RÉTABLIR LA CONFIANCE dans le Big Data

*Avançons en confiance

*Move Forward with Confidence**

BUREAU VERITAS

La Privacy
PAR BUREAU VERITAS

BV se positionne uniquement comme organisme certificateur ou vérificateur indépendant et propose d'aider à la création d'une certification mondiale autour de la protection des données privées. Cette certification sera déployée sur trois niveaux :

Une certification « Privacy checked » / « Privacy by Design »

- Permet de revendiquer un Label « Privacy by Design » en mettant en œuvre une conception d'offre, une architecture de données et des moyens de type « pseudonymisation » ou autres
- Permet de démarrer dans la certification Privacy sans transformer l'ensemble de l'architecture IT
- Accessible à certaines entreprises plus facilement

Une certification « Gouvernance »

- Une labellisation internationale – indépendamment des exigences locales de compliance
- Permet de se concentrer sur le système de management de la donnée, sans entrer dans des audits techniques de moyens
- Instaure un processus d'amélioration continue sur la Privacy
- Déclinable sur le modèle de la Responsabilité Sociale des Entreprises (RSE)
- S'applique à tous les types d'entreprises

Une certification au titre du Règlement Européen (RGPD)

- En réponse à l'article 42 du règlement européen
- Décernée sur la base d'un référentiel découlant du règlement
- Certification volontaire pour les entreprises

Les processus internes vérifiés sont ceux de la gouvernance des données.

Le modèle opérationnel de la certification dépend des géographies et des activités couvertes ainsi que de la complexité organisationnelle de l'entreprise.

MOVE FORWARD WITH... PRIVACY

Les données sont partout. Elles nous promettent un monde d'anticipation, d'efficacité et de services personnalisés. Mais leur mauvaise utilisation par de nombreuses entreprises a créé un climat de défiance. L'individu se sent dépossédé. Comment restaurer la confiance et profiter des bénéfices attendus de la voiture connectée, du bâtiment intelligent, de la santé personnalisée ?

Les entreprises s'efforcent d'apporter des réponses sur le plan technique, en renforçant par exemple la sécurité. Les gouvernements tentent d'imposer des règles sur le plan juridique. Des initiatives intéressantes (chartes…) se développent pour apporter plus de communication et de transparence. Le *Privacy by Design* est désormais adopté par une grande partie des entreprises pour proposer de nouveaux produits ou services. Toutes ces démarches ne pourront rassurer que si elles sont connues, et que si les assurances données sur le respect de la vie privée sont crédibles.

Sur ce point, seule une tierce partie indépendante est légitime pour affirmer le bon respect des règles éthiques.

Bureau Veritas, un leader mondial des tests, de l'inspection et la certification, est aujourd'hui à aux côtés des entreprises de tous secteurs qui veulent s'engager sur le respect de la *Privacy* de façon rigoureuse et transparente. Nous travaillons avec des acteurs majeurs, sur l'ensemble de la chaîne de valeur de la donnée, pour les aider à anticiper des offres respectueuses de la vie privée et à progresser dans leur management de la data.

Bureau Veritas propose un ensemble de certifications et labels pour garantir la transparence et la bonne utilisation des données personnelles.

Nous accompagnons aujourd'hui l'émergence de la *Privacy* comme un levier d'opportunité pour les entreprises qui sauront s'en saisir. La responsabilité numérique des entreprises se dessine comme l'un des enjeux majeurs des années à venir.

PHILIPPE LANTERNIER
Executive Vice President,
Chief Development Officer
Bureau Veritas

Bureau Veritas — · Rétablir la confiance dans le Big Data

DONNÉES PERSONNELLES : CONSOMMATEURS ET ENTREPRISES NAGENT EN PLEIN PARADOXE

LES CONSOMMATEURS SE DISENT INQUIETS DE L'UTILISATION DE LEURS DONNÉES…

1/3 des internautes

aux États-Unis ont déjà subi une utilisation abusive de leurs données personnelles sur la dernière année.

- Source : GfK

Les données les plus sensibles

pour eux sont leurs données de

localisation (82 %) · **santé** (81 %) · **navigation** (70 %) · **amitié** (68 %)

- Source : Pew Research Center, Janvier 2014

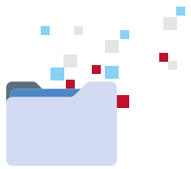
Plus de 80 %

(81 % FR, 88 % US) craignent que leurs données soient volées ou détournées.

- Source : GfK

Ils ont peur…

d'une surexposition à la **publicité** (87 %), de **l'impossibilité du droit à l'oubli** (85 %), du piratage de **leurs données bancaires** (77 %) ou **d'identité** (75 %).



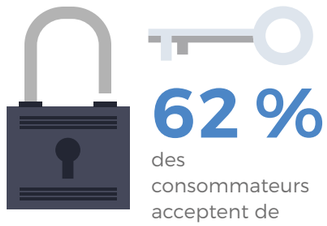
- Source : Enquête Ipsos pour Elia

… MAIS PARADOXALEMENT, LA MAJORITÉ ACCEPTENT DE PARTAGER LEURS DONNÉES

92 %

des internautes estiment (en France) que leurs données **peuvent être utilisées** par le fournisseur de service (54 % pensent que leur accord n'est pas requis).

- Source : Ispos/Elia



62 % des consommateurs acceptent de **partager plus d'informations** personnelles pour bénéficier de nouveaux services numériques.

- Source : Livre blanc Microsoft (p 16)

Les consommateurs interrogés dans le monde en attendent :

- à **100 %** une récompense financière,
- à **89 %** des réductions importantes,
- à **65 %** des points de fidélité.

- Source : Livre blanc Microsoft (p 14)

LES ENTREPRISES COLLECTENT TOUTES DES DONNÉES…

LA PLUPART DES ENTREPRISES EN LIGNE COLLECTENT DE LA DATA

visites · profils · paiement · …

BEAUCOUP ONT COMMENCÉ À LES ANALYSER

130 milliards dépensés en 2016 en data et business analytics

- Source : IDC

… MAIS PEU PROPOSENT UNE VRAIE GOUVERNANCE

En 2013, **44 %** (Amérique du Nord) n'avaient pas encore de politique d'utilisation des données. - Source : Rand

En France, **16 000 organismes** (e-commerce, administration…) ont désigné un correspondant informatique et libertés (CIL),

alors que l'e-commerce seul représente **200 000 sites marchands actifs environ.**

- Source : AFDCP, Fevad

LES INTERNAUTES LE PRESSENTENT BIEN

leur confiance est faible dans les acteurs du secteur :

- **38 %** cartes de crédit
- **31 %** opérateurs téléphoniques
- **29 %** fournisseurs d'e-mail
- **26 %** commerçants en ligne
- **16 %** moteurs de recherche
- **7 %** webmarketeurs

- Source : GfK

SEULE UNE CERTIFICATION INDÉPENDANTE RESTAURERA LA CONFIANCE

LES ENTREPRISES TENTENT DE MONTRER ELLES-MÊMES PATTE BLANCHE

La plupart affichent en ligne une « politique de confidentialité » peu contraignante…

que seuls **10 %**
des internautes qui s'inscrivent chez eux lisent en entier.

- Source : CNIL

Quelques grands groupes publient des « chartes éthiques ».

LA RÉGLEMENTATION LES CONTRAINDRA BIENTÔT À SE STRUCTURER

Aux États-Unis,
le Consumer Privacy Bill of Rights
a déjà été présenté deux fois.

En Europe,
la RGPD a été votée en avril et prévoit des obligations plus fortes d'ici à 2018 :
Droit à l'oubli, portabilité des données, obligation d'information en cas de piratage (y compris pour les données transférées hors d'Europe)
Amende jusqu'à 4 % du CA…

Problème : 92 %
des entreprises en France, Allemagne ou au Royaume-Uni
s'inquiètent de ne pas être prêtes pour 2018.

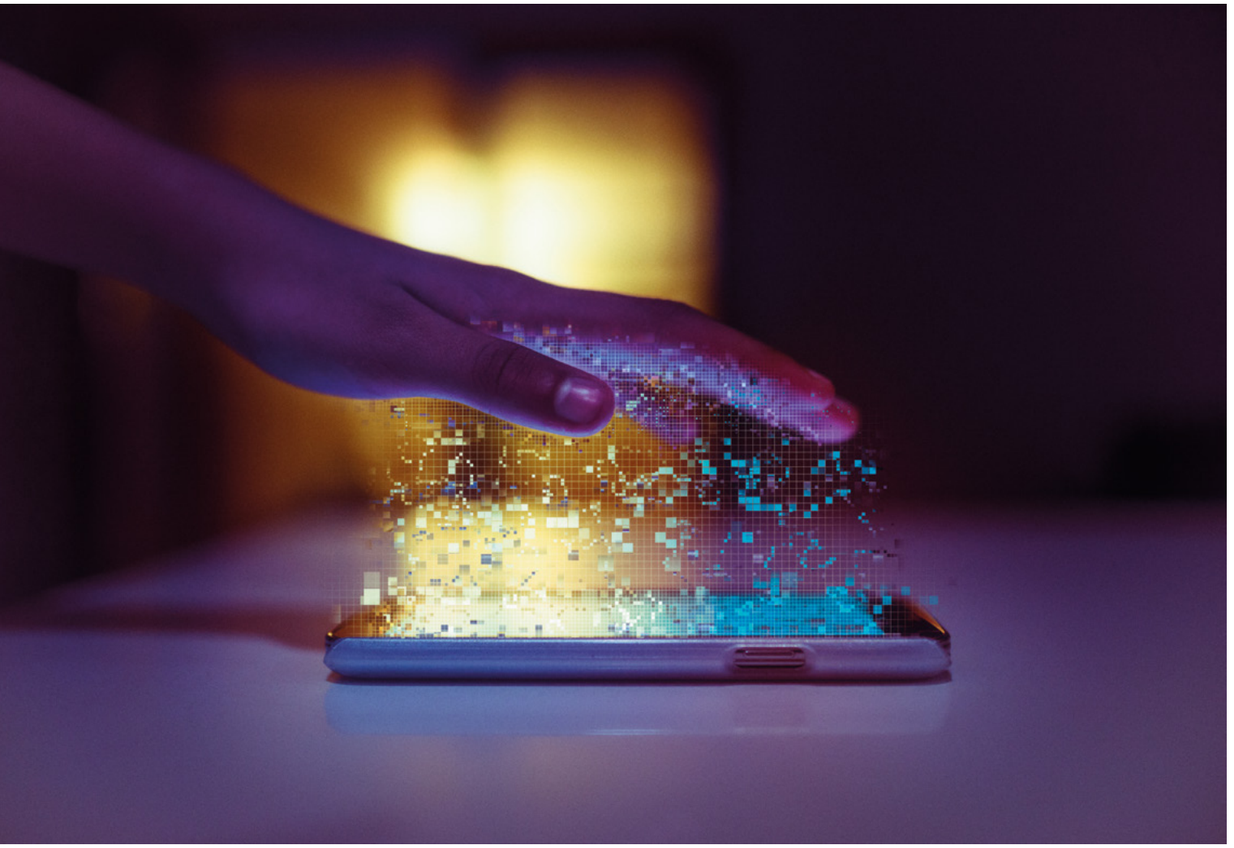
Quoiqu'il en soit, pour les consommateurs,
obéir à la réglementation, c'est juste le minimum.

MAIS SEULE UNE CERTIFICATION DE BONNE GESTION DES DONNÉES PARAÎT ADAPTÉE

- Compréhensible du public
- Légitimée par le marché
- Adaptable et évolutive
- Déployable à l'international
- Attribuable à plusieurs niveaux : produit, entreprise, sous-traitants

CETTE CERTIFICATION DOIT ÊTRE DÉCERNÉE PAR UN ORGANISME INDÉPENDANT, QUI ALLIE :

- Légitimité
- Impartialité
- Réputation sans faille
- Outils analytiques transparents
- Capacité à soutenir le label



Restaurer la confiance dans le Big Data

SEULE UNE CERTIFICATION INDÉPENDANTE POURRA RESTAURER LA CONFIANCE DANS L'UTILISATION DES DONNÉES PERSONNELLES

SÉCURITÉ, RÉGLEMENTATION, *PRIVACY BY DESIGN*… CES DÉMARCHES NE POURRONT RASSURER QUE SI ELLES SONT CONNUES ET CRÉDIBLES

Les données sont partout. Elles nous promettent un monde d'anticipation, d'efficacité et de services personnalisés. Car lorsque l'on parle de données, on parle en particulier des données personnelles que toutes les entreprises aujourd'hui s'efforcent de recueillir sur leurs clients – et sur le marché en général. Cependant, loin de créer un monde où les relations entre les individus et les marques seraient plus fortes, l'utilisation de données personnelles par de nombreuses entreprises a défrayé la chronique et a récemment créé un climat de défiance. Sans parler bien sûr des grandes affaires qui ont engagé les États eux-mêmes dans des controverses de même teneur…

Comment restaurer la confiance ? Comment faire en sorte que les doutes des consommateurs et citoyens ne viennent pas à l'avenir se mettre en travers des bénéfices tant attendus de la voiture connectée, du bâtiment intelligent, de la santé personnalisée ? Le monde du Big Data attire mais fait peur. Capacités de stockage, instantanéité des traitements, ubiquité des informations… Ce monde est complexe et l'individu peut se sentir dépossédé.

Les entreprises s'efforcent d'apporter des réponses sur le plan technique, en renforçant par exemple la sécurité. Les gouvernements tentent d'imposer des règles sur le plan juridique. Des initiatives intéressantes se développent pour apporter plus de communication et de transparence – ou éduquer progressivement le citoyen dans une meilleure maîtrise des outils qui lui permettront de protéger finement sa vie privée. Le *Privacy by Design* est désormais adopté par une grande partie des entreprises quand elles veulent proposer de nouveaux produits ou services : à elles d'intégrer des options ou des moyens de minimiser l'impact sur l'utilisation de données personnelles dès la conception de leur offre.

Reste un point essentiel : toutes ces démarches ne peuvent rassurer que dans la mesure où elles sont connues, et où les assurances données sur le respect de la vie privée sont considérées comme crédibles par le public. Or sur ce point, seule une tierce partie indépendante est légitime à affirmer le bon respect des règles éthiques par un acteur économique.

La responsabilité numérique des entreprises se dessine comme l'un des enjeux majeurs des années à venir. Bureau Veritas, un leader mondial des tests, de l'inspection et la certification, est aujourd'hui à aux côtés des entreprises de tous secteurs qui veulent s'engager sur le respect de la *Privacy* de façon rigoureuse et transparente - en proposant tout un ensemble de labels.

Sur l'ensemble de la chaîne de valeur de la donnée, Bureau Veritas travaille avec des acteurs majeurs pour les aider à anticiper des offres respectueuses de la vie privée et à progresser dans leur gestion des données personnelles. Notre vision du numérique nous fait entrevoir son extraordinaire pouvoir de création de valeur et de transformation. Forts de nos savoir-faire portés par notre vision et conscients de nos responsabilités comme acteur de la confiance dans les échanges économiques, nous accompagnons aujourd'hui l'émergence de la *Privacy* comme un levier d'opportunité pour les entreprises qui sauront s'en saisir.

130 milliards

de dollars ont été dépensés en 2016 en data et business analytics. Combien pour rassurer les consommateurs ?

1

DE PLUS EN PLUS DE DATA, DE MOINS EN MOINS DE CONFIANCE

LES INTERNAUTES SE MÉFIENT DE L'USAGE QU'ON FAIT DE LEURS DONNÉES

L'innovation est devenue le cheval de bataille de toutes les entreprises pour conserver leurs marchés. La plupart de ces innovations concernent des services numériques. Et pourtant, aujourd'hui 80 à 90 % des citoyens (selon les pays) se disent inquiets au sujet de la protection de leurs données personnelles – et la situation se dégrade régulièrement. Environ 60 % admettent que leur niveau d'inquiétude a augmenté ces dernières années.

Les récentes affaires ont accéléré le mouvement vers davantage de défiance. L'affaire Snowden en 2013 a révélé l'espionnage organisé au niveau de l'État des simples citoyens, et pas seulement aux États-Unis. D'autres affaires, touchant des entreprises commerciales, ont montré des failles de sécurité (*data breaches*, en anglais) ou des manquements importants à l'éthique dans la relation clients.

Dans un monde où il est maintenant admis que « les données seront le pétrole du XXIe siècle », le sujet est critique. Le Big Data est loin d'avoir rempli ses promesses et déjà la question de la donnée commence à inquiéter. Clairement, c'est bien la confiance dans la relation entre les entreprises, les institutions, les marques et le public qui est en jeu.

Le risque sur les entreprises est grand – et elles en sont conscientes. Car il ne s'agit plus seulement d'une inquiétude sur la sécurité des données à l'égard du piratage par exemple. Il s'agit aussi de l'usage que les entreprises en font. Dans l'échelle des risques redoutés sur Internet, les sujets liés à la sécurité ne sont plus aujourd'hui les plus inquiétants : l'usurpation d'identité et le piratage des données bancaires sont considérés comme possibles (75 % et 77 %) mais moins probables que la surexposition à la publicité (87 %), le non-respect de la vie privée (85 %) ou l'impossibilité d'effacer les données partagées (85 %).

Comment continuer à développer de nouveaux services, plus personnalisés, si en deux ans le pourcentage de clients acceptant l'utilisation de leurs données de localisation en échange d'avantages commerciaux diminue de moitié ?

80 à 90 %
des citoyens (selon les pays) **se disent inquiets au sujet de la protection de leurs données personnelles**

LA *PRIVACY* N'EST PLUS UNE QUESTION DE SÉCURITÉ MAIS UNE QUESTION DE CONFIANCE

Les institutions et gouvernements se sont emparés de la question sous l'angle règlementaire. Il est naturel que leurs efforts portent sur des principes contraignant les entreprises à garantir un haut niveau de protection des données. L'Europe a adopté en avril 2016 son nouveau règlement sur la protection des données personnelles (RGDP). Celui-ci institue de nouveaux droits pour le public (tels que le droit à l'oubli ou à la portabilité) et renforce la notion de contrôle de chacun sur ses propres données. Du côté des États-Unis, une « Consumer Privacy Bill of Rights » a été proposée en mars 2015 en vue d'aboutir à une loi. Au Canada, les principes de la *Privacy* ont donné lieu à de nombreuses initiatives autour du *Privacy by Design*.

Du côté des entreprises « traditionnelles », non digitales nativement, la réaction s'organise mais dans une certaine perplexité.

La question de la sécurité des données est traitée depuis longtemps. Le DSI en est chargé, son rôle étant d'être en alerte et en avance de phase par rapport aux tentatives de hacking. Ses outils sont technologiques (cryptage, firewalls, etc.) et organisationnels. Les systèmes ne sont pas sans faille, mais l'exemple du paiement en ligne montre que les technologies peuvent apporter des réponses valables face aux inquiétudes du public. Les différents modes d'identification comme le système 3D Secure ont clairement fiabilisé la démarche. L'essor du commerce en ligne le montre clairement.

La question de la relation de confiance, elle, est finalement plus difficile à traiter. Le principal axe de réponse réside encore dans la recherche de services personnalisés à valeur ajoutée, qui viendraient démontrer aux clients l'intérêt de confier leurs données aux marques. D'autres stratégies visent à éditer des chartes, faire de la pédagogie, prendre des engagements verbaux. Mais sur ce point, de nouveaux clivages apparaissent parfois au sein d'une même entreprise : entre le Marketing et le Juridique, entre la Business Intelligence et la Relation Clients, etc. **À l'intérieur du Marketing, on retrouve ceux qui veulent préserver la marque et se méfient d'une mise en cause sur la *Privacy*, et ceux qui veulent préserver une liberté maximale dans l'exploitation future des données** (aujourd'hui souvent recueillies en larges volumes, de façon non structurée, avec l'idée que les technologies du Big Data pourraient leur apporter une pertinence à l'avenir).

Aujourd'hui, la protection des données personnelles est souvent débattue comme un sujet transverse au Marketing, à la Relations clients, au Juridique et aux Systèmes d'information. Mais face à des impératifs contradictoires, comment rassurer et préserver la capacité des entreprises à capitaliser sur la connaissance client pour préserver leur position acquise et leur croissance future ?

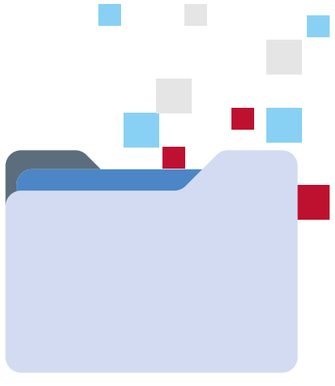
2

LA *PRIVACY* EST UN SUJET ANCIEN, C'EST SON BUSINESS MODEL QUI EST EN PLEIN BOOM

NOS TRACES NUMÉRIQUES SE MULTIPLIENT

Quelle que soit l'aire géographique concernée, les grands principes de la protection des données personnelles restent globalement les mêmes. Certes, on a tendance à dire que certains États sont plus permissifs que d'autres. Mais sur le fond, c'est bien des mêmes principes dont on parle dans tous les cas.

Les dernières évolutions de la réglementation européenne RGDP (droit à l'oubli, consentement clair et explicite, etc.) mettent en lumière les nouvelles appréhensions à l'égard de la protection de la vie privée. Car si les principes de protection de la vie privée sont stables, qu'est-ce qui a changé ? Les fichiers clients existent depuis l'origine du commerce ; la vente par correspondance et le marketing relationnel du XX[e] siècle reposaient déjà sur une connaissance client de premier niveau. La protection des données personnelles était déjà une pratique connue des entreprises.



Aujourd'hui, c'est bien évidemment l'échelle, mais aussi les technologies et les buts poursuivis autour de nos données personnelles, qui ont changé. Chacun de nous est conscient d'avoir transmis un certain nombre de données, volontairement, à des partenaires commerciaux par exemple qu'il serait capable d'identifier. En revanche, la navigation sur Internet, la géolocalisation, les paiements dématérialisés ont ouvert la voie à une acquisition de données entièrement passive, pour laquelle un consentement a initialement été demandé dans certains cas et parfois pas du tout ! Face à cette génération de données en grandes quantités, liée à l'usage de nos téléphones mobiles, de nos navigateurs Internet, déjà de nos voitures, thermostats ou téléviseurs, **c'est bien la notion de trace numérique qui est en question : multiples, compliquées à tracer et à effacer, ces traces numériques correspondent à une catégorie de données privées qu'il est particulièrement difficile de contrôler.**

LES DONNÉES SONT COLLECTÉES SANS FORCÉMENT SAVOIR CE QU'ON EN FERA

Du côté des entreprises, l'acquisition de données devient massive. La chute du coût des capacités de stockage, l'augmentation de la performance des réseaux et outils de calculs ont ouvert la voie à l'analyse de données en volumes. Toute information sur l'usage d'un service, sur le comportement d'un client quel que soit le contexte, est potentiellement porteuse de connaissance, donc de valeur.

Les technologies d'analyse, le Big Data, sont désormais là pour identifier des patterns et donner du sens à ces volumes de données non structurées.

Et c'est bien là ce qui inquiète. **La vision de la finalité tend à s'effacer. Notre approche actuelle des données personnelles repose sur l'idée qu'elles seront génératrices de valeur – mais d'une façon qu'il est bien difficile d'anticiper au moment où un individu les confie à une entreprise.** Certes, la demande de services plus personnalisés se fait croissante, les recommandations d'achat sur des sites e-commerce sont parfois appréciées. Mais les interrogations sont importantes quant à la somme d'informations que chacun fournit sur sa vie privée par le biais des objets connectés en santé, de la messagerie privée, ou des capteurs qui équipent désormais nos foyers – et qui semblent avoir des finalités variables.

IL FAUT AUSSI SÉCURISER TOUTE LA CHAÎNE DE PRESTATAIRES

Si la notion de finalité s'éloigne, il est d'autant plus important pour le public que ses données personnelles soient aux mains d'institutions et d'entreprises en lesquelles il a confiance. Or, sur la chaîne de valeur de la donnée personnelle, les acteurs se multiplient. Quand on parle d'avoir confiance en une entreprise à laquelle on confie sa vie privée, c'est en réalité d'un écosystème entier qu'on devrait parler.

Fournisseur du service, hébergeur des données, opérateur de traitements, prestataire… **La nouvelle donne de la donnée personnelle exige d'avoir une cohérence parfaite sur toute la chaîne.** Motivées en grande partie par les inquiétudes du public, et initialement adressée aux entreprises du B2C, les questions sur la *Privacy* touchent en réalité une large sphère de services en B2B :

- **Les entreprises en contact direct avec les clients prennent l'engagement principal.** Elles doivent s'exprimer clairement sur la finalité pour laquelle elles recueillent les données, recueillir le consentement, rassurer sur les mesures de sécurité mises en œuvre, organiser la communication avec leurs clients. Ce sont elles qui définissent la stratégie de l'entreprise par rapport à l'exploitation des données, et qui prennent les grandes décisions sur les différents traitements (anonymes / personnalisés, statistiques / individualisés, etc.). Bien sûr ce sont elles qui portent la responsabilité de la qualité dans la gestion de la donnée. Sans parler du risque d'image si une faille venait à se produire.

- **Les hébergeurs de données sont leurs partenaires immédiats et garantissent le stockage des données.** Ils sont spécialisés (comme les hébergeurs de données de santé) ou généralistes, mastodontes du secteur (Amazon, Microsoft, etc.) ou petits acteurs. Ils sont responsables de la sécurité, de l'accessibilité de la donnée pour les différents traitements programmés, et parfois de leur organisation. Leur business model entier repose sur le service apporté à leurs clients. La notion de confiance et de fiabilité est essentielle et à la base même de leur pérennité en tant qu'entreprise.

- **Les analystes de la donnée sont responsables de la Data Intelligence.** Ce sont des sociétés externes en général – même si une fonction interne de Business Intelligence oriente leurs actions. Il s'agit davantage de recherche et d'exécution. Leur compétence est statistique, algorithmique, en un mot scientifique. À leur niveau l'exigence d'éthique est maximale, puisque les traitements algorithmiques les plus poussés peuvent remettre en question l'anonymat de la donnée, avec des puissances de calcul et des finesses d'analyse qui rendent aujourd'hui possible de circonscrire la vision à un individu.

- **Les acteurs qui enfin utilisent les résultats de l'analyse – ou se servent de la donnée brute** – sont en général à nouveau internes à l'entreprise : Département Marketing qui va fonder sa vision des nouveaux services sur les enseignements de l'analyse Big Data, Direction Clients qui va pouvoir s'adresser de façon personnalisée à chacun en temps réel, etc. C'est ce maillon de la chaîne qui doit apporter une valeur ajoutée au client – après un détour plus ou moins long.

3

TOUTES LES ENTREPRISES ONT INTÉRÊT À JOUER LA TRANSPARENCE (PAS SEULEMENT LES PURE PLAYERS)

LES DÉMARCHES DE TRANSPARENCE EXISTENT, MAIS SONT TIMIDES

Responsables aux yeux du public de la protection des données personnelles sur l'ensemble de la chaîne, les marques ont pris conscience de leur devoir de rassurer. Quelques-unes mettent en place des actions – cependant encore peu visibles du public. Et c'est bien cela qui frappe : la faible notoriété – ou la faible connaissance – de ces initiatives, ainsi que la prise en main encore plus limitée des outils de gestion des données personnelles par tout un chacun. Combien d'utilisateurs Google ont-ils déjà cherché à régler finement leur historique d'activité (en désactivant la collecte de données relatives au visionnage de vidéos sur YouTube par exemple, ou en excluant ses données de localisation de l'historique conservé par Google) ? Qui connaît même l'existence de cette possibilité ?

Peu d'entreprises font de l'engagement sur les données personnelles l'un des piliers de leur marque. **Celles qui lancent des initiatives originales sont assez discrètes : elles craignent de trop afficher leur engagement et de se retrouver prises en faute ensuite, ou elles ne veulent pas se priver à l'avenir de l'utilisation de données personnelles.** Qui leur permettra d'affiner leur offre et se ménager ainsi une marge de manœuvre en termes de Business intelligence future. Pourtant aujourd'hui, 80 % des citoyens se disent intéressés par des outils leur permettant de « gérer leur identité numérique », et ce chiffre croît d'année en année.

GRANDE DISTRIBUTION OU PURE PLAYERS SOUFFRENT DE LA MÊME SUSPICION

Toutes les catégories d'entreprises auront tôt ou tard besoin de faire preuve de transparence, car toutes font l'objet de suspicion. Les plus puissantes, les géants de l'Internet, effraient par leur puissance et le volume énorme de données qu'ils traitent. Paradoxalement, ce sont aussi celles qui cherchent le plus à apporter des garanties (qu'on pense par exemple au récent choix de WhatsApp de crypter les échanges de bout en bout) qui sont les plus soupçonnées d'abus. Quant aux entreprises issues de l'économie traditionnelle, elles inquiètent moins sur le sujet des données - mais elles sont bien en risque réel, n'ayant souvent pas encore suffisamment investi dans des systèmes adéquats de management de la donnée privée.

Prenons le cas des grands acteurs de la distribution, qui montre bien que les entreprises ne sont pas égales quant au traitement de la donnée. Issues de la distribution physique, ces entreprises ont mis en place depuis longtemps des programmes de fidélité qui contiennent des données personnelles. Ces données ont été collectées dans le respect de la réglementation et ont été utilisées pour les objectifs déclarés à l'époque : informer le client sur des promotions notamment, permettre la mise en place de services tiers (tels des solutions de financement), etc. **Ces données ont été confiées à des partenaires (acteurs du CRM) capables de les traiter et de les exploiter dans le cadre d'actions ciblées.** Aujourd'hui, avec la multiplication des canaux de vente et de distribution, ces mêmes acteurs sont confrontés à plusieurs sujets :

- **Les canaux d'acquisition des données se sont élargis :** les données clients sont issues des magasins physiques, mais également de la navigation sur le site Internet par exemple.
- **Les catégories de données recueillies se sont diversifiées :** en plus des données transactionnelles, des données sur la navigation web ou sur l'itinéraire d'un client en magasin peuvent être recueillies, permettant ainsi une meilleure anticipation marketing.
- **Le périmètre des individus suivis s'élargit également,** avec un suivi (en magasin, sur le web ou sur mobile) de clients identifiés par un profil déjà connu par l'enseigne, mais également de simples visiteurs – qu'il sera possible de « re-cibler » à l'avenir en leur créant ainsi un historique par rapport à l'enseigne, sans qu'ils aient jamais consenti à avoir un profil dans la base de données clients.
- **Et surtout, ces bases de données ne sont pas toujours coordonnées entre elles,** avec des « master profiles » et donc une gestion de la relation suffisamment fine pour respecter par exemple les choix de opt-ins d'un canal sur l'autre.

Difficile pour les marques de la grande distribution de prendre des engagements quand le périmètre des données privées est si complexe et que l'historique aboutit à de multiples couches de données gérées différemment dans le temps.

À l'opposé, les pure players du numérique : ces entreprises ont été conçues autour du management de la donnée, soit pour l'exploiter en rendant des services de toutes sortes (e-commerce, e-santé, services en mobilité, etc.), soit pour en faire le cœur de leur business model (comme Google ou Facebook par exemple). La gestion de la donnée y est a priori sans faille : un profil unique, un historique contextualisé, des catégories de données bien identifiées – et en conséquence une description claire des traitements appliqués aux données, des engagements pris à l'égard du public, des interfaces permettant aux clients de gérer eux-mêmes certains paramètres dans certains cas. Cela pourrait leur donner un avantage certain par rapport aux entreprises moins mûres sur le sujet. Or, ce n'est pas le cas, et **la défiance à leur égard est aussi importante.**

LA RÉGLEMENTATION NE SUFFIRA PAS À RÉTABLIR LA CONFIANCE

La réglementation peut-elle ici apporter une réponse ? Elle peut aider, très certainement. Mais **la simple conformité (la « compliance ») apparaît comme un simple niveau « zéro », un niveau minimum qui n'est plus porté au crédit des entreprises** – même si le fait de se retrouver pris en faute peut leur porter préjudice. Certes, les études montrent que les citoyens attendent des efforts de la part des institutions pour mieux les protéger à l'avenir. Et certes, cette demande est entendue, en particulier du côté européen où l'on s'efforce d'encadrer strictement l'utilisation des données. Mais la réponse réglementaire n'a pas suffi par le passé à rassurer sur les pratiques des géants du numérique, ni sur celles des acteurs de l'économie traditionnelle, parfois « épinglés » pour mauvais usage des données privées.

D'un côté, des entreprises qui aimeraient s'engager mais sont encore en courbe d'apprentissage sur le management de la donnée ; de l'autre, des acteurs du numérique qui offrent une certaine transparence et des outils de contrôle, mais sont confrontés à une défiance importante : les deux catégories d'entreprises font face au défi de la confiance.

Avec un léger avantage finalement pour la première, ces marques souvent anciennes qui ont su préserver un territoire de valeurs autour de la proximité et de l'engagement.

À l'heure du digital et de la globalisation des produits et des services, toutes les entreprises font face à cette même question. **La seule réponse passe par la mise en place d'une transparence totale, de multiples façons : en expliquant ce que l'on fait, en démontrant par tous les moyens de preuve possible, en valorisant des bénéfices très pragmatiques auprès des clients.**

4

QU'ON L'ASSUME OU PAS, **NOS DONNÉES PERSONNELLES FONT DÉJÀ PARTIE DE L'ÉQUATION ÉCONOMIQUE DES SERVICES EN LIGNE**

NOUS PARTAGEONS DÉJÀ TACITEMENT NOS DONNÉES EN ÉCHANGE DE SERVICES PERSONNALISÉS

Le droit à la vie privée est bien un droit fondamental. Comme tous les droits fondamentaux cependant, son application reste à interpréter, décliner, encadrer dans la réalité des relations économiques, en particulier dans le domaine numérique. Or, on a parfois l'impression que certains législateurs souhaiteraient faire de la *Privacy* un absolu. À cette tendance s'opposerait une vision plus « libérale », selon laquelle c'est à chacun d'entre nous de choisir son degré souhaité de partage ou d'exposition de ses données.

Or, c'est bien sur ce terrain que s'établit aujourd'hui une sorte de consensus implicite. Nous partageons de nombreuses données avec de multiples marques, administrations, réseaux sociaux, etc. De fait, nous en retirons des avantages. Et les entreprises l'ont bien compris. Pour nous inciter à le faire encore davantage, leur principal axe de réponse réside encore dans la recherche de services personnalisés à valeur ajoutée, qui viendraient démontrer aux clients l'intérêt de confier leurs données.

« Nous partageons de nombreuses données avec de multiples marques. Nous en retirons des avantages. Et les entreprises l'ont bien compris. »

Les exemples ne manquent pas : suggestions d'achats de produits susceptibles de vous intéresser, anticipation de vos besoins lors de l'organisation d'un voyage par exemple, propositions de contrats d'assurance personnalisés dimensionnés sur vos habitudes de conduite automobile et votre profil personnel, etc. Et bien sûr, services gratuits, largement adoptés, démontrant une acceptation tacite du public à aller vers des services qui utilisent ouvertement nos données – plutôt que de choisir des solutions payantes.

La *Privacy* fait ainsi aujourd'hui partie des paramètres de l'offre de services numériques. Connectez-vous à un site sans vous identifier, et vous aurez accès aux services les plus basiques. Créez un profil puis identifiez-vous à chaque visite : c'est maintenant un contenu adapté à vos intérêts supposés, identifiés et anticipés par des algorithmes, qui vous sera proposé. Même les contenus non sollicités (publicitaires, petites annonces par exemple) seront décrits comme des éléments à valeur ajoutée potentielle.

PARADOXALEMENT, NOUS REGRETTONS TOUJOURS CE PARTAGE APRÈS-COUP

Cet accord tacite n'est pas toujours bien assumé. La notion d'échange de valeur autour de la donnée personnelle laisserait penser, selon les termes d'une économie basique, que le public ferait de lui-même l'équivalence entre ses données et les bénéfices retirés d'un service. Les enquêtes montrent une attitude très ambivalente sur ce point.
Le dilemme entre protection de la vie privée et personnalisation commence à être bien connu. **Comme utilisateurs de bon nombre de services, nous sommes pris entre les bénéfices immédiats offerts par une plus grande personnalisation, et les dangers éventuels futurs liés au partage de données sensibles. Le présent l'emporte dans la plupart des cas – avec cependant une arrière-pensée négative,** qui s'exprime ensuite dans les études d'opinion qui réclament davantage de protection de la vie privée – bien que nos comportements quotidiens démontrent le contraire.
Un ajustement fin des paramètres de confidentialité peut apparaître comme une solution, en permettant à chacun d'adapter l'utilisation de ses données selon sa propre sensibilité.

LÀ ENCORE, LA RÉGLEMENTATION SEULE NE RESTAURERA PAS LA CONFIANCE

Généralement décrit comme une « négociation », cet ajustement suppose d'avoir mis en place des systèmes fins de gestion des autorisations – ce qui n'est pas donné à tous les types de services. Et la relation à la donnée personnelle reste le plus souvent vécue sur un mode « affectif » par les individus – et non sur un mode économique. Nous sommes encore loin d'une situation où les données personnelles pourraient être considérées comme une monnaie d'échange. Comme le souligne une étude récente de l'agence Edelman, l'acceptation des différentes innovations proposées par les marques (souvent des innovations de services qui se fondent sur la détention de données privées), ne peut s'acheter : elle se mérite (« *Consumer acceptance of brand innovation cannot be bought. It must be earned* »).

Par quels moyens ? C'est bien là que les entreprises doivent prendre leurs responsabilités.

Dans ce rapport unique entre l'individu et la marque, **la simple conformité à une réglementation, aussi contraignante soit-elle, n'est d'aucun secours. Elle correspond à un niveau minimum de sécurité pour le citoyen, et elle n'est porteuse d'aucune valeur,** d'aucune charge symbolique dans la relation. C'est dans la revendication de moyens supplémentaires au « minimum légal » que se joue la confiance – des moyens qui doivent être remis dans les mains du public pour que celui se réapproprie la gestion de ses données personnelles, et redevienne maître de sa relation avec les marques. Encore faut-il que les services numériques soient conçus pour rendre cet « *empowerment* » possible.

5

LE GRAAL DU *PRIVACY BY DESIGN*

LA *PRIVACY* DOIT S'INTÈGRER DÈS LA CONCEPTION

Pouvoir gérer de façon fine le niveau de *Privacy* associé à chaque service a certaines implications techniques, que toutes les entreprises ne sont pas prêtes à assumer. Sans parler de solutions structurelles, touchant à l'organisation des informations dans les bases de données, ou à la mise en place de procédures complexes, des technologies permettant de renforcer la protection de la vie privée (*Privacy Enhancing Technologies*), peuvent être proposées. Elles sont de plusieurs types – certaines à la main de l'utilisateur lui-même, d'autres mises en œuvre du côté de l'entreprise. Elles visent plusieurs objectifs, parmi lesquels rendre anonymes les profils, minimiser les données collectées, ou limiter les traces liées à l'usage des services numériques. Des solutions techniques existent, mais elles sont peu efficaces si elles interviennent comme des palliatifs a posteriori. Les utiliser pour la meilleure efficacité revient à adopter une démarche de ***Privacy* ou *Data Protection by Design* : la protection des données personnelles intégrée dès la conception.**

L'historique du *Privacy by Design* est bien connu. Il guide la plupart des réflexions des régulateurs sur la protection des données personnelles aujourd'hui, et vise à inscrire la *Privacy* dans la configuration même des services proposés au public. On règle ainsi en amont la question des usages possibles de la donnée une fois recueillie. L'éthique doit ainsi s'inscrire dans la dimension technique et organisationnelle des systèmes d'information, et plus seulement dans les pratiques commerciales et la relation clients.

Le règlement européen sur la protection des données personnelles adopté en avril 2016 lui a adjoint un autre principe : celui de la ***Privacy by default* : protéger les données privées n'est plus une option, mais une obligation dans toute l'Europe.** Ce n'est plus à l'utilisateur de demander le niveau maximal de *Privacy* ; c'est à l'entreprise de le lui garantir. Si ce principe a été retenu en Europe, il est encore en débat dans d'autres régions du monde.

DANS CE SYSTÈME, LA DATA SE GÈRE COMME UN ACTIF

Reste que ces deux concepts, au-delà de leurs implications techniques, ont des impacts forts en termes de management. De même qu'on gère les finances d'une entreprise, une marque ou un portefeuille de produits ou de services, **il faut maintenant gérer ses données, en envisageant ce nouvel « actif » dans l'ensemble de ses dimensions.** Elles ont un cycle de vie (ou d'usage) qui les fait passer dans les mains de multiples acteurs, de façon brute ou transformée. Sur l'ensemble de ce cycle, il est nécessaire de définir une responsabilité transverse – sous peine d'avoir une gestion désordonnée, non cohérente, et finalement risquée de la *Privacy*.

À ce stade, ce management est rarement structuré. **Rares sont les entreprises qui ont fait un bilan complet des données qu'elles détiennent ou utilisent, sur l'ensemble du périmètre.** Même quand on sait énumérer ce que recouvrent les données personnelles dans une entreprise, sait-on précisément comment elles sont structurées ? A-t-on démêlé les différentes « couches » de données acquises par divers canaux à divers stades de développement de l'entreprise, acquises suite au rachat d'un concurrent… A-t-on défini ensuite ce que l'on veut faire avec ces données ? A-t-on délimité ce que l'on a le droit de faire ? Pour quels bénéfices attendus ? Selon quels processus ? En autorisant quels types d'interventions, conduits par quelles ressources internes ou externes ? En prenant quelles garanties ? En se donnant quels moyens, en particulier humains, pour y parvenir ? Il ne s'agit pas là de s'assurer simplement que les pratiques sont en cohérence avec la réglementation.

WANTED : UN CHIEF DATA OFFICER ET UNE ORGANISATION CENTRÉE SUR LA DATA

Il faut profiter de la contrainte pour construire une vraie fonction de management des données personnelles, en lui donnant une dimension stratégique et opérationnelle, porteuse de valeur ajoutée. En clair, en faire une fonction constructive, plus que défensive.

Car la première révolution est culturelle : **il faut d'abord faire comprendre en interne que les données personnelles sont porteuses de valeur… dans la mesure où leur management se fait selon les meilleures pratiques uniquement.** Or, ces meilleures pratiques ne sont pas seulement techniques (rapprochement des bases de données pour les connecter entre elles, intégration d'analyses temps réel, etc.), mais aussi éthiques. Le respect des règles de base de la *Privacy* doit être le premier combat du *Chief Data Officer* et du *Data Protection Officer*. Ce combat s'accompagne en général de rappels fondamentaux sur le sens de la relation clients, les valeurs de l'entreprise, son rôle dans la société…

> **« *La Privacy* doit être le premier combat du *Chief Data Officer*. »**

La deuxième révolution est organisationnelle. Elle va toucher les processus de développement des nouveaux services, mais aussi toute la chaîne qui va de l'acquisition des données à leur stockage et à aux différents traitements qu'elles vont subir, sur l'ensemble de leur « cycle de vie ». Elle concerne là encore un périmètre de fonctions assez large dans l'entreprise, mais surtout des fonctions qui vont faire un usage stratégique de la donnée, en amont de la mise à disposition des services. Pour ces fonctions, de la Business Intelligence, du développement produits/services, de la relation clients et les chefs de projets techniques, ce sont des processus nouveaux qu'il faudra mettre en place. En intégrant à chaque étape la préoccupation éthique de la bonne gestion des données personnelles : minimisation, finalité, information…

La troisième révolution est très différente car elle va toucher à la veille nécessaire pour suivre l'évolution des outils disponibles pour mieux gérer les données, à l'intégration de ces technologies dans les processus opérationnels, et à la mise en œuvre effective de toutes les précautions sur l'ensemble du « cycle de vie » des données personnelles. Elle touche profondément à la façon d'organiser le domaine SI autour des données privées. Elle vise à garantir les principes du *Privacy by Design* de façon effective, une fois pris en compte dans la conception des services digitaux. Si les deux premières révolutions visent toute l'entreprise, et doivent ouvrir la voie à des garanties sur le système de gouvernance général de la donnée, cette troisième révolution va être plus facilement applicable service par service, projet par projet. On voit bien comment une entreprise va pouvoir s'engager sur le respect de grands principes d'organisation, la création de règles de gestion, ou la mise en place de moyens de contrôle. **On voit mal comment l'entreprise va pouvoir revendiquer, avec 100 % de certitude, que dans la totalité de ses systèmes et bases de données, sur un périmètre élargi à l'ensemble de ses filiales, à l'ensemble de ses fonctions, la protection de la *Privacy* est sans faille.** Les écueils les plus cités par les dirigeants IT sont celui de « l'héritage IT » (*IT legacy*, en anglais), et la mise en cohérence des outils et méthodes utilisés à l'échelle globale, pour les entreprises multinationales.

TOUTE LA CHAÎNE DE TRAITEMENT DEVRA SUIVRE

Si une entreprise peut s'engager sur le respect des règles de *Privacy* à l'échelle d'un service, c'est à condition que l'ensemble de ses fournisseurs et sous-traitants soit aussi fiable qu'elle sur ce point. Si un service inclut par exemple la possibilité pour l'utilisateur de gérer de façon autonome son niveau de *Privacy*, alors l'opérateur devra aussitôt tenir compte de toute modification – pensons à l'utilisation des données personnelles à des fins de marketing par exemple (emails personnalisés, publicité ciblée…). **Il est à parier que des offres vont se développer dans l'écosystème des fournisseurs IT sur l'ensemble de la chaîne de valeur de la donnée.** Hébergeurs de données, opérateurs en Big Data, éditeurs de logiciel d'analyse, les entreprises de services du numérique vont bientôt devoir être en mesure de revendiquer, ouvertement, leur conformité aux totale aux bonnes pratiques de la *Privacy* – pour que leurs propres clients puissent rassurer le public à son tour. C'est ainsi qu'une chaîne de services labellisés « *Privacy by Design* » va sans doute se développer – créant une opportunité de différenciation et de création de valeur.

Reste à le démontrer. Dans un monde où la suspicion n'a fait que grandir, comment une entreprise peut-elle être crédible à s'autoproclamer « éthique » dans le domaine de la donnée privée ? C'est ici qu'entrent en jeu les tierces parties, seules à pouvoir apporter une objectivité dans l'évaluation des bonnes pratiques sur la *Privacy*.

6

SEULE UNE CERTIFICATION EXTERNE PEUT CRÉDIBILISER **L'ENGAGEMENT DES ENTREPRISES**

UNE CERTIFICATION ENGAGE POUR L'AVENIR

L'innovation ne peut prospérer sans confiance, au-delà des bénéfices directs que cette innovation apporte tant aux individus qu'aux sociétés humaines dans leur ensemble. Comment les entreprises peuvent alors créer les conditions de la confiance dans leurs innovations ? D'après Edelman, grâce à la transparence. C'est-à-dire, plus concrètement, en rendant publics les résultats de tests, en se rapprochant de tierces parties comme les ONG ou les gouvernements…

Le règlement européen encourage lui-même la certification et la labellisation aux fins de démontrer le respect des dispositions du règlement (article 42 du RGPD). La certification apparaît dans ce règlement comme un engagement de l'organisation et aussi un moyen de le mettre en œuvre opérationnellement.

C'est dans ce registre que les organismes privés de certification, comme Bureau Veritas, interviennent. En tant qu'acteur économique, l'organisme certificateur se prononce sur la réalité d'une situation donnée. Celle-ci est évaluée non seulement au travers de la performance passée, mais aussi en projetant l'efficacité des process internes de l'entreprise sur le maintien de la performance dans le futur (c'est ce qui fait la spécificité de l'audit). **La certification et le label sont des garanties données pour le futur,** bien entendu limitées dans le temps (en général, entre 1 et 3 ans). Sur la base de cette garantie, d'autres parties prenantes (le client final, le partenaire commercial) prendront des décisions économiques de continuer - ou non - à « faire confiance ».

Au-delà de l'aspect temporel, **la certification ou la labellisation permettent de garantir des engagements qui par nature diffèrent du seul respect de la réglementation,** comme, par exemple, l'engagement de faire mieux sur plusieurs années. Ces démarches sont dites volontaires de la part des entreprises. Vu des parties prenantes elles préjugent de leur intégrité quant aux caractéristiques des produits ou services qu'elles souhaitent faire certifier.

L'histoire nous enseigne que **la certification privée et volontaire précède la normalisation publique.** Alors que la normalisation publique cherche le consensus a priori, la certification ou la labellisation privée le constate a posteriori, dans l'usage et dans la reconnaissance du label.

LES 6 AVANTAGES CLÉS D'UNE CERTIFICATION

1. Légitimée par le marché
Quelques acteurs d'une industrie peuvent lui donner sa légitimité en l'adoptant. Les entreprises leader sur leur marché deviennent des exemples à suivre et entraînent la majorité dans leur sillage.

2. Compréhensible du public
L'un des principaux reproches faits aux entreprises est la complexité de leur communication sur la protection de la vie privée : qui peut affirmer lire les CGU de tous les services auxquels il est abonné ?

3. Évolutive, facteur de progrès
Un label ouvre la voie à une démarche d'amélioration continue. Il peut comporter plusieurs « niveaux », et peut évoluer dans le temps pour devenir plus exigeant, ou recommander l'intégration de nouvelles solutions techniques. Il définit un standard pour le marché, discriminant sans viser l'élitisme.

4. Déployable dans le monde
Un label s'attache aux bénéfices utilisateurs plus qu'à la conformité aux réglementations qui varient selon les pays. C'est la seule démarche internationale.

5. Ouverte et transparente
Se faire certifier volontairement est un acte de transparence sur ses processus internes. Vis-à-vis de clients et partenaires industriels, c'est une garantie de performance réelle.

6. Capable d'adresser des sujets de gouvernance
Un label peut garantir que l'entreprise a mis en place une démarche structurée (stratégie, déploiement, responsable) pour gérer les données personnelles de ses clients, et pour s'améliorer régulièrement. Cette boucle de l'amélioration continue, à la base des normes « qualité » depuis un demi-siècle, est un processus puissant, comme le montrent les centaines de milliers d'audits réalisés chaque année par Bureau Veritas.

LA CERTIFICATION « DATA » DEVRA SE DÉCERNER À PLUSIEURS NIVEAUX

La certification ou la labellisation peut être conçue comme un système statique, se rapprochant de la conformité. Ou comme un processus dynamique lié à l'engagement de faire mieux dans le futur. C'est là un des points essentiels si l'on veut apporter une meilleure visibilité sur les pratiques des entreprises en matière de Privacy. La crédibilité d'un label dépend de sa capacité à apporter une certitude totale sur ce qu'il garantit : à voir trop grand ou à revendiquer des critères trop élevés, il serait inopérant. Un label devrait ainsi comporter différents « niveaux » :

- **Un label « entreprise », de type « *privacy best-in-class company* »** : On parle ici de management de la donnée, des procédures en place pour former, informer, intégrer progressivement les technologies de protection de la vie privée aux processus de l'entreprise. Il s'agit bien de limiter les risques, pas sur la sécurité informatique, mais sur le traitement des données par des individus ou partenaires externes ayant chacun des rôles et responsabilités définis sur une chaîne opérationnelle. Et ce type de label doit évidemment aussi inclure la prise en compte du sujet *Privacy* au plus haut niveau de l'entreprise, englobant les chartes et déclarations existantes. Un tel label sur la gouvernance peut à l'évidence être déployé sur un périmètre large, international, comme cela est le cas pour d'autres systèmes de certification (RSE par exemple)
- **Un label « produit ou service », de type « *privacy by design proofed product/service* »** : Ce label devrait être capable de garantir la réalité effective du respect de la vie privée dans le cadre de produits ou services précis – en garantissant que sa conception a bien pris en compte le respect de la vie privée dès l'origine – et en incluant cette fois des aspects techniques, marketing, ou de processus applicatifs, et l'ensemble des partenaires et sous-traitants.
- Le règlement européen prévoit enfin **des obligations pour l'ensemble des acteurs de la chaîne de traitement** dans une approche classique en matière de qualité, où le donneur d'ordre doit transférer ses propres obligations sur ses sous-traitants.

On doit donc plutôt parler d'un système de labels ou de certifications, que d'un label unique. Et on voit bien qu'une partie de la labellisation s'apparente à de l'audit de management, alors que l'autre est en réalité une certification de service.

Gouvernance	**Service**	**Gouvernance**
Type ISO 26000	**Privacy by design "checked"**	**Type RGPD**
Certification globale	**Certification délimitée**	**Certification globale**
Engagement volontaire	**Conformité**	**Conformité**
Amélioration continue		

UNE CERTIFICATION NE PEUT SE DÉCERNER QUE PAR UN TIERS DE CONFIANCE

Il existe déjà de nombreux abels. Plus d'une cinquantaine, rien qu'en Europe**.** D'initiatives entièrement privées ou liées à des efforts institutionnels, certains s'appuient sur des réglementations nationales voire régionales (européenne notamment), d'autres définissent leur propre liste de critères et de bonnes pratiques. Certains incluent un audit légal, d'autres un audit technique déclaratif uniquement, d'autres encore des outils de test automatiques pour identifier les failles de sécurité. Tous n'incluent pas la dimension essentielle, celle de la clarté et de l'exhaustivité de l'information au public sur la gouvernance de ses données personnelles. La multiplicité des labels pourrait produire l'inverse de l'effet visé : au lieu de restaurer la confiance, augmenter la confusion.

Établir un label n'est pas donné à toutes les organisations, publiques ou privées. **On ne s'improvise pas tiers de confiance. Il faut avoir solidement établi :**

- **Une légitimité** reposant sur une connaissance réelle des industries que l'on entend auditer et certifier.
- **Une réputation** sans faille, acquise au cours de nombreuses années.
- **Des outils** et processus analytiques, 100 % transparents.
- **Une position d'impartialité** envers entreprises et autorités.
- **Une capacité à soutenir le label** autour d'une image de marque internationale et forte.

C'est en effet un transfert de crédibilité de l'émetteur du certificat, comme Bureau Veritas, vers l'entreprise certifiée, qui se joue. La confiance dans l'émetteur du certificat se transmet à l'entreprise certifiée.

BIENVENUE DANS L'ÈRE DE LA RESPONSABILITÉ NUMÉRIQUE DES ENTREPRISES

Sur la *Privacy*, les enjeux sont de taille pour les entreprises. Perte de confiance, évolution ralentie sur certains secteurs, perte d'opportunités sur des services à très haute valeur ajoutée… Si le commerce électronique a été un facteur essentiel du développement de l'économie, c'est grâce à la réaction rapide des écosystèmes bancaires sur les sujets de sécurité des transactions. La même réaction est aujourd'hui attendue par les entreprises qui offrent des services supposant l'utilisation de données privées. La *Privacy* est l'un des enjeux majeurs à venir, et pas seulement pour les acteurs du numérique.

Le déploiement des réflexions et efforts autour de la *Privacy* est comparable à ce que l'on a pu observer ces 30 dernières années avec la responsabilité sociale et environnementale des entreprises. **D'abord vue comme une contrainte, la RSE s'est révélée une opportunité : meilleure maîtrise des risques, recherche d'optimisation des coûts liés aux consommations** (eau, matières premières, énergie) et au traitement des déchets, nouveau territoire de communication et de différentiation… L'émergence de la RSE s'est faite de façon non réglementée d'abord, encadrée par la suite. Elle s'est accompagnée d'initiatives spontanées (chartes, labels, etc.) qui se sont inscrites dans le paysage au fil du temps. Et elle a finalement été sanctionnée par l'apparition de normes dédiées. Ce qui n'a pas empêché l'existence de réglementations et de lois dans le domaine du travail, de l'environnement, etc.

Les réglementations sont nécessaires mais ne peuvent suffire. Elles ne « parlent » pas au public. Le retour à la confiance, et donc au développement de nos économies, dépend de démarches qui permettront à l'individu de se sentir remis au centre du jeu. En reprenant le contrôle sur ses données, en ayant la certitude que les services sont construits sur une relation équilibrée, chacun pourra à nouveau adhérer sans arrière-pensée à la relation gagnant-gagnant que proposent aujourd'hui les entreprises : une maîtrise de ses données, pour des services plus personnalisés et davantage de valeur ajoutée.

Le terme de « responsabilité numérique des entreprises » commence à apparaître, çà et là. Elle pourrait inclure de nombreux aspects (l'inclusion numérique, par exemple), mais elle englobe avant tout la protection des données privées. C'est un domaine transverse et stratégique dans l'entreprise, qui renforce la position de l'entreprise sur ses marchés – tout comme la RSE. De même que les sujets environnementaux sont de plus en plus coordonnés par un Directeur RSE, ne pourrait-on pas imaginer que les questions de *Privacy* soient confiées à un garant interne, transverse à toutes les directions, rattaché au plus haut niveau de l'entreprise ? C'est ainsi que nous voyons se dessiner l'avenir de la protection des données personnelles en entreprise : rattachés à la RSE, considérés de la même façon que ces questions qui ont gagné de figurer aux ordres du jour des *Executive committees* ces dernières années. L'évolution se fera à moyen terme.

Avec plus de 70 années de pratique, reconnue dans le monde entier, la certification volontaire est un outil parfaitement adapté au contexte et aux besoins de l'économie digitale. Disposant à la fois d'une marque reconnue en B2B et en B2C, sur tous les continents, Bureau Veritas se positionne comme l'organisme de certification de référence de la gouvernance des données.

Bureau Veritas lance une offre de certification, à décliner avec l'ensemble des acteurs industriels de tous secteurs, pour leur permettre de faire leur propre mutation digitale, en toute sécurité.

Bureau Veritas a plus de 180 années d'expérience aux côtés des acteurs de l'économie pour les soutenir dans leurs engagements de transparence et d'amélioration envers leurs parties prenantes. Notre vision du numérique digital nous fait entrevoir son extraordinaire pouvoir de création de valeur et de transformation pour les années à venir. Forts de nos savoir-faire, portés par notre vision, conscients de nos responsabilités comme acteur de la confiance dans les échanges économiques, nous accompagnons aujourd'hui l'émergence de la *Privacy* comme un levier d'opportunité pour les entreprises qui sauront s'en saisir.

La Privacy
PAR BUREAU VERITAS

BV se positionne uniquement comme organisme certificateur ou vérificateur indépendant et propose d'aider à la création d'une certification mondiale autour de la protection des données privées. Cette certification sera déployée sur trois niveaux :

Une certification « Privacy checked » / « Privacy by Design »

- Permet de revendiquer un Label « Privacy by Design » en mettant en œuvre une conception d'offre, une architecture de données et des moyens de type « pseudonymisation » ou autres
- Permet de démarrer dans la certification Privacy sans transformer l'ensemble de l'architecture IT
- Accessible à certaines entreprises plus facilement

Une certification « Gouvernance »

- Une labellisation internationale – indépendamment des exigences locales de compliance
- Permet de se concentrer sur le système de management de la donnée, sans entrer dans des audits techniques de moyens
- Instaure un processus d'amélioration continue sur la Privacy
- Déclinable sur le modèle de la Responsabilité Sociale des Entreprises (RSE)
- S'applique à tous les types d'entreprises

Une certification au titre du Règlement Européen (RGPD)

- En réponse à l'article 42 du règlement européen
- Décernée sur la base d'un référentiel découlant du règlement
- Certification volontaire pour les entreprises

Les processus internes vérifiés sont ceux de la gouvernance des données.

Le modèle opérationnel de la certification dépend des géographies et des activités couvertes ainsi que de la complexité organisationnelle de l'entreprise.

BUREAU VERITAS

En savoir plus sur la protection des données personnelles :
move-forward-with-privacy.bureauveritas.com

Pour nous contacter sur ce sujet :
move-forward-with-privacy@bureauveritas.com