Réglementations sur la confidentialité des données : comment soulager le fardeau administratif ?

Un rapport Ovum, commandé par Intralinks

Table des matières

Synthèse 1

Introduction 2

Les entreprises sont confrontées à des défis majeurs en matière de réglementation 4

La généralisation des solutions cloud est inévitable 4

Trop d'entreprises ne prennent même pas les mesures élémentaires pour protéger leurs données sensibles 5

Le caractère hétéroclite des règles sur la confidentialité des données rend les entreprises vulnérables 6

Les prochaines réglementations européennes risquent de nuire au dynamisme économique de l'UE 7

L'emplacement des données est le principal point de contrôle, mais il reste difficile à définir 8

La mise en conformité aux nouvelles réglementations est extrêmement coûteuse 9

Les entreprises basées aux États-Unis sont sous pression 9

Recommandations 10

Annexe 11

Méthodologie 11

Auteur 11

Ovum Consulting 11

Avis relatif aux droits d'auteur et clause de non-responsabilité 11

Synthèse

Le mouvement mondial pour la défense du droit à la vie privée engendre de nouveaux risques économiques et commerciaux

Les États adoptent de nouvelles lois, particulièrement strictes, en matière de respect de la vie privée pour protéger les données de leurs citoyens, préserver la sécurité nationale et, potentiellement, stimuler certains secteurs d'activité. Cette intensification des mesures de protection des informations sensibles et des données personnelles menace les stratégies, les pratiques et les processus des entreprises évoluant dans un cadre international.

Pour explorer l'impact de l'évolution des règles de confidentialité et de souveraineté des données, Intralinks a commandé au cabinet Ovum une grande enquête internationale, menée auprès de 366 décideurs IT au cours du troisième trimestre 2015.

Principales conclusions du rapport :

Les règlementations sur la confidentialité des données entrent en conflit direct avec les pratiques des entreprises concernant le cloud, les solutions Software-as-a-service (SaaS) et l'informatique mobile.

Le cloud computing fait désormais clairement partie du paysage IT des entreprises, et devrait continuer à se généraliser au cours de la décennie à venir. La généralisation, d'une part des processus métier à forte intensité informationnelle s'appuyant sur le modèle SaaS, et d'autre part des plateformes mobiles, rend extrêmement complexe la tâche consistant à contrôler l'emplacement des données tout en se conformant aux règlementations sur la vie privée. Pourtant, 78 % des répondants de l'enquête envisagent d'avoir recours à des applications SaaS et cloud au cours des trois prochaines années, y compris pour stocker et partager des données sensibles et réglementées.

Les dirigeants d'entreprise se montrent profondément pessimistes sur les conséquences potentielles des nouvelles réglementations en matière de protection des données

Notre enquête montre que les entreprises ont pris conscience des enjeux potentiellement problématiques de la confidentialité des données, mais peinent à leur apporter une réponse claire. Lorsqu'on les interroge sur la proposition de règlement européen sur la protection des données personnelles (GDPR / Data Protection Regulation), 52 % des répondants pensent que cela exposera leur entreprise à des amendes, et les deux tiers pensent que cela va les contraindre à réviser leur stratégie commerciale en Europe.

Les coûts associés à la mise en conformité réglementaire vont être substantiels, mais les coûts de la non-conformité seront encore plus élevés

Plus de 70 % des répondants prévoient d'augmenter leurs dépenses afin de répondre aux exigences en matière de souveraineté de données, et plus de 30 % envisagent une hausse de plus de 10 % des budgets au cours des deux prochaines années. Parmi les entreprises qui ont l'intention de revoir leurs stratégies de protection des données au cours des trois prochaines années, 38 % envisagent de recruter des experts en la matière, et 27 % vont nommer un *Chief Privacy Officer*.

Les entreprises basées aux États-Unis sont particulièrement vulnérables

L'effet Snowden est bien réel. Parmi les 20 plus grandes économies mondiales, les États-Unis sont considérés comme le pays le moins fiable et le plus susceptible de permettre un accès non autorisé à des informations sensibles, la Chine et la Russie arrivant respectivement en deuxième et troisième positions. Par ailleurs, 63 % des répondants estiment que le projet de règlement GDPR de l'UE va entraver encore davantage la compétitivité des entreprises américaines, et 70 % s'attendent à ce que cette nouvelle législation favorise les entreprises basées en Europe.

La plupart des entreprises n'utilise pas efficacement les technologies disponibles pour relever les défis de la confidentialité des données

De façon quelque peu alarmante, nombreuses sont les entreprises qui ne tirent pas parti des technologies étant à leur disposition pour protéger leurs données sensibles. Seulement 44 % des répondants surveillent les activités de leurs utilisateurs et prévoient un système d'alerte en cas de violation de leur politique de confidentialité, et seulement 53 % des entreprises disposent d'une méthode de classification de l'information pour contrôler les différents accès. Près de la moitié (47 %) ne dispose d'aucune politique ou mesure de contrôle régissant l'emploi des solutions grand public de stockage et partage de fichiers cloud (Dropbox, par exemple).

Les grandes entreprises mondiales doivent déployer une approche orchestrée de la souveraineté de données, couvrant à la fois les personnes, les processus et les technologies

Les dirigeants d'entreprise reconnaissent la nécessité d'adopter une approche équilibrée pour relever les défis de la souveraineté et de la confidentialité des données. Lorsqu'on les interroge sur leurs stratégies d'investissement, 55 % d'entre eux indiquent qu'ils envisagent de nouvelles formations pour leur personnel, 51 % qu'ils vont modifier et adapter des politiques existantes, et 53 % qu'ils vont déployer de nouvelles technologies.

En matière de confidentialité, les entreprises sont confrontées à un véritable patchwork de réglementations, souvent contradictoires et conflictuelles. Elles doivent donc s'ouvrir aux nouvelles technologies pour parer à toutes les éventualités

La révolution de la souveraineté des données risque d'engendrer une balkanisation du paysage technologique, différentes juridictions imposant des contraintes incompatibles les unes avec les autres quant aux modalités de stockage, de traitement et de partage des informations. Cette tendance est d'ores et déjà source de confusion et d'incertitude, laissant sans réponse un certain nombre de questions fondamentales, concernant notamment l'interprétation des exigences relatives à l'emplacement des données. Les entreprises doivent s'ouvrir aux nouvelles technologies pour se donner les moyens de s'adapter à un environnement réglementaire qui évolue très rapidement.

Introduction

Avant même que les révélations d'Edward Snowden n'exposent l'étendue des pratiques de surveillance électronique de la NSA (National Security Agency), la question de la protection des données était déjà en passe de devenir un problème majeur à l'échelle mondiale. Dans le sillage des controverses sur les pratiques d'espionnage des citoyens et des fuites massives de données survenues au cours de ces dernières années, les États ont dû reconnaître que leurs arsenaux juridiques existants en matière de confidentialité, conçus à l'ère du document imprimé, étaient désormais obsolètes et qu'il fallait intégrer les réalités de l'économie numérique. Cela a donné lieu à une vague de nouvelles législations sans précédent, visant à régir les modalités selon lesquelles certaines données sensibles peuvent être collectées, stockées, traitées et partagées.

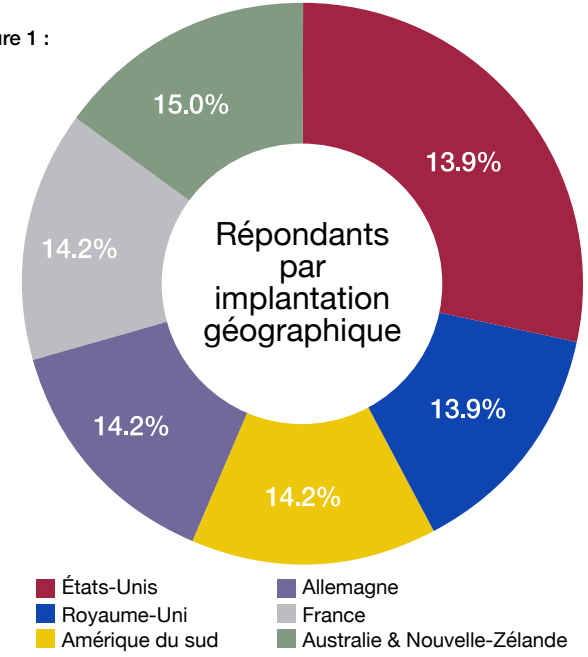
Des pays aussi divers que le Brésil, Singapour et la Russie procèdent actuellement à un durcissement de leurs réglementations. L'Union européenne (UE) est sur le point de finaliser un long processus de réforme réglementaire dans ce domaine, qui aura un impact sur toutes les entreprises implantées dans ses États membres. Si ces restrictions sont effectivement indispensables au moment où les frontières nationales des entreprises tendent à disparaître et où leurs employés deviennent de plus en plus mobiles, le recours croissant aux systèmes IT fondés sur le cloud est susceptible d'engendrer des conflits avec ces nouvelles dispositions. Les obligations de conformité découlant des nouvelles législations sont de plus en plus complexes, en particulier pour les entreprises qui opèrent dans une multiplicité de juridictions, et notamment pour les données stockées dans le cloud.

Au cours du troisième trimestre 2015, Intralinks, leader des solutions cloud de collaboration et de gestion du contenu d'entreprise, a commandé au cabinet Ovum une étude visant à mieux comprendre les implications de ces nouvelles réglementations pour les grandes entreprises mondiales. Plus spécifiquement, cette enquête visait à explorer les questions suivantes :

- Dans quelle mesure les grandes entreprises sont-elles préparées pour relever les défis de la souveraineté des données ?
- Quel sera l'impact des nouvelles réglementations en matière de confidentialité des données ?
- Comment les entreprises vont-elles adapter leur activité pour répondre aux nouvelles obligations en matière de protection des données personnelles ?
- Quelles sont les différences d'approche selon les pays et les juridictions ?
- Quelles seront les décisions technologiques qui permettront aux entreprises de se conformer aux nouvelles obligations en matière de confidentialité ?
- Quelles sont les meilleures pratiques pour s'adapter aux nouveaux cadres réglementaires ?

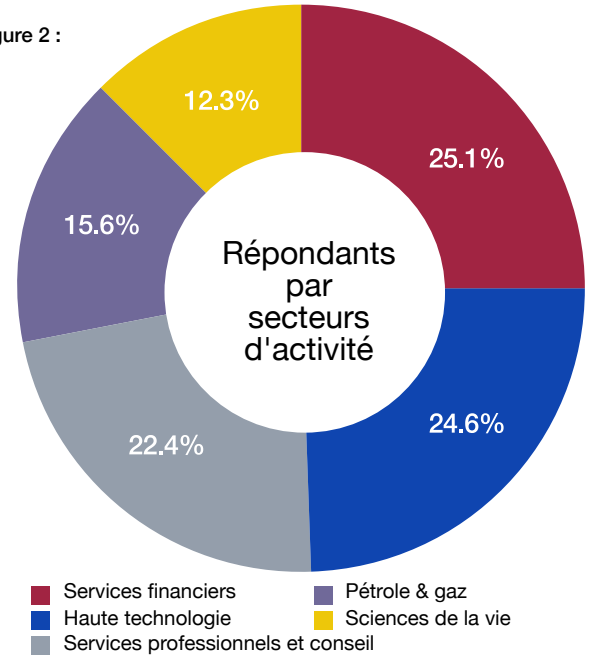
Ovum a mené son enquête auprès de 366 personnes à travers le monde, représentant des entreprises de différentes tailles et de divers secteurs d'activité (cf. figures 1, 2 et 3). Les profils des répondants ont été sélectionnés de façon à constituer un échantillon représentatif des différents types d'entreprise et des pays affectés par les nouvelles réglementations en matière de respect de la vie privée et de souveraineté des données.

Figure 1 :



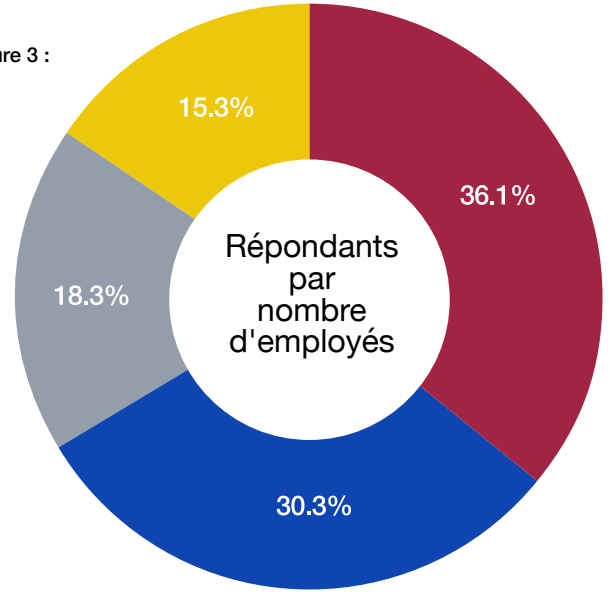
Source : Ovum

Figure 2 :



Source : Ovum

Figure 3 :



Source : Ovum

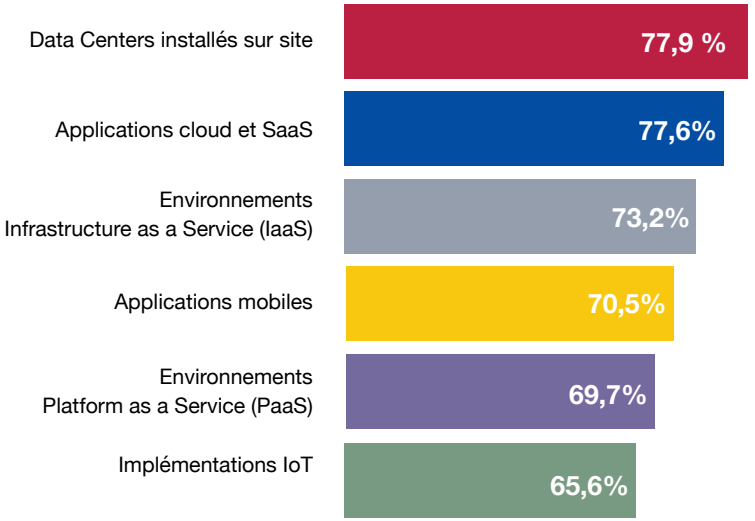
Les entreprises sont confrontées à des défis réglementaires majeurs

La généralisation des solutions cloud est inévitable

Le *cloud computing* est un levier de productivité pour l'entreprise moderne. Il permet en effet de connecter l'ensemble du personnel, et d'établir des relations entre les entreprises, leurs partenaires commerciaux et leurs clients. C'est également un vecteur de lien social pour chacun d'entre nous. Le cloud computing a transformé la façon dont nous communiquons et dont nous traitons l'information. Il a radicalement bouleversé la façon dont les plus grandes entreprises du monde conduisent leurs affaires et, en particulier, gèrent leurs budgets IT. Une récente enquête d'Ovum a ainsi établi qu'un sixième des budgets IT globaux des entreprises est d'ores et déjà consacré aux solutions SaaS, et que les solutions cloud sont appelées à fortement se développer. Environ les quatre cinquièmes des entreprises ont désormais recours, ou envisagent d'avoir recours, au cloud computing en s'appuyant sur différents modèles de déploiement (privé/public/hybride) et de service (IaaS/PaaS/SaaS). Cette proportion était de deux tiers au début de l'année 2014. Le marché est en pleine expansion avec les arrivées successives de nouvelles générations d'adoptants. La deuxième vague d'adoption a atteint son pic d'activité, et une troisième vague, formée par les retardataires, a commencé à prendre de l'ampleur en 2015.

Cette enquête consacrée aux enjeux de la souveraineté fournit de nouveaux éléments qui permettent de mesurer à quel point le cloud est aujourd'hui jugé suffisamment fiable pour l'hébergement des données sensibles et réglementées. Cela constitue un contraste frappant avec la situation qui prévalait il y a encore quelques années, lorsque la fiabilité du cloud soulevait de nombreux doutes et préoccupations. Cette technologie est désormais jugée suffisamment fiable pour protéger les actifs les plus sensibles (cf. figure 4), ce qui démontre une évolution nette des perceptions concernant sa contribution positive à la performance des entreprises. L'étude révèle également que 58 % des répondants s'appuient sur le cloud pour l'ensemble de leurs opérations métier, en dépit de l'impact potentiel des prochaines réglementations en matière de protection des données, qui visent toutes à encadrer les modalités selon lesquelles les données sont stockées, transférées, et traitées partout dans le monde. Il apparaît donc que, en dépit des évolutions du contexte réglementaire, les technologies liées au cloud computing sont désormais entrées dans les mœurs. Il n'en reste pas moins que l'encadrement juridique des données détenues dans le cloud est rapidement en train de s'imposer comme la problématique numéro un pour les services juridiques, les décideurs politiques et les entreprises, dans leurs efforts visant à instaurer un juste équilibre entre respect de la vie privée et impératifs de facilité d'accès et de productivité.

Figure 4 : Réponses à la question « Dans lesquels de ces environnements technologiques vos données sensibles et réglementées seront-elles utilisées au cours des prochaines années (jusqu'à la mi-2018) ? »



Pour Ovum, l'une des raisons qui explique le succès du cloud computing est le caractère limité des ressources. En effet, les ressources des entreprises sont souvent trop limitées pour assurer un degré de protection adéquat de leurs données sensibles ou réglementées, ou pour documenter leurs efforts de conformité si les données sont détenues en interne. La protection des données est d'ailleurs en train de devenir un nouveau facteur d'adoption du cloud : les clients attendent en effet que les prestataires cloud intègrent les meilleures solutions de sécurité au sein même de leurs services.

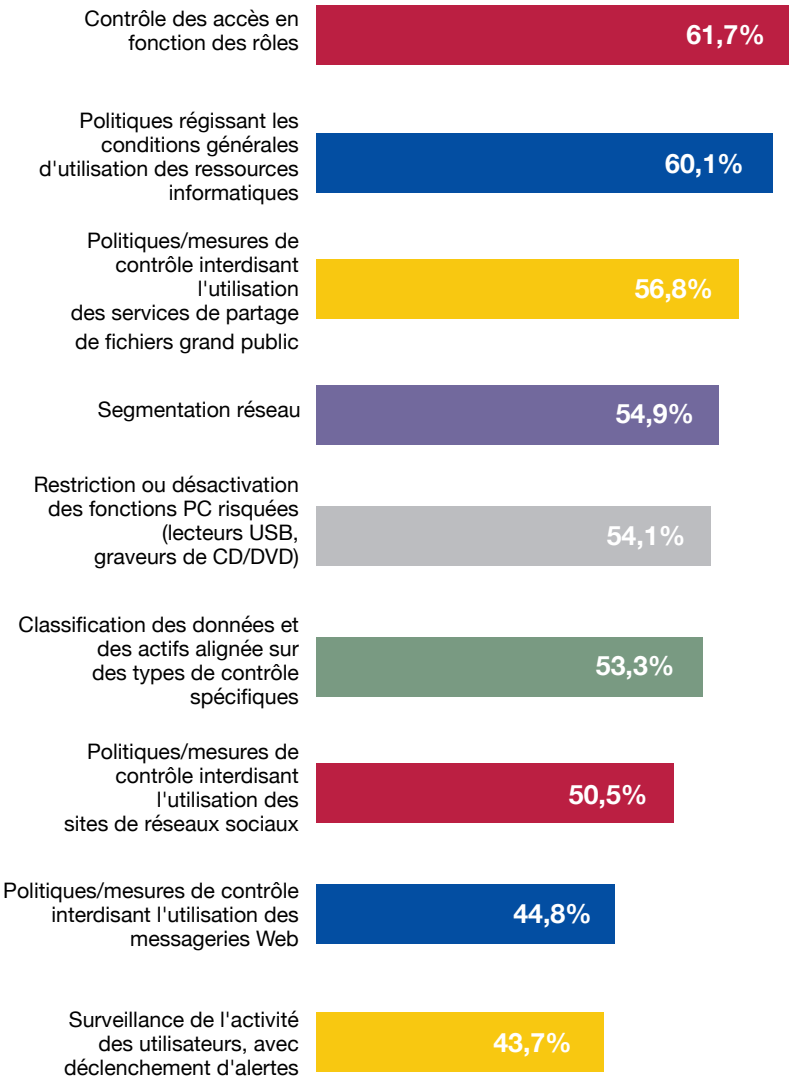
Trop d'entreprises ne prennent même pas les mesures élémentaires pour protéger leurs données sensibles.

Nous avons également constaté que de nombreux répondants ne prennent même pas les mesures les plus élémentaires pour protéger leurs données et se conformer aux exigences de conformité (cf. figure 5). Seulement 44 % des répondants surveillent les activités de leurs utilisateurs et prévoient un système d'alerte en cas de manquement aux dispositions de leurs politiques ; et seulement 62 % ont adopté des mesures de contrôle des accès à base de rôles. Un peu plus de la moitié (53 %) des entreprises classent leurs actifs informationnels de façon à faciliter le contrôle des accès. Notre enquête montre même que certaines mesures rudimentaires ne sont pas prises : ainsi, seulement 54 % des entreprises désactivent des fonctionnalités PC telles que les lecteurs externes connectés, et seulement 57 % bloquent l'accès aux applications de stockage et partage de fichiers grand public (Dropbox, etc.).

Les entreprises qui souffrent de telles lacunes en matière de protection des données se tourneront vraisemblablement vers les services cloud, plutôt que de devoir consacrer du temps et des ressources pour tenter de résoudre ces problèmes en interne. Une analyse plus approfondie des résultats de l'enquête montre que ce déficit général sur les mesures de confidentialité des données affecte en particulier les petites et moyennes entreprises pour lesquelles une mise à niveau des capacités de protection nécessitera vraisemblablement un investissement proportionnellement plus élevé.

Toutes les entreprises devraient renforcer la définition de leurs mesures de protection, à mesure qu'elles prennent conscience de l'élargissement de leurs responsabilités concernant la sécurité des données sensibles, et font appel aux prestataires cloud et SaaS pour accéder aux technologies requises.

Figure 5 : Réponses à la question « Quels politiques, processus et mesures de contrôle votre entreprise applique-t-elle actuellement pour assurer la protection des données et éviter les abus ? »



Source : Ovum

Le caractère hétéroclite des règles sur la confidentialité des données rend les entreprises vulnérables

Pour les entreprises qui n'ont pas encore mis en place de mesures de protection des données standard, l'entrée en vigueur de nouvelles lois plus strictes en la matière ne fera qu'aggraver la situation. Ces nouvelles lois sont déployées au plan local, sans le moindre cadre de gouvernance mondiale. Les grandes entreprises mondiales qui opèrent dans une multiplicité de juridictions doivent composer avec un véritable patchwork de cadres juridiques, chacun exigeant des réponses particulières (cf. tableau 1). La façon dont vont évoluer les cadres juridiques existants reste peu claire. *Safe Harbor*, l'accord qui régit depuis 15 ans les modalités de transfert de données entre l'UE et les États-Unis, a ainsi récemment été déclaré invalide. Cela affecte plus de 4 000 entreprises, qui ne peuvent plus transférer légalement leurs données de l'UE vers les États-Unis sans avoir recours à d'autres dispositifs juridiques tels que les clauses types ou les règles internes d'entreprise (BCR / *Binding Corporate Rules*). Cela engendre une certaine confusion parmi les grandes entreprises mondiales, en particulier celles qui sont implantées en Europe, quant à leur conformité aux cadres réglementaires en vigueur et aux mesures à prendre.

Tableau 1 : État actuel de la réglementation en matière de protection des données

Pays/région	Définition des données personnelles	Formulaires de consentement exigés pour le traitement de données à caractère personnel	Règles relatives au transfert de données personnelles à l'étranger	Demandes de données émanant d'entités publiques	Sanctions
UE	Informations relatives à une personne physique identifiée ou identifiable. Le projet de règlement couvre notamment les adresses IP.	« Consentement sans équivoque » Le projet de règlement vise à introduire la notion de consentement explicite.	Il appartient à la Commission européenne et aux États membres de décider si un pays tiers assure une protection adéquate ; si cela n'est pas le cas, des mesures de garantie doivent être mises en place.	Incertain après l'abrogation de la directive sur la conservation des données. Les lois nationales restent formellement en place.	Les sanctions sont décidées au niveau national. Le projet de règlement prévoit des amendes allant jusqu'à 2 % du chiffre d'affaires annuel de l'entreprise.
États-Unis	Peu clair. Variable selon les lois et les secteurs d'activité concernés.	Notion de « consentement par écrit ou par voir électronique » dans le Communications Act.	Absence de règles spécifiques. La Federal Trade Commission (FTC) soutient que le droit américain reste applicable même lorsque les données quittent les États-Unis.	Une ordonnance du tribunal (*court order)* est généralement requise. Le FBI et d'autres agences jouissent de certaines exceptions au titre du Patriot Act.	Sanctions variables selon les lois.
Australie	« Information ou opinion, qu'elle soit vraie ou non, et qu'elle soient enregistrée sous une forme matérielle ou non, concernant une personne physique identifiée ou étant raisonnablement identifiable. »	Les entreprises sont tenues de prendre des « mesures raisonnables au regard des circonstances » pour notifier un individu de la collecte des données.	Les entreprises procédant au transfert de données doivent prendre des mesures raisonnables pour veiller à ce que les principes de la loi ne sont pas violés une fois que les données auront été transmises dans un autre pays.	Une entité publique n'est pas habilitée à collecter des informations à caractère personnel si celles-ci ne sont pas raisonnablement nécessaires ou directement liées à une ou plusieurs de ses fonctions ou activités.	Sanctions civiles pouvant aller jusqu'à 1,57M USD (1,7M AUD) en cas de manquement grave ou répété à la loi.
Singapour	« Données, qu'elles soient vraies ou non, concernant une personne pouvant être identifiée à partir de ces données seules ou avec d'autres données ou informations auxquelles l'entreprise est susceptible d'avoir accès. »	Le consentement doit être obtenu par écrit ou, s'il est donné oralement, enregistré de manière à ce qu'il soit possible de s'y référer ultérieurement.	Les transferts de données ne sont autorisés que si le pays d'accueil garantit le même niveau de protection.	Les agences et organisations agissant au nom d'un organisme public sont exemptées des obligations découlant de la Loi sur la protection des données personnelles (PDPA/*Personal Data Protection Act*).	Sanction financière plafonnée à 799 000 USD (1M SGD).
Brésil	Peu clair. Le « Cadre des droits civils d'Internet » va être complété par une réglementation plus détaillée.	« Consentement libre, éclairé et explicite. » Cela devrait être défini plus en détails dans une règlementation à venir.	Le transfert de données est autorisé, mais les entreprises doivent se conformer à la législation brésilienne en cas de collecte/traitement de données survenant au Brésil.	La durée légale de rétention des informations est d'un an pour les registres de connexion des FAI, et de six mois pour les fournisseurs d'applications. La police ou les tribunaux sont habilités à exiger une prolongation.	Jusqu'à 10 % du chiffre d'affaires hors taxes de l'entreprise contrevenante au Brésil, et suspension temporaire ou complète des activités de collecte et traitement des données.

Source : Ovum, et extraits des textes législatifs

Les prochaines réglementations européennes risquent de nuire au dynamisme économique de l'UE

L'UE est la première économie mondiale en termes de PIB, selon le Fonds monétaire international (FMI) et la Banque mondiale. Cela lui confère la puissance nécessaire pour imposer ses normes réglementaires aux autres régions du monde, et toute législation européenne aura inévitablement un impact sur les entreprises qui conduisent leurs affaires dans un cadre international. L'UE a introduit ses premières dispositions en matière de confidentialité en 1995, avec la directive relative à la protection des données à caractère personnel. Il y a quelques années, cependant, un large consensus a émergé au sein des autorités de l'UE, sur le fait que les technologies avaient évolué, et qu'un nouveau cadre réglementaire (projet de GDPR) était nécessaire pour prendre en compte la généralisation des smartphones/tablettes, de la connectivité à haut débit et des services cloud dans les entreprises. Le tableau 2 résume les principaux changements introduits par le GDPR.

Notre enquête révèle que les grandes entreprises mondiales envisagent de modifier leurs opérations dans certains pays européens lorsque le GDPR sera entré en vigueur. Sur la base de notre échantillon, 78 % des entreprises américaines, 62 % des entreprises britanniques, 58 % des entreprises françaises, 46% des entreprises sud-américaines et 71 % des entreprises allemandes, australiennes et néo-zélandaises envisagent de revoir leur approche. Cela pourrait nuire sérieusement à l'économie de l'UE, dont la prospérité repose en grande partie sur les échanges internationaux. Ces décisions sont essentiellement fondées sur des considérations de gestion des coûts : 68 % des répondants estiment en effet que le GDPR va considérablement augmenter le coût des affaires dans l'UE. On constate par ailleurs que 85 % des entreprises américaines pensent qu'il sera plus difficile de rivaliser avec les entreprises européennes, ce qui pourrait entraîner une réduction du nombre de sociétés américaines implantées dans l'UE. Ces résultats montrent clairement l'immense incertitude générée par le projet GDPR : les entreprises anticipent un impact négatif sur leur activité mondiale et, vraisemblablement, sur l'économie de l'UE en général.

Une autre préoccupation soulevée par nos répondants est le risque lié aux amendes et pénalités. Les amendes infligées aux entreprises en cas de manquement aux dispositions du GDPR pourraient potentiellement représenter jusqu'à 2 % de leur chiffre d'affaires mondial, soit plusieurs milliards de dollars pour les plus grandes entreprises de la planète. Selon nos recherches, plus de 50 % des grandes entreprises mondiales anticipent des amendes au titre du GDPR. Si l'on procède à une analyse par pays et régions, on constate que 62 % des entreprises allemandes, 59 % des entreprises américaines, 53 % des entreprises britanniques, 42 % des entreprises françaises, 56 % des entreprises australiennes et néo-zélandaises, et 32 % des entreprises sud-américaines pensent qu'elles feront l'objet d'amendes au titre du GDPR.

Tableau 2 : Principaux changements introduits par le GDPR.

Problème abordé par le GDPR	Changement apporté	Impact
Guichet unique	Les entreprises devront assurer leur conformité avec une réglementation unique à l'échelle européenne, au lieu d'une par État membre	Simplification de la mise en conformité NB : il n'est toujours pas certain que ce plan entre en vigueur
Responsables du traitement des données	La législation en matière de protection des données couvre non seulement les responsables du contrôle des données (*data controllers*), mais également une nouvelle classe d'acteurs : les responsables du traitement des données (*data processors*).	Les prestataires de services cloud, fournisseurs de solutions SaaS et autres sont tenus de se conformer à la réglementation de l'UE relative à la confidentialité des données
Extra-territorialité	Les entreprises dont le siège est basé hors de l'UE sont tenues de se conformer à la réglementation si elles traitent des données relatives à des personnes résidentes de l'UE	Les prestataires de services tiers basés hors de l'UE pourraient avoir besoin d'investir dans des Data Centers locaux (approche « *as one* »)
Résidence des données	Les données relatives à des personnes citoyennes de l'UE ne peuvent pas être transférées hors de l'EEE sans couverture légale. (se reporter aux informations fournies en dehors de ce tableau pour plus de détails concernant la fin de la protection au titre de la certification *Safe Harbor*)	Comme ci-dessus
Profilage	Une personne concernée doit donner son consentement pour que ses données soient transmises à des responsables du contrôle des données autres que celui à qui elle les a initialement confiées à des fins de profilage	Cela aura un impact sur les responsables du traitement des données si ceux-ci transmettent les informations à d'autres responsables du contrôle des données, ou s'ils les utilisent eux-mêmes à des fins de profilage. NB : la question de savoir si le consentement doit être systématiquement explicite ou s'il peut être implicite fait encore l'objet de débats

Source : Ovum

De manière générale, la majorité des grandes entreprises mondiales (57 %) estime que le GDPR constitue une réaction excessive faisant suite aux révélations sur les pratiques de surveillance révélées par Edward Snowden. Curieusement, les répondants européens partagent également ce sentiment, puisque 57 % des répondants allemands, 51 % des répondants britanniques et 46 % des répondants français estiment que le GDPR est une réponse excessive aux problématiques de confidentialité des données. Encore une fois, la motivation sous-jacente à ces réponses est probablement liée à l'impact, en termes de coût, des amendes et de la nécessité de réviser les stratégies d'entreprise.

L'emplacement des données est le principal point de contrôle, mais il reste difficile à définir

Du point de vue juridique, la question de la localisation physique des données est essentielle. Dans le débat sur la souveraineté des données, les préoccupations centrales incluent notamment l'emplacement de ces dernières et la définition du point de contrôle pour les données à caractère personnel. Notre recherche montre que ces concepts, pourtant apparemment simples, engendrent de l'incertitude et de la confusion. La capacité à préserver la souveraineté des données d'entreprise (pour en contrôler l'accès) et à garantir la conformité est fortement tributaire de leur localisation physique, qui détermine les juridictions compétentes et les niveaux d'accès applicables. Or il est difficile, pour bon nombre d'entreprises, de contrôler précisément la localisation physique des données, dans la mesure où la plupart des systèmes (en particulier ceux qui opèrent dans le cloud) n'ont tout simplement plus recours à ce concept. La complexité engendrée par ce problème est aggravée par le fait que la définition exacte de la notion d'emplacement des données peut varier selon les différents volets d'un cadre législatif, et peut être ouverte à différentes interprétations juridiques. Pour garantir leur conformité, les entreprises auront donc vraisemblablement besoin de disposer d'options leur assurant un degré de contrôle sur l'emplacement physique, logique, juridique et politique de leurs données. De fait, des procédures juridiques sont d'ores et déjà en cours dans différents tribunaux à travers le monde. Elles reposent sur la définition du lieu à partir duquel les données sont hébergées et contrôlées, et sur la juridiction compétente concernant ces dernières (prenons par exemple le cas de l'affaire Microsoft portant sur des données stockées à Dublin, en Irlande, ouverte à la demande d'un juge américain).

Notre enquête montre qu'il n'y a actuellement aucun consensus clair sur les réponses à apporter aux problématiques liées à l'emplacement des données (cf. tableau 3) . Nous avons également constaté que 50 % des entreprises sondées avaient l'intention de revoir leur approche générale du contrôle des données au cours des trois prochaines années. Cela reflète l'incertitude des répondants quant au bien-fondé de leur approche actuelle compte tenu des nouvelles exigences, et aux nouvelles réponses à apporter. Cela pourrait également indiquer que les entreprises attendent l'émergence d'une norme claire avant d'agir. Tout cela plaide fortement en faveur d'une approche offrant diverses options technologiques, permettant notamment de contrôler l'emplacement physique et logique des données.

Tableau 3 : Approches actuelles/possibles des répondants en matière de confidentialité des données

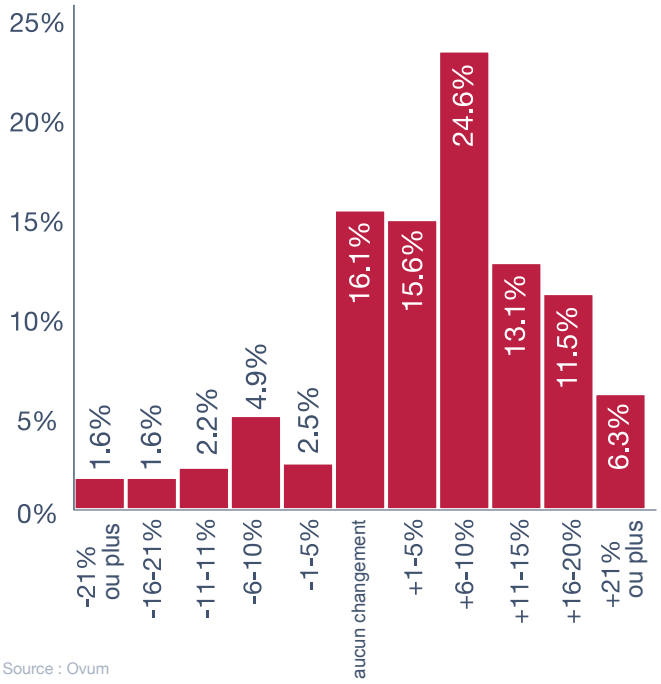
Réponse	Approche principale actuellement suivie	Approche envisagée
Nos décisions en matière de confidentialité sont basées sur l'emplacement juridique des données (c'est-à-dire le ou les pays susceptibles d'être juridiquement compétents sur les données, et la juridiction dont les lois doivent être violées pour établir un accès non autorisé à des données à caractère personnel)	26 %	27 %
Nos décisions en matière de confidentialité des données sont fondées sur l'emplacement logique des données (emplacement géographique à partir duquel un contrôle est exercé sur le traitement informatique, c'est-à-dire où réside le point de chiffrement.)	27 %	33 %
Nos décisions en matière de confidentialité des données sont fondées sur l'emplacement physique des données (traditionnellement, le ou les emplacements géographiques où les informations sont effectivement écrites à des fins de stockage.)	33 %	24 %

Source : Ovum

La mise en conformité aux nouvelles réglementations est extrêmement coûteuse

Les budgets sont inévitablement affectés par l'évolution des différents environnements réglementaires (par exemple à Hong Kong, à Singapour et en Russie). Si les réglementations relatives à la protection de la vie privée étaient traditionnellement confinées au volet juridique, elles impactent désormais également les métiers de l'entreprise liées aux technologies et à la mise en conformité. Notre recherche montre par ailleurs que de nombreuses entreprises prévoient de procéder à des recrutements dans ces domaines pour gérer les implications des nouveaux cadres réglementaires à venir. Plus spécifiquement, 19 % des répondants envisagent des recrutements dans la fonction juridique, 31 % dans la fonction technologique, et 34 % dans les métiers de mise en conformité. Cela fait à son tour émerger de nouvelles questions ayant trait à l'évolution des responsabilités et des compétences dans ces domaines, lorsque les nouvelles réglementations seront effectivement entrées en vigueur.

Figure 6 : Réponses à la question : « Quelles modifications budgétaires prévoyez-vous au cours des deux prochaines années suite aux réformes réglementaires mondiales en matière de protection et de souveraineté des données ? »)



Source : Ovum

On observe parmi les répondants à notre enquête une conviction selon laquelle les compétences technologiques et de mise en conformité seront les plus appropriées pour aborder ce challenge, qui reste pourtant à la base un problème juridique. On peut donc raisonnablement anticiper que les spécialistes des questions de technologie et de mise en conformité chercheront à renforcer leur connaissance juridiques en matière de protection des données au cours des prochaines années.

De toute évidence, un tel impact se traduira par une hausse des coûts pour les entreprises. Notre enquête permet de jauger l'impact anticipé sur les budgets globaux des entreprises (cf. figure 6). Il est intéressant de constater que plus de 30 % des répondants anticipent une augmentation des budgets d'au moins 10 %, et près d'un quart prévoit une hausse comprise entre 6 et 10 %. Dans l'ensemble, plus de 70 % des répondants anticipent une hausse des budgets liée aux nouvelles réglementations en matière de protection des données.

Les entreprises basées aux États-Unis sont sous pression

Les révélations d'Edward Snowden concernant l'étendue des pratiques de surveillance électronique de la NSA (*National Security Agency*) ont sérieusement dégradé le capital-confiance dont bénéficiaient les États-Unis. Lorsqu'on demande aux répondants quels sont, selon eux, les grands pays industrialisés les plus susceptibles d'accéder à leurs données sans autorisation, les États-Unis sont cités en premier, devant la Chine et la Russie. Si les procédures juridiques en vigueur aux États-Unis assurent en réalité une forte protection de la vie privée (sans doute même meilleure que dans certains pays européens), les perceptions ont de toute évidence été fortement influencées par la tempête médiatique suscitée par ces révélations.

Les nouvelles réglementations européennes vont également placer les entreprises américaines dans une situation défavorable. On constate en effet que 63 % des répondants estiment que le projet de GDPR de l'UE va entraver encore davantage la compétitivité des entreprises américaines, et que 70 % s'attendent à ce que cette nouvelle législation favorise les entreprises basées en Europe.

Recommandations

Les problématiques de souveraineté des données induites par cette nouvelle législation vont avoir un impact majeur sur un très grand nombre d'entreprises dont les activités sont conduites à l'échelle mondiale. Lorsqu'elles traitent des informations à caractère personnel, les entreprises doivent trouver le juste équilibre entre considérations commerciales, contraintes juridiques et exigences des consommateurs. Les actions à prendre dans ce domaine incluent :

Définir une stratégie claire en matière de souveraineté des données

Les entreprises qui opèrent dans un cadre international et qui collectent des informations à caractère personnel doivent se conformer aux réglementations en matière de protection des données dans tous les pays dans lesquels elles conduisent leurs affaires. Le recours à des prestataires cloud tiers pour gérer les données n'exonère pas les entreprises de leurs responsabilités. La première étape doit donc consister à reconnaître cette responsabilité, puis à définir une stratégie en conséquence. Cette stratégie doit être pilotée par une équipe dédiée, constituée de cadres dirigeants, qui sera chargée d'établir les mesures de contrôle, les politiques et les procédures visant à garantir la conformité de l'entreprise. Peut-être votre équipe GRC (gouvernance, risque et conformité) a-t-elle déjà engagé ce processus, mais il est important que celui-ci soit engagé à l'initiative de l'équipe dirigeante de votre entreprise.

Procéder à une évaluation des risques liés au respect de la vie privée

Pour être efficace, la gestion de la gouvernance doit reposer sur un travail d'identification des risques significatifs pour l'entreprise. Le contexte est extrêmement important lorsqu'on évalue le risque d'impact sur la vie privée, et certains secteurs d'activité comme la santé et l'assurance doivent composer avec des environnements réglementaires et des procédures de surveillance particulièrement stricts. L'évaluation de l'impact sur la vie privée doit commencer par une classification de l'information en grandes catégories (ex. : informations à caractère personnel, informations confidentielles de l'entreprise), et la réalisation d'une carte des processus métier existants et des zones géographiques concernées. Identifiez et examinez les réglementations applicables en matière de respect de la vie privée dans chacun des pays dans lesquels vous êtes implanté. Soyez prêt à adapter vos processus métier pour satisfaire à vos obligations réglementaires. Peut-être disposez-vous déjà de technologies qui pourront vous aider à procéder à une évaluation de votre contenu (outils de classification de données de type Atlas par exemple). À l'inverse, vous avez vraisemblablement recours à des technologies qui aggravent les risques (outils de partage de fichiers grand public de type Dropbox par exemple).

Inclure le personnel dans le processus

Un certain nombre de considérations juridiques et technologiques sont à prendre en compte lors de l'évaluation d'impact des problématiques de souveraineté des données. Il est important de reconnaître que la confidentialité et la souveraineté de données sont des questions complexes qui affectent l'ensemble de votre organisation. La formation et la sensibilisation de votre personnel sont des aspects aussi importants que le déploiement des solutions technologiques pour gérer vos flux de données. Il ne serait ni financièrement viable, ni juridiquement fondé, de se focaliser exclusivement sur la technologie, les processus ou l'activité des employés : ces trois aspects revêtent une importance égale.

Ouvrez les discussions dès aujourd'hui

Engagez un dialogue avec les fournisseurs de technologies et les prestataires de services existants pour mieux connaître les solutions qu'ils envisagent pour répondre aux nouvelles exigences législatives. Certains fournisseurs proposent d'ores et déjà différentes options permettant de répondre aux nouveaux enjeux de la confidentialité des données. La flexibilité des solutions proposées est essentielle dans la mesure où les cadres réglementaires sont différents d'un pays à l'autre et évoluent rapidement. Les fournisseurs doivent se montrer capables de répondre à vos interrogations concernant l'emplacement logique et physique des données, et de vous proposer des contrats de service offrant toute la flexibilité juridique requise.

Annexe

Méthodologie

L'enquête Ovum a é été réalisée au cours du troisième trimestre 2015 et auprès de 366 personnes, représentant différentes tailles d'entreprises, régions d'implantation et activités. L'analyse des résultats de l'enquête a été menée dans le contexte des consultations en cours avec des clients d'Ovum, de discussions avec les fournisseurs du secteur et de recherches complémentaires.

Auteur

Alan Rodger, analyste principal, gestion des systèmes IT d'entreprise
alan.rodger@ovum.com

Ovum Consulting

Nous espérons que cette analyse vous aidera à prendre des décisions éclairées et créatives pour votre entreprise. Si vous avez des questions ou des besoins complémentaires, l'équipe de consultants Ovum se tient à votre disposition.

Pour plus d'informations sur les services de conseil du cabinet Ovum, veuillez nous contacter directement à l'adresse consulting@ovum.com.

ovum

NOUS CONTACTER

www.ovum.com
askananalyst@ovum.com

BUREAUX INTERNATIONAUX

Pékin
Dubaï
Hong Kong
Hyderabad
Johannesburg
Londres
Melbourne
New York
San Francisco
Sao Paulo
Tokyo

INTRA LINKS