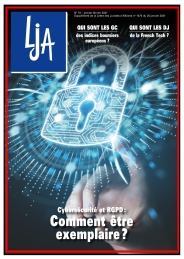
LJA LE MAGAZINE HORS-SERIE
Pays : FR
Périodicité : Bimestriel



Date : Janvier - fevrier 2021
Page de l'article : p.1,18,19,20,...,
Journaliste : Ondine Delaunay

N° 70 – janvier-février 2021
Supplément de la Lettre des Juristes d'Affaires n° 1475 du 25 janvier 2021

LJA

QUI SONT LES GC des indices boursiers européens ?

QUI SONT LES DJ de la French Tech ?

Cybersécurité et RGPD :

Comment être exemplaire ?

LES DÉBATS LJA

Cybersécurité & RGPD : exemplaire que jamais ?

Propos recueillis par Ondine Delaunay

À l'automne dernier, l'ICO britannique a infligé des amendes records à deux groupes – British Airways et Marriott International – pour ne pas avoir suffisamment protégé les données de leurs clients, en violation de leur obligation de sécurité au titre du RGPD. Ces décisions ont été rendues en application du mécanisme de coopération européen, le guichet unique, prévu par le RGPD. La CNIL n'est pas en reste et enchaîne les amendes pour des manquements liés aux données personnelles. Carrefour, Amazon, Google, la start-up Nestor, ou encore très récemment le ministère de l'Intérieur… Ces décisions traduisent la nécessité impérieuse de mettre en place des mesures de sécurités adaptées et une vigilance permanente. Dans ce cadre de coopération entre les autorités de protection des données européennes, comment les entreprises se sont-elles adaptées ? Qu'est-ce qui reste perfectible ? Comment le contexte actuel de crise nuit à l'exemplarité et comment y remédier ?

Éric Barbry, associé, cabinet Racine, Jeanne Bossi Malafosse, associée, cabinet Delsol Avocats, Florence Graveline, chef du service des études juridiques et DPO de la SACEM, Guillaume Desgens-Pasanau, magistrat - professeur des universités associé, responsable du certificat de spécialisation DPO, Alain Bouillé, délégué général du Cesin (club des experts de la sécurité de l'information et du numérique) & Clara Hainsdorf, associée, cabinet White & Case

© PHOTOS : MARK DAVIES. DR

LES DÉBATS LJA

Comment être plus

État des lieux de la mise en conformité des entreprises françaises avec le RGPD au niveau de la sécurité des données

GUILLAUME DESGENS-PASANAU : Les entreprises et administrations sont montées en compétences sur le sujet de la sécurité des données pour s'adapter au nouvel environnement du RGPD. Une prise de conscience s'est effectuée. La question de la sécurité informatique est, aujourd'hui, au centre de l'évaluation du risque de conformité. La Commission nationale de l'informatique et des libertés (CNIL) a clairement annoncé qu'elle se positionnait comme un acteur incontournable de la cybersécurité, avec l'Agence nationale de sécurité des systèmes d'information (ANSSI) et l'autorité judiciaire. Sa politique de contrôles et de sanctions le démontre parfaitement. Depuis 2018, plus de la moitié des sanctions porte sur la sécurité informatique. Des sanctions allant jusqu'à plusieurs millions d'euros ont ainsi été prononcées par la CNIL au cours des deux dernières années.

Ceci-dit, en termes d'analyse du risque, il ne faut pas considérer uniquement celui lié à la CNIL. Le risque d'un contentieux judiciaire qui pourrait être engagé par une personne fichée ne doit pas être négligé.

ÉRIC BARBRY : Il y a deux types d'entreprises. Celles qui ont effectué un travail d'analyse sérieux en matière de sécurité et se sont aussi assurées contre les risques cyber ; et celles qui pensent que les fuites n'arrivent qu'aux autres et qui conservent leur niveau de sécurité préalable au RGPD. Elles font des économies à court terme en se satisfaisant de leur niveau de sécurité relatif.

Le nombre de sanctions rendues est pourtant significatif dans le seul domaine des manquements en termes de sécurité. Les contrôles de la CNIL ont été réguliers, même en période de pandémie. Nombre d'entre eux ont porté sur des aspects liés à la sécurité. C'est un point d'extrême attention de la part de la CNIL, qui nous avait d'ailleurs prévenus.

Avant l'entrée en vigueur du RGPD, la CNIL avait rappelé les articles 34 et 35 de la loi Informatique et libertés de 1978 et que pour elle les obligations de sécurité, même renforcées, n'étaient pas une nouveauté. L'article 34 fixait l'obligation pour les responsables de traitement de sécuriser leurs traitements. L'article 35 était relatif à l'obligation de gérer la sécurité avec les sous-traitants. La

CNIL avait alors déclaré qu'il ne fallait pas attendre de mansuétude de sa part sur ce sujet puisque le RGPD n'est pas une novation. Il prévoit simplement des renforcements et quelques procédures nouvelles, telles que l'analyse d'impact ou l'obligation de notification des violations de sécurité. Le *privacy by design* vient aussi renforcer toute la réflexion sur la protection des données avant la mise en œuvre du traitement. La CNIL n'a donc pas changé de philosophie, elle a dit ce qu'elle allait faire et fait ce qu'elle a dit. Elle a toujours eu une vision attentive des problématiques de sécurité. Le RGPD lui a juste donné une opportunité, une résonance nouvelle.

Il est clair que la prise de conscience relative à l'obligation de sécurité est directement liée aux nouvelles sanctions du RGPD. Un risque de condamnation administrative important auquel s'ajoute un risque de contentieux généralisé de type *class action* en matière de réparation de préjudice. Aujourd'hui les entreprises s'en sortent encore bien en ne supportant que des amendes administratives, mais la *class action* envisagée contre British Airways fait réfléchir.

JEANNE BOSSI MALAFOSSE : Pourquoi parle-t-on d'avantage de cybersécurité qu'auparavant ? D'une part, en raison du phénomène de digitalisation et de numérisation de tous les secteurs d'activité qui n'existait pas au préalable. Mais aussi parce que le RGPD impose des obligations non pas nouvelles, mais qui doivent être démontrées à tout moment. Elles supposent de documenter et de s'interroger sur des sujets sur lesquels on passait un peu vite auparavant. Il faut cependant nuancer selon les secteurs car, dans certains, par définition, la sécurité a toujours été au centre de l'attention. Je pense notamment aux données de santé ou à celles touchant à la sécurité publique.

Je perçois néanmoins aujourd'hui une forme de normalisation de la sécurité. En effet assurer la sécurité d'une application consiste souvent à devoir être homologué, certifié ou agréé. Il faut être en mesure de respecter des normes qui sont de plus en plus nombreuses et qui ont tendance à élever le niveau de sécurité requis en fonction des situations bien sûr. Par exemple, il est impossible d'héberger des données de santé à caractère personnel sans être certifié et le niveau de sécurité est élevé.

Bien gérer aujourd'hui la sécurité pour éviter une attaque cyber, c'est donc d'abord et avant tout anticiper les actions malveillantes : documenter ses actifs, cartographier ses traitements, faire des études d'impact pour évaluer le niveau de sécurité à mettre en place et sensibiliser l'ensemble du personnel aux enjeux de sécurité. C'est ensuite agir si malheureusement vous êtes victime d'une attaque en menant toutes les investigations nécessaires pour identifier la source et gérer ses effets notamment en termes de communication.

Clara Hainsdorf
associée,
cabinet White & Case

La notification des violations de sécurité

ÉRIC BARBY : Il ne me semble pas que les notifications à la CNIL des violations de sécurité aient beaucoup de résonnance. La CNIL est sans doute débordée, mais je ne vois pas de corrélation entre le nombre nécessairement exponentiel de notifications et celui des contrôles. Les contrôles relatifs à la sécurité proviennent encore plus souvent de « dénonciations » que de suite à une notification.

JEANNE BOSSI MALAFOSSE : Je crois que les entreprises ont tendance aujourd'hui à notifier trop rapidement à la CNIL, en quelque sorte pour se protéger. La CNIL communique peu à cet égard sur les notifications de violation de données qu'elle reçoit. Lorsqu'il y a une violation de données — définie très largement par le RGPD — les entreprises notifient trop souvent sans même avoir mené une enquête. Il faut pourtant faire intervenir des techniciens informatiques, savoir comment les données à caractère personnel ont pu être impactées

par le problème, si la rupture de sécurité a pu être de nature à porter atteinte aux droits et libertés individuelles des personnes concernées, etc.
Il convient de prendre un peu de temps pour apprécier la nature de la violation, savoir s'il est vraiment nécessaire de notifier à la CNIL et surtout auprès des personnes concernées, ce qui peut avoir des conséquences importantes pour l'image de l'organisation.

GUILLAUME DESGENS-PASANAU : Dans son dernier rapport annuel, la CNIL explique qu'un de ses projets est de rendre publiques, de manière anonymisée, les notifications de violations de données qui lui sont adressées et de les traduire dans des fiches visant à orienter les professionnels. Ce serait très utile car il n'existe aucun référentiel sur ce sujet. Le RGPD prévoit une notification à la CNIL lorsqu'il y a un risque pour les libertés, la vie privée et la protection des données. Cette notion de risque est d'interprétation variable et aujourd'hui il n'existe quasiment aucun référentiel. Ce manque de précision assure au régulateur un large pouvoir d'interprétation. D'ailleurs dans toutes les décisions de sanction récentes, on peut lire que la CNIL reproche au responsable de traitement de ne pas avoir notifié le problème de sécurité.

FLORENCE GRAVELINE : Rappelons que l'entreprise doit notifier à la CNIL mais, s'il y a des conséquences sur la vie privée, également individuellement aux personnes concernées par la violation de données. Les attaques sont de plus en plus médiatisées et les entreprises ont conscience de ces problèmes de sécurité. Tout particulièrement avec la crise sanitaire, les cyberattaques et la communication de l'ANSSI ont donné de l'écho à ces problématiques qui paraissent de moins en moins hypothétiques. Les dirigeants y sont désormais très attentifs. La communication autour du RGPD a aidé les DPO à obtenir des leviers. Et la médiatisation actuelle autour des cyberattaques interpelle les dirigeants qui se demandent si, dans leur entreprise, tout est conforme en termes de sécurité.

CLARA HAINSDORF : Ce qui est aussi intéressant, c'est que tant les responsables de traitement que les sous-traitants ont une obligation de notification au titre du RGPD. L'obligation de sécurité transcende ainsi la question de savoir quel est le statut de l'entreprise : responsables et sous-traitants doivent en effet tous deux garantir la sécurité des données. Cette obligation est véritablement pérenne.

Le risque de sanction

CLARA HAINSDORF : Tout manquement au RGPD et à la loi Informatique et libertés fait encourir aux entreprises un risque de sanctions financières mais également un risque réputationnel. Sur les questions de cybersécurité, cependant, les manquements peuvent avoir des conséquences bien plus substantielles, notamment un risque de paralysie de l'activité de la société. Les salariés peuvent ainsi être empêchés de travailler, sans avoir accès aux données, et ce risque concerne toutes les entreprises, quelle que soit leur taille, quel que soit leur secteur. Ce risque touche même des personnes physiques puisque la CNIL en a sanctionné encore récemment. Les responsables de traitement passent alors rapidement du statut de victime à celui d'auteur de manquements s'ils n'agissent pas en temps et en heure pour notifier la violation (délai de 72 heures à respecter). C'est pourquoi, en cas de doute sur la gravité ou l'impact de la violation des données, il reste prudent de notifier la violation de données dans les 72 heures, quitte à compléter la notification ultérieurement.

GUILLAUME DESGENS-PASANAU : Si le risque de sanction de la part du régulateur est plus important qu'avant, les statistiques globales sur les contrôles et les sanctions démontrent tout de même que le risque reste limité. Je

Éric Barbry
associé,
cabinet Racine

m'étonne d'ailleurs que trois ans après la mise en place du RGPD, la CNIL ne soit pas plus montée en puissance sur ce sujet. Elle effectue 300 contrôles par an, et a prononcé 8 sanctions au cours de l'année 2019 selon le dernier rapport. Ces statistiques sont à peu près les mêmes qu'avant l'adoption du RGPD, quoique le montant des amendes prononcées est plus important.

La sécurité constitue en outre l'arbre qui cache la forêt du RGPD. Les professionnels ne doivent pas s'imaginer que les questions de protection des données personnelles ne sont que des sujets de sécurité informatique. C'est un écueil dans lequel il ne faut pas tomber mais les professionnels issus du monde de la sécurité et des systèmes d'information ne s'en rendent pas forcément compte, contrairement aux juristes. Aujourd'hui, les questions de conformité au RGPD, au-delà de la sécurité, couvrent d'autres sujets comme la question centrale de la licéité et de la proportionnalité des traitements mis en œuvre, les durées de conservation, la proportionnalité, les transferts de données à l'étranger. Force est de reconnaître qu'en sanctionnant beaucoup sur les questions de sécurité, la CNIL n'a pas forcément envoyé un bon message. C'est peut-être aussi parce qu'elle avait indiqué que, durant les premières années de mise en œuvre du RGPD, elle serait davantage dans une approche pédagogique et qu'elle n'irait pas, par exemple, sanctionner les professionnels sur les nouvelles obligations de documentation de la conformité, telles que la rédaction d'études d'impact, ou la tenue d'un registre de traitement des données. D'ailleurs, sur le plan statistique, on remarque que, cette année, elle a un peu moins sanctionné sur le fondement de la sécurité et davantage sur d'autres. Dans les années à venir, les professionnels devront au-delà de la sécurité, veiller à leur conformité sur les autres points de conformité évoqués dans le RGPD.

Alain Bouillé
délégué général du Cesin (club des experts de la sécurité de l'information et du numérique)

JEANNE BOSSI MALAFOSSE : La sanction que la CNIL a prise contre l'application Nestor, qui livre des repas à domicile, est par exemple très didactique. Elle attire l'attention de toutes les autres sociétés qui ont la même activité et qui ne sont pas rigoureuses avec leur fichier clients et leur fichier prospects. Chaque nouvelle sanction de la CNIL est toujours très commentée et a une valeur didactique afin que chacun prenne conscience des normes de sécurité à respecter.

On peut néanmoins aussi constater que la CNIL, prenant en compte les nouvelles dispositions du RGPD, a renforcé ses exigences sur la sécurité. Je suis frappée de voir le niveau de sécurité exigé par certains textes, que ce soit dans des délibérations de la CNIL, dans des méthodologies ou même dans des arrêtés pris après avis de la CNIL, et de constater surtout que la réalité du terrain reste encore loin de ces exigences et parfois même de leur compréhension par les acteurs. Il suffit d'aller dans les entreprises pour voir que les règles de bases — comme les mots de passe personnels — ne sont même pas respectées. Tandis qu'on exige le chiffrement des données, voire des niveaux de sécurité parfois inatteignables. Je crois qu'il existe encore un « gap » entre ce qui est attendu et la réalité de ce que les entreprises peuvent faire en pratique, en termes de coût notamment. C'est pourquoi la notion d'étude d'impact me paraît très intéressante, car elle permet d'apprécier ce niveau de sécurité en fonction de la société.

ÉRIC BARBRY : Depuis deux ans et demi, il aurait été utile que la CNIL ne fasse pas que réagir par des sanctions, mais ait également une démarche de construction de bonnes pratiques. Des lignes directives en matière de sécurité sont nécessaires, surtout pour les PME qui sont beaucoup touchées par les violations. Or force est de constater que la norme 27701 est encore peu connue et n'est pas adaptée aux ETI, PME et PMI c'est-à-dire à 95 % de notre tissu économique.

GUILLAUME DESGENS-PASANAU : Les responsables de traitement sont souvent livrés à eux-mêmes dans l'analyse du niveau de conformité et de la documentation interne, malgré l'assistance de leur DPO et de conseils externes. La logique du RGPD c'est que la CNIL n'intervient plus a priori, mais uniquement a posteriori. Or pour que ce système fonctionne, le régulateur doit fixer des règles du jeu précises et des référentiels

permettant aux entreprises d'évaluer correctement leurs risques, de connaître les préconisations en matière de sécurité et donc d'avoir un peu de prévisibilité. La situation actuelle est source d'une certaine insécurité juridique pour les entreprises. Les référentiels publiés par la CNIL sur ces questions de sécurité nous laissent un peu sur notre faim. C'est donc un challenge pour elle de développer ces outils d'aide à l'évaluation de la conformité, dans les prochaines années. Car le guide sur la sécurité des données date d'il y a plus de deux ans. Il existe par ailleurs une recommandation sur les mots de passe et trois ou quatre documents de ce type — qui sont en outre difficile à trouver sur le site internet de la CNIL — mais qui n'ont pas la même valeur juridique. Ce manque de référentiel clair met aujourd'hui les responsables de traitement en difficulté. Lors des contrôles, la CNIL déclare par exemple systématiquement vérifier les obligations de sécurité. Pourquoi ne pas directement publier le document qu'elle utilise pour faire ses contrôles ?

Récemment la sanction de Carrefour pour plus de 2 millions d'euros a révélé une multitude de manquements sur des sujets différents, dont celui de la sécurité. En parallèle il y a eu une sanction de médecins libéraux condamnés à quelques milliers d'euros pour avoir mal configuré leur box internet. On se demande comment s'y retrouver dans l'évaluation des risques au regard d'acteurs si différents… Les référentiels existant ne sont pas suffisants, et ils devraient être adaptés en fonction de la taille du responsable de traitement. Il y a un vrai sujet sur la conformité des TPI/TPE qui disposent de moyens très limités pour mettre en œuvre un plan de conformité.

La gestion des sous-traitants

ALAIN BOUILLÉ : J'étais, jusqu'à la fin de l'année dernière, le directeur cybersécurité du groupe Caisse des Dépôts. J'ai préalablement exercé des fonctions similaires au sein du groupe La Poste et dans une banque américaine. Or dans les grands groupes que j'ai traversés, nous n'avons pas attendu le RGPD pour nous occuper de la sécurité des données et en particulier celles à caractère personnel. Nous n'avons pas découvert la sécurité au mois de mai 2018. Le travail a été bien plus intense sur les aspects de pure conformité, c'est-à-dire les questions de documentation, etc. Avec parfois des questionnements sur l'utilité de ces mesures et la jauge pour être compliant.

Les entreprises qui ne s'étaient jusqu'alors pas trop préoccupées de sécurité informatique, en ont clairement payé le prix. Remarquons d'ailleurs que les victimes d'attaques ne sont pas les grandes banques qui ont investi dans la sécurité informatique depuis près de 30 ans. Ce sont celles qui ont informatisé leurs process que plus récemment, en intégrant tout et n'importe quoi sur les mêmes réseaux, notamment certaines entreprises industrielles, qui avaient les plus gros gaps en matière de sécurité informatique, et pas seulement d'ailleurs, sur les données à caractère personnel.

Après cette étape, est apparue la transformation digitale. Toutes les entreprises, y compris celles qui étaient très avancées sur le sujet, ont alors commencé à se digitaliser, c'est-à-dire à informatiser tous leurs process à grand renfort d'économies. On a demandé au DSI moyen de faire 30 % d'économies sur le budget de l'année d'avant, tous les ans. Les DSI ont alors externalisé à peu près tout. Ils ont analysé tous les traitements qui n'étaient pas vitaux pour l'entreprise, puis le développement et le support informatique ont suivi. Lorsque l'on regarde aujourd'hui quels sont les incidents liés au RGPD, dans 90 % des cas ce sont des problématiques de sous-traitants. Malgré toutes les exigences vis-à-vis des fournisseurs, les plus gros et en particulier les GAFAM, nous répondent ce qu'ils veulent dans des contrats qui pour la plupart ne peuvent être audités.

Jeanne Bossi Malafosse
associée, cabinet Delsol Avocats

Il est en outre important d'aborder la question du risque de déséquilibre. Le RGPD a mis, à juste titre, la lumière sur les données à caractère personnel. Mais les responsables cybersécurité s'en occupaient depuis longtemps ainsi que des autres données, à savoir les données stratégiques d'entreprise. Or, 90 % des données stratégiques d'entreprise ne sont pas à caractère personnel. Et aucun texte législatif n'oblige les entreprises à sécuriser ces données sauf celles très à la marge des OIV. J'ai été frappé, au milieu de cette « cloudification » massive des entreprises, par la légèreté de certains grands groupes, qui avaient d'un côté de grands chantiers RGPD mobilisant de grands cabinets externes et, de l'autre côté, la tendance à massivement externaliser, chez Google, Microsoft ou Salesforce, des données stratégiques d'entreprise. Il conviendrait de revenir à un juste équilibre car lorsque l'on recherche la conformité avant tout, l'on créé un déséquilibre car l'entreprise va rechercher à être en règle en se préoccupant du respect de la loi pour les données à caractère personnel au détriment des autres.

Guillaume Desgens-Pasanau
magistrat - professeur des universités associé, responsable du certificat de spécialisation DPO

CLARA HAINSDORF : Ce déséquilibre a en effet été constaté, mais nous avons aussi connu l'inverse. De grandes entreprises ayant l'habitude de traiter un important patrimoine informationnel constitué de données à caractère personnel et de données stratégiques non personnelles, se sont dit qu'elles allaient décliner la protection déjà mise en place et très robuste aux données personnelles. D'ailleurs, pour certains grands groupes qui dépendent de quelques sous-traitants clés, cette protection est déclinée non seulement au sein de l'entreprise pour l'ensemble des données, mais aussi auprès de ces sous-traitants clés, afin de limiter le risque de contamination, en cas de violation de données constatée chez ces sous-traitants dont le niveau de sécurité est souvent bien moins élevé. Cela peut prendre la forme d'une aide, d'un accompagnement, d'un financement, pour la mise en place de leur conformité. Si vérifier le niveau de sécurité de ses partenaires relève bien des obligations incombant à un responsable de traitement, cette obligation met également en lumière les difficultés que rencontrent aujourd'hui certains grands groupes à coopérer avec des start-up dont la maturité de protection n'est pas la même. Sans oublier que beaucoup de ces start-up sont situées en-dehors de l'Union Européenne, ce qui rend les transferts de données vers ces partenaires d'autant plus risqués compte tenu de la récente décision de la CJUE « Schrems II » supprimant le Privacy Shield.

JEANNE BOSSI MALAFOSSE : Ne pensez-vous pas que le risque vient souvent des sous-traitants tout simplement parce que l'architecture technique des systèmes d'information conduit aujourd'hui à beaucoup faire appel à eux ? Et peut-être davantage qu'hier ? Il peut exister pour certains traitements une multitude de sous-traitants qui doivent agir sous la responsabilité du responsable de traitement qui veille sur la chaîne de sous-traitance. Les risques de rupture de sécurité viennent donc souvent des sous-traitants. Il peut s'agir d'une insuffisance de sécurité, parfois découverte par hasard, par exemple au moment de beta tests ou à l'occasion d'un changement de BDD. On se rend alors compte qu'il y a une faille dans la base, que quelqu'un a essayé de la hacker et que les données ont été lues par des personnes non-autorisées. Et il est d'autant plus difficile ensuite de notifier que la faille de sécurité est ancienne.

ÉRIC BARBRY : Je souscris totalement à vos propos. La volumétrie de la sous-traitance est liée au développement des solutions cloud qui démultiplient les problématiques. Mais il faut quand même reconnaître que les entreprises ne sont pas très attentives. L'article 28 impose aux responsables de traitement de faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes. Les entreprises ont donc adopté des questionnaires de qualification mais force est de constater que l'on y trouve à boire et à manger et que ce questionnaire est plus souvent un alibi qu'un véritable travail d'analyse du niveau de maturité du sous-traitant au RGPD. Et même lorsqu'un prestataire le remplit, personne ne fait de vérifications réelles via des audits ou des inspections, sauf bien sûr à ce qu'il y ait eu des violations de sécurité avérées chez le sous-traitant auquel cas le DPO organise une « descente », en général avec le RSSI, pour mieux comprendre ce qu'il s'est passé. Les entreprises exemplaires sur ce sujet sont rares.

La course au PIA

ÉRIC BARBY : Je voulais également aborder la question de la course au PIA (Privacy Impact Assessment — en français EIVP : étude d'impact sur la vie privée). Il y a une grande confusion dans la nature même d'un PIA qui n'est pas une analyse de sécurité mais une appréciation plus globale du respect du RGPD dans sa totalité pour tel ou tel traitement. La sécurité en fait partie mais elle n'est pas l'alfa et l'omega du PIA. Faire faire des PIA par des consultants en sécurité seul est une hérésie et ne permet pas de répondre aux exigences du RGPD.

JEANNE BOSSI MALAFOSSE : L'étude d'impact n'est en effet pas seulement dédiée aux mesures de sécurité et à l'évaluation de leur niveau. C'est avant tout la description d'un traitement « passé au crible » des principes de protection des données, pour être en mesure d'en apprécier les risques au regard des droits et libertés individuelles.

CLARA HAINSDORF : Les entités dont nous parlions tout à l'heure qui notifient trop souvent sont d'ailleurs bien souvent les mêmes qui vont faire des PIA pour le moindre traitement à petit risque, alors même qu'il n'y a pas forcément de nécessité.

ALAIN BOUILLÉ : Lorsque la présence d'un DPO dans l'entreprise est devenue obligatoire, il a fallu recruter plusieurs milliers de personnes simultanément. Mais tous les profils n'avaient pas nécessairement le niveau de compétences requis. Bien sûr les outils proposés par la CNIL sur son site, comme le PIA, ont été très utiles mais il faut les utiliser avec pragmatisme. Nombre de DPO qui n'avaient pas forcément de recul, ou de formation nécessaire pour apprécier le PIA, ont appliqué les textes à la lettre en déployant des moyens exagérés pour traiter de minuscules sujets. J'ai vu des PIA de 200 pages sur des traitements qui ne valaient rien. Ils font perdre du temps, de l'énergie et de l'argent aux entreprises. Il y a une forme de jeunesse des méthodes et l'on n'a pas encore trouvé le juste équilibre dans l'application du RGPD.

FLORENCE GRAVELINE : Je trouve vertueux, dans cette appréhension du risque, de devoir se poser la question de savoir si c'est un traitement qui doit être soumis à une étude d'impact, de l'identifier en amont, au moment de la conception, pour mettre en place les mesures de sécurité adaptées au traitement, cela fait partie du *privacy by design*.

J'ai été CIL (correspondant informatique et libertés) avant d'être DPO, je traite des problématiques de données personnelles depuis de nombreuses années. Mais je reconnais mes propres limites en matière de sécurité étant, à la base, juriste. Je m'en remets donc entièrement à notre RSSI. Pendant un moment cette fonction a été externalisée. La Sacem a souhaité l'internaliser pour mettre en place une gouvernance de la sécurité renforcée et les mesures et process du RSSI participent à la conformité au RGPD. Notre travail est collaboratif et complémentaire. J'ai toujours considéré que le DPO, dans la mise en conformité au RGPD, était un chef d'orchestre, et le RSSI son premier violon. La sécurité est un socle de cette conformité qui doit être solide et le travail doit être mené main dans la main. Nommer un DPO s'il est seul à travailler à la conformité RGPD ne permet pas à l'entreprise de remplir ses obligations. La conformité au RGPD est l'affaire de tous. Tout le monde doit participer, en premier lieu la direction générale qui impulse cette conformité.

Florence Graveline
chef du service des études juridiques et DPO de la SACEM

La coopération européenne

CLARA HAINSDORF : À cette imprévisibilité juridique liée au manque de référentiel français, s'ajoute une insécurité globale sur la manière d'appliquer les différents référentiels européens. Une entreprise qui s'est établie dans un pays, s'attend bien sûr à être potentiellement sanctionnée par le régulateur local. Sauf qu'en raison d'arguments juridiques comme ceux de l'arrêt Google Spain, elle peut se voir finalement sanctionnée dans un pays où

elle ne s'était jamais considérée comme établie.

JEANNE BOSSI MALAFOSSE : Ne pensez-vous pas qu'il faut laisser le temps au temps ? L'objectif du RGPD est de parvenir à une certaine harmonisation européenne, mais il n'est entré en application que depuis trois ans ! Il faut aussi laisser du temps à la CNIL pour s'adapter et répondre aux besoins. Le développement de la numérisation a élevé le niveau de sécurité des données, c'est indéniable. Je me souviens que lorsque j'exerçais à l'ASIP Santé (aujourd'hui l'ANS), la mise en place de la procédure d'agrément des hébergeurs de données de santé avait suscité au départ quelques réticences au vu du niveau de sécurité exigé. Finalement, cela a permis de sécuriser davantage les données de santé et chacun aujourd'hui s'en félicite.

ÉRIC BARBRY : Pour l'instant je n'ai vu aucun effet positif de cette coopération européenne affichée entre les différentes autorités. J'ai plutôt vu des entreprises qui n'étaient pas spécialement localisées dans tel ou tel pays, mais qui à cause de la présence de clients locaux, se sont fait rattraper par la patrouille.

CLARA HAINSDORF : C'est pourquoi j'évoquais cet arrêt Google Spain et les risques de dérive liés à son application systématique. Il existe désormais un risque de sanction au niveau national dès que le groupe est plus ou moins établi dans un pays. Les autorités tentent néanmoins de lutter contre ce forum shopping.

ALAIN BOUILLÉ : Il y a quelques semaines, une entreprise française s'est faite condamner sur le fondement du RGPD au maximum

de la sanction, c'est-à-dire 4 % du chiffre d'affaires du groupe. C'était un montant énorme pour elle. Je perçois que les petites entreprises ressentent qu'il existe une certaine injustice dans le traitement des dossiers, notamment au regard de la manière dont sont traitées les GAFAM qui violent à longueur d'années, au vu et au su de tout le monde, les données à caractère personnel. Lorsque Facebook connaît une fuite, elle porte sur des centaines de millions, voire de milliard, de données. Et je n'ai pas encore vu une amende de 4 % de son chiffre d'affaires. Je constate donc un traitement à deux vitesses des amendes et il me semblerait utile de faire jouer le poids de l'Europe lorsque l'on s'attaque à de tels mastodontes. Rappelons tout de même que le RGPD trouve sa genèse dans les problématiques de gestion des données par les GAFAM. Mais finalement ces groupes restent dans une relative impunité.

GUILLAUME DESGENS-PASANAU : Je suis parfaitement d'accord avec vous. Si l'objectif du RGPD est d'harmoniser au niveau européen la gestion et la sécurité des données pour la renforcer, la réalité n'est pas encore celle-ci. Il y a clairement deux poids deux mesures entre des grandes structures qui peuvent s'organiser pour utiliser le processus de « guichet unique », se positionner dans un pays de l'UE où peut être que le régulateur sera moins exigeant, où le corps judiciaire sera moins mature sur ces sujets, et l'entreprise plus petite et française qui, elle, doit se confronter au régulateur français connu pour être l'un des plus exigeants en Europe.

JEANNE BOSSI MALAFOSSE : On ne peut que partager votre avis sur les GAFAM. Mais il faut reconnaître qu'ils ont l'habileté d'associer la personne à ce qu'ils font. Ils se protègent à travers leurs CGU. Rien de nouveau, mais finalement n'est-on pas partie prenante à tous ces excès ?

FLORENCE GRAVELINE : Bien évidemment l'attitude des GAFAM dans l'utilisation des données est choquante. Mais s'ils étaient seuls à faire l'objet de sanctions, les entreprises auraient l'impression que seuls les gros sont visés. En sanctionnant de plus petits acteurs dans différents secteurs d'activité, cela permet aussi de faire passer le message que tout le monde doit se sentir concerné par cette conformité et balayer devant sa porte. ■