ASUWISH
Marketing Thinking

RGPD

et si on en faisait une opportunité ?

V 1.1

AVRIL 2018

Accélérateur de projets AsUWish est une structure de fertilisation pour révéler et stimuler des initiatives dans les domaines de la communication et du marketing.

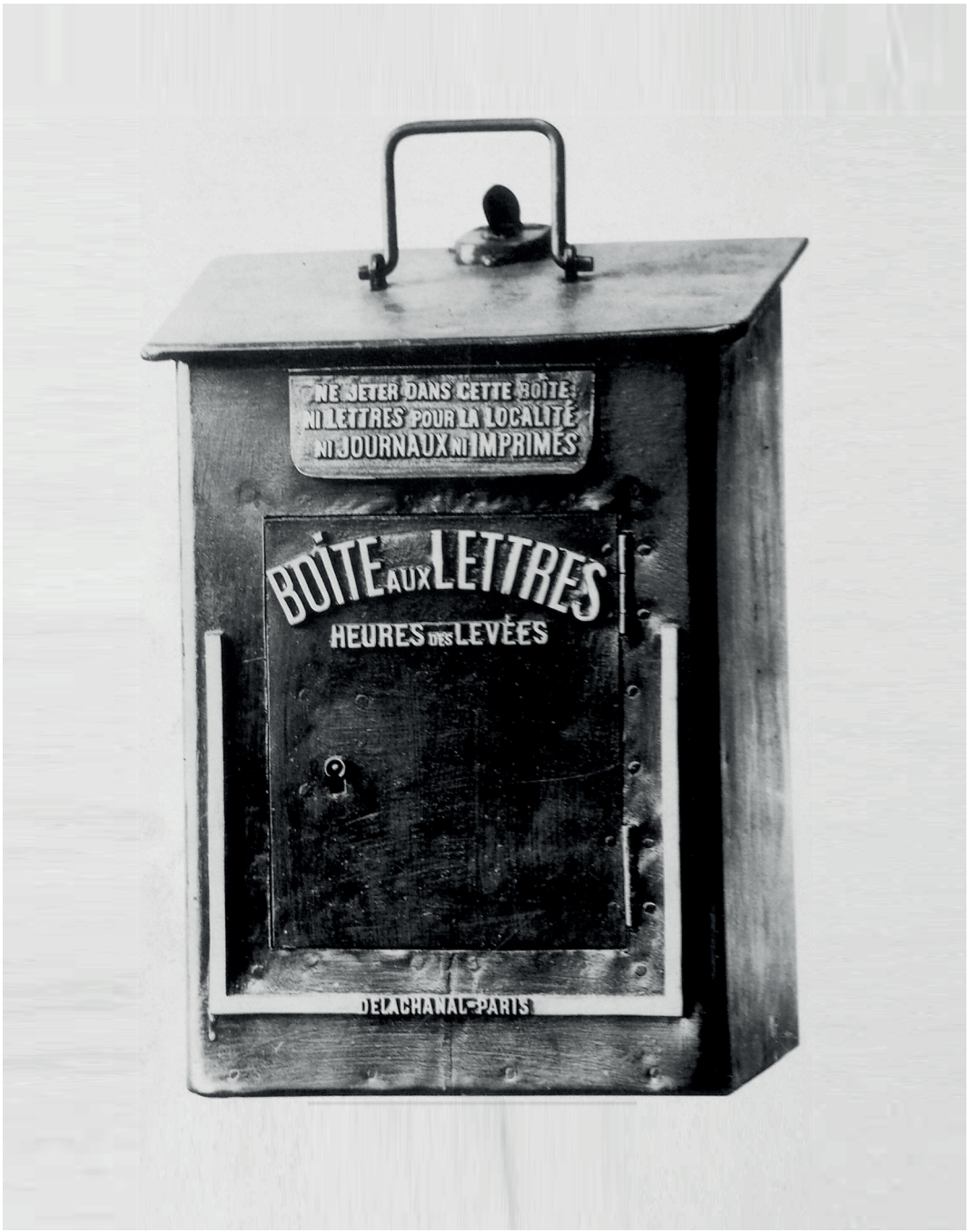
Avec une vision stratégique du secteur, AsUWish et ses 40 experts mettent leurs compétences en commun afin de rendre manifeste une idée.

Tel un accompagnant, le groupe apporte sa vision entrepreneuriale, son analyse de l'environnement, ses conseils en stratégie marketing et communication, ses méthodes, et une optimisation de la visibilité et de l'attractivité via son réseau local et national.

arcange klub casusbelli ÅSGARD BANGARANG

***Sébastien Finot**, Directeur technique associé Casus Belli*
*& **Jérôme Caudrelier**, Directeur associé As U Wish*

SOMMAIRE



INTRODUCTION

Bienvenue dans un nouveau monde

« Si c'est gratuit c'est vous le produit » …
« La donnée est le nouvel or noir du 21e siècle[1] »

Autant d'affirmations synonymes de tentatives d'assimilations des citoyens-consommateurs à des puits de pétrole en puissance. Les GAFAM[2] et autres BATX[3] sont explicitement visés par le RGPD qui ambitionne de remettre de l'ordre dans ce far-west numérique en imposant aux organisations de faire le tri entre les bonnes et les mauvaises pratiques en matière de collecte et d'utilisation des données.

Jusqu'à présent, le consentement est plus ou moins explicite en bas d'un formulaire ou pour valider des Conditions Générales d'Utilisation (CGU). L'utilisateur n'a qu'une connaissance réduite, voire inexistante, des traitements qui peuvent être effectués avec ses données car la description de leur utilisation est noyée dans ces CGU qui sont validées trop souvent sans les lire.

De la même façon, il n'est pas rare que des données dont l'usage n'est pas encore défini soient demandées dans un formulaire en prévision d'une exploitation ultérieure. Par exemple, une date de naissance pour une inscription à un site de e-commerce dont le contenu n'a pas de caractéristique nécessitant de s'assurer de la majorité du client. Mais on ne sait jamais, des fois qu'on veuille lui faire une offre spéciale pour son anniversaire… Et bien ce règlement met un terme à ces pratiques.

Que ce soit dans des CGU ou dans un formulaire, il faudra expliciter à l'utilisateur le champ d'affectation de ses données et obtenir son consentement.

Alors qu'internet croule sous un nombre croissant d'articles rivalisant sur les meilleures façons d'être le moins impacté par le règlement, nous vous proposons de porter un autre regard. Comme bien souvent, cette menace réglementaire sera, à n'en pas douter, une formidable opportunité pour les structures qui sauront rapidement prendre position dans ce nouveau terrain de jeu. Cette menace est une invitation à changer d'angle…

[1] *On estime qu'en 2020, les données personnelles en Europe auront une valeur de 1trillion d'euros par an https://www.zettabox.com/sites/default/files/data-protection-big-data_factsheet_web_en.pdf*
[2] *GAFAM : Google, Apple, Facebook, Amazon, Microsoft*
[3] *BATX : Pendants chinois des GAFAM, Baidu, Alibaba, Tencent et Xiaomi*

LE RGPD, QU'EST-CE QUE C'EST ?

Le RGPD (Règlement Général sur la Protection des Données[4]) définit, au niveau européen, les nouvelles règles concernant la gestion des données personnelles. Il sera mis en application à compter du 25 mai 2018. A cette date, vous devez être en règle.

Il définit, précise et renforce un certain nombre de droits et de devoirs relatifs à la protection et gestion des données personnelles au sein de l'Union Européenne.

Le texte commence d'ailleurs par rappeler que cette protection est un droit fondamental de l'Union Européenne. Cette prise de position, forte, a guidé la conception de ce nouveau règlement.

Le RGPD est un texte long qui parfois exige, souvent conseille, suggère ou indique ce que les pays membres, les autorités de contrôle, les entreprises, les pouvoirs publics et les sous-traitants doivent faire. Cependant, les zones d'ombre et de flou sont nombreuses et demanderont à être précisées avec le temps.

Sanctions

Les sanctions maximales encourues en cas de non-respect du RGPD sont pour le moins dissuasives : jusqu'à 4% du chiffre d'affaires annuel mondial ou 20 millions d'euros (la plus élevée des deux étant retenue).

Ces sanctions viennent, bien entendu, en plus de celles qui pourraient viser les responsables ou dirigeants qui contreviendraient à d'autres lois (telles que la loi Informatique et Libertés) et dont les sanctions peuvent, au maximum, atteindre 5 ans de prison et 300 000 euros d'amende.

On pourra également y ajouter les éventuels dommages et intérêts suite à un recours en justice pour préjudice subi pour non respect du RGPD.

Il est donc impossible d'ignorer le RGPD ou de retarder sa mise en conformité. Rappelons que, en théorie, il y a eu 2 ans de préparation depuis son adoption le 14 avril 2016.

[4] *En anglais, GDPR pour General Data Protection Regulation*

À qui s'applique le RGPD ?

Le RGPD s'applique à toute organisation qui traite des données personnelles de résidents européens, indépendamment de leur taille, secteur ou si elles sont publiques ou privées.

Il n'y a que les particuliers, et seulement dans un cadre parfaitement non lucratif (ie, sans affichage de publicité, sans revente de données, sans partenariat, etc.), qui en sont exemptés.

Les sociétés (et les personnes qu'elles emploient) sont toujours concernées, même si la collecte est réalisée dans un but non lucratif.

Objectifs du RGPD

Le RGPD poursuit trois objectifs principaux :

- Harmoniser la réglementation européenne sur la protection des données personnelles des résidents européens.
- Renforcer le droit des personnes sur leurs données.
- Responsabiliser les acteurs de la collecte et du traitement des données personnelles, notamment au niveau de la sécurité.

Une évolution plus qu'une révolution

Au début des années 1970, la révélation d'un projet de centraliser toutes les données administratives de chaque Français dans un fichier unique mit en lumière les dérives potentielles de l'informatique. Cet événement contribua à donner naissance à la première version de la loi Informatique et Libertés (en 1978) dont le but est de s'assurer que l'informatique reste au service des Français et ne puisse pas être utilisée afin de porter atteinte à leurs droits et les protéger (autant que possible) du fichage administratif et policier.

Cette loi sera réformée plusieurs fois, et notamment en 1995 pour intégrer la directive européenne 95/46/CE, qui posait les bases de la protection des données à caractère personnel au niveau européen. C'est cette directive que le RGPD vient dépoussiérer.

Cependant, une partie conséquente du RGPD existe déjà dans la loi Informatique et Libertés, que l'on connaît souvent plus de nom que ce qu'elle offre ou exige concrètement.

Un projet de loi transposant le RGPD dans la loi Informatique et Libertés a été présenté par le gouvernement en décembre 2017 et globalement validé par la CNIL, chargée de s'assurer du bon respect de nos droits dans le cadre des données personnelles.

[5] *Dans le reste de ce livre blanc, nous remplacerons souvent cette longue liste par "les entreprises".*

Harmonisation européenne

Rappelons que le RGPD s'applique à toutes les entreprises, pouvoirs publics ou associations qui traitent des données personnelles[6] des résidents de l'Union Européenne (et donc y compris les entreprises situées hors de l'UE).

Il définit les règles à respecter a minima au niveau européen. La France, bien pourvue et leader sur le sujet sera modérément impactée. D'autres pays, moins bien protégés, profiteront donc de ce rehaussement des standards.

Le RGPD permet également aux états membres d'appliquer des règles plus strictes et plus protectrices (soit parce qu'elles existent déjà, ou parce qu'elles seront créées ultérieurement). Appliquer le RGPD n'est donc pas la garantie absolue d'être en règle dans tous les pays de l'Union sur les données personnelles.

À noter que le Royaume-Uni est également concerné pour l'instant, en dépit du Brexit. En effet, tout continue de s'appliquer tant que la rupture n'est pas effective. Après le Brexit, il est plus que probable que le RGPD continue de s'y appliquer, ne serait-ce que pour pouvoir continuer de traiter des données des résidents européens.

[6] *Les entreprises de moins de 250 personnes qui réalisent des traitements occasionnels peuvent être dispensées d'une partie des obligations, notamment le registre des traitements mais la CNIL recommande de ne pas s'en priver. Et comme c'est elle qui contrôle…*

Renforcement des droits des utilisateurs

Consentement renforcé et transparence

Il ne suffit plus de rajouter une case à cocher au bas des formulaires pour pouvoir traiter les données. Le RGPD définit que les utilisateurs doivent être informés du traitement qui sera réalisé sur leurs données et à qui elles seront éventuellement communiquées.

La matérialisation de ce consentement doit être non ambiguë et doit pouvoir être prouvée en cas de contrôle.

Si les formulaires sont bien entendu visés par cette mesure, c'est surtout les achats de base de données, les emailings de prospection sauvage ou les traitements de données non explicités qui seront les plus impactés.

C'est d'autant plus vrai que les droits d'accès, de rectification, d'effacement, d'oubli et d'opposition sont renforcés.

Droits sur ses données

Le RGPD monte au niveau européen la barre des droits des utilisateurs sur leurs propres données. On y trouve maintenant l'équivalent (à quelques nuances près) de notre droit d'accès et de rectification.

Rappelons que ce droit comprend aussi le droit de demander d'effacer les données personnelles qu'une entreprise peut avoir sur le demandeur.

Le droit à la portabilité est ajouté. Il permet aux utilisateurs de récupérer leurs données sous une forme exploitable et structurée, pour éventuellement les confier à un autre responsable du traitement.

Il consacre également le droit à l'opposition sur un traitement et le droit de changer son consentement, et facilite l'expression de ces droits.

Tous ces droits sont nuancés par un certain nombre d'exceptions, notamment en cas d'obligation de traiter des données (par exemple, un employeur doit traiter les données de ses employés pour pouvoir remplir le contrat qu'il a avec eux).

Droit des enfants

L'information sur les traitements de données qui concernent les enfants de moins de 16 ans doit être rédigée en des termes simples et clairs, facilement compréhensibles par l'enfant. Cependant, le consentement doit être donné par le responsable de l'autorité parentale.

Responsabilisation des acteurs

De mémoire d'agence, nos clients nous ont rarement (voir jamais) demandé de collecter moins de données sur les utilisateurs, malgré nos suggestions et conseils. Que les raisons fussent bonnes ou mauvaises, le résultat demeure le même : la collecte des données personnelles a rarement été très raisonnée.

Ce temps de collecte insouciante est terminé puisque le RGPD exige que seules les données réellement utiles au traitement soient demandées à l'utilisateur. Demander l'adresse postale pour une newsletter électronique risque de ne plus passer. C'est la minimisation des données qui est ainsi inscrite dans la loi.

Le RGPD demande aussi qu'un effort conséquent soit réalisé pour la protection de la vie privée. Cette protection est attendue tant d'un point de vue organisationnel que logiciel et, surtout, dès la conception[7] !

Les éléments attendus de la sécurité couvrent notamment que :

- Les entreprises devront s'assurer que seules les personnes qui doivent avoir accès aux données y aient bien accès.
- La sécurité des serveurs et réseaux doit être garantie, notamment contre le piratage.
- La pseudonymisation et l'encryption des données sont plus qu'encouragées.

Attention, toutes ces demandes sont à nuancer en fonction des risques liés aux données personnelles spécifiques concernées. Hélas, le texte ne donne aucune indication de comment ces nuances sont évaluées ou évaluables. Cependant, on peut imaginer que la collecte d'un simple e-mail pour l'envoi d'une newsletter sera moins sensible que le fait d'avoir nom, prénom, adresse postale et scan de la pièce d'identité.

En cas de contrôle, il faudra pouvoir démontrer à la CNIL que tous ces points ont été respectés. Cela passe notamment par la tenue d'un registre des traitements, établi dès le début d'un projet, et mis à jour régulièrement.

[7] *privacy by design, privacy by default en VO*

Registre des traitements

Ce registre doit contenir principalement la liste des traitements réalisés, la finalité et les destinataires de ces traitements, mais aussi les mesures de sécurité organisationnelles et techniques mises en oeuvre ou la durée de conservation des données personnelles.

Pour faciliter la mise en œuvre de toutes ces problématiques, la CNIL recommande (et l'exige dans certains cas) la nomination d'un délégué à la protection des données (Data Protection Officer ou DPO en anglais). Interne ou externe à l'entreprise, ses missions comprennent notamment :

- Informer, conseiller, former les responsables du traitement, les sous-traitants et les employés qui traitent des données personnelles sur leurs obligations.
- S'assurer que le RGPD et les lois liées à la protection des données personnelles soient bien respectés.
- Coopérer avec l'autorité de contrôle et faire office de point de contact.

La CNIL et le RGPD encouragent les entreprises à nommer un DPO même si elles n'y sont pas obligées.

Le DPO participera également aux "études d'impacts sur la vie privée". Pour certains types de données (notamment les données sensibles), pour certaines finalités, ou lorsque le risque de violation des droits à la protection des données est élevé, une étude d'impact doit être menée au préalable. Elle doit comprendre, en plus de l'évaluation des risques, une approche méthodologique, technique et organisationnelle pour réduire la portée des risques évalués. Cette étude doit être soumise à la CNIL pour validation avant de pouvoir commencer le projet.

Enfin, en cas de piratage de données, la CNIL et les utilisateurs concernés doivent être avertis 72h après la violation des données. Sachant que, généralement, la violation des données ne laisse pas toujours de trace ou de dégât, on est en droit de se demander comment cette mesure sera concrètement applicable. Quoi qu'il en soit, si la découverte du piratage intervient après cette durée, il faudra motiver les raisons du retard (on imagine que les négligences seront un élément négatif dans l'évaluation des conséquences).

Le cas des sous-traitants

Avant le RGPD, les sous-traitants, étaient souvent masqués derrière le responsable du traitement et étaient rarement inquiétés légalement en cas de problème. Le RGPD change radicalement la donne puisque chaque entreprise devra s'assurer (contractuellement) que chacun de ses sous-traitants respecte et est capable de faire respecter le RGPD.

Le contrat devra de plus comprendre des informations sur l'objet, la durée, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées et préciser les tâches et responsabilités spécifiques du sous-traitant.

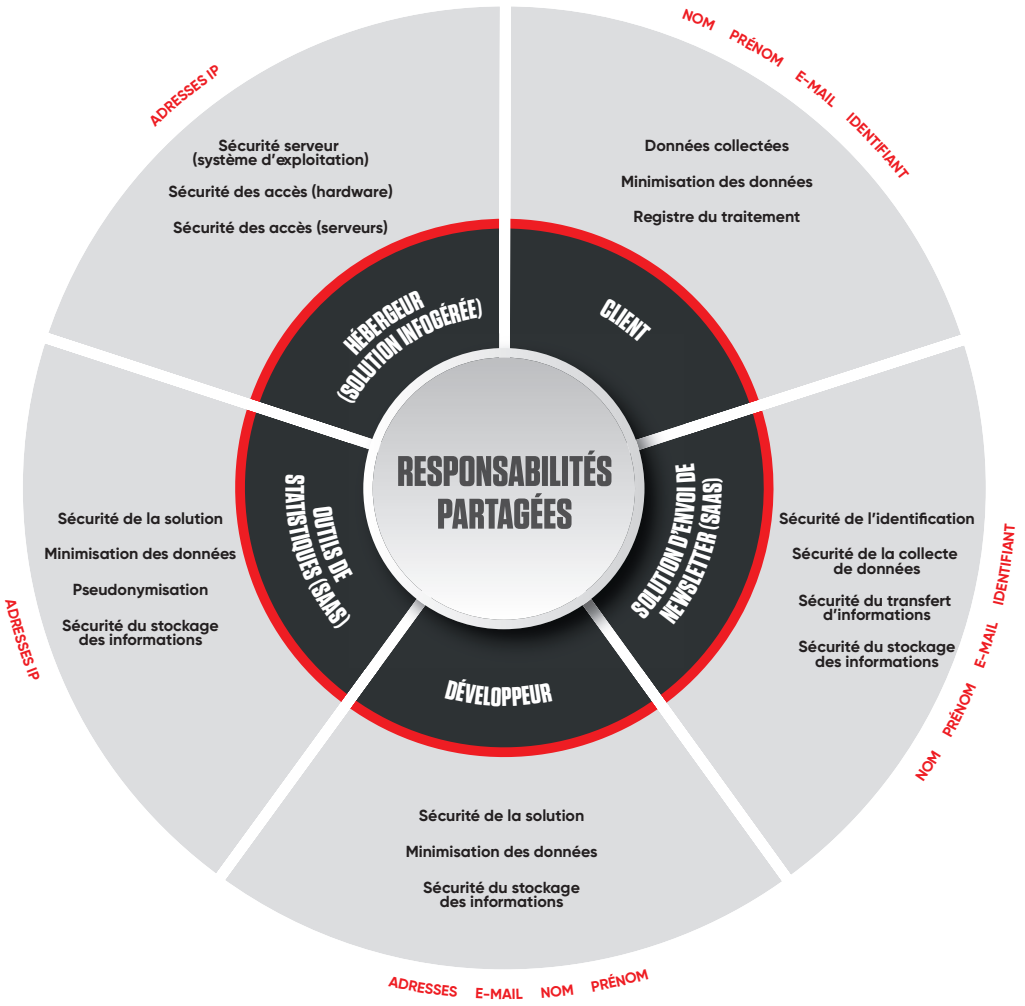
Le sous-traitant doit par ailleurs s'engager à renvoyer ou supprimer les données personnelles une fois le traitement terminé.

Et si d'aventure, le sous-traitant fait appel à un autre sous-traitant, la chaîne de la responsabilité ne s'arrête pas.

Des responsabilités partagées

Les responsabilités de chaque intervenant vont être beaucoup plus partagées du fait du RGPD.

Par exemple, pour un site “simple” qui permet de s’inscrire et de gérer ses listes de courses, les responsabilités pourraient se répartir de la façon suivante :



EXEMPLE CONCRET

Exemple concret

Un exemple récent pour mettre en lumière l'intérêt de protéger des données personnelles anodines en apparence.

Le 27 mars 2018, la CNIL a mis en demeure Direct Energie pour une absence de recueil de consentement concernant les données issues du compteur[8].

Après un contrôle inopiné, la CNIL a constaté que le consentement des clients n'était pas recueilli dans des conditions attendues puisque le consentement au traitement de données personnelles n'était pas libre, éclairé et spécifique.

La CNIL reproche à Direct Energie d'avoir demandé au gestionnaire du réseau de distribution de lui communiquer les données de consommation de ses clients à la journée et à la demi-heure suite à l'activation du compteur Linky.

La CNIL considère que cette collecte n'est aucunement la conséquence nécessaire de l'activation du compteur. En outre, la finalité de « facturation au plus juste », affichée lors du recueil du consentement, n'est pas exacte puisque Direct Energie ne propose pas d'offres basées sur la consommation horaire. Enfin, la cadence précise de la remontée des données de consommation, par demi-heure, n'est pas indiquée au client.

Elle reproche également à Direct Energie de ne pas avoir demandé l'accord de ses clients au préalable.

Elle base son avis sur le fait que ces données peuvent en effet révéler de nombreuses informations relatives à leur vie privée (heures de lever et de coucher, périodes d'absence ou nombre d'occupants du logement).

Cet exemple est très révélateur de ce que le RGPD tente de faire respecter : la vie privée des utilisateurs, y compris lorsque ceux-ci ne sont pas au courant des risques ou des enjeux.

[8] *https://www.cnil.fr/fr/direct-energie-mise-en-demeure-pour-une-absence-de-consentement-concernant-les-donnees-issues-du*

CONCRÈTEMENT ÇA DONNE QUOI ?

Un état d'esprit avant tout

Au-delà de la loi et des obligations que le RGPD représente, la meilleure manière d'appréhender ce texte est de le considérer comme un contrat qu'une entreprise va passer avec ses utilisateurs.

Les termes de ce contrat étant "nous vous demandons de nous confier vos données personnelles dans un but clair et précis et nous nous engageons à ne pas dévier de ce but. Nous nous engageons également à tout mettre en oeuvre pour garantir le respect de votre vie privée et la sécurité de vos données".

En somme, une approche noble et vertueuse à laquelle l'utilisateur est en droit de s'attendre. Pour les entreprises qui le font déjà, il est cependant primordial de communiquer sur le sujet, intelligemment et pertinemment.

Collecte de données

Nous l'avons déjà évoqué, tout traitement (et la collecte en est le premier) ne peut être réalisé que si l'utilisateur a donné son consentement de manière claire et explicite, avec une information préalable.

La crainte, immédiate, est que les utilisateurs ne donnent pas leur consentement.

Dernièrement, le mouvement #DeleteFacebook né du dernier scandale de transmission illégitime de données a de nouveau braqué le projecteur sur ce réseau social qui, depuis toujours, peine à légitimer sa boulimie de données personnelles, pas toujours récoltées de manière très éclairée.

Certains utilisateurs de Google s'émeuvent également des données parfois collectées de manière tout aussi irraisonnée. D'ailleurs, le moteur de recherche Duck Duck Go[9] se positionne exclusivement sur le respect de la vie privée de ses utilisateurs : "Notre politique de confidentialité est simple : nous ne collectons ou ne partageons aucune de vos informations personnelles. Nous n'avons donc rien à vendre aux annonceurs qui vous pistent sur internet."

Entre fatalisme et agacement des utilisateurs sur l'exploitation non consentie de leurs données, la grogne continue de s'installer.

Pourtant, des internautes autorisent certains sites à afficher des publicités, malgré leur bloqueur de publicité et des utilisateurs de logiciels leurs permettent de remonter des statistiques d'utilisation anonymes.

[9] *https://duckduckgo.com/*

L'utilisateur final n'est pas aussi idiot que certains aimeraient le croire. Il peut ne pas être au fait de certains usages, ignorant de certaines pratiques, mais lorsqu'on prend le temps de lui expliquer le pourquoi des choses, il peut prendre la bonne décision.

C'est d'autant plus vrai que, RGPD oblige, l'utilisateur sera de plus en plus sensibilisé à ces problématiques, tant sur leur nécessité que sur ses droits. Jouer effectivement la carte de la transparence et de la minimisation ne pourra avoir que des effets bénéfiques sur la relation avec l'utilisateur.

Rappelons également que le RGPD oblige les entreprises à expliquer à qui ces données seront transmises. Paypal a récemment publié ces informations[10] et on arrive à un édifiant total de plus de 600 partenaires différents à travers le monde…

Les aventuriers des données perdues

Il faut savoir que, parfois, les entreprises collectent des données personnelles sans le savoir. En effet les serveurs web, dans leur configuration par défaut, conservent souvent l'adresse IP[11] de l'utilisateur dans les logs. En théorie, cette collecte indirecte doit être autorisée par l'utilisateur.

Sécurité des données

Indépendamment de l'étude d'impact qui doit être validée par la CNIL lorsque l'on traite des données sensibles, chaque projet existant ou à venir nécessitera d'évaluer les risques liés au traitement des données personnelles.

Cette évaluation est volontairement très large et couvre tant les impacts potentiels sur la vie privée des utilisateurs que les vecteurs d'attaque potentiels ou dégradations accidentelles.

De cette évaluation découlera les solutions techniques et opérationnelles à mettre en œuvre pour minimiser les risques identifiés.

Toujours dans l'esprit de redonner de la confiance il peut être judicieux d'expliquer à l'utilisateur les mesures mises en œuvre pour assurer la sécurité de ses données et la limitation des gens qui y ont accès.

[10] *https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list*
[11] *Oui, l'adresse IP est une donnée personnelle, puisque le FAI peut identifier la personne grâce à celle-ci (http://curia.europa.eu/juris/document/document.jsf?docid=184668):*

Portabilité des données

À la base, ce droit est là pour permettre aux utilisateurs de transférer leurs données d'un service à un autre. Les données doivent être envoyées sous une forme structurée, couramment utilisée et lisible par machine[12].

Le texte encourage les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données et permet la transmission directe d'un responsable du traitement à un autre, lorsque c'est possible. On imagine, par exemple, que cette portabilité automatisée des données pourrait être mise en œuvre lorsqu'un utilisateur change d'opérateur téléphonique.

L'export est donc obligatoire, mais pas l'import. Néanmoins, mettre en place des mesures pour faciliter l'import depuis des responsables du traitement concurrents (soit de façon automatisée, soit manuellement) sera potentiellement un élément différenciant également.

Droit d'accès, de rectification à l'effacement et à l'oubli

Ce point étend sensiblement le droit d'accès et de rectification des données existantes. Le texte incite les entreprises à fournir ce service par voie électronique et dans "les meilleurs délais", avec un maximum d'un mois pour y répondre.

Comme auparavant, une personne a le droit de demander si des données personnelles la concernant sont traitées, et de quelle manière. En théorie, après le RGPD, elle devrait déjà le savoir.

Elle peut également demander à ce que ses données soient rectifiées. À noter que, dans le cas où les données sont transmises à d'autres responsables du traitement, les modifications et effacements doivent leur être notifiés également.

Attention aussi au temps de réponse, qui doit être au maximum de 1 mois. Si la demande est particulièrement complexe, le délai peut être prolongé de 2 mois en notifiant l'utilisateur au préalable.

Plus particulier, les données doivent être exactes sinon le responsable du traitement a l'obligation de les rectifier ou de les effacer. Dans quelle mesure le responsable peut savoir que ces données ne sont plus correctes ? C'est un des mystères qui restera à éclaircir.

Quoi qu'il en soit, ce droit fourni aux utilisateurs sert également aux entreprises puisque cela leur permet d'être certaines que leurs données sont globalement correctes.

[12] *Les formats XML ou JSON sont les plus évidents.*

Les changements mesurés

Certains sujets sont plus ou moins impactés, retour rapide sur les plus courants.

Cookies

En soi, le cookie[13] n'est pas une information personnelle mais son utilisation est largement couverte, notamment par la directive européenne 2009/136/CE transposée dans la loi Informatique et Libertés en France[14].

En substance, dès que l'utilisation du cookie n'est pas indispensable à la délivrance d'un service expressément demandé par l'utilisateur, il faut l'informer et lui demander son consentement préalable.

Le RGPD ne change rien à ces règles. Pour rappel, la durée de vie maximale d'un cookie doit être de 13 mois.

Statistiques, mesures d'audience et publicité

Sujet quasi indissociable des cookies, la mesure d'audience ne change pas énormément dans le RGPD. Le prestataire du service est dorénavant considéré comme un sous-traitant (donc contrat, etc.).

Le responsable du traitement est toujours chargé de recueillir le consentement préalable sauf si la solution choisie respecte parfaitement la loi (pas de recoupement, statistiques anonymes, pas de multi-site, pas de prorogation du cookie, pas de conservation des données "brutes" plus de 13 mois, géolocalisation par IP limitée).

La publicité peut se passer de demande de consentement préalable… Sous réserve qu'elle n'utilise ni cookie (au sens large du terme), ni outils de ciblage.

Dans le doute… Informez et demandez le consentement.

[13] *On fait ici le même raccourci sémantique que la loi : Cookie désigne ici n'importe quel type de traceur (Cookie http, flash, pixels invisibles, identifiants uniques permettant de tracer un utilisateur, etc).*
[14] *https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi*

Réseaux sociaux

Les boutons de partage récupérant parfois des informations considérées personnelles (dans des quantités astronomiques avec Facebook) et posant souvent des cookies, sont soumis aux mêmes règles que les cookies et la mesure d'audience (notice d'information, consentement préalable, possibilité de modifier son consentement, etc.).

Newsletter

La bonne nouvelle c'est que la majeure partie des newsletter réalisées en France sont déjà compatibles dans les grandes lignes avec le RGPD. En effet, la plupart présupposent une acceptation préalable d'être contacté et proposent un lien de désinscription qui permet de changer son consentement.

En revanche, il reste souvent du travail concernant la suppression des données ainsi que l'intégration des mentions obligatoires et d'informations.

Parrainage

Encore un sujet qu'il faudra aborder avec beaucoup plus de circonspection qu'avant. On suppose le scénario suivant : on propose à un utilisateur (qui a déjà donné son consentement) de parrainer ses amis pour recevoir des avantages. On ne lui demande que l'adresse e-mail de ses amis pour les inviter.

Problème, le parrainé n'a pas donné son consentement. La bonne nouvelle, c'est qu'on peut tout de même le contacter. En revanche, on ne peut pas conserver son email (sauf s'il s'inscrit suite à ce parrainage et qu'il le donne par lui-même).

CONCLUSION

Conclusion

Le RGPD s'inscrit dans une stratégie européenne de régulation des GAFAM via un arsenal réglementaire s'attaquant à la question de la marchandisation de la donnée personnelle. Les aspects les plus coercitifs du règlement sont la traduction tactique de cette ambition.

Si l'on peut légitimement se féliciter de cette volonté de mettre à mal ce modèle de « netarchie[15]» c'est-à-dire de hiérarchie du réseau, il faudra s'assurer que ce dessein s'applique réellement via des condamnations notamment.

Dans le cas contraire ce ne sera qu'une incarnation pernicieuse de plus du mille-feuilles réglementaire européen car le RGPD s'applique à toutes les organisations quelles que soient leur taille et leur difficulté à se mettre en conformité.

À date, les services de l'Etat se veulent rassurants sur la tolérance quant à la mise en conformité effective au 25 mai des entreprises. Il s'agira de pouvoir démontrer que l'organisation a planifié sur un temps « raisonnable » sa mise en conformité.

En revanche, en cas de contrôle, la preuve du manquement sera plus simple et plus rapide à établir, avec potentiellement des sanctions drastiques en cas de récidive. Nombreuses sont les habitudes que les organisations vont devoir faire évoluer et ce document n'a pas vocation à étreindre de manière exhaustive l'ensemble des cas de figure spécifiques à chaque entreprise.

[15] Michel Bauwens "Sauver le monde" edt LLL 2015

Changement de paradigme

Et si cette nouvelle contrainte était une formidable opportunité pour faire émerger de nouvelles approches basées sur la valeur d'usage et la valeur d'échange de la donnée ?

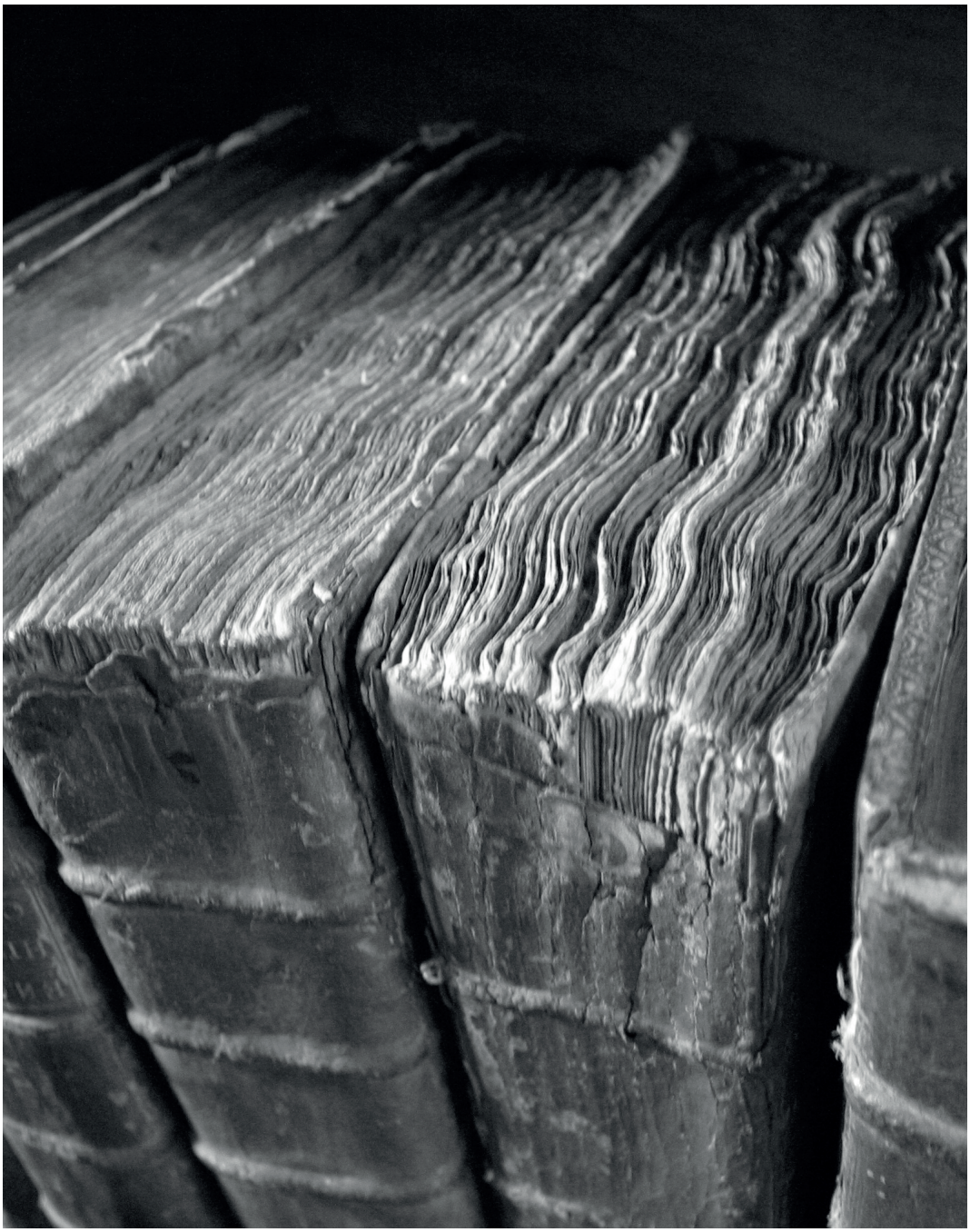
Un nouveau schéma relationnel reposant sur une nouvelle concorde entre des agents économiques/ institutionnels et des citoyens-consommateurs :

- Il s'agit de faire émerger des produits ou services à valeur ajoutée, c'est-à-dire acceptables et désirables par les utilisateurs. En s'appuyant sur des approches basées sur la co-création, la co-production et qui assument cette position en la revendiquant.
- Créer ou recréer de la confiance. La société évolue, donc les marques, les entreprises et les organisations doivent faire de même. Il est vital de dire ce en quoi on croit, d'exprimer des valeurs cardinales, d'engager une réflexion transparente sur la responsabilité sociale de l'organisation.

Appliqués à la donnée, ces principes s'organisent de la manière suivante :

- Prendre soin des données des utilisateurs est une démarche à forte valeur ajoutée.
- Présenter et expliciter ce qui sera fait de la donnée au moment de la demande de consentement.
- Informer et demander à nouveau le consentement pour de nouveaux usages et traitements.
- Permettre à l'utilisateur d'administrer en temps réel l'usage qui est fait de sa donnée.
- Garantir que ces principes sont respectés et protégés.

Il s'agit de mettre l'utilisateur, l'usager, le client, « réellement » au centre et d'assumer la confrontation-dialogue afin de questionner les habitudes, les certitudes et les choix évidents.



DÉFINITIONS

Délégué à la protection des données

Un DPO est désigné lorsque :

- Le traitement est effectué par une autorité ou un organisme public.
- Les activités consistent en des opérations qui exigent un suivi régulier et systématique à grande échelle des personnes concernées.
- Les activités consistent en des opérations sur des données sensibles.

Les missions du DPO sont, a minima, les suivantes :

- Informer, conseiller, former, sensibiliser.
- Contrôler le respect du RGPD (ou de toute loi sur la protection de données).
- Aider aux analyses d'impact.
- Coopérer et faire office de point de contact pour l'autorité de contrôle.

C'est une fonction indépendante qui se rapproche du délégué syndical : il ne peut recevoir d'instructions en ce qui concerne l'exercice de sa mission de DPO et ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de sa mission de DPO.

Données personnelles

Définition du règlement : Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données sensibles

Origine raciale/ethnique, orientation politique et appartenance syndicale, philosophique et religieuse, santé, biométrique et génétique, infractions et condamnations.

Définition officielle : Les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Données biométriques

Définition officielle : Les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Données concernant la santé

Définition officielle : Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Profilage

Toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels, notamment pour analyser ou prédire des aspects concernant le rendement au travail, sa situation économique ou de santé, ses préférences (politiques, religieuses, syndicales, sexuelles…) ou centres d'intérêt, sa fiabilité, son comportement, sa localisation et ses déplacements, etc.

Protection de la vie privée

Définie par l'article 9 du code civil, la protection de la vie privée garantit que : "Chacun a droit au respect de sa vie privée". Il donne donc le droit de s'opposer à la reproduction de son image ou la diffusion de tout commentaire relatif à la vie privée.

Le concept de "vie privée" n'a pas été défini avec précision par le législateur. Néanmoins, la jurisprudence a permis de fixer des cas d'usage :

- Les informations sur ses relations sexuelles, sa vie sentimentale ou sa vie familiale.
- La situation financière.
- Les souvenirs personnels.
- La santé.
- Les convictions politiques et religieuses.

Le fait d'être en règle avec le RGPD ne permet bien entendu pas de s'affranchir du respect de la protection de la vie privée.

Pseudonymisation

Définition officielle : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

Registre des activités de traitement

Chaque responsable de traitement tient un registre des activités de traitement effectuées sous leur responsabilité. Il contient les informations suivantes :

- Noms et coordonnées des responsables de traitements.
- Noms et coordonnées des responsables de l'éventuel DPO.
- Finalités du traitement.
- Catégories de personnes et de données concernées.
- Catégories de destinataires des données.
- Les délais prévus pour l'effacement des données.
- Si possible une description générale des mesures de sécurités techniques et organisationnelles.

Le registre est optionnel pour les entreprises de moins de 250 salariés sauf si le traitement n'est pas occasionnel ou concerne des catégories particulières de données.

Responsable du traitement

Définition officielle : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant

Définition officielle : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Traitement

Définition officielle : Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Violation de données à caractère personnel

Définition officielle : Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

ASUWISH
Marketing Thinking

7 place de l'Europe
14200 Hérouville Saint Clair
contact@asuwish.fr

arcange klub casusbelli ÅSGARD BANGARANG