RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) :

MISE EN OEUVRE ET IMPACTS ECONOMIQUES

Conférence

AFDIT
ASSOCIATION FRANÇAISE DE DROIT DE L'INFORMATIQUE ET DE LA TÉLÉCOMMUNICATION

organisée
le 1er Décembre 2017 à Marseille
Programme : https://tinyurl.com/programme-2017

Synthèse de
Valérie Laure Benabou
Professeur à l' Université d'Aix-Marseille

Sommes-nous tous dataholic ? A la fois dévoreurs d'informations et dévorés par les ogres infobèses ? L'arsenal législatif qui est mis en œuvre dans le cadre du RGDP est-il comparable, comme le suggère **Arthur Langer** à la prohibition américaine qui voulait obliger les citoyens à rompre avec leurs addictions ? Est-il promis au même destin funeste car le niveau de contrainte risque de conduire les acteurs à développer des mécanismes de contournement tellement massifs que la norme, elle-même, sera étouffée ? Faut-il, à l'extension du domaine de la donnée, opposer l'extension du domaine de la lutte ?

D'où doit venir le sursaut qui permettra de réaliser un équilibre efficient entre besoin de protection des individus et nécessité de fluidité dans une économie de la data ? De la loi ? Du Marché ? De la conscience citoyenne ? De la responsabilité individuelle ?

« *My privacy is none of your business* » clame **Max Schrems,** non sans écho avec le slogan de la série Le prisonnier dans laquelle le personnage principal répète sans relache qu'il n'est pas un numéro mais un homme libre. Fort de son succès auprès de la Cour de Justice ayant conduit à l'invalidation du « *Safe Harbor* » conclu par la Commission européenne, il met désormais en place des mécanismes d'action collective visant à activer, non seulement la conscience citoyenne, mais également à pousser les personnes en charge du traitement de données à davantage d'orthodoxie dans leurs méthodes sous le regard des individus en quête de la maitrise de leurs destins numériques.

Faut-il opposer les moyens ou, au contraire, chercher à les allier ? Tous les intervenants de la journée, ont chacun à leur manière, souligné qu'on assistait à un changement de société où la donnée devient à la fois le cœur de la vie privée et l'actif convoité de la société de l'information. Dans cette double perspective, faut-il redouter « l'implémentation » du RGPD ou faut-il se précipiter ? En tout état de cause, qu'on le regrette ou qu'on s'en réjouisse, il est temps de sauter à pied joint dans le « lac de données » (**Yves Léon**) et d'apprendre à nager en données troubles**.**

Pour ce faire, je vous propose d'abord de franchir le Styx et de dépasser le « marketing de la peur » selon l'expression de **Paul Hebert** (I) pour examiner ensuite les éventuelles vertus de la « conformité » (II).

I. Dépasser « le marketing de la peur »

La période d'implémentation du RGDP est source d'inquiétudes multiples : incertitude de la norme, délais rapprochés, difficulté de compréhension de la différence d'approche avec le système existant et des mécanismes à mettre en place. Il convient, par conséquent, de recenser ces motifs de crispation (1.1.) avant d'en proposer une lecture qui permette de les dépasser (1.2.).

1.1. Les entreprises au bord de la crise de nerfs ?

La journée entière a été l'occasion de montrer que les entreprises étaient, s'agissant de la mise en place du RGDP, sur des charbons ardents. Les termes de désarroi, panique, stress ont été employés. On a parlé de nouveauté, de changement d'environnement, d'évolutions lesquelles pourraient même mener à dépression, selon **Nathalie Laneret** de CapGemini qui nous a proposé, avec humour, un nouveau développement de l'acronyme GDPR : **G**etting **D**epressed **P**retty **R**apidely.

Il s'est par conséquent agi de saisir les facteurs qui occasionnent ce stress.

Le premier est sans doute l'imminence de l'échéance : le 25 mai 2018, date d'entrée en vigueur du règlement se rapproche à grands pas et nombre d'entreprises, nous a démontré la société ALTARES, font le constat qu'elles ne sont pas encore prêtes pour assurer la conformité de leur politique de traitement avec les exigences du texte, voire ce qui est préoccupant, qu'elles n'ont pas l'intention de l'être. A dire le vrai, ce n'est probablement pas ce facteur qui est le plus générateur d'angoisse puisque **Paul Hebert** de la CNIL nous a rassuré à ce sujet, insistant sur le fait que la date ne serait nullement un couperet et que la mise en place des solutions idoines pouvait se faire en toute sérénité dans le temps nécessaire, à condition bien sûr d'entreprendre effectivement cette mise en conformité.

Le constat le plus anxiogène, à plusieurs reprises effectué, tient à l'insaisissabilité même des exigences. On peut, à cet égard, évoquer un phénomène de norme glissante ou encore, selon les mots de **François Baudienville** du Crédit Agricole de « cible mouvante ». **Thierry Million** d'ALTARES a évoqué un millefeuille législatif et l'établissement de contraintes sans avoir envisagé les moyens d'y répondre. Il est vrai que le règlement n'est pas « *self-executing* » et suppose – ce qui est inhabituel pour ce type d'instrument – qu'une loi nationale vienne le mettre en œuvre. **Emmanuel Laforêt** a évoqué à ce sujet un règlement qui ne s'assume pas ou encore au terme d'une concrétion entre les termes règlement et directive de « *régletive* ». Non moins de cinquante (ou cinquante-six) renvois à la loi nationale y sont opérés. La loi française en préparation est en préparation et des décrets nombreux devraient l'accompagner, sans compter les lignes directrices des autorités de régulation.

Cet enchevêtrement normatif effraye d'autant que la loi nationale n'est pas encore adoptée. Certains acteurs ont d'ailleurs mis en garde contre un risque de désintérêt potentiel des acteurs concernés si l'identification de la norme applicable s'avère trop complexe. A tout prendre, plutôt que de chercher à se conformer à une règle qui change sans cesse, autant l'ignorer, au moins jusqu'à sa stabilisation relative.

A cet enchevêtrement des normes répond un possible enchevêtrement des sanctions administratives et pénales qui appelle un risque de multi-condamnation, comme nous l'a fait remarquer **Jean-Luc Sauron,** ce qui ne va pas sans difficultés quant au respect de la règle non bis in idem – on ne condamne pas deux fois une personne à raison des mêmes faits -. Or ce risque est d'autant plus redouté qu'un des changements majeurs de l'entrée en vigueur du RGDP est l'aggravation potentielle des sanctions allant de pair avec l'augmentation des pouvoirs des autorités de régulation en ce domaine. La menace qui pèse sur les entreprises s'accroît également à mesure que les citoyens s'emparent de la norme. En effet, les échos multiples dans la presse mettent en lumière le besoin de protection des individus et cette conscientisation accrue peut potentiellement augmenter les recours. Ainsi non seulement les entreprises ou entités réalisant des traitements sont plus exposées par cet éclairage médiatique même s'il est sans doute éphémère, mais elles ne peuvent pas négliger les règles à adopter à défaut de mettre en péril leur économie du fait de l'importance des sanctions pécuniaires.

Ainsi, bien que tous les intervenants aient insisté sur l'absence de modification fondamentale du droit existant, ce sont essentiellement les quelques ajouts substantiels du règlement et le changement de contexte qui mobilisent l'attention. Quels sont effectivement les nouveautés apportées par le dispositif qu'il faut redouter ?

Du côté du renforcement de la protection, il s'est agi essentiellement d'obliger les entreprises à davantage de transparence et de simplicité vis-à-vis des individus quant à leur processus de collecte et de traitement des données à caractère personnel. Vont ainsi dans ce sens la mise en place de guichets uniques et la consécration d'un véritable droit à l'oubli, venant consacrer et étendre la jurisprudence de la CJUE dans l'affaire Google Spain/ Costeja.

L'accent a été mis également sur la nécessité de protéger davantage des publics vulnérables, tels que les mineurs et particulièrement exposés en raison des usages qu'ils font des outils numériques.

Mais le règlement s'est également donné pour objectif d'accompagner les nouveaux usages des données à l'ère du Big Data. Ainsi, pour consacrer une véritable mobilité, les entreprises doivent désormais s'organiser pour permettre aux individus dont elles traitent les données de se tourner vers d'autres services sans être captifs d'un opérateur qui détiendrait ces données et voudrait les retenir pour lui seul. Il s'agit donc de mettre en place un instrument concurrentiel en organisant la portabilité des données.

Pour les personnes rompues aux règles de la protection des données à caractère personnel, force est d'admettre qu'il ne s'agit pas d'une révolution mais tout au plus, selon l'expression de **Jean-Luc Sauron**, d'un « chamboulement ».

Il n'y a donc pas tant à redouter puisque, comme l'a fait valoir **Nicolas Courtier**, dans de nombreux cas, le nouveau système est même d'une facilité renforcée pour les acteurs. La déclaration préalable systématique disparaît et contrairement à ce qui peut être entendu, il n'est nullement nécessaire d'avoir un Data Protection Officer (DPO) dans chaque entreprise. Le règlement s'efforce d'aller vers la simplification y compris pour les transferts internationaux à travers notamment le mécanisme du guichet unique. Ainsi, plus qu'une aggravation des obligations, la mise en place du RGDP constituera un allégement du formalisme et des contraintes pour les petites entreprises.

Au fond, ce qui inquiète le plus c'est le changement de perspective ou encore le changement de paradigme qui accompagne le règlement. On passe en effet, d'un contrôle ex ante à un contrôle ex post : les entreprises ne peuvent plus désormais s'assurer de la conformité de leurs pratiques avant ou au moment de leur mise en œuvre ; elles doivent s'efforcer de s'inscrire dans cette démarche de « compliance » sans plus avoir de signal positif de la part des autorités de régulation et redoutent, par conséquent, de contrarier la norme et d'entrer en territoire dangereux.

Mais les acteurs ne peuvent en ce domaine, pas plus que dans d'autres, être prisonniers de leurs angoisses : ils sont contraints par les textes de se jeter dans le grand bain et, le plus sûr dans la peur est d'avancer pour la dépasser.

1.2. Apprendre à marcher sur ses deux jambes ou le rôle du droit dans la culture de la donnée

Les opérateurs n'ont pas le choix de l'immobilisme et doivent aller de l'avant. On a beaucoup, aujourd'hui, filé la métaphore maternelle ; signe sans doute d'ouverture à l'évolution des mœurs, on a même vanté la double maternité du règlement. Or, il se dégage de tout ce qui a été dit l'impression que l'évolution tant redoutée n'est en réalité que la manifestation d'un passage de l'adolescence à l'âge adulte ; d'une mue signe d'une certaine maturité.

Qu'on s'en souvienne : la loi française date de 1978 et va donc l'année prochaine célébrer ses 40 ans. La convention 108, de 1981 nous rappelle **Sophie Kwasny** avec 37 ans n'est guère beaucoup plus jeune et même si l'on s'en tient au droit européen, et à la directive 1995… 22 ans déjà. N'était-il pas temps de lâcher le bébé et de le laisser aller seul sur le chemin de conformité, selon l'expression imagée de **François Baudienville** ?

Qu'il me soit permis ici d'opérer une comparaison avec l'évolution du droit de la concurrence. Pendant longtemps, les entreprises ont pu s'assurer de la conformité de leurs pratiques avec le droit de la concurrence à travers des mécanismes de notification des accords ou des demandes d'exemptions individuelles. La Commission européenne y répondait au cas par cas et fournissait à chacun des

instruments de navigation pour mettre leurs contrats ou pratiques en accord avec les exigences du droit. Cette voie était rassurante pour les acteurs mais s'est vite révélée non seulement impraticable mais encore inefficace au regard des objectifs. En effet, la Commission fut rapidement submergée par des demandes qu'elle n'était plus en mesure de traiter ce qui de surcroît ne lui permettait pas de dégager le temps et les ressources nécessaires pour traquer les entités qui, plus que celles qui passaient par ces mécanismes de validation préalable, développaient de manière confidentielle des pratiques bien plus attentatoires au droit de la concurrence.

Ainsi, au terme d'une évolution dont on ne peut que constater le parallèle avec les nouveaux mécanismes du RGDP, les autorités de régulation concurrentielle ont abandonné les mécanismes individuels ex ante pour mieux se concentrer sur deux axes : d'une part, la rédaction de codes de conduite, de « guide lines » afin de fournir une boussole efficace à ceux qui étaient en quête de la bonne orientation ; d'autre part, la concentration des moyens pour vérifier la mise en place correcte des règles chez les acteurs et l'éventuelle sanction de leur manquement.

Ainsi l'accent est mis sur le rôle performatif de la norme dont l'énoncé contribue à sa réalisation mais d'accompagner ce rôle par l'établissement d'une culture du rendre compte et **Nicolas Courtier** nous rappelait que**,** dans cette perspective, si les normes sont nécessaires à l'accountability mais elles ne sont pas l'accountability. En d'autres termes, si le nouveau dispositif fournit les directions à suivre, il appartient aux opérateurs de mettre en place non seulement les instruments de la réalisation de la compliance mais aussi les moyens d'en rendre compte.

Dans cette transition entre l'adolescence et l'âge adulte, le rôle respectif des acteurs se transforme. L'autorité de régulation sort de sa position de « censeur » de lycée pour s'apparenter davantage à celle de conseiller pédagogique. Les opérateurs sont eux appelés à davantage d'initiative personnelle et de responsabilité.

L'autorité de régulation n'est plus là pour dire « autoriser » mais pour accompagner et soutenir d'une part et sanctionner d'autre part. S'agissant de la fonction d'accompagnement, celle-ci s'accomplit en élaborant un référentiel à l'intention des acteurs. Il convient dit **Paul Hebert** de faire connaître et de faire comprendre, notamment par des actions de sensibilisation des publics cibles, comme les sous-traitants. De ce point de vue, on ne peut que constater une évolution de la texture de la norme, laquelle doit, à l'instar des besoins qu'elle vient combler s'adapter aux configurations variées qu'elle doit envisager.

Le « patrimoine normatif » selon les mots de Paul Hebert ne va pas disparaître, mais bien au contraire, s'étoffer via des instruments de droit souple. Il s'agit de fournir des lignes de conduite, proposer des systèmes de labels ou de certification qui permettent aux acteurs de garantir à leurs interlocuteurs la « qualité » des outils mis en place pour se conformer aux exigences de la protection des données à caractère personnel. Des études d'impact ont été réalisées et des outils sont mis en ligne sous format open source. Une version bêta d'une cartographie des risques est déjà à disposition des acteurs.

Ces mécanismes doivent être pensés en fonction d'une grande variété de configurations et être agiles. Telle administration devra penser à certains processus

de mise en conformité pour éviter le croisement intempestif de fichiers des citoyens, tandis que telle entreprise devra s'assurer de la sécurité de la circulation des données au sein de son groupe. Des packs sectoriels notamment pour les objets connectés ou véhicules communicants sont élaborés dans cette perspective d'appropriation de la norme par les acteurs.

Ce droit souple n'est pas toutefois sans poser de question quant à son opposabilité. Quelle est l'autorité d'une ligne directrice ? A quelle sanction s'expose celui qui l'aura méconnue ? La personne victime d'une pratique pourra-t'elle s'en prévaloir pour demander réparation de son préjudice du fait de cette méconnaissance ? Le droit souple est-il véritablement du droit et s'accompagne-t-il d'une forme de contrainte ? Faut-il en ce domaine se contenter des effets de réputation ? Ces questions ne sont pas nouvelles et les réponses multiples peuvent, là encore, être puisées dans le droit de la concurrence. Une réponse néanmoins a été donnée par **Sophie Kwasny,** qui évoquant l'arrêt du 5 septembre 2017 de la CEDH dans l'affaire Barbulescu c/ Roumanie, montre que la référence aux outils d'interprétation, en l'occurrence une recommandation de 2015, dans la décision fait précisément basculer la *soft law* en une norme juridiquement opposable. La souplesse du référentiel n'en signe pas la faiblesse.

Dans le nouveau paysage dessiné par le RGDP, le rôle des opérateurs est également amené à se modifier dans le sens d'une plus grande autonomie ; ils deviennent en quelque sorte co-constructeur de la norme. **Isabelle Cantero** indiquait, à cet égard, l'importance du dialogue entre les DPO pour comparer les bonnes pratiques et dans la gouvernance.

Plusieurs intervenants sont venus exposer les process mis en œuvre dans la perspective de la mise en conformité, ce dont il est émergé au moins une conclusion convergente. La réussite d'une politique consiste à intégrer la compliance dans le cadre d'une stratégie plus générale de la sécurité des données et des systèmes informatiques. Nathalie Laneret nous a dit qu'on en vient à « gaspiller l'argent si on n'investit pas dans la sécurité ».

Pour que les données puissent circuler de façon sécurisée et fluide à l'intérieur du groupe, il faut « éviter le lien le plus faible » ; quelle que soit la filiale, quel que soit le type d'activité, il faut s'assurer que les diverses entités répondent au même niveau d'exigence. **Jean-Pierre Mistral** a expliqué les différentes étapes de la politique de Gemalto, pilotée au niveau mondial, pour se mettre en conformité, au terme d'un processus entamé il y a quatre ans. Il a insisté sur la nécessité de penser en amont l'architecture des mécanismes de traitement pour les intégrer dans les produits et services et s'inscrire ainsi réellement dans les principes de privacy by design et de privacy by default qui inspirent le règlement. Il a également insisté sur la nécessité d'organiser un contrôle interne accompagné d'une formation permanente des équipes. Le coût de cette mise en place n'est pas dirimant dès lors que des personnes compétentes s'en saisissent ; il s'agit donc essentiellement de prévoir des coûts d'une formation qui ne se termine pas en mai 2018 mais qui, a, au contraire, vocation à accompagner la politique de l'entreprise sur le long terme. En d'autres termes, l'établissement d'une politique de compliance repose pour l'essentiel sur la responsabilisation des acteurs.

II. Vertu de la « compliance » /conformité ?

Certains avancent que se mettre en conformité avec un niveau d'exigence élevé de la protection des données des individus peut être porteur d'un point de vue concurrentiel – une concurrence par les mérites, avec une perspective de satisfaction du consommateur, si cette perspective d'une vertu concurrentielle de la compliance est séduisante, elle est toutefois sujette à interrogation quant à l'alignement des grands acteurs sur de telles exigences (2.1.). Toutefois, à supposer même qu'un tel résultat économique ne soit pas nécessairement atteint, il demeure utile de faire valoir une autre vertu de la compliance, citoyenne celle-là (2.2.)

2.1. Vertu concurrentielle ?

Plusieurs intervenants ont mis en avant la nécessité de procéder à un bilan coût/ avantage de l'investissement, notamment à travers une analyse de risque (**Karim Jouany**). Cette approche « risque » (**Isabelle Cantero)** suppose une analyse d'impact des éventuels problèmes nés d'une politique défaillante de protection des données personnelles (voir l'exemple des fuites chez Uber ou Orange).

Il convient aussi d'envisager la compliance comme une opportunité pour la valorisation du capital informationnel et de développement de nouveaux business models fondés sur l'expérience du consommateur. La qualité de traitement de la donnée, sa sécurité et l'adhésion des individus à cette politique de traitement constituent autant d'éléments permettant une meilleure monétisation du capital data et de création de services qualitatifs.

Il échet enfin de créer des éléments de confiance qui constituent autant de marques de qualité vis-à-vis des clients, lesquels deviennent les premiers vérificateurs et certificateurs des entités qui traitent leurs données.

Toutefois, il ne faut pas exagérer les perspectives positives de la compliance, car il existe des risques de dysfonctionnement. Le premier tient à la conduite du changement. Il se peut en effet que l'effort de compliance ne soit fait qu'en surface et qu'il ne parvienne pas à atteindre les objectifs assignés. Ce sera sans doute le cas si cette politique de conformité se réalise sans un changement d'architecture de la distribution de la ressource ou de la culture des « données » au sein de l'entité.

Paul-François Fournier de la BPI a également mis en lumière le risque non négligeable qu'un degré d'exigence important conduise à renforcer la position dominante de certains acteurs économiques et, partant la rente de ces derniers.

Karim Jouany a fait valoir que l'investissement nécessaire, notamment pour une entreprise fanco-tunisienne, comme la sienne est considérable car la complexité s'accroît ici en raison des possibilités de transferts internationaux de données. Or, les entreprises infobèses ont des capacités d'investissement dans les architectures de sécurité des données que n'ont pas les petites entreprises, lesquelles peinent par conséquent à atteindre la taille critique de collecte et de traitement de données pour pouvoir rivaliser avec les grands acteurs américains. Ainsi le niveau de contrainte

pourrait paradoxalement pénaliser les entreprises les plus innovantes et favoriser celles qui sont déjà en place et capables d'amortir les investissements nécessaires.

A l'opposé, il ne faut pas non plus taire le risque, bien réel, que certains acteurs économiques, notamment du fait de localisation géographique opportune – soit en dehors de l'Union, soit même en opérant une sorte de forum shopping au sein des Etats membres – contournent les exigences du RGDP ; il n'est que de voir le lobbying forcené - et partiellement couronné de succès - auquel se sont livrés certains GAFAM pour alléger autant que faire se peut les conditions du règlement. Bien que les mécanismes de coopération entre autorités nationales aient précisément pour objectif de contrer ces effets d'aubaine au sein de l'Union, il n'est pas exclu que certains opérateurs puissants refusent de se plier aux exigences européennes, créant de ce fait une distorsion de concurrence entre acteurs locaux – contraints d'obéir à la norme – et acteurs internationaux qui trouvent les moyens de ne pas y satisfaire.

En dépit des incertitudes qui entourent l'avantage concurrentiel à court terme que peuvent tirer les entreprises de la compliance, il est une autre vertu, moins immédiate, mais socialement plus importante que les opérateurs peuvent espérer dégager d'une politique responsable de conformité ; c'est la vertu citoyenne.

2.2. Vertu citoyenne

Cette vertu citoyenne se manifeste à deux degrés différents : au plan individuel comme au plan politique.

Au plan individuel, il ne fait nul doute que la mise en œuvre des obligations du RGPD a pour objectif de maintenir voire d'augmenter la protection des personnes quant à l'usage qui est fait de leurs données à caractère personnel. Il s'agit, nous dit **Karim Jouany** de remettre le citoyen au cœur du dispositif. Mais pour rendre cette protection effective, il conviendra sans doute d'aller plus loin que la simple mise en place de normes substantielles ; il convient de les accompagner d'actions garantissant cette effectivité. Ainsi, il serait souhaitable de dépasser le carcan de la loi pour une République numérique qui rend en pratique quasiment impossible l'action collective dans ce domaine. Il serait heureux que la loi en cours d'élaboration remédie à ce blocage. Il faut saluer les initiatives telles que celle de **Max Schrems** visant à éviter que les protections mises en place ne demeurent pas simplement formelles et qu'elles soient également opposables aux acteurs internationaux.

De façon plus anecdotique, la mise en place aura également des répercussions positives au plan individuel pour les futurs DPO puisqu'on anticipe environ 28 000 postes potentiels, dont certains nous a-t-on dit seront payés de façon marginale pour cette fonction. Il n'en demeure pas moins qu'il s'agit d'une opportunité d'embauche importante pour les étudiants présents dans la salle.

Plus sérieusement, le RGDP s'inscrit au plan politique dans le cadre d'une bataille de souveraineté, comme l'a souligné **Paul-François Fournie**r de la BPI. Il s'agit de se positionner au sein d'une confrontation de logiques entre deux mondes. A cet égard, et sans manichéisme excessif, il convient de choisir un modèle de société entre ceux qui pensent que la donnée est avant tout un avoir ou un actif économique et ceux qui pensent qu'elle est constitutive de l'individu et de sa liberté individuelle. Il a été indiqué que la place qu'occupe la France au sein du G29 incite à l'optimisme du point de vue de sa capacité à faire valoir certaines de ses valeurs au sein de l'Union et même au-delà.

Sophie Kwasny, dans cette même perspective a évoqué la fonction de modèle de la convention 108 et sa viralité à mesure que de nouveaux pays témoignent leur intérêt d'y adhérer. Ainsi, l'impulsion politique des Etats ou des organisations européennes peut conduire à éviter qu'un modèle unique de comportement, essentiellement fondé sur la rationalité économique s'impose au monde.

Mais dans une économie mondialisée où les Etats perdent peu à peu leur place essentielle dans la définition de la norme, l'objectif de diversité ne peut se satisfaire d'une seule dynamique « *top/bottom* ». La réussite du modèle n'interviendra que si les acteurs économiques y adhèrent, s'en emparent et le véhicule. A cet égard, même si certains doutes peuvent jaillir sur les risques de forum shopping notamment au sein de l'Union avec le rôle ambigu joué par l'Irlande, l'essentiel des intervenants semblent témoigner d'une volonté de participer à l'effet d'entrainement que la mise en place des règles du RGPD peut avoir sur une politique de la donnée qui serait respectueuse des libertés individuelles. Puisqu'il faut investir dans une politique de la sécurité des données, autant le faire par le haut indique **Jean-Pierre Mistral** et se conformer à l'exigence la plus élevée dans le domaine qui est le RGPD. Or, éviter le maillon faible conduit à assurer un niveau de conformité homogène et équivalent en Europe mais également hors de l'Europe. C'est ainsi par souci de commodité et d'économie que le RGPD pourra devenir viral et véhiculer ainsi les valeurs qu'il promeut.

En conclusion, il convient sans doute de modérer cet enthousiasme sur les vertus attendues de la mise en place du RGDP et de ne pas ignorer le scepticisme légitime qui l'entoure. Bien évidemment, il sera sans doute illusoire d'atteindre une conformité complète. **Nathalie Laneret** a rappelé que 100% de compliance était un objectif impossible à atteindre et **Arthur Langer** a fait valoir que - « *almost complying is not complying and almost winning is losing* »-, qu'une conformité approximative pouvait en réalité se résumer à pas de conformité du tout. Certes.

Mais est-ce parce que l'objectif est impossible à atteindre qu'il ne faut pas néanmoins essayer d'y parvenir ? N'avons-nous pas si ce n'est une obligation de résultat, au moins une obligation de moyen ? Un proverbe camerounais dit que « *le singe a appris à sauter de l'arbre en plusieurs essais* » et comme un écho, un autre proverbe, français celui-là répond « *Ne sait ce qui est bien qui nul n'essaie*. » Nous ne pouvons être sûrs d'aboutir et de construire une société digitale respectueuse des libertés individuelles mais est-ce parce que la tâche est immense et aléatoire qu'il faut y renoncer. Ne devons-nous pas, tel Sisyphe qui pousse son rocher inlassablement recommencer et, comme le disait Camus, y trouver une forme d'aboutissement car « il faut imaginer Sisyphe heureux » ?

Conférence co-organisé par :

HEC PARIS ALUMNI

CNEJITA EXPERTS

R.P.I.S.E.
REVUE DE PROPRIÉTÉ INTELLECTUELLE DU SUD-EST

en partenariat avec :

Faculté de Droit et de Science Politique
Aix*Marseille Université

AFCDP
Association Française des Correspondants à la protection des Données à caractère Personnel

COLUMBIA UNIVERSITY
IN LVMINE TVO VIDEBIMVS LVMEN

BARREAU DE MARSEILLE
MARSEILLE CITÉ DU DROIT

AVOCATS AIX-EN-PROVENCE