

Souveraineté numérique :

impacts et enjeux pour les entreprises
françaises et européennes



LIVRE BLANC

Table des matières



Introduction	4
• Quand c'est gratuit, c'est que vous êtes le produit	4
• Souveraineté numérique : un devoir et une nécessité	4
Souveraineté numérique : l'urgence au-delà du concept	5
• Souveraineté numérique : état des lieux	5
• Enjeux stratégiques et économiques	5
• Enjeux démocratiques et citoyens	6
Les forces étrangères à la conquête des données numériques européennes	7
• Privacy Shield et CLOUD Act : cyberintrusions en un claquement de lois	7
• La grande muraille numérique de Chine : le poids du nombre	8
• Russie : pragmatisme et sémantique	9
Législations : intensifier les efforts et les initiatives	9
• RGPD : contexte actuel et objectifs à long terme	10
• États-Unis : au nom de la libre concurrence	10
• Initiatives législatives et décisions de justice européennes et françaises : certaines visent à renforcer, d'autres à concrétiser	11



Entreprises privées françaises : prendre toute la mesure de la bataille à mener	12
• Un partenariat nécessaire entre les pouvoirs publics et les entreprises pour sensibiliser et informer	13
• Promotion des entreprises et des technologies Made in France	13
• Gouvernance d'entreprise et souveraineté des données les plus confidentielles : l'importance du choix de son prestataire	13
Conclusion	14
A propos de DiliTrust	15
• Le Partenaire privilégié des organes de gouvernance, des comités et des directions juridiques	15

Introduction

L'existence de programmes de surveillance de masse américains et britanniques fut révélée au grand public par Edward Snowden dès le 5 juin 2013. Et ce, par le biais de plusieurs médias dont The Guardian et The Washington Post. Ainsi, après des années passées à utiliser les solutions numériques étrangères “gratuites”, et avant tout américaines, pour collecter, stocker et partager l'ensemble de leurs données, les entreprises européennes et françaises prirent conscience de l'importance de protéger leurs informations les plus sensibles et d'assurer leur souveraineté numérique.

Quand c'est gratuit, c'est que vous êtes le produit

Sept ans plus tard, les GAFAM se portent mieux que jamais, dominant tout le marché numérique. Ces géants américains passés maîtres dans le Cloud computing, les systèmes d'exploitation pour les ordinateurs de bureau et sur mobiles, les systèmes de messagerie et de navigation web, la vidéo en ligne, l'intelligence business et la fibre optique, ont créé au fil des ans une véritable dynamique oligopolistique. En France par exemple, deux tiers des administrations et des entreprises utilisent des boîtes de messagerie Google et/ou Microsoft. Une situation de dépendance numérique axée sur un nombre restreint de plateformes.

D'une part, cette situation témoigne d'un manque de prospective des institutions françaises mais aussi européennes quant au numérique. Et ce, alors même que la France inscrit dès le 17 juin 2008 le cyberspace et ses menaces potentielles dans les champs de la défense et de la sécurité nationales. D'autre part, elle conforte le leadership des GAFAM dans le monde. 45% : c'est la part que ces derniers représentent à eux seuls en 2019 dans la valeur de l'indice NASDAQ. Intelligence artificielle, Machine Learning, Big Data, mais aussi lobbying : leur capacité d'investissement constitue une véritable force de frappe à l'échelle mondiale.

Souveraineté numérique : un devoir et une nécessité

Si la Chine et la Russie ont mis en place des contre-mesures numériques, économiques et législatives pour conserver toute leur souveraineté numérique et se prémunir de l'hégémonie des GAFAM et des effets du CLOUD Act américain, l'Europe espère toujours l'émergence de ses propres GAFAM. En attendant, les données des entreprises et des institutions européennes, notamment les plus sensibles, sont toujours à découvert et encore plus vulnérables depuis l'annulation du Privacy Shield. Et ce, malgré le RGPD en application dans toute l'Union depuis le 25 mai 2018, qui ne concerne que les données personnelles des utilisateurs individuels.

Alors que faire face à l'urgence ? Comment faire face au CLOUD Act américain promulgué le 23 mars 2018, permettant l'accès à toutes les données stockées dans les datacenters appartenant à des entreprises d'origine américaine, même au-delà des frontières des États-Unis ? Quelles autres initiatives les pouvoirs publics et les conseils d'administration en Europe peuvent-ils mener pour préserver leur souveraineté numérique ? Comment les éditeurs français peuvent-ils assurer la sécurité des données hautement confidentielles de leurs clients ?

Souveraineté numérique : l'urgence au-delà du concept

« La souveraineté nationale fonde le pacte républicain, pacte par lequel le citoyen accepte une discipline collective fondée sur la loi, en contrepartie d'une protection. [...] Aujourd'hui, la question de la souveraineté numérique est totalement actuelle, car si l'ère numérique est à la fois une chance et une certitude partagées dans le monde entier, elle constitue pour la France, comme pour les pays de l'Europe, un triple défi d'éthique, de sécurité et de liberté économique. »

C'est par ces mots que le président Franck Montaugé et son rapporteur Gérard Longuet introduisent leurs principales recommandations incluses dans le rapport de la Commission d'enquête sur la souveraineté numérique remis le 1er octobre 2019 à la Présidence du Sénat. Au-delà, les perspectives qu'ils décrivent forment pour les entreprises et les institutions françaises et européennes des réalités complexes qui recouvrent des enjeux stratégiques, économiques, cybersécuritaires et démocratiques majeurs.

Souveraineté numérique : état des lieux

L'avènement du web a considérablement impacté l'économie mondiale et les usages. Et ce, tant au niveau des particuliers qu'à celui des entreprises et des institutions. Il a donné lieu à l'émergence de nouveaux modèles socio-économiques, culturels mais également juridiques et politiques. En parallèle, il a initié une ère numérique dont un nombre restreint d'acteurs privés a su tirer parti. Ces derniers sont devenus les GAFAM américains, les BATX chinois et certaines entités russes à l'instar de Yandex.

Bénéficiant de l'appui de leurs gouvernements respectifs par la promulgation de lois favorisant leur développement économique tout autant que la préservation des données numériques qu'ils collectent et partagent, non seulement sur leur sol national mais également à l'étranger, ces mêmes acteurs ont profondément ébranlé la souveraineté des citoyens, des entreprises et des institutions de l'Union Européenne. Par conséquent, les efforts de cette dernière portent désormais sur la protection de sa souveraineté numérique. Une souveraineté outrepassant les frontières de par sa dimension mondiale.

Enjeux stratégiques et économiques

« Avec la numérisation exponentielle de l'économie, la cybersécurité et la confidentialité des données sont unanimement perçues comme étant des enjeux majeurs pour les entreprises », explique Yves Garagnon, CEO du groupe DiliTrust. « De fait, il est nécessaire d'avoir une vue d'ensemble suffisamment claire de ses données et de disposer de moyens permettant de les protéger au maximum, tout en sachant saisir les nouvelles opportunités de croissance et de création de valeur qu'apportent les technologies. »

C'est dans ce sens que le groupe français DiliTrust a conçu des solutions digitales sécurisées pour gérer les données ultrasensibles des conseils d'administration ou encore des directions juridiques. Son offre complète alliant technologies et services pour la digitalisation sécurisée des conseils d'administration, des comités et des directions juridiques le positionnent à la pointe de la protection des données

sensibles et hautement stratégiques des entreprises privées et publiques en Europe. Certifiée ISO 27001, la norme de sécurisation la plus élevée au monde, avec des données hébergées en Europe, cette offre globale échappe qui plus est à l'emprise des législations extraterritoriales à l'instar du CLOUD Act américain.



“

L'arrivée du CLOUD Act qui, de l'avis de tous les experts, constitue une ingérence juridique jamais vue, est une menace pour le secret des affaires de toute entreprise tricolore contractant avec un prestataire Cloud américain.

Yves Garagnon, CEO de DiliTrust

”

Enjeux démocratiques et citoyens

En outre, il s'agit d'appréhender précisément la compétition entre États se jouant dans le cyberspace, mais également les enjeux allant au-delà des stratégies commerciales et financières. Ainsi, comme l'écrivaient Thomas Gomart, Julien Nocetti et Clément Tonon en juillet 2018 dans leur rapport intitulé L'Europe : sujet ou objet de la géopolitique des données : « *Les données ne doivent plus seulement être comprises comme un sujet juridique et commercial, mais comme un enjeu de politique internationale à part entière.* » Autrement dit, éluder cette dimension reviendrait à faire fi du risque de disparition de l'État tel que nous le connaissons aujourd'hui.

À l'ère numérique, les initiatives à mener pour préserver la souveraineté des entreprises et des institutions apparaissent comme déterminantes pour faire perdurer la démocratie. Si le RGPD a permis de protéger les données personnelles individuelles au sein de l'Union Européenne, les forces étrangères sont en marche pour conquérir les données numériques des sociétés privées et publiques. Leurs moyens sont considérables et servent une logique de substitution aux États. Quelles sont ces forces et quelles stratégies leur opposer ?



La souveraineté des données constitue un triple défi d'éthique, de sécurité et de liberté économique pour les entreprises européennes.

Les forces étrangères à la conquête des données numériques européennes

Au même titre que la conquête de nouvelles terres et de nouveaux espaces maritimes ou aériens, la conquête du cyberspace et des données numériques qui le constituent attise les plus grandes convoitises. Les acteurs privés rivalisent sur toute la planète jusqu'à entrer en concurrence avec les États eux-mêmes. Et parfois ces mêmes États sont de mèche avec eux pour asseoir leur développement économique et leurs innovations à des fins stratégiques et géopolitiques.

5000 milliards de dollars : il s'agit de la capitalisation boursière cumulée des GAFAM américains en 2020. Ces derniers sont sur le point de devenir la troisième économie mondiale. Grâce à leurs capacités financières conséquentes, les GAFAM multiplient les actions de lobbying auprès de tous les gouvernements mondiaux, dont certains membres deviennent finalement leurs lobbyistes. Au sein des institutions et des entreprises françaises et européennes, les avis divergent. Quand certains prônent des actions volontaristes en faveur des licornes européennes pour disposer d'un arsenal numérique défensif et offensif semblable à celui des GAFAM américains et des BATX chinois, d'autres mettent en avant la notion d'autonomie de décision. Dès lors, l'interdépendance numérique n'est plus exclue. Il s'agit d'en choisir les modalités pour « conserver les composantes les plus traditionnelles de la souveraineté vis-à-vis de menaces nouvelles tirant partie de la numérisation croissante de la société. »

Privacy Shield et CLOUD Act : cyberintrusions en un claquement de lois

Face à la loi fédérale américaine, le CLOUD Act (Clarifying Lawful Overseas Use of Data Act), l'Union Européenne a rétorqué avec la mise en application, dès le 25 mai 2018, du RGPD (Règlement Général sur la Protection des Données). Il est tout autant destiné à protéger les personnes et leurs données à caractère personnel qu'à responsabiliser les entités publiques et privées qui les collectent et les stockent. Toutefois, il demeure un vide juridique quant à la sécurisation des données sensibles des entreprises et des institutions européennes. Et ce, alors que le CLOUD Act modifie profondément le Stored Communications Act (SCA) qui l'a précédé.

En effet, le CLOUD Act permet aux forces de l'ordre et aux agences américaines du renseignement d'obtenir des opérateurs télécoms et des fournisseurs de services du Cloud computing américains des informations stockées sur leurs serveurs. Et ce, que ces données soient localisées à l'intérieur du territoire américain ou à l'extérieur, sans que la personne ciblée propriétaire de ces données ni le pays où elles sont conservées en soient informés.

Par ailleurs, le CLOUD Act vient aggraver les conséquences d'un dispositif antérieur, en vigueur depuis le 1er août 2016 : le Privacy Shield. Jugé conforme au RGPD dans un premier temps, celui-ci permettait aux entreprises européennes d'exporter leurs données personnelles vers des partenaires américains, dans la mesure où ceux-ci s'étaient auto-certifiés auprès de la Federal Trade Commission pour garantir d'un niveau suffisant de protection desdites données. Le Privacy Shield a cependant été annulé en juillet 2020 par la Cour de Justice de l'Union Européenne. Une décision salutaire qui empêche désormais les entreprises européennes de se jeter d'elles-mêmes dans la gueule du loup,

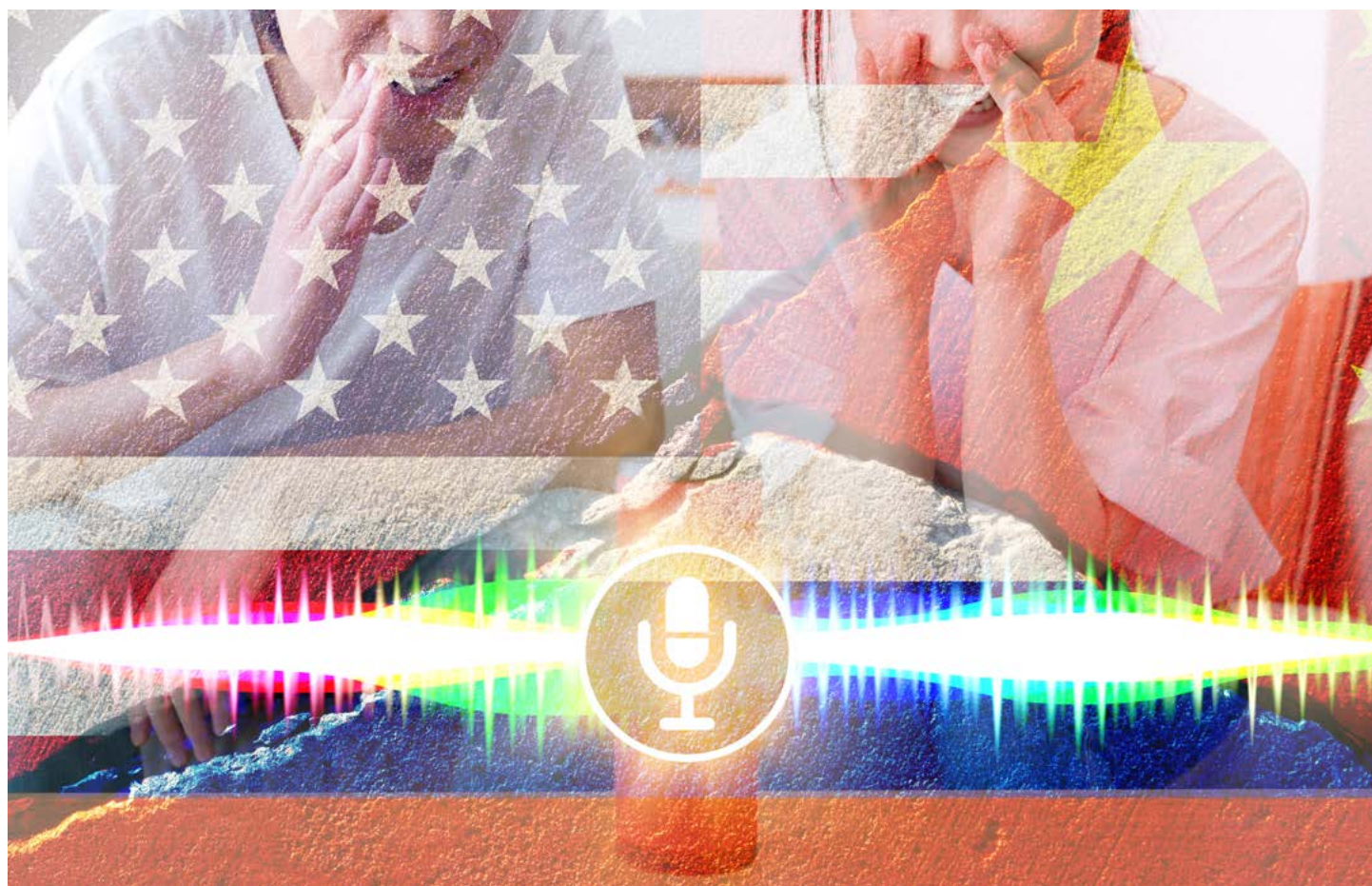
mais qui malheureusement ne les protège pas de la prédation arbitraire autorisée par le CLOUD Act.

Dès lors, on comprend tout l'intérêt de solutions telles que celles développées par DiliTrust pour la gouvernance d'entreprise, la digitalisation des conseils d'administration et le partage sécurisé des données confidentielles. 100% françaises et compatibles RGPD, elles échappent au CLOUD Act américain.

La grande muraille numérique de Chine : le poids du nombre

La Chine compte le plus grand nombre d'utilisateurs d'Internet, en l'occurrence 854 millions sur les 4,4 milliards d'utilisateurs dans le monde. Soit près de trois fois plus qu'aux États-Unis. L'approche chinoise quant à la préservation de sa souveraineté numérique et nationale vise tout autant l'autonomie vis-à-vis des produits et des services américains que le contrôle de tous les pans du cyberspace sur son propre territoire. Il s'agit non seulement du contrôle des données à l'entrée de celui-ci, mais également du contrôle des critiques diffusées sur le web et qui pourraient mettre à mal le système politique et social chinois.

Enfin et surtout, l'objectif est de soutenir le développement de solutions locales et contrôlables par le gouvernement chinois à destination de sa population par le biais d'opérateurs nationaux. Au fil des plans quinquennaux favorisant l'investissement dans les secteurs d'activité les plus innovants tels que l'intelligence artificielle, les NTIC ou les biotechnologies, ces derniers sont devenus les géants du web chinois. Baidu, Alibaba, Tencent, Xiaomi : ils forment les BATX. Leurs taux de croissance respectifs dépassent parfois largement celui des GAFAM américains : plus de 50% pour Tencent, Alibaba et Xiaomi sur les deux dernières années.



Russie : pragmatisme et sémantique

Afin de protéger sa souveraineté numérique et nationale, la Russie a emboîté le pas à la Chine en instaurant des réglementations strictes quant à l'accès aux données, à leur stockage et à leur partage. C'est le cas des lois Yarovaya de 2016 encadrant la diffusion de contenu sur Internet. De plus, les instances gouvernementales ont mis à l'étude début 2019 une nouvelle loi pour la création d'un Internet souverain. Et ce, afin de se prémunir des cyberattaques extérieures d'envergure, mais aussi pour se protéger du CLOUD Act américain.

Si Yandex, le moteur de recherche russe historique, s'est associé avec la Sberbank, la première banque nationale, pour la création d'une société commune de commerce en ligne, la Russie ne dispose pas des acteurs privés aptes à concurrencer les GAFAM et les BATX. En revanche, elle est régulièrement accusée de fomenter des actions d'infiltration au sein des infrastructures numériques de pays tiers, à l'instar du Royaume-Uni et des États-Unis. Cette situation révèle les cybermenaces bien réelles planant sur la souveraineté des États. D'où la nécessité de mettre en place et de renforcer une prospective pérenne quant à la sécurisation des données dématérialisées des entreprises et des instances de l'Union Européenne. Une prospective qui considère d'une part la compétition internationale, et l'organisation du web et de ses acteurs d'autre part.

Législations : intensifier les efforts et les initiatives

Comme le rappelle justement Boubacar Diallo, analyste en intelligence économique : « *la souveraineté numérique se résume à trois éléments fondamentaux : la maîtrise de la création de valeur, la maîtrise de la technologie et la maîtrise du patrimoine informationnel.* » 37 millions : il s'agit du nombre d'utilisateurs actifs chaque jour en France, revendiqué par Facebook en 2020. Une information qui révèle l'ampleur de la tâche, notamment quant aux efforts à poursuivre pour déployer les moyens légaux destinés à maîtriser les systèmes d'informations et les données des États de l'Union Européenne et de leurs entreprises.

« *Lorsque Mark Zuckerberg doit se rendre au Parlement européen pour s'expliquer sur les violations de données des utilisateurs du réseau social Facebook, cela s'avère être plus puissant qu'un seul pays qui tente de se battre pour ses propres citoyens. À ce titre, la protection de la souveraineté doit être à la fois française et européenne* », ajoute Yves Garagnon, CEO du groupe français DiliTrust. Dans cette optique, le RGPD et la Commission d'enquête sur la souveraineté numérique constituent des premières initiatives louables. Quelles sont les autres dispositions législatives à développer ou à concrétiser en France et en Europe pour réguler le cyberspace et les plateformes numériques oligopolistiques ?

RGPD : contexte actuel et objectifs à long terme

La prise de conscience en Europe existe bel et bien aujourd'hui. L'équipe de la Commission européenne chargée de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace, parmi laquelle figure Thierry Breton, démontre une grande appétence quant aux questions liées au numérique. En parallèle, les dispositifs juridiques mis en place comme le RGPD renforcent le pouvoir régalien des États dans leur capacité à légiférer pour protéger les citoyens et leurs informations. Le RGPD est une première étape dans la constitution d'une souveraineté numérique juridique européenne. Toutefois, il présente le défaut de ne pas protéger les données sensibles et stratégiques des entreprises et des institutions.

Il y a urgence à mettre en place une telle protection, notamment pour éviter le rachat systématique des entreprises européennes du numérique. Mais également pour contrer l'extraterritorialité de certaines législations étrangères, comme c'est le cas avec le CLOUD Act américain, pouvant dès lors s'appliquer à n'importe quelle donnée individuelle, d'entreprise ou institutionnelle, quelle que soit sa localisation. C'est pourquoi les conseils d'administration et les directions juridiques d'entreprises de toute taille sont de plus en plus nombreux à choisir des solutions de gouvernance hébergées dans des datacentres situés hors d'atteinte du CLOUD Act, comme c'est le cas des solutions de DiliTrust. Objectif : stocker, exploiter et échanger les informations stratégiques et sensibles, dans le respect de leur confidentialité, tout en se prémunissant des risques de violation des données et d'espionnage industriel.

États-Unis : au nom de la libre concurrence

Les législations tierces comme le CLOUD Act américain constituent une menace pour la cybersécurité et la propriété des données des entreprises et des institutions européennes. Elles peuvent inspirer les dispositifs juridiques et législatifs à développer au sein de l'Union Européenne en faveur de sa souveraineté numérique. Dans ce sens, si l'émergence et la suprématie actuelle des GAFAM tiennent en grande partie au choix des gouvernements américains successifs d'intégrer la captation et l'utilisation des données numériques à la stratégie économique et à la politique de sécurité nationales, les États-Unis sont aussi historiquement attachés à la libre concurrence.

Les positions de chaque acteur en présence se précisent, quitte à remettre en cause les modèles existants et leur hégémonie. Depuis longtemps, la porosité des liens entre les autorités politiques américaines et les intérêts économiques des GAFAM ne faisait plus aucun doute. Pourtant, au nom de la libre concurrence, les premières évoquent de plus en plus sérieusement la piste du démantèlement de ces géants du numérique, à l'image des démembrements opérés par le passé dans le domaine de l'exploitation pétrolière puis dans celui des télécommunications. Quant aux GAFAM, la volonté de certains d'entre eux de protéger les données de leurs clients stockées en Europe se renforce. Et ce, pour conserver leur confiance et donc leurs parts de marché. C'est le cas notamment pour Microsoft Europe. Si l'intention est bonne, dans les faits, le CLOUD Act tel qu'il existe aujourd'hui s'appliquera malgré tout. Et ce, sans que la personne propriétaire des données visées en soit informée, pas plus que l'État dans lequel elles sont hébergées.

Initiatives législatives et décisions de justice européennes et françaises : certaines visent à renforcer, d'autres à concrétiser

En France, le rapport de la Commission d'enquête sur la souveraineté numérique officialisé en octobre 2019 pointe un certain nombre de mesures à appuyer et/ou à transposer dans le droit français lorsque celles-ci existent déjà à l'échelle européenne. C'est le cas pour la directive européenne appelée ECN+ publiée en janvier 2019. Celle-ci vise à "doter les autorités de concurrence des États membres des moyens de mettre en œuvre plus efficacement les règles de concurrence et à garantir le bon fonctionnement du marché intérieur." Par exemple, l'obligation de céder une branche d'activité dans le cadre de sanctions suite à des pratiques anticoncurrentielles avérées.

En parallèle, un ajustement du droit des concentrations, pour empêcher un rapprochement d'entreprises dont les effets pourraient être anticoncurrentiels, est préconisé. Tout comme la révision du champ d'application du contrôle des concentrations, pour lutter contre les « acquisitions prédatrices ». Les instances françaises et européennes visent ainsi un renforcement du droit de la concurrence et de son adaptation au marché du numérique. « L'inaction n'est plus une option » et la transparence est de mise. Non seulement envers les consommateurs mais également envers les professionnels. Publié en juillet 2019, le règlement européen Platform-to-business l'instaure et constitue un nouveau pas pour équilibrer les relations entre plateformes et entreprises.

La volonté de souveraineté européenne s'affirme notamment par la décision de la Cour de Justice de l'Union Européenne, en date du 16 juillet 2020, qui fait l'effet d'un coup de tonnerre dans le ciel de la planète numérique : [l'annulation du Privacy Shield](#). La CJUE justifie sans ambiguïté sa décision par une insuffisance des contrôles de la Federal Trade Commission sur les pratiques des entreprises américaines signataires en matière de protection réelle des données personnelles fournies par leurs partenaires européens ; une situation par ailleurs aggravée par la promulgation du CLOUD Act. Concrètement, les entreprises européennes souhaitant malgré tout exporter des données personnelles aux États-Unis doivent désormais intégrer des « Clauses Contractuelles Type » réglementaires dans chacun de leurs contrats de partenariat transatlantique.



Entreprises privées françaises : prendre toute la mesure de la bataille à mener

Les données ont fait leur révolution et forment désormais le « terreau » des activités de tous les grands acteurs mondiaux de l'économie numérique. En parallèle, elles induisent de nouvelles approches géopolitiques de la part des États afin d'élaborer leurs défenses numériques. D'une part, pour préserver leur souveraineté. D'autre part, pour nourrir les stratégies offensives de développement de leurs entreprises pour que ces dernières ne se substituent pas à eux.

Le but ? Éviter que l'État et la démocratie, tels que nous les connaissons aujourd'hui, ne finissent par exister uniquement pour la forme.

Par conséquent, la préservation de la souveraineté numérique des entreprises et des institutions françaises repose avant tout sur des actions pédagogiques relevant de la sensibilisation, de l'information et de la recherche. De plus, elle nécessite un soutien à toute coopération européenne privée encadrée par les États et dépassant les clivages politiques, à l'instar d'Airbus à son époque. *« Enfin, il s'agit de choisir les champs stratégiques pouvant être inscrits dans le cadre de la sécurité nationale », conclut Boubacar Diallo. « C'est d'ailleurs ce qui fait la force des États-Unis. »*



Promouvoir les acteurs privés français est, à l'heure actuelle, le biais à privilégier pour se donner les moyens de la souveraineté numérique du pays et pour développer une politique industrielle forte.

Un partenariat nécessaire entre les pouvoirs publics et les entreprises pour sensibiliser et informer

La transition numérique est telle que certains vont jusqu'à parler de grande métamorphose. C'est notamment le cas de Francis Jutand, Directeur général adjoint de l'Institut Mines-Télécom. « *Cette métamorphose n'est pas darwinienne, c'est une véritable succession de vagues rapprochées auxquelles l'humanité doit s'adapter au mieux* », explique-t-il. « *Il y a d'abord eu la vague de l'automatisation, puis celle de l'informatique, de la mobilité, puis de l'Internet, celle des big data, de l'Internet des objets, etc. Nous ne pouvons nous adapter complètement à cette succession de vagues très rapides, mais nous devons nager dedans et tenter de prendre du recul par rapport aux vagues qui suivent.* »

Dans cette optique, la sensibilisation et la formation des acteurs publics et privés français doivent concerner les informations connectées, la cybersécurité des données sensibles des entreprises et les risques inhérents au cyberspace mondial. En réalité, il s'agit surtout d'amener les pouvoirs publics et les entreprises à se projeter ensemble dans un partenariat pérenne soutenant la recherche, l'innovation et la conquête numérique et économique, notamment dans le Big Data. Sans oublier l'émancipation progressive des entreprises françaises et européennes vis-à-vis des GAFAM et des BATX.

Promotion des entreprises et des technologies Made in France

Promouvoir les acteurs privés français est, à l'heure actuelle, le biais à privilégier pour se donner les moyens de la souveraineté numérique du pays et pour développer une politique industrielle forte afin de soutenir le développement des technologies clés, comme le cloud et l'intelligence artificielle. Pour cette dernière, les entreprises françaises plébiscitent notamment la mutualisation des données privées sectorielles. Quant au cloud, il s'agit non pas de se retrouver nez-à-nez avec les géants américains, mais de favoriser les technologies nationales axées sur une stratégie de différenciation. Autrement dit, un cloud de confiance respectueux de la vie privée des utilisateurs dès sa conception.

Le secteur privé va beaucoup plus loin que l'État pour toutes les problématiques que soulève le numérique en matière d'innovation technologique. Il s'agit donc aujourd'hui pour les pouvoirs publics d'accompagner et d'encadrer le secteur privé pour qu'il puisse entre autres proposer des solutions tant en matière de gouvernance et d'aide à la prise de décision rapide, qu'en matière de protection des données. Et si possible, des solutions qui puissent être étendues en France et dans le monde entier.

Gouvernance d'entreprise et souveraineté des données les plus confidentielles : l'importance du choix de son prestataire

DiliTrust s'inscrit depuis toujours dans une approche très européenne en matière de protection des données sensibles d'entreprise. Le rapprochement stratégique de la société française avec l'éditeur italien de logiciels Dromedian en 2019 l'a encore confirmé tout en faisant naître le nouveau leader sur le marché italien de la gouvernance d'entreprise, plus précisément de la digitalisation des conseils d'administration. Objectif : sécuriser les données hautement confidentielles que les entreprises collectent, mais également celles qui participent à leur différenciation, à leur innovation et à leur compétitivité.

A ce titre, le board portal de DiliTrust a été conçu pour offrir un espace parfaitement sécurisé qui permet de gérer les réunions des conseils d'administration. En matière de gouvernance, les organisations peuvent également s'appuyer sur la solution de DiliTrust dédiée aux directions juridiques. Elle permet d'optimiser la gestion des entités juridiques, des contrats ou encore des litiges



et contentieux de n'importe quelle structure tout en renforçant la productivité des juristes d'entreprise. Enfin, DiliTrust propose également un service de data room électronique pour héberger et partager en toute sécurité toutes les données sensibles liées, par exemple, aux opérations de fusion-acquisition, à la gestion et à la cession de biens immobiliers, à la propriété intellectuelle ou encore aux levées de fonds.

Toutes les solutions de DiliTrust utilisent les protocoles de sécurité les plus récents et sont certifiées ISO 27001. Elles échappent au CLOUD Act et visent l'exploitation intelligente et la structuration des données.

Conclusion

Au-delà des bouleversements qu'elle a engendrés, l'ère numérique se distingue par l'ambivalence de la nature profonde de ses effets. Source infinie de savoirs, de connexions, d'échanges et de réinventions, elle abrite également des parts d'ombre nourries notamment par la volonté de certains acteurs privés et publics de contrôler des données toujours plus critiques. Et ce, au détriment de l'intimité des individus, de la diversité des composantes entrepreneuriales et de la souveraineté des nations.

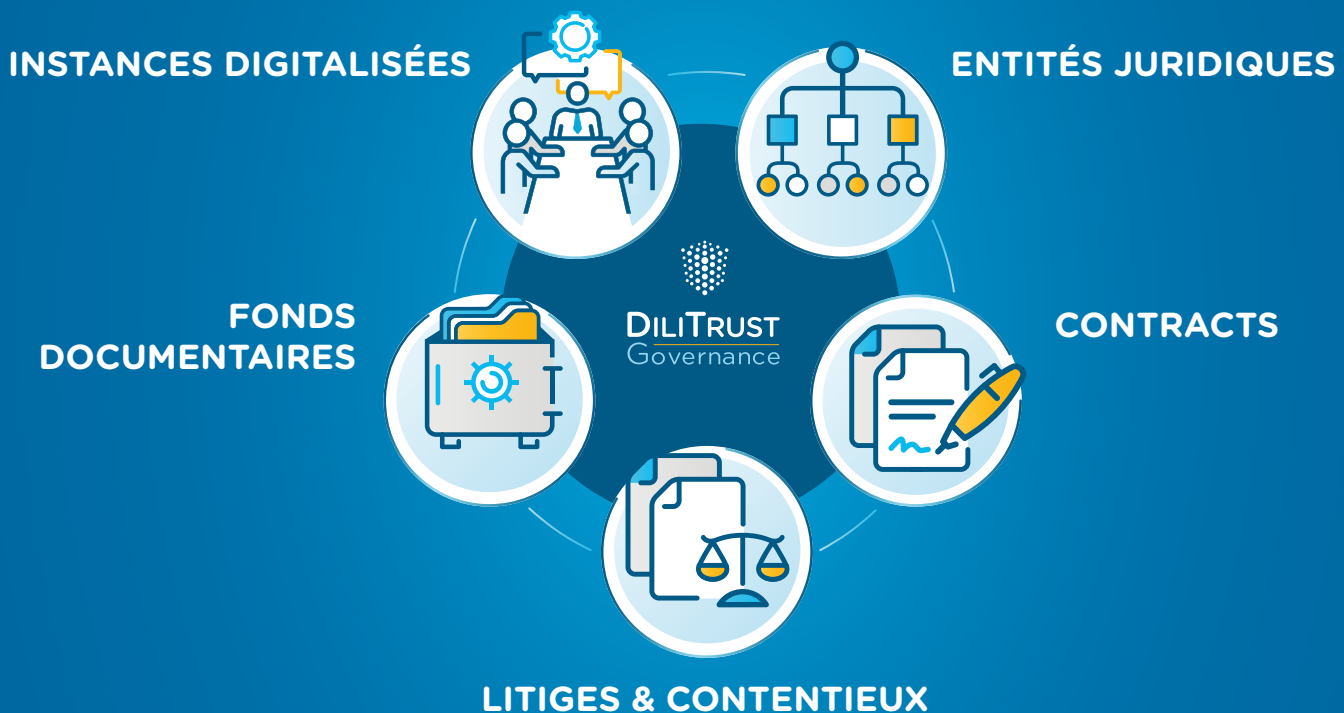
Aussi, la souveraineté numérique de chaque entité intègre l'ingéniosité, la proactivité et la détermination qui seules permettent de réguler la domination de certaines grandes structures de l'économie numérique. Mieux encore, la souveraineté numérique constitue par essence un enjeu fondamental de vision. « *Il faut avoir conscience qu'un monde numérique invisible, très puissant, est en train de naître* », déclarait le Digital champion pour la France auprès de la Commission Européenne, Gilles Babinet. « *La seule limite, ce sera l'art et la part sensible de l'homme. Pour le reste, les machines nous dépassent et nous dépasseront en termes d'efficacité. C'est un processus à court terme et c'est une certitude. Cette robotisation généralisée répond à la logique de progrès, progrès lui-même guidé par l'efficacité. C'est précisément là qu'est tout le débat. Une société efficace nous rendra-t-elle heureuse ? Je ne le pense pas. Ce qui m'inquiète, c'est le développement d'une société orwellienne. Il faut absolument que cela devienne un débat citoyen qui nous pousse à nous interroger sur la société que l'on souhaite, aux contrepouvoirs à proposer. Sinon, ce sont les grands groupes d'outre-Atlantique, comme les GAFAM, qui décideront pour nous.* »

A propos de DiliTrust

Le Partenaire privilégié des directions juridiques, des organes de gouvernance et des comités.

Éditeur et intégrateur de logiciels depuis plus de vingt-cinq ans, DiliTrust offre une gamme complète de solutions et de services dédiés à la gouvernance d'entreprise et au partage sécurisé de données sensibles et confidentielles.

L'entreprise propose sa suite logicielle « DiliTrust Governance » permet d'**automatiser les processus des directions juridiques**. Disponible sur abonnement via un accessible via un portail sécurisé, la suite DiliTrust Governance est composée de différents modules : *Instances digitalisées, Entités juridiques, Contrats, Litiges & Contentieux* et *Fonds documentaires*.



Reconnue pour son savoir-faire et son expertise pointue dans son domaine, DiliTrust s'engage chaque jour auprès de ses 1600 clients dans plus de 50 pays pour accompagner leurs dirigeants dans l'atteinte de leurs objectifs en termes de conformité aux réglementations, d'efficacité opérationnelle, de transparence et de communication juridique et financière. 85 % des entreprises du CAC 40 ainsi que des groupes majeurs en Europe, en Amérique du Nord, en Afrique et au Moyen-Orient font confiance à DiliTrust, parmi lesquels :

Almarai, AccorHotels, Ahli United Bank, Ecobank, Royal Bank of Canada, BNP Paribas, Bouygues, Caisse de Dépôt et de Gestion du Maroc, Campari, Capgemini, Carraro, Commercial Bank of Dubai, Desjardins Capital, EDF, Engie, Eurazeo, Eureden, Eutelsat, Foyer, Geox, Ingenico, Koç, Les Domaines Agricoles du Maroc, Loto-Québec, LVMH, Luxempart, Octo, Renault, Richelieu Hardware, Groupe Robert, Safran, SFR, SNCF, Société Générale, Société Nationale de Radiophonie et de Télévision du Maroc, Société de Transport de Montréal, Tamweel Africa Holding, Tereos, UJA Federation, UNICEF, Veolia Environnement, City of Montreal et Vivendi.

DiliTrust est présente à Paris, Milan, Madrid, Montréal, Toronto et Dubai.



SOLUTIONS DE GOUVERNANCE SÉCURISÉES

**Vous souhaitez sécuriser les données de votre Conseil d'Administration,
de vos comités ou encore votre direction juridique ?**

Contactez DiliTrust !

DiliTrust

Les Collines de l'Arche - 76 route de la Demi-Lune
92057 Paris La Défense Cedex - France

+33 (0)1 42 91 92 00
contact-fr@dilitrust.com

www.dilitrust.com

