RGPD : COMMENT GÉRER LES DONNÉES SENSIBLES ?

Un livre blanc conçu par

COHERIS

AVANT-PROPOS

Le nouveau Règlement général sur la protection des données (RGPD), applicable dans les Etats membres de l'Union européenne dès le 25 mai 2018, a suscité de nombreuses publications privilégiant le plus souvent l'angle juridique. Ce livre blanc, conçu par Coheris, prend le parti de se focaliser plutôt sur les problématiques concrètes des entreprises, sur les démarches et sur les outils qui permettent de se mettre en conformité avec le RGPD.

Il vise en particulier à apporter aux entreprises des pistes pertinentes et des solutions efficaces pour résoudre le problème important des données personnelles « sensibles » – relatives à certains sujets comme l'origine ethnique, la religion, les opinions politiques, la santé ou la sexualité – dont la collecte et le traitement sont interdits par le nouveau règlement.

Disséminées notamment dans les zones de texte libre des applications (CRM, RH, ERP, etc.), ces « données personnelles à caractère particulier » sont trop souvent négligées par les entreprises car difficiles à exploiter et à contrôler avec des moyens humains.
Elles sont pourtant cruciales pour la conformité au RGPD et leur détention peut exposer à de très lourdes sanctions.

Nous sommes convaincus qu'en adoptant une démarche proactive et en utilisant, par exemple, des outils d'analyse, de *data mining* et plus précisément de *text mining*, les entreprises peuvent faire de cette nouvelle contrainte réglementaire une opportunité de mieux maîtriser leurs données, comme les amène à le faire le RGPD.

SOMMAIRE

I. LES PROBLÉMATIQUES

1. RGPD : toutes les entreprises sont concernées
2. Données personnelles : raison légitime ou consentement obligatoire
3. Données « sensibles » : traitement interdit

II. LA DÉMARCHE

1. Sensibiliser les collaborateurs et nommer un DPO
2. Cartographier les données et les traitements
3. Analyser le risque encouru
4. Fiabiliser les données des zones de texte libre
5. Mettre en place des outils de pilotage et de contrôle

III. LES SOLUTIONS

1. Cartographie des données sensibles : traiter l'historique
2. Outil de « contrôle de texte » : accompagner les pratiques en temps réel
3. Transformer la contrainte réglementaire en opportunité

COHERIS

LES PROBLÉMATIQUES

LES PROBLÉMATIQUES

RGPD : toutes les entreprises sont concernées

Le règlement général sur la protection des données (RGPD) – ou GDPR en anglais (*General Data Protection Regulation*) – est le nouveau texte de référence en matière de protection des données personnelles dans l'Union européenne.

Ses dispositions sont directement applicables dans l'ensemble des 28 Etats membres.

Visant à harmoniser et à renforcer la protection des données personnelles des individus dans l'UE, le RGPD se décline en une série de droits pour les citoyens et d'obligations pour les entreprises.

Toutes les entreprises, quelle que soit leur taille, qui « traitent » des données personnelles sont concernées, que ces données concernent des clients, des fournisseurs, des salariés ou toute autre catégorie de personnes... Et la notion de « traitement des données » doit s'entendre ici au sens large, puisqu'il inclut notamment la collecte, l'enregistrement, la structuration, le stockage, la modification, la consultation, l'utilisation, la diffusion ou toute autre forme de mise à disposition des données.

Autant dire qu'aucune entreprise ne peut s'exonérer de ce règlement et que celui-ci impacte directement la manière dont sont gérées les données personnelles.

Concrètement, un client peut, par exemple, accéder gratuitement à ses données personnelles et demander quel usage l'entreprise en fait une fois qu'elle les a collectées, ou encore exiger que l'entreprise efface ses données.

« *Avec le RGPD, les entreprises doivent mieux maîtriser les données personnelles dont elles disposent* », souligne Jean-Baptiste Gardebled, datascientist senior de Coheris. « *Auparavant, il suffisait quasiment, pour être dans la légalité, de déclarer ses fichiers de données à la CNIL (Commission nationale de l'informatique et des libertés). Désormais, c'est différent : cette déclaration* a priori *des fichiers n'est plus obligatoire… Mais* ***à chaque instant, l'entreprise doit être en mesure d'expliquer dans le détail de quelles données elle dispose, à quelles fins elle les utilisent et quels traitements elle applique*** ».

Le RGPD met l'accent sur la finalité du traitement : l'entreprise doit donc s'assurer, et pouvoir prouver, que toutes les données qu'elle récolte ont une utilité.

LES PROBLÉMATIQUES

Données personnelles : raison légitime ou consentement obligatoire

Les données personnelles, qu'est-ce que c'est ?

L'article 4 du RGPD définit *la « donnée à caractère personnel »* comme ***« toute information concernant une personne physique identifiée ou identifiable »*** – c'est-à-dire pouvant être identifiée, directement ou indirectement.

Autrement dit, est une « donnée personnelle » toute information qui peut être rattachée à une personne physique.

Sont ainsi considérées comme des données personnelles le nom, le prénom ou la photographie du visage, mais aussi la date et le lieu de naissance, l'adresse du domicile, l'adresse électronique, le numéro de téléphone, le pseudonyme, l'adresse IP ou certains « cookies », qui peuvent être reliés à la personne par recoupement d'informations.

Ces données personnelles peuvent même être subjectives, comme des avis ou des appréciations figurant par exemple dans les zones de commentaires des logiciels de l'entreprise (CRM, RH, ERP, etc.).

Même si le nom ne figure pas et que l'on a juste un identifiant codé (pseudonymisation), à partir du moment où dans le système d'information de l'entreprise, il est possible de rattacher cet identifiant codé à l'identité de la personne, on est dans le cadre du traitement de données personnelles et le RGPD s'applique.

LES PROBLÉMATIQUES

A quelles conditions une entreprise peut-elle détenir des données personnelles ?

Pour avoir le droit de détenir ces données personnelles, l'entreprise a besoin d'une base légale, en d'autres termes, d'une **raison légitime.**

L'exécution du contrat est l'exemple le plus courant de base légale utilisée en entreprise pour traiter une donnée à caractère personnel. C'est le cas, par exemple, d'une adresse postale collectée pour envoyer un courrier ou une commande. Dans ce cas, le consentement de la personne est considéré comme implicite puisqu'il fait partie intégrante de l'exécution du contrat.

De même, si pour l'exécution d'un contrat, il existe des catégories d'âge ou des niveaux de revenus qui déclenchent l'accessibilité à un service ou à un produit, l'entreprise doit nécessairement – et donc peut – détenir ces informations pour réaliser la prestation pour le compte de son client.

Pour autant, avoir une raison légitime de détenir l'information n'est pas forcément suffisant en soi… Car le RGPD précise également que tout traitement d'une donnée à caractère personnel, sorti de l'exécution stricte de la finalité pour laquelle elle a été collectée tel que par exemple l'exécution d'un contrat, doit faire l'objet d'une information au client, avec le droit pour celui-ci de s'y opposer.

Par exemple, si un site marchand a besoin de l'adresse postale de son client pour livrer ses produits, il n'a pas, en revanche, de raison légitime de détenir le numéro de sécurité sociale de son client. Pour recueillir et traiter ce type d'informations, il devra donc obtenir une base légale justifiant le traitement de cette donnée tel **le consentement – libre et éclairé –** des personnes concernées.

LES PROBLÉMATIQUES

Données « sensibles » : traitement interdit

Les données « sensibles », qu'est-ce que c'est ?

Le RGPD distingue des « catégories particulières de données à caractère personnel », également dénommées « données sensibles » par la CNIL, qu'il est strictement interdit de collecter, de détenir et de traiter (sauf dérogations spéciales).

Selon l'article 9 du RGPD, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, sont interdits.

Il est également interdit de stocker des commentaires inappropriés sur un individu, comme des jugements de valeur ou des insultes.

Quel est le risque encouru ?

Même si la CNIL imposait déjà des règles strictes dans ce domaine et si certaines entreprises ont été condamnées en France pour avoir détenu, dans les fichiers de données sur leurs clients, des informations relatives à l'origine ethnique ou à l'orientation sexuelle, ou même des insultes, l'application du RGPD devrait néanmoins se traduire par des contrôles renforcés.

Et surtout l'ampleur du risque augmente considérablement, puisque le montant maximal d'amende pour non-respect de la réglementation peut atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel de l'entreprise, auquel s'ajoute un risque pénal pour les responsables de l'entreprise pouvant aller jusqu'à la prison.

LES PROBLÉMATIQUES

DE NOUVEAUX DROITS POUR LES PERSONNES

Le RGPD étend et conforte les droits des citoyens sur les données personnelles que les entreprises détiennent sur eux. Autant de nouvelles fonctionnalités à intégrer dans les applications et les outils d'analyse des entreprises.

- Droit d'accès (article 15)
Une personne peut obtenir du responsable du traitement l'accès aux données personnelles la concernant. Elle doit également pouvoir connaître les finalités du traitement réalisé, la durée de conservation des données, ainsi que les destinataires éventuels de ces données.

- Droit de rectification (article 16)
Un individu a également le droit de faire rectifier, dans les meilleurs délais, les données personnelles le concernant, dans le cas où celles-ci sont inexactes ou incomplètes.

- Droit d'effacement, « droit à l'oubli » (article 17)
Il peut aussi obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de ses données personnelles.

- Droit à la portabilité (article 20)
Le droit de portabilité permet à un individu de demander à une entreprise de lui fournir, « *dans un format structuré, couramment utilisé et lisible par machine* », l'intégralité de ses données personnelles, afin qu'il puisse les transférer à un autre prestataire.

- Droit d'opposition à un traitement (article 21)
La personne concernée peut s'opposer à un traitement de ses données personnelles, notamment en cas de profilage à des fins de prospection.

LES PROBLÉMATIQUES

Des données difficiles à traiter mais à ne pas négliger !

Ces données sensibles ne sont donc pas à négliger car elles peuvent nuire à la conformité au RGPD et entraîner un risque juridique et financier important.

Or, elles sont trop souvent ignorées des entreprises car elles sont notamment disséminées dans les zones de texte libre des applications (CRM, RH, ERP, etc.), où sont saisis des commentaires sur les personnes (clients, fournisseurs, employés, etc.).

Ces données peuvent prendre la forme de commentaires du type « *Mme Untel est en congé maladie / en congé de maternité, la rappeler plus tard* » ou « *M. Untel ne peut pas être contacté à cette date parce que c'est ramadan / parce que c'est shabbat* ».
Derrière ces commentaires a priori anodins, saisis le plus souvent sans intention malicieuse, se cachent pourtant des données sensibles, qui doivent au minimum lever une alerte. Même si, dans certains cas, on peut se demander si les indications en question sont suffisamment précises pour entrer dans le cadre des données personnelles, la force du RGPD nécessite au minimum une attention nouvelle.

UN CONSENTEMENT « POSITIF, LIBRE ET ÉCLAIRÉ »

Pour recueillir et exploiter des données personnelles non nécessaires à l'exécution du contrat avec son client, l'entreprise doit obligatoirement obtenir le consentement de ce dernier et pouvoir prouver qu'elle l'a obtenu.

Selon le RGPD, ce consentement doit être donné « *par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord* ». Il n'est donc plus question de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.

Pour cela, le principe de « traitement loyal et transparent », sur lequel se fonde le nouveau règlement, exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. Elle doit savoir si ses données personnelles sont exploitées, par qui et à quelle fin.

Ce principe de transparence impose également que l'information communiquée au public sur ce sujet soit concise, aisément accessible, facile à comprendre et formulée en des termes clairs et simples.

LES PROBLÉMATIQUES

Il faut donc être en mesure d'identifier les données sensibles présentes dans les zones de commentaires libres des applications des entreprises.
Mais ce n'est pas simple car ces données sont très volumineuses et non structurées, donc difficiles à maîtriser et à exploiter pour les entreprises.

Il est en effet quasiment impossible de contrôler humainement tous ces champs de commentaires : ce serait trop long et trop coûteux. Pour une seule base de données, les masses existantes de commentaires varient généralement de quelques centaines de milliers à plusieurs millions. Si l'on multiplie par le nombre d'applications de l'entreprise, on conçoit aisément que la tâche devienne vite titanesque.

« *Pour apurer un historique ou contrôler au fil de l'eau ce qui rentre, il faudrait pouvoir relire avec un regard réglementaire chacun des commentaires qui passent*, précise Jean-Baptiste Gardebled. *Pour donner un ordre de grandeur, pour une personne, lire 1 000 commentaires par jour est une tâche lourde mais à peu près réalisable. Si on a un million de commentaires, le seul projet de relecture de ces commentaires se chiffrerait à 1 000 jours-hommes ! Ce qui n'est pas tolérable pour une entreprise* ».

ETUDE D'IMPACT SUR LA VIE PRIVÉE

Lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le RGPD impose au responsable du traitement d'effectuer préalablement une analyse d'impact sur la vie privée des personnes concernées.

Cette étude d'impact sur la vie privée ou PIA (*Privacy Impact Assessment*) doit notamment contenir une description des traitements envisagés et de leurs finalités, une évaluation des risques pour les droits et libertés des personnes concernées, ainsi que les mesures envisagées pour faire face à ces risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection de ces données.

LES PROBLÉMATIQUES

Faut-il effacer ses données sensibles ?

En continuant à détenir ce type de données dites « sensibles », les entreprises se retrouvent donc en situation de risque juridique.

Pour ne plus détenir ces données sensibles, la décision « de facilité » serait d'effacer tous les commentaires. Mais en écartant ainsi un risque juridique, elles prendraient le risque de perdre des informations utiles pour la gestion des dossiers (clients, salariés, etc.).

Si elles veulent conserver ces champs de commentaires, auxquels elles accordent une valeur et qui peuvent contenir « de la donnée précieuse », les entreprises peuvent se doter, comme le suggère la CNIL, d'outils d'analyse qui permettent de fiabiliser ces données et de limiter le risque réglementaire.

LA DÉMARCHE

LA DÉMARCHE

L'application de ce nouveau règlement s'inscrit clairement comme une nouvelle étape dans le changement de culture déjà amorcé depuis quelques années vers des entreprises centrées sur la donnée. Il représente aussi l'opportunité de « remettre à plat » ses datas et de balayer l'ensemble des problématiques de données au sein de l'entreprise.

Pour respecter la réglementation, les entreprises doivent mieux maîtriser leurs données. Cela passe par l'organisation, les process, le système d'information, mais aussi très probablement par l'analyse et l'utilisation de nouveaux outils de *data mining* comme le *text mining*.

Concrètement, quelle démarche adopter et quelle méthodologie mettre en place pour se mettre en conformité avec le RGPD sur les données sensibles ?

Sensibiliser les collaborateurs et nommer un DPO

Il est d'abord indispensable de sensibiliser l'ensemble des collaborateurs aux nouvelles règles du RGPD et aux impacts qu'il a sur les processus de l'entreprise.

Les commerciaux par exemple, qui collectent directement des données sur des clients ou des prospects, doivent se poser un certain nombre de questions afin de s'assurer d'être en conformité avec les droits des personnes et les obligations des entreprises. Selon l'article 13 du RGPD, le responsable de traitement doit également fournir, lors de la collecte de données personnelles, un certain nombre d'informations à la personne concernée.

Il convient également, dès le départ, de nommer un Data Protection Officer dit **DPO** (Délégué à la Protection des Données en français) ou un « représentant RGPD » pour les petites entreprises – dont la mission est de s'assurer de la conformité avec le règlement.

Il faut aussi, pour commencer, dresser un état des lieux de la situation actuelle afin de construire sa feuille de route, de prévoir les actions à mener et de définir les mesures techniques et organisationnelles à déployer.

LA DÉMARCHE

Cartographier les données et les traitements

« ***Pour s'inscrire dans le cadre du règlement, la première étape consiste à réaliser une cartographie des données et des traitements*** », **explique le data scientist de Coheris.** « ***Cela impose en amont que l'entreprise soit capable d'identifier, de retracer et de détailler l'ensemble des données personnelles dont elle dispose sur chacun des individus et la manière dont elle les utilise (qui, comment et à quelle fin)*** ».

« *De plus, le règlement suggère fortement, voire impose, la constitution d'un «* registre des traitements *», qui détaille l'ensemble des enregistrements, transformations, calculs et autres utilisations de la donnée dans l'entreprise* ».

Il s'agit de cartographier les données personnelles collectées et les traitements associés, et d'identifier le lieu de stockage des datas. Une tâche difficile à réaliser de manière précise, mais une tâche à laquelle les entreprises vont pourtant devoir s'atteler.

« ***Il faut pouvoir identifier et lister tous les types d'informations personnelles détenues sur un individu (client, salarié, etc.) et en assurer la légitimité le plus souvent soit au travers de l'exécution du contrat soit au travers du consentement éclairé de l'individu*** », souligne l'expert.

Cette étape doit conduire en particulier à la mise en place de process permettant un accès aux différents droits ouverts aux personnes par le RGPD sur les données que l'entreprise détient sur eux : droits d'accès, de consultation, de modification, d'effacement (« droit à l'oubli »), à la portabilité…

LA DÉMARCHE

En vertu du droit à la portabilité, un client peut par exemple demander à une entreprise une extraction de l'ensemble des données que celle-ci détient sur lui de façon à faciliter la transmission de ces informations à un nouveau prestataire, par exemple dans le secteur des télécoms, de la banque ou du e-commerce.

Dans ce cadre, l'ensemble des données personnelles à transmettre doit être vu de manière large, puisque les listes d'achats, par exemple, en font partie.

LE RÔLE CENTRAL DU DPO

Selon le RGPD, toute entreprise qui traite de manière massive ou récurrente des données personnelles doit désigner un DPO (*Data Protection Officer*, en français Délégué à la protection des données).
Sa principale mission est de s'assurer que l'entreprise soit en conformité avec le cadre légal relatif aux données personnelles. Il est le garant du respect du règlement et le point de contact avec l'autorité de contrôle, en l'occurrence la CNIL.
Il conseille également les responsables des traitements sur l'application du règlement et supervise les réponses aux sollicitations des personnes souhaitant exercer leurs droits dans le cadre du RGPD. Le DPO joue le rôle de chef d'orchestre de la gouvernance des données dans l'entreprise.
Pour certaines entreprises, le recours à la création d'un comité de pilotage « RGPD », composé par exemple de membres du Comité de direction ou du Comité exécutif et de représentants RGPD par métiers ou services, peut suffire avec la contribution du service juridique de l'entreprise ou des Conseils externes.

LA DÉMARCHE

Analyser le risque encouru

En même temps que la cartographie des données et des traitements, il faut aussi réaliser une analyse du risque encouru.

De manière plus générale, le RGPD va solliciter de plus en plus des arbitrages des juristes d'entreprise ou des Conseils externes, qui vont devoir valider la licéité des traitements.

Fiabiliser les données contenues dans les zones de texte libre

Au cours de la phase de cartographie, il faut veiller en particulier à différencier les données personnelles « classiques » et les données personnelles dites « sensibles ».

Le contrôle des commentaires figurant dans les zones de texte libre des applications de l'entreprise (CRM, etc.), dans lesquelles peuvent figurer des données sensibles, pose en effet un problème spécifique, qui n'est pas résolu par les méthodes classiques d'analyse des systèmes d'information.

Ce contrôle, indispensable à la conformité avec le RGPD, nécessite l'utilisation d'outils spécifiques et peut être mené en parallèle des adaptations des process et du système d'information. Pour traiter ce problème, la CNIL recommande de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants. Cette solution n'est cependant pas satisfaisante pour bon nombre d'entreprises pour lesquelles l'utilisation de ces zones de texte libre permet d'assurer un meilleur suivi des dossiers clients et de personnaliser la relation commerciale. Dans ce cas, la CNIL préconise de réaliser des audits réguliers et de recourir à des outils automatiques.

NE PAS NÉGLIGER LA SÉCURITÉ

La question de la sécurité des données ne doit pas non plus être négligée.

Les données doivent être utilisées uniquement dans le cadre des finalités pour lesquelles elles ont été collectées. Les entreprises doivent ainsi être proactives dans la détection d'anomalies, de piratage ou de vol de données.

Les mesures de sécurité, qu'elles soit de nature informatique ou physique, doivent être adaptées en fonction de la sensibilité des données, des risques et conséquences qui pèsent sur les personnes en cas d'incident.

Mettre en place des outils de pilotage et de contrôle

Au-delà des enjeux juridiques et de gouvernance, les entreprises ont en effet besoin concrètement d'outils de monitoring et de contrôle pour la mise en œuvre opérationnelle de la conformité au RGPD.

On peut par exemple utiliser des solutions de type *data mining* ou *text mining* permettant d'identifier et de monitorer, en temps réel ou en différé, les données sensibles saisies dans les zones de commentaires des applications de l'entreprise. Ainsi, toute saisie non conforme peut être détectée et corrigée.

« *Ce type d'outils permet non seulement d'« apurer le passif », de traiter tout l'historique et les masses existantes de commentaires figurant dans le CRM, mais aussi d'accompagner, en temps réel, les pratiques quotidiennes de saisie des commentaires par les différents opérateurs concernés (commerciaux, téléconseillers, etc.)* », précise Jean-Baptiste Gardebled.

LES SOLUTIONS

LES SOLUTIONS

Cartographie des données sensibles : traiter l'historique

La cartographie des données sensibles vise donc à identifier les données de ce type saisies dans les champs de texte libre des applications de l'entreprise.

Les outils de *text mining* fouillent dans les zones de commentaires libres pour identifier des mots, des expressions ou des notions rattachées aux domaines considérés comme « sensibles » par la réglementation.

Conçues grâce la data science, ces méthodes de « fouille de texte » permettent ainsi une reconnaissance efficace des données sensibles en utilisant un dictionnaire de mots et d'expressions classés par thématiques et correspondant à la définition des données personnelles « à caractère particulier » du RGPD.

Une analyse et des tableaux de bord permettent ensuite de mettre en avant les thématiques « sensibles » les plus présentes dans les textes, de façon à pouvoir se concentrer sur les risques potentiels les plus importants.
L'entreprise et ses juristes peuvent alors arbitrer, en fonction des risques et de l'intérêt des données, s'ils valident ou s'ils écartent certaines détections ou alertes.

Les règles de détection dépendent bien sûr du contexte, en particulier du secteur d'activité et du « métier » de l'entreprise. Par exemple, la détention d'informations de santé sur les clients est légitime pour une mutuelle d'assurance, mais elle ne l'est pas pour un vendeur d'électroménager.
Les règles de détection et les algorithmes de lecture doivent donc être suffisamment souples et « calibrables » pour que l'on puisse les adapter au contexte de chaque entreprise.

Ce type de solution permet de traiter une volumétrie importante de données et permet ainsi d'éviter la charge – difficilement soutenable sur les plans humain et économique – d'une relecture exhaustive par des collaborateurs en interne.

Le contrôle régulier, en mode différé, de la présence d'expressions interdites ou correspondant à des données « sensibles » dans les champs de texte libre des applications des entreprises permet également d'appliquer le calcul d'un score de criticité à de nouveaux verbatim.

LES SOLUTIONS

Outil de « contrôle de texte » : accompagner les pratiques en temps réel

Mais les entreprises ont également besoin d'outils de « contrôle de texte » pour accompagner les pratiques quotidiennes de saisie des commentaires. Des outils capables de détecter les données sensibles en temps réel, au moment même de la saisie.

Il s'agit donc ici d'une démarche proactive : plutôt que de nettoyer l'existant régulièrement, on met toutes les chances de son côté pour que les nouvelles données entrées dans l'application (CRM, RH, etc.) soient conformes au règlement.

Ce type d'outil réalise ainsi une pré-validation du contenu des commentaires : si l'on prend l'exemple du CRM, lorsqu'un opérateur (un commercial, un téléconseiller ou tout autre collaborateur ayant accès au CRM) saisit un commentaire, l'algorithme indique les points non conformes ou présentant un risque vis-à-vis des règles sur la protection des données sensibles, qui peuvent se glisser dans le texte saisi.

Une notification immédiate (blocage ou alerte) s'affiche alors dans la zone de texte et permet une action corrective immédiate ou ultérieure par un superviseur ou un opérateur.

L'outil suggère également des alternatives pour remplacer les mots ou les expressions interdits par des mots ou des expressions conformes au RGPD.

LES SOLUTIONS

Grâce à l'intégration de ce type d'outil dans les applications des entreprises, les responsables de traitement peuvent ainsi contrôler ces zones de risques pouvant nuire à la conformité de l'entreprise à la nouvelle réglementation.

Ces solutions de *data mining* et de *text mining* sont beaucoup plus avantageuses pour les entreprises qu'un éventuel traitement humain, dont la durée et le coût ne seraient pas soutenables.

PRIVACY BY DESIGN

Le RGPD introduit également le principe de **« protection des données dès la conception »** (*privacy by design*), qui impose aux entreprises de prendre en compte les exigences relatives à la protection des données personnelles dès la conception des produits, des services et des systèmes exploitant des données à caractère personnel.

Le nouveau règlement consacre également la règle de la « sécurité par défaut » (*security by design*), qui impose à toute organisation de disposer d'un système d'information sécurisé (article 25).

CONCLUSION

Transformer la contrainte réglementaire en opportunité

Bien qu'il puisse apparaître a priori comme une contrainte lourde pour les entreprises, ce nouveau règlement peut être une réelle opportunité de nouer des relations bien plus qualitatives avec les clients et les prospects.

En effet, la digitalisation et les nouvelles technologies ont permis aux entreprises de collecter un volume considérable de données personnelles, y compris sensibles, sur lesquelles les personnes concernées n'avaient plus aucun contrôle.

A l'heure où certaines affaires défraient la chronique, la transparence sur l'usage des données personnelles imposé par le RGPD est aujourd'hui nécessaire pour créer le climat de confiance indispensable à une relation client de qualité.

Pour les plus proactives, celles qui sauront se doter des outils nécessaires pour mieux maîtriser et analyser leurs données, le RGPD pourrait donc se révéler finalement plus un bénéfice qu'un coût.

Le RGPD oblige à repenser la gestion des données dans l'entreprise. Compte tenu des règles restrictives qu'il édicte, des mesures structurelles et organisationnelles qu'il impose et des lourdes sanctions qu'il prévoit en cas de manquement, **le nouveau règlement pousse les entreprises à passer d'une simple « gestion des données » à une véritable « gouvernance des données »**.