et à la portabilité se heurtent notamment à des complexités techniques et des conflits d'intérêt.

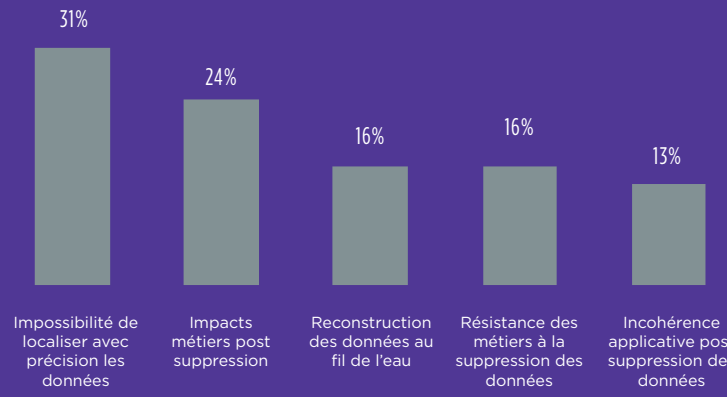
FOCUS SUR LE DROIT À L'OUBLI

Seulement un tiers des organisations du panel interrogées parvient à garantir la suppression de l'intégralité des données d'un client dans le cadre du droit à l'oubli. La mise en œuvre de ce droit se heurte à des complexités techniques. Par ailleurs, les organisations sont également confrontées à une réticence des métiers à acter la suppression en l'absence de maîtrise des impacts collatéraux éventuels.

COMMENT TRAITEZ-VOUS LE DROIT À L'OUBLI ?



DIFFICULTÉS RENCONTRÉES PAR LES ENTREPRISES DANS LA MISE EN PLACE DU DROIT À L'OUBLI



FOCUS SUR LE DROIT D'OPPOSITION

La complexité de ce type de demande est intimement liée à la collecte du consentement. Des interfaces ont été mises en place pour permettre la bonne réception des demandes mais elles sont exécutées application par application dans la majorité des cas entrainant mécaniquement des risques d'incohérence.

FOCUS SUR LE DROIT À LA PORTABILITÉ ET À LA LIMITATION

Ces deux droits n'ont pas été priorisés au sein des programmes de mise en conformité RGPD en l'absence de retours d'expérience et de lignes directrices sectorielles. Il est à noter néanmoins que ces droits font l'objet de peu de demandes à date.

L'idéal pour les organisations serait de **multiplier les points de vérité omnicanal**. Autrement dit, l'idéal serait de structurer leur système d'information autour de bases de données maîtres faisant référence pour tous les utilisateurs, qu'il s'agisse d'applications comme d'humains. Par exemple, si je disposais d'un point de vérité unique des informations d'adresse postale de mes clients, modifier une adresse en cas de déménagement pourrait être répliqué dans mon SI en renseignant simplement l'évolution dans cette base. L'avantage de cette approche est multiple : **les données sont cohérentes, vraies partout et l'exercice des droits en est largement simplifié.**

BESOIN DE CONSTRUIRE UN POINT DE VÉRITÉ UNIQUE

PASCAL VIDAL, Expert Cybersécurité & Confiance Numérique, Wavestone

COMMENT EXPLIQUER QUE LES ENTREPRISES ONT DU MAL À MAITRISER LES DONNÉES CLIENTS ?

Pour le comprendre, il faut remonter à l'origine des systèmes d'information des entreprises. Ces derniers, tout comme l'entreprise, ont été conçus de sorte à répondre à des besoins urgents de support technique aux fonctions métiers : à chaque besoin, son application et son référentiel de données en propre (application web, mobile, programme de fidélité, SAV, logistique, boutiques, etc.).

Les entreprises se retrouvent maintenant avec un système d'information siloté par fonction métier, **constitué d'autant de bases clients que d'applications**. En d'autres termes, **un système d'information qui ne permet pas d'avoir une vue globale des données clients, et ainsi de les maitriser**.

QUELS ENJEUX POUR LES ENTREPRISES ET COMMENT LES AIDER À MIEUX MAITRISER LES DONNÉES CLIENTS ?

À l'ère du RGPD, le principal enjeu des entreprises est de **construire une relation de confiance avec leurs clients**.

Une confiance qui passe à la fois par une communication transparente des traitements réalisés sur les données du client, mais surtout par le fait de **rendre le client maitre de ses données personnelles et lui en faciliter l'accès.**

Cela impose aux entreprises de **repenser leur système d'information avec une approche globale, orientée données, en plaçant le client au centre des réflexions** : Quelles sont les données de mes clients ? Où se trouvent ces données ? Comment y accéder ? Quels traitements appliqués ?

Néanmoins, les entreprises rencontrent des difficultés dans cette nouvelle approche, du fait de la prise en considération d'un historique SI important, et donc peu agile, et l'ouverture de leur SI à de nouvelles sources de données, principalement digitales (ex : réseaux sociaux).

Ces difficultés sont symptomatiques d'un manque essentiel dans le SI des entreprises : avoir un point de vérité unique, garant de la gestion transverse des données, **le référentiel des identités clients.**

EN QUOI CONSTRUIRE UN RÉFÉRENTIEL D'IDENTITÉS CLIENTS VA ACCÉLÉRER LA MISE EN CONFORMITÉ RGPD DES ENTREPRISES ?

Le référentiel d'identités clients constituera le point central de gestion des données clients. Il aura pour rôle de recueillir, centraliser et mettre à disposition ces données à tous les systèmes de l'entreprise, aussi bien physiques que digitaux.

Au-delà de ce rôle central, il permettra aux entreprises de plus facilement répondre aux exigences du RGPD, notamment :

- Savoir **quelles données personnelles l'entreprise possède et dans quels systèmes,** au travers d'une vue agrégée des données, qu'on appellera « l'identité client ». Cette identité fera office de point de rattachement de l'ensemble des données personnelles du client et des systèmes y ayant accès.
- **Fiabiliser les données clients**, afin d'en contrôler leur qualité et de les mettre à jour dans l'ensemble des systèmes du SI concerné, indépendamment du point de contact (boutiques, canaux digitaux, service client…).
- **Rendre le client maitre de ses données**, en lui donnant accès à une vue centralisée de ses données personnelles afin de lui permettre d'exercer ses droits (rectification, extraction, oubli…).

Le projet de construction de ce référentiel d'identités peut s'avérer long, notamment pour des entreprises de grande envergure. Toutefois, il existe aujourd'hui des solutions clés en main, qui permettent de rapidement constituer un tel référentiel : **les solutions « Customer IAM »** (gestion des identités et accès des clients).

QU'EST-CE QU'UNE SOLUTION CUSTOMER IAM ?

Une solution « Customer IAM » vise à simplifier et fiabiliser les processus de gestion et la protection des données clients, aussi bien pour des clients que des prospects.

Ces solutions embarquent des accélérateurs technologiques permettant de **créer une couche de gestion et de sécurité des données, transverse aux silos historiques des systèmes d'information.**

Elles s'articulent autour de trois principales fonctionnalités :

- **Centralisation et partage des données personnelles et consentements clients** en fournissant un référentiel des identités centralisé en charge de synchroniser les données clients dans les systèmes du SI, notamment via des interfaces temps réel pour satisfaire les contraintes des canaux digitaux.
- **Sécurisation des accès aux données clients** en fournissant des services de contrôle d'accès pour les clients eux-mêmes (mot de passe, social login, Single Sign On, multi-facteur, biométrie, etc.) et les systèmes traitant la donnée.
- **Suivi de la conformité des traitements et usages des données clients** en fournissant au DPO et aux métiers des tableaux de bord de suivi des consentements, des données personnelles référencées ou encore le respect des préférences clients.

L'ensemble de ces solutions sont inscrites dans **une démarche d'agilité et d'interopérabilité (orientées API)** de sorte à pouvoir s'intégrer de manière transparente dans le SI des entreprises.

EST-CE QU'UNE SOLUTION CIAM EST LE REMÈDE MIRACLE AUX MAUX RGPD ?

Non. Bien que ces solutions fournissent des accélérateurs permettant de créer une couche de gestion et de protection des données clients transverses au SI, elles n'enlèvent en rien la nécessité de **définir et mettre en place une gouvernance globale des données clients** (processus, sécurité, traitements, stockage…).

...METTRE EN PLACE UNE GOUVERNANCE DE LA DONNÉE COHÉRENTE, TRANSVERSE ET INTÉGRANT LE VOLET VIE PRIVÉE

La mise en place d'une gouvernance de la donnée est une priorité stratégique pour les organisations. Cependant, face à l'urgence de la mise en conformité à la règlementation Européenne, les organisations n'ont pas nécessairement eu le temps de traiter de front cet enjeu avec les impératifs liés à la protection des données personnelles. Pour rendre la conformité pérenne et optimale, il est maintenant temps de lier ces deux dimensions pour que le respect de la vie privée soit légitimement ancré dans les pratiques.

> Les principes et exigences du RGPD nécessitent la mise en place d'une gouvernance propre à la donnée intégrant les problématiques de vie privée au sein des organisations.
>
> *GWENDAL LE GRAND, Directeur des technologies et de l'innovation CNIL*

Il s'agit ainsi de repenser la stratégie de valorisation de la donnée en prenant en considération les exigences de la règlementation. L'important volume de données collectées avec le développement du numérique et les nouvelles technologies offre de nouvelles perspectives pour les métiers, mais présente aussi un risque. Selon une étude menée par le groupe Infopro pour Wavestone, parue en mai 2019 « la révolution de la data », l'un des principaux freins à la valorisation des données au sein des organisations est la faible qualité de celles-ci, qui les rend parfois inexploitables. **Un équilibre est à trouver entre une collecte massive de données et une valorisation optimale de la donnée**. Autrement dit, il est fondamental de concilier une approche quantitative et une approche qualitative. Le RGPD pousse à cet équilibre au travers du principe de minimisation et cette approche n'est pas nécessairement préjudiciable à la performance du marketing digital. Cependant, sur le terrain, même si l'on observe un effort de certaines organisations pour qualifier correctement leurs bases de données, le changement de posture n'est pas encore marqué. Cela s'illustre par le fait qu'une faible partie des organisations ait lancé une campagne de renouvellement des consentements ou encore que seulement la moitié des organisations ait mis en place des processus permettant de vérifier que la donnée collectée est limitée, appropriée et pertinente par rapport à son utilisation.

Une opportunité à saisir pour désensibiliser les données : la pseudonymisation !

Il existe une distinction claire entre pseudonymisation et anonymisation. L'anonymisation est supposée être irréversible et sort ainsi la donnée concernée du périmètre d'application du RGPD (car dépossédée de l'aspect « à caractère personnel »). L'anonymisation est complexe à mettre en place au sein des organisations et ne permet pas toujours une maximisation de la valeur de la donnée. Par exemple, dans la mesure où elle rompt le lien avec l'individu, elle ne permet pas un suivi dynamique d'un comportement dans le temps. La pseudonymisation est dans ce sens une bonne alternative et est d'ores et déjà exploitée par certaines organisations.

À date, les principales techniques de pseudonymisation relèvent de l'utilisation de systèmes cryptographiques, de fonctions de hachage ou bien de dispositifs de tokenisation. Grâce à ces techniques, un nouvel identifiant sera attribué automatiquement aux données collectées. La clé d'identification, qui permet d'établir directement le lien entre le nouvel identifiant et la personne concernée, est conservée dans une base de données dont la protection est accrue et les accès limités aux administrateurs techniques. Les données pseudonymisées sont quant à elles stockées dans une autre base de données, **permettant aux métiers d'analyser les tendances et suivre des comportements dans le temps.**

Dans les contextes où cela a un sens, pseudonymiser toutes les données directement ou les données facilement identifiantes (nom, prénom, adresse mail, numéro de téléphone...) peut apporter trois avantages clés :

- **Une sécurisation accrue**. Il faudrait attaquer les deux bases (la base pseudonymisée et celle qui fait la correspondance avec les individus) pour faire converger les données et identifier directement les personnes concernées.
- **Une optimisation de la valorisation de la donnée**. Comme mentionné précédemment, les données pseudonymisées permettent de garder un lien avec l'individu et donc de pouvoir suivre un comportement dans le temps.
- **Une simplification de l'exercice des droits sur le périmètre pseudonymisé**. Si un citoyen demande à exercer son droit à l'oubli, supprimer la clé d'identification correspondante dans la table de correspondance et les données pseudonymisées pourrait se rapprocher d'un effacement du caractère personnel du jeu de données. Cela préfigure néanmoins que les données conservées (non pseudonymisées) soient suffisamment bien calibrées pour ne pas permettre de remonter facilement à l'individu par déduction sur la base des informations manipulées.

… FAIRE DE LA PROTECTION DES DONNÉES PERSONNELLES UN RÉFLEXE AU QUOTIDIEN

96% des organisations du panel **ont inséré une étape d'évaluation des risques liés aux données à caractère personnel dans leurs méthodologies projet… Mais une organisation du panel sur 3 n'estime pas que celle-ci soit suffisante pour assurer une conformité dans la durée.**

Passer d'une phase projet à un fonctionnement au quotidien réserve toujours son lot de complexités. L'engouement, volontaire ou forcé, de la mise en conformité passé, il faudra alors s'assurer de maintenir la dynamique vie privée dans le temps. Et cela s'anticipe !

1/4 des organisations du panel considère **avoir une équipe *«privacy»* adaptée** par rapport aux besoins.

Notre benchmark met en évidence, sans surprise, que la plus grande crainte des acteurs de la filière vie privée des organisations est le manque de ressources une fois la phase projet achevée. Seulement un quart des organisations considère avoir une équipe «*privacy*» adaptée par rapport aux besoins, et la pénurie de compétences sur le marché ne contribue pas à les rassurer. Cela signifie également qu'un investissement plus lourd dans la filière ne permettra pas facilement du jour au lendemain une augmentation des effectifs.

Dès lors, faire fonctionner le *privacy by design* et *by default*, et ce malgré un potentiel manque de ressources est un enjeu, voire l'enjeu clé pour les organisations. Les équipes «*privacy*» ne pourront pas porter à elles seules la conformité de l'organisation au RGPD sur le long-terme. L'eldorado ? Faire de la protection des données personnelles l'affaire de tous et positionner l'équipe «*privacy*» en facilitateur et accompagnateur des métiers :

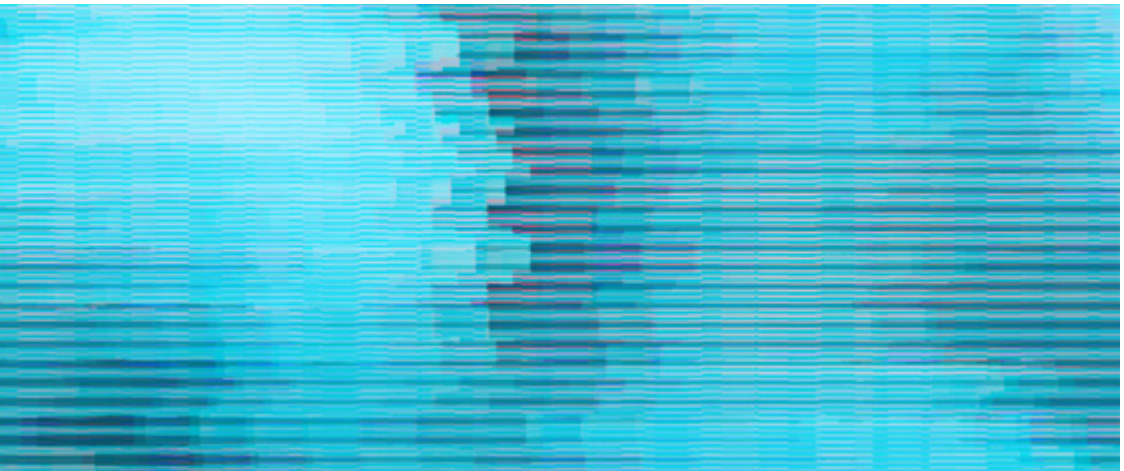
- **Créer une culture du respect de la vie privée en sensibilisant et formant les collaborateurs**. A force de manipuler quotidiennement des données (données bancaires par exemple), les individus n'en perçoivent plus la sensibilité et mettent ainsi la donnée à risque. Il est donc fondamental d'ancrer dans les gestes du quotidien les bonnes pratiques concrètes de protection des données et de faire prendre conscience à ses employés des enjeux autour des données à caractère personnel. En particulier, valoriser auprès des équipes marketing la qualité de la donnée de consentement et leur faire réaliser les gains d'une telle stratégie permettra de réduire les sollicitations non adaptées et donc les réclamations.
- **Au fur et à mesure, le prisme de la sensibilisation doit évoluer.** Les messages passés à date sur le RGPD ont beaucoup tourné autour de la crainte (contrôles, amendes etc.). Pour faire appliquer les bonnes pratiques, il ne suffira pas de communiquer à répétition sur les impacts potentiels d'une non-conformité. Il faudra engager les employés dans la démarche, plus optimiste, **du renfort de la confiance** avec les individus qui confient leurs données à l'organisation. Il faudra également leur donner les outils et les modes opératoires concrets afin d'assurer ce renfort.
- **Responsabiliser les métiers**. La dimension vie privée doit être une composante comme une autre de leur métier et non pas une contrainte. Pour les achats par exemple, maintenir à jour le listing des partenaires à qui nous effectuons des transferts de données ou inclure les clauses RGPD au sein d'un contrat doit être aussi naturel que négocier un contrat. Sur cette thématique, nous observons d'ailleurs un vrai élan positif (91% des organisations du panel ayant effectué le travail d'identification des partenaires, transferts). Pour ne pas gâcher les efforts fournis, il faut maintenir la dynamique dans le temps en capitalisant sur les travaux effectués sur les contrats et en embarquant naturellement la prise en compte du RGPD dans le flux. Un levier pour cela peut consister à ajouter explicitement des objectifs «*privacy*» dans la fiche de poste et/ou la feuille de route des employés.
- **Mettre en œuvre une « *privacy agile* » simple d'utilisation**. Il est essentiel de ne pas alourdir les processus en place plus que nécessaire, sinon la vie privée sera systématiquement perçue comme une contrainte. Le *privacy by design* doit être outillé simplement pour être accessible et compréhensible pour les chefs de projets, afin de leur permettre d'être autant que possible autonome sur le sujet.
- **Se positionner en accompagnateur de l'innovation.** Selon une étude menée par le groupe Infopro pour Wavestone, parue en mai 2019 « la révolution de la data », seulement 37% des sondés considèrent le RGPD comme un atout. Cela représente un risque pour la pérennisation de la conformité. Aussi, la filière «*privacy*» ne doit pas être cantonnée à un rôle de validation du bon respect de la règlementation par les projets, mais être dans un rôle de conseil et de contribution à l'innovation. Pour ne pas brider les métiers et trouver un bon équilibre, il est obligatoire de comprendre leurs problématiques et leurs enjeux et donc de contribuer au déploiement des nouvelles technologies au sein de l'organisation. Pour ce faire, une veille est fondamentale pour anticiper l'identification des nouveaux risques sur les données induites par les solutions innovantes. Typiquement, dans le monde de la grande distribution, il faudra que le DPO monte en compétence sur le marketing digital et les offres d'acteurs comme Google Ad ou Critéo.

Cela permettra de répondre plus rapidement aux questions que se poseront les métiers, de leur soumettre les recommandations en avance de phase, etc. Dans cette optique, pour accompagner les organisations, l'autorité française de contrôle a instauré un laboratoire d'innovation, le LINC, qui anticipe les questionnements et étudie comment concilier innovation et conformité. Le laboratoire a notamment étudié les questions du design des interfaces, des assistants vocaux, etc.

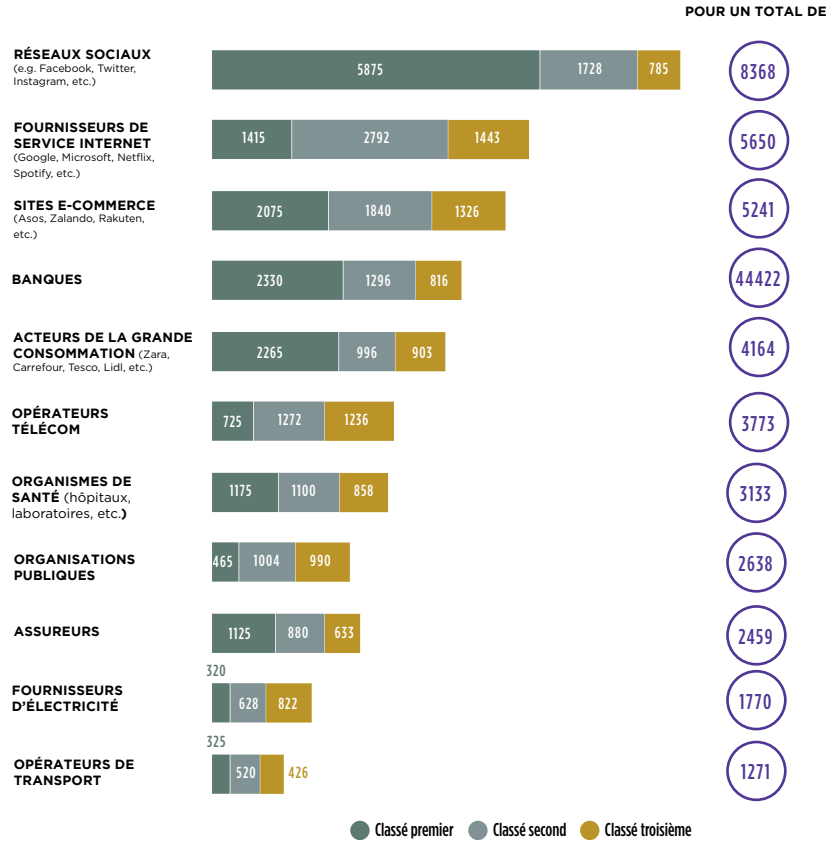
Ainsi, repenser les processus pour assurer le maintien du niveau de conformité va encore demander des efforts aux organisations. Mais la conformité n'est pas une finalité en soi. Le sondage mené auprès des citoyens prouve que leur compréhension du RGPD n'est pas parfaite (pour les trois quarts des sondés). En guise d'exemple, on s'aperçoit que les banques, secteur qui investit le plus dans sa mise en conformité et est le plus habitué à ce genre de programme, ont perdu leur place de tiers en lequel les citoyens ont le plus confiance.

Les **banques** sont historiquement placées parmi les acteurs **bénéficiant le plus de la confiance** des citoyens. En 2016, 51% des interrogés plaçaient la banque en première position en termes de tiers de confiance…

… Comme le démontre le schéma ci-après, aujourd'hui, les banques **ont chuté au 8ème rang** des acteurs de confiance. 10% des sondés positionnent même les banques comme le type d'organisation envers lequel ils ont **le moins confiance**.



À quels types d'organisations faites-vous le moins confiance pour utiliser vos données uniquement dans un but que vous avez approuvé ?



Dès lors, nous comprenons que la conformité à la règlementation n'est pas la condition nécessaire et suffisante pour gagner ou maintenir la confiance des citoyens. Il s'agit aussi de convaincre les individus concernés. Les marques devront innover pour s'adapter à ce changement d'orientation des consommateurs et de comportement d'achat. **La protection de la vie privée est porteuse de valeur pour les organisations qui sauront en faire un argument de vente voire la monnayer mais aussi pour la mise en place de nouveaux modèles et de nouvelles organisations.**

ALLER AU-DELÀ DU RGPD POUR LE RESPECT DE LA VIE PRIVÉE ?

DE VÉRITABLES OPPORTUNITÉS BUSINESS

Le RGPD, et le respect de la vie privée plus globalement, représentent en réalité une véritable opportunité pour les organisations. Il en va ainsi de l'innovation : aux nouvelles contraintes, de nouvelles solutions.

> « L'innovation, les idées novatrices et les nouveaux usages peuvent et même doivent aller de pair avec la protection de la vie privée de l'utilisateur. La réalisation du potentiel de la technologie en dépend »
>
> *TIM COOK, CEO Apple, Magasine Time*

À date, les premières initiatives commencent à voir le jour et font parler d'elles, comme le prouve l'engouement autour des problématiques de vie privée lors de l'édition 2019 du CES. De nombreuses réflexions sont menées autour de nouvelles solutions, de nouveaux business models, plus offensifs, se démarquant sur la protection de la vie privée des citoyens et la maîtrise de leurs données à caractère personnel : en voici quelques exemples.

FAIRE DE LA VIE PRIVÉE UN DIFFÉRENTIATEUR COMMERCIAL

Répondre au défi de la confiance numérique ne doit pas être perçu uniquement comme un enjeu règlementaire ou de sécurité, mais bien comme une transformation en profondeur de la relation client et de la façon dont le numérique est utilisé. **Faire de la vie privée un levier pour vendre plus**, tel serait l'objectif ultime. Aujourd'hui, nous sommes encore dans une phase d'acculturation et d'évangélisation : les citoyens prennent conscience des enjeux liés à leur vie privée. Ils sont ainsi de plus en plus enclins à opter pour des services davantage protecteurs de celle-ci. Mais ce mouvement pourrait être amené à se renforcer.

La confiance est en passe de devenir un marqueur fort de différentiation dans la relation client. Pour cela, quelques pistes sont à envisager. L'enjeu ? Faire toujours preuve de plus de transparence pour bâtir une relation de confiance profonde entre l'organisation et ses clients.

Renforcer la relation client en leur rendant le contrôle de leurs données

Afin de responsabiliser les citoyens sur la gestion de leurs propres données, et afin de faire preuve de toujours plus de transparence, certaines organisations, comme Adidas et Asos, se sont d'ores et déjà dotées de « *privacy centers* ». Un *privacy center* est un espace personnel où l'utilisateur peut consulter et gérer ses informations personnelles, moduler ses préférences et consentements, et exercer ses droits facilement. En rendant l'utilisateur maître de ses données, le *privacy center* est gage de confiance et de transparence de la part de l'organisation, ce qui assure une meilleure expérience client. Cette plateforme, parce qu'elle est automatisée et parce qu'elle est l'unique point d'interaction pour les sujets de protection de la vie privée, **facilite grandement le passage à l'échelle, notamment pour tout ce qui touche aux exercices de droit.**

Cependant, à date, le *privacy center* est un dispositif complexe à intégrer au SI. En effet, celui-ci requiert une parfaite interconnexion entre les interfaces clients (mobile, site internet, physique, etc.) et les différentes bases de données clients existantes (la vision client étant rarement complètement unifiée). Ainsi, la refonte du SI et la mise en place d'une véritable gouvernance de la donnée seront, pour la plupart des organisations dites « historiques », un prérequis de taille. Pour les organisations purement digitales, ayant bâtit leur SI autour de la donnée et du parcours client, la mise en place de ce dispositif est envisageable sur le court terme.

Attention cependant, malgré une amélioration de la relation de confiance avec le client sur le long-terme, la mise en place d'un *privacy center* peut être perçue à première vue comme un risque par les équipes marketing et digital. La mise à disposition d'un outil facilitant l'exercice des droits et en particulier le retrait du consentement peut susciter des craintes. Preuve qu'un véritable changement doit être mis en œuvre et un rythme de croisière « *privacy* » adopté avant d'envisager ces solutions.

Se différencier de ses concurrents grâce à une stratégie marketing orientée vie privée

Comme vu dans la partie précédente, il y a un écart fort entre les efforts fournis par les organisations dans le cadre de leur mise en conformité et la perception des citoyens de ces efforts. Ainsi, il y a un véritable enjeu pour les organisations à **passer d'une dynamique projet de conformité à une dynamique projet de communication et de valorisation des travaux réalisés auprès du grand public**. Un champion en la matière : Apple. Lors du CES de l'édition 2019 à Las Vegas, Apple a mis en place une stratégie de communication offensive pour contrer son concurrent Google. Alors que Google avait envahi la ville d'affiches publicitaires pour promouvoir sa nouvelle technologie d'assistance vocale, Apple s'est contenté d'une affiche imposante mettant en avant leur slogan « *What happens on your iPhone, stays on your iPhone* » avec un lien vers la plateforme *privacy* d'Apple. Apple a pleinement décidé de mettre à profit sa posture forte sur le respect de la vie privée comme un différenciateur face à ses concurrents. Est-ce que l'organisation est avant-gardiste d'une tendance amenée à se généraliser ? Ce ne serait pas la première fois.

L'autorité de contrôle française met actuellement en place **un système de certification qui viendra amplifier ce mouvement**. Deux référentiels en matière de certification de DPO ont d'ores et déjà été adoptés par la CNIL. Dans le long-terme, nous pourrions envisager la mise en place d'un label certifiant la bonne conformité d'une organisation au RGPD. Les réflexions sont en cours au sein des autorités de contrôles.

Ces stratégies marketing participent à la sensibilisation de la population sur l'importance de la vie privée et de comment celle-ci s'applique dans le numérique. Aujourd'hui, pour ceux qui se saisissent du sujet de la vie privée, cela représente un avantage concurrentiel.

À terme, un manque d'attention prêté à la protection de la vie privée des citoyens pourrait devenir un véritable handicap.

FAIRE DE LA VIE PRIVÉE UNE SOURCE DE NOUVEAUX REVENUS

1/3 des sondés serait **prêts à payer pour bénéficier d'une protection accrue de leurs données** et pour **des services davantage protecteurs** de leurs données

Dans notre étude de 2016, Tina A. Larsen (présidente de l'autorité de contrôle du Luxembourg) nous indiquait : « les citoyens souhaitent bénéficier des services générés par la collecte massive des données (services personnalisés, réseaux sociaux etc.) tout en préservant leur vie privée ». Quel équilibre trouver ? Il semble en tout cas nécessaire de donner le choix aux individus.

À la suite de l'analyse des résultats de notre sondage, nous nous sommes interrogés sur le type d'offre à proposer aux 25% de sondés réfractaires au partage de leurs données (« *les privacy absolutists* »). Nous avons ainsi demandé aux sondés s'ils avaient déjà ou s'ils seraient enclins à payer pour bénéficier d'un service plus protecteur de leur vie privée.

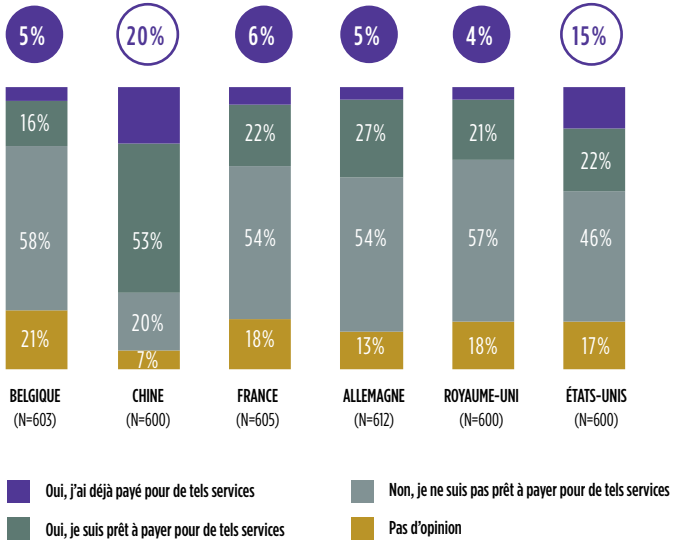
Il semble qu'un mouvement soit bien enclenché au-delà des frontières de l'Europe, comme le démontre le schéma ci-après. En Chine et aux Etats-Unis, une moyenne de 18% des citoyens déclarent avoir déjà payé un frais supplémentaire pour un service davantage protecteur de la vie privée contre 5% uniquement en Europe (incluant le UK). L'Europe est en retard sur l'offre de services protecteurs de la vie privée.

Il y a un véritable virage à prendre. D'autant que la demande existe : 1/3 des sondés serait prêts à payer pour bénéficier d'une protection accrue de leurs données et pour des services davantage protecteurs de leurs données. Le « *privacy-as-a-service* », une piste à creuser ?

En analysant les secteurs pour lesquels les citoyens seraient le plus enclins à payer pour un service protégeant leurs données à caractère personnel, il en ressort que les réseaux sociaux, les services sur internet et les banques sont les secteurs les plus concernés. Pour ces secteurs au moins, il existe de vraies opportunités consistant à proposer des offres innovantes, potentiellement payantes, pour lesquelles la collecte et l'utilisation de données personnelles seraient minimisées et la sécurisation accrue afin de répondre aux attentes de cette nouvelle catégorie de consommateurs. De sorte que comme nous l'avons vu plus haut, sans la proposition de ces nouveaux services, le pourcentage de sondés arrêtant l'utilisation de certains services pourrait continuer à progresser dans les prochaines années. Irons-nous vers un Facebook payant ?

Clairement certains utilisateurs voudront conserver les services gratuits, mais

Seriez-vous prêt à payer un petit supplément ou une petite augmentation de prix pour des produits/services, qui seraient autrement gratuits, en échange de la garantie de votre vie privée ?



accepteront, en connaissance de cause, les publicités qui y seront associées. D'autres seront prêts à payer pour des services plus protecteurs.

FAIRE DE LA VIE PRIVÉE LA BASE DE NOUVELLES OFFRES

Les lois ne sont pas suffisantes pour permettre aux individus de contrôler leurs données et ainsi protéger leur vie privée. Il faut leur donner des outils qui leur permettront de mettre en place des actions concrètes leur permettant de protéger leur vie privée. Nous remarquons d'ores et déjà que de nouvelles organisations se sont créées autour de la protection et la maîtrise de la donnée personnelle. Wavestone s'est intéressé à deux tendances émergentes permettant de redonner confiance : le *self-data* et la 0-collecte de données.

S'engager dans le self-data

L'enjeu est de répondre à la « crise de confiance » causée par l'asymétrie de l'information entre organisations et citoyens, **en replaçant les données dans les mains de ces derniers**. Avec le *self data*, les organisations ont accès aux données mais n'en sont plus propriétaires. Ce sont les individus qui restent propriétaires de leurs données. Cela leur permet de créer de la valeur grâce à de nouvelles utilisations de la donnée, à leur initiative et sous leur contrôle.

D'une initiative lancée par la Maison Blanche en 2011 est né le « *Green Button* » pour le secteur de l'énergie aux Etats-Unis. Celui-ci permet aux citoyens de télécharger leurs données de consommation sous un format standard leur permettant de faire des croisements pour ainsi optimiser leur consommation d'énergie. Il leur offre également la possibilité de rendre automatique le transfert de celles-ci vers des tiers qui ont été autorisés à les recevoir. Cette logique est également mise en place pour la manipulation de données de santé, données particulièrement sensibles, avec le « dossier médical partagé ». Ce dispositif permet à l'individu de gérer finement qui a accès à ses données par exemple, pour permettre un médecin autre que son médecin traitant d'accéder à certaines données de manière temporaire.

Allons-nous vers une généralisation de ce dispositif ?

INTERVIEW COZY CLOUD

BENJAMIN ANDRÉ, co-fondateur et CEO de Cozy Cloud

RESSENTEZ-VOUS UNE PRÉOCCUPATION DES CITOYENS CONCERNANT LEUR VIE PRIVÉE ?

Ce n'est pas véritablement une préoccupation à ce stade sauf pour une minorité (5 à 10% de la population d'après certains sondages). Cette minorité comprend bien la manipulation commerciale dont elle est l'objet et conséquemment le poids du ciblage sur son comportement. Le constat intéressant est qu'aujourd'hui ce ne sont plus spécifiquement les « geeks » qui prennent conscience de cette manipulation mais des profils de plus en plus divers. Cela se traduit pour la grande majorité par un agacement, parfois même une exaspération liée à la sensation d'être un produit. La puissance des géants devient dérangeante, les big tech sont en train de devenir les méchants.

COMMENT CETTE ÉVOLUTION SE TRADUIT-ELLE DEPUIS L'ENTRÉE EN VIGUEUR DU RGPD ?

Je ressens une meilleure compréhension des enjeux, notamment lorsque je donne mon pitch, et je pense que les réactions que je récolte sont un bon échantillonnage de l'ère du moment. Il y a 4 ans, je passais parfois pour un fou : « la confidentialité ça n'intéresse personne », « le modèle GAFA c'est le seul qui fonctionne pour l'internet » etc. Aujourd'hui, ce n'est plus du tout le cas : c'est un marqueur énorme, très tangible.

QUE PROPOSE COZY CLOUD POUR LES AIDER ?

Aujourd'hui, nos données numériques sont dispersées. Notre vie numérique se fragmente du fait de sa diversification : vie scolaire, parcours de santé, interactions avec les pouvoirs publics, objets connectés etc. Ces données circulent dans des écosystèmes étanches les uns aux autres et cela créer une friction. L'usage que l'on peut en tirer est freiné et limité. Pour un numérique utile, pratique, commode et personnalisé, il faut réunir les données. Le fait d'ôter de la friction entre ces écosystèmes étanches, d'ajouter de la simplicité aux usages numériques a une valeur énorme. Tout le principe de Cozy est de **centraliser les données d'un individu dans un cloud personnel, contrôlé par celui-ci, lui permettant d'accéder à de nouveaux services numériques**. Finalement, récupérer ses données c'est le meilleur moyen de mutualiser les données.

QUELS SERVICES PROPOSEZ-VOUS AUX INTERNAUTES ?

Cozy cloud, ce n'est pas seulement un coffre-fort « statique » comme on en voit beaucoup. L'utilisateur centralise ses données sur un cloud personnel **pour pouvoir y adosser des services, pour pouvoir rajouter des usages et effectuer des croisements entre ses données**. Nous appelons cela du « *transverse data* » : communiquer avec ses différents fournisseurs via une plateforme unique, accéder à des nouveaux services purement numériques, tout ceci **en conservant ses données localement dans son coffre-fort numérique.** Nous permettons aux individus d'accéder à un service **sans pour autant céder le contrôle de leurs données.**

ET QUEL APPORT POUR LES ORGANISATIONS ?

On peut valoriser la donnée sans la monétiser pour autant. **Ce qui a de la valeur, ce n'est pas la donnée en tant que tel, c'est plutôt de créer de l'interaction entre les données quand c'est pertinent.** Les organisations doivent le comprendre. Nous nous positionnons comme opérateur d'interactions digitales. Cela leur permet de ne pas être définitivement désintermédiées, mais au contraire d'accéder à davantage de données.

CELA NE PARAIT PAS NÉCESSAIREMENT ÉVIDENT AU PREMIER ABORD : COMMENT LES CONVAINCRE ?

Aujourd'hui, le constat est sans équivoque : les GAFA connaissent mieux les clients des « *brick and mortar* » que les « *brick and mortar* » eux-mêmes. En revanche, les « *brick and mortar* » bénéficient d'une confiance historique. **Nos clients sont des grands comptes, menacés par les puissances du net, qui veulent se repositionner à l'ère du numérique et valoriser cet asset qu'est la confiance.** Dans un premier temps, les organisations pourront avoir la fausse impression de se faire prendre leurs données. Mais en réalité, Cozy Cloud vient les aider à développer des outils et des usages plus intelligents. Soit ces organisations ouvrent le pas, et c'est une bonne chose pour elles, soit c'est Google qui le fera…

Pour les organisations particulièrement matures sur le volet vie privée, une réflexion à ce sujet peut d'ores et déjà être lancée afin de se démarquer. Nous pouvons même imaginer que, dans un futur lointain, les individus pourront faire payer l'accès à leurs données ? Les données personnelles, seraient-elles la nouvelle monnaie ? En Europe, c'est un sujet décrié : l'État protège les citoyens, même possiblement contre leur volonté mais pour le bien commun (à l'exemple de la vente d'organe). Mais cette pratique pourrait être envisagée ailleurs.

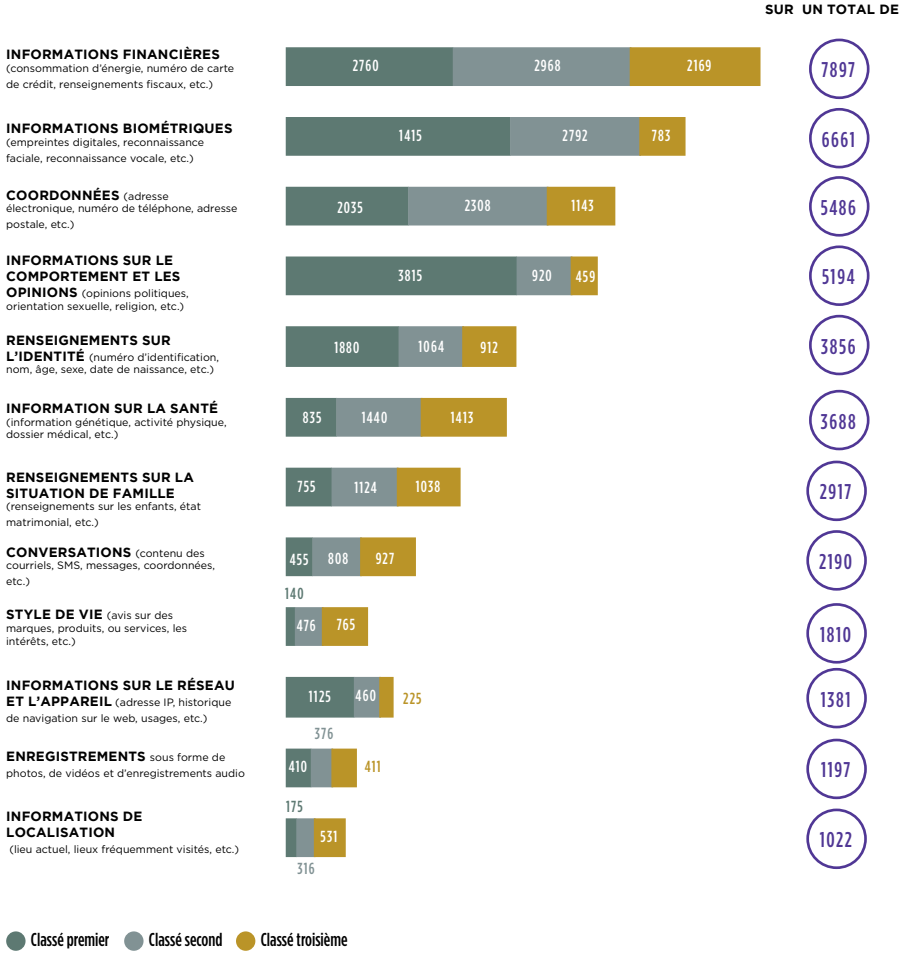
Proposer des services sans aucune collecte de données

À travers notre sondage, nous observons une méfiance marquée envers les organisations du net, notamment envers les réseaux sociaux. Pourquoi ?

/ **Les citoyens semblent attacher toujours plus d'importance à leur e-réputation**. Dans son bilan annuel, l'autorité française souligne l'augmentation de plaintes concernant la diffusion de données sur Internet (37,5% de la totalité des plaintes). Aller à l'encontre des business models des géants du Net et proposer un service en rupture est donc véritablement une opportunité business.

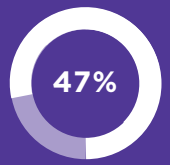
/ Autre constat du sondage, nous observons **une tendance pour l'anonymat**. En effet, du fait de leur statut de « porte d'entrée » dans l'intimité, que ce soit physique ou numérique, les données de contact et d'identité sont les données les plus citées lorsque l'on demande aux citoyens les données qu'ils considèrent comme privées (comme le démontre le schéma ci-après). Elles sont même plus citées que les données sensibles au sens du RGPD (données de santé, localisation etc.).

Parmi les catégories de données ci-dessous, lesquelles considérez-vous comme les plus privées ?

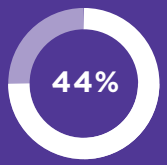


Plus concrètement, nous observons d'ores et déjà l'adoption par les citoyens de nouveaux usages pour préserver leur anonymat et protéger leur vie privée Ainsi, développer des services alternatifs permettant à l'individu de préserver son anonymat peut représenter une véritable opportunité. Cela dénote l'importance que l'anonymat pourrait prendre dans les prochaines années.

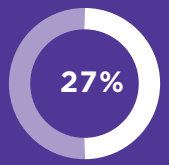
DE NOUVEAUX USAGES POUR PRÉSERVER L'ANONYMAT



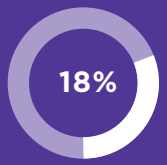
des sondés suppriment les **COOKIES** lors de leur visite sur des sites web



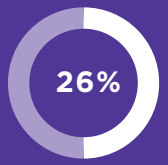
des sondés gèrent les **PARAMÈTRES DE CONFIDENTIALITÉ** (ce qui inclue le retrait de consentement)



des sondés utilisent le **MODE INCOGNITO**



des sondés utilisent des **OUTILS DE CYBERSÉCURITÉ** pour protéger leurs données (VPN, etc.)



des sondés **A ARRÊTÉ D'UTILISER CERTAINS SERVICES** afin de **PROTÉGER** et **GARDER LA MAÎTRISE** de leurs **DONNÉES** à caractère personnel

INTERVIEW QWANT

TRISTAN NITOT,
VP advocacy chez Qwant

QU'EST-CE QUE QWANT ?

Qwant est une société française dont le premier produit est un moteur de recherche possédant deux particularités.

La première est qu'il respecte la vie privée de ses utilisateurs : il ne laisse pas de cookies et **ne collecte aucune donnée personnelle**. La deuxième est qu'il est souverain et européen. Il couvre l'ensemble des langues européennes et répond à la nécessité stratégique d'avoir un moteur de recherche en Europe car chacune des grandes puissances possède son propre moteur de recherche. En somme, Qwant se positionne comme un acteur numérique responsable, au business model raisonnable et éthique.

COMMENT EST ACCUEILLI L'INITIATIVE DE QWANT PAR LES CITOYENS ?

L'initiative Qwant est bien accueillie, nous ressentons parfois même un véritable soulagement de la part des citoyens. Néanmoins, la sensibilité au sujet du respect de la vie privée numérique reste encore trop peu développée à mon sens. Bien sûr, nous remarquons une certaine prise de conscience : le RGPD est un sujet de discussion et les derniers scandales ont eu une véritable valeur pédagogique (on l'a remarqué par exemple à la hausse de la fréquentation de Qwant à la suite de la médiatisation de l'affaire Cambridge Analytica). Cependant, il y a encore un long chemin à parcourir, une véritable hygiène du numérique à adopter. De façon quasi systématique je me sens encore obligé d'expliquer à mes interlocuteurs le business model des géants de l'internet. **Ce que les individus ne réalisent pas c'est qu'ils sont utilisateurs et non pas clients d'un service dont le véritable client est l'annonceur publicitaire.**

QUEL AVENIR POUR LES MOTEURS DE RECHERCHE ?

Aujourd'hui l'économie numérique suit une logique de centralisation. Les quelques géants du web, type Google ou Facebook, récoltent un maximum de données personnelles par défaut afin d'acquérir une connaissance pointue de ses usagers et ainsi personnaliser et améliorer son service. **Cette collecte va à l'encontre de tout principe de minimisation.** Ce n'est pas une solution viable car cela va à l'encontre des libertés individuelles, c'est toxique pour la société. Et c'est pour cela qu'il est nécessaire, je pense, de proposer des alternatives qui assurent le respect de la vie privée.

COMMENT EST-CE QUE VOUS SITUEZ FACE À CE CONSTAT ?

Si nous voulons mettre en place un numérique pérenne, il faut reconstruire une relation de confiance avec les usagers et ainsi respecter leur droit à la vie privée. C'est en décentralisant et en minimisant la collecte de données par défaut que ce sera possible. Qwant se positionne ainsi comme une nouvelle génération de service qui respecte la vie privée de ses usagers, qui est éthique et nous l'espérons, pérenne.

UN BUSINESS MODEL RESPECTUEUX DE LA VIE PRIVÉE, C'EST NÉCESSAIREMENT UN MODÈLE SANS AUCUNE COLLECTE DE DONNÉES À CARACTÈRE PERSONNEL ?

Pas nécessairement. Il faut cependant laisser aux citoyens le choix et le contrôle. Qwant développe actuellement un nouveau produit appelé Masq, qui enregistre localement vos recherches successives sur votre ordinateur ou smartphone. L'utilisateur est donc le seul à avoir accès à son historique et cela permettra au moteur de recherche d'affiner ses suggestions.

CONCLUSION

La révolution de la donnée ne se fera pas sans la confiance…

Le numérique suscite des craintes pour les citoyens. A cela s'ajoute l'émergence d'associations de consommateurs qui se positionnent pour les aider à préserver leur vie privée sur le Net. Les autorités de contrôle renforcent également leur régulation afin de les protéger face à des organisations toujours plus consommatrices de données. Le but ? Leur permettre de préserver leur intimité numérique.

Pour les organisations, **il est ainsi grand temps de faire du digital autrement.** La grande majorité des organisations l'a d'ores et déjà compris : la révolution de la donnée ne se fera pas sans la confiance. Ainsi, nous observons une dynamique en place au sein des entreprises et des efforts pour minimiser la collecte de données, qualifier les bases de données grâce à la collecte d'un consentement éclairé quand nécessaire, faire preuve de transparence sur les traitements effectués et responsabiliser les citoyens sur leurs données en leur offrant la possibilité d'exercer leurs droits. La relation de confiance est un lien fragile, ainsi, afin d'instaurer une confiance durable sur le futur il sera essentiel de respecter ses engagements sur le long-terme.

De l'ère de la donnée, avec une collecte basée sur une approche massive et l'affleurement de business models basés sur leur revente, nous passons à l'ère de la confiance. Et cette transition s'exprime à travers notre sondage : les citoyens seront de moins en moins enclins à partager leurs données avec les tiers qu'ils ne considèrent pas de confiance. Aujourd'hui, les acteurs historiques peuvent capitaliser sur une confiance historique du grand public là où les acteurs digitaux disposent d'une maîtrise plus importante de la donnée et par extension de la connaissance des clients. Nous anticipons la convergence de ces deux mondes dans un futur proche.

… Il s'agit désormais de réfléchir à de nouveaux leviers pour faire de la confiance le cœur de la relation client, au-delà de la simple conformité

Le RGPD, par nature, est un règlement qui incite à la collaboration de profils variés au sein des organisations, et des profils qui n'avaient jamais été amenés à travailler ensemble par le passé ! **Il est ainsi crucial pour les organisations de capitaliser sur cette dynamique positive**. Le but ? Repenser ensemble les usages faits des données afin **d'imaginer la relation client de demain : plus symétrique, source de confiance et de croissance économique.** Il faut investir avant qu'il ne soit trop tard !

The Positive Way

WAVESTONE

www.wavestone.com