La réforme de la **protection des données** dans l'Union européenne

Jan Philipp Albrecht, eurodéputé

GREEN EUROPEAN FOUNDATION

Les Verts | ALE
au Parlement européen

Mentions légales

Jan Philipp Albrecht, eurodéputé

Parlement Européen
Rue Wiertz 60
1047 Bruxelles
Belgique

Green European Foundation
15, Rue d'Arlon
1050 Bruxelles
Belgique

rédaction **Ralf Bendrath**
textes **Jan Philipp Albrecht, Ralf Bendrath, Florian Jotzo, Zora Siebert**
relecture **Levka Backen, Benjamin Breitegger, Pia Kohorst, Siana Rott**
coordination de la version française **Fiona Costello**
design et illustration **p*zwe**
imprimeur **AktivDruck, Göttingen**

Décembre 2015

Avec le soutien financier du Parlement européen.

Les Verts | ALE
au Parlement européen

GREEN EUROPEAN FOUNDATION

Sommaire

Chère lectrice, cher lecteur,

Lorsqu'ils entendent parler de «protection des données», beaucoup de gens pensent encore qu'il s'agit d'un sujet technique, qui ne les concerne pas vraiment. Or cette idée n'est plus vraie depuis longtemps. En réalité, la protection des données ne vise pas à protéger les données, mais à protéger les personnes. Au début des années 1980, lorsque les autorités allemandes ont décidé de procéder à un recensement de la population, de nombreux citoyens se sont plaints que la collecte de leurs informations personnelles (comme leur niveau de revenu ou leur religion) représentait une atteinte à leurs droits fondamentaux. La Cour constitutionnelle fédérale a alors rendu un jugement reconnaissant l'existence d'un droit fondamental à l'»autodétermination informationnelle», fondé sur la dignité de l'homme et sur le droit au libre développement de la personnalité. Ce concept encombrant marquait le début du long développement du droit fondamental à la protection des données en Europe.

Aujourd'hui, ce n'est plus seulement par intervalles de quelques années que le montant de nos revenus ou notre appartenance religieuse est jaugée. La numérisation et la mise en réseau de tous les objets et de tous les domaines de la vie nous soutirent en une seconde toute une série d'informations qui peuvent être - et, dans la majorité des cas, sont effectivement - envoyées aux quatre coins du monde à une vitesse proche de celle de la lumière et stockées pour toujours dans des banques de données pratiquement illimitées. Dès lors, la question qui se pose est de savoir comment, dans cette situation, nous pouvons encore garder le contrôle sur notre propre vie et sur notre propre personne. À moins que nous ne soyions déjà devenus le produit d'une société des données, dans laquelle des fournisseurs de services de technologies de l'information tiennent notre travail, notre économie et notre vie privée dans leurs mains ? Cette brochure a pour but d'apporter des réponses et des informations contextuelles à ces questions et aux potentielles actions politiques et individuelles.

Avec mes salutations les plus respectueuses des données personnelles,

Jan Philipp Albrecht

Député au Parlement européen, Vice-président de la commission des libertés civiles, de la justice et des affaires intérieures, Rapporteur pour le règlement européen sur la protection des données

POURQUOI PROTÉGER LES DONNÉES ?

D'où vient cette idée ?

La formule « my home is my castle » (ma maison est mon château) est apparue en Angleterre en 1604, dans le contexte d'un conflit juridique, et limitait le droit des soldats du roi à pénétrer dans une habitation sans motif et sans s'être annoncés. Le droit à la vie privée s'appliquait donc initialement aux quatre murs du domicile. La notion d'« autodétermination informationnelle » apparaît à la fin du XIXe siècle : en 1895, à Boston, les avocats Samuel Warren et Louis Brandeis écrivent un essai intitulé « The Right to Privacy » (« Le droit à la vie privée »), dans lequel ils définissent le droit à conserver un certain contrôle sur ce que les autres savent de nous. Cette initiative est motivée par l'émergence de développements technologiques nouveaux à l'époque : les premiers appareils photo portatifs instantanés et l'apparition des journaux quotidiens modernes ont en effet donné naissance au métier de paparazzi, que Samuel Warren et Louis Brandeis souhaitaient contrecarrer. Déjà à l'époque, l'objectif n'était pas de résister à la technologie ou à l'innovation, mais bien d'en assurer une utilisation respectueuse du droit des citoyens à l'autodétermination.

Au XXe siècle, le traitement automatisé des données par des machines est mis au point : avant même l'invention de l'ordinateur, on utilise des cartes perforées pour traiter automatiquement de grandes quantités de données. Ces cartes permettent d'effectuer des calculs techniques, mais aussi de traiter automatiquement des données sur les individus, par exemple à des fins administratives. Les nazis utilisèrent d'ailleurs des machines à cartes perforées produites par la filiale d'IBM Hollerith pour organiser le massacre de masse des Juifs européens.

Dans les années 1960, l'apparition de macroordinateurs dans les institutions publiques et les entreprises suscite un vaste débat sur le pouvoir de ces nouvelles machines. À l'époque, tout comme aujourd'hui, la protection des données a pour objectif d'exploiter les opportunités et les possibilités des nouvelles technologies, sans pour autant rabaisser les individus au statut de simples objets d'opérations informatiques automatisées. C'est à cette époque qu'apparaît le concept de « protection des données ».

La protection des données n'est fondamentalement pas une question technique. Ce qu'il faut protéger, ce ne sont pas les données, mais les individus. Il s'agit de nous permettre de décider nous-mêmes, dans un monde numérisé, ce que chacun sait à notre sujet, comment ces informations sont utilisées et quelles répercussions cela peut avoir sur notre vie. La toute première loi relative à la protection des données est adoptée en 1970, dans le Land de Hesse, en Allemagne. Aux États-Unis, lors des soulèvements étudiants, des discussions ont également eu lieu sur la possibilité d'utiliser les ordinateurs pour exercer un contrôle politique, par exemple avec des banques de données sur les opposants radicaux. Ces discussions ont mené à l'adoption, en 1974, du Privacy Act américain. Toutefois, cette loi ne réglemente la protection des données que pour les administrations publiques : il n'y a toujours pas de législation globale en matière de protection des données aux Etats-Unis pour les entreprises.

Des législations nationales relatives à la protection des données sont progressivement adoptées, surtout dans l'Union européenne. Elles fixent des limites aux opérateurs qui traitent des données et accordent des droits aux personnes concernées, c'est-à-dire à nous-mêmes, par exemple pour recevoir des informations sur nos données ou pour les effacer. Dans sa décision historique sur le rencensement de 1983, la Cour constitutionnelle fédérale allemande a inventé le concept plus précis d' « autodétermination informationnelle ». Puisque de plus en plus d'informations sur notre vie sont disponibles numériquement, nous devons avoir le droit de contrôler qui sait quoi sur nous et ce qu'il peut être possible de faire de ces informations avec un ordinateur. La Cour constitutionnelle fédérale a ainsi reconnu avec beaucoup de clairvoyance qu'une société dans laquelle les gens se sentent en permanence observés, fichés, évalués et numérisés n'est plus une société ouverte de citoyens libres et égaux.

En 1980, les lignes directrices de la Convention n° 108 du Conseil de l'Europe et de l'Organisation de coopération et de développement économiques (OCDE) ont constitué une première tentative d'harmonisation du droit sur la protection des données au niveau international et, ainsi, de prise en considération de la dimension de plus en plus internationale de la circulation de données. Pour l'Union européenne, la principale avancée en la matière reste à ce jour l'adoption, en 1995, de la directive européenne 1995/46 relative à la protection des données à caractère personnel. La Charte des droits fondamentaux de l'Union européenne, qui revêt un caractère contraignant sur la législation européenne depuis 2009, établit également la protection des données en tant que droit fondamental au sein de l'Union.

Malheureusement, bon nombre d'entreprises ne respectent pas le droit européen relatif à la protection des données et continuent à disposer de nos données comme bon leur semble. La réforme de la protection des données dans l'Union européenne actuellement en préparation esr donc la prochaine étape importante pour enfin nous permettre d'exercer véritablement nos droits. La réforme de la protection des données dans l'UE constitue une tentative de reconquête de notre droit à l'autodétermination numérique. C'est aussi une composante de l'achèvement du marché unique numérique européen.

LA RÉFORME DE LA PROTECTION DES DONNÉES dans l'Union européenne

La situation aujourd'hui : une bonne réglementation, mais qui n'est pas respectée partout

Les principes de la protection européenne des données sont toujours valables. Malheureusement, leur application dans la plupart des États membres de l'Union laisse à désirer : les autorités chargées de la protection des données ne sont pas suffisamment outillées et le montant des amendes qu'elles peuvent infliger en cas de non-respect des règles est négligeable pour bon nombre de grandes entreprises. À l'inverse, les entreprises respectueuses des lois qui souhaitent respecter la confidentialité de nos données sont confrontées à 28 législations différentes si elles veulent exercer leurs activités dans l'ensemble de l'Union et profiter du marché unique européen. Les nombreuses entreprises qui n'ont qu'un seul siège en Europe et utilisent Internet pour offrir leurs services sur l'ensemble du marché unique posent également un problème sérieux pour les consommateurs, qui se retrouvent laborieusement aux prises avec le système juridique s'appliquant au siège de l'entreprise s'ils veulent s'opposer à elle. L'étudiant autrichien Max Schrems en est un exemple : il a dû intenter son procès à Dublin, avec des dépenses importantes, afin de faire valoir ses droits contre Facebook.

Dans le même temps, les entreprises établies en dehors de l'Union qui y proposent leurs services en ligne font souvent preuve d'un mépris total pour le droit européen. Si les firmes informatiques de la Silicon Valley et d'ailleurs ne respectent pas les règles de la même façon que les entreprises européennes, une faible application de la législation signifie que leur localisation leur offre un avantage manifeste. En outre, les entreprises, tant américaines qu'européennes, dissimulent souvent les informations sur l'utilisation qui est réellement faite de nos données en les noyant dans des déclarations de confidentialité longues et compliquées.
C'est pour toutes ces raisons que l'Union européenne travaille depuis plusieurs années à une refonte du droit sur la protection des données. Plusieurs procédures de consultation publique ont été menées depuis 2009 et, en novembre 2010, la Commission européenne a présenté une communication intitulée « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ». Le Parlement européen et le Conseil des ministres de l'intérieur et de la justice des États membres de l'Union ont rendu leurs avis sur cette proposition en 2011. À cette occasion, le Parlement européen a, entre autres, clairement indiqué qu'une réforme ne devait en aucun cas affaiblir le niveau actuel de protection des données.

En janvier 2012, la commissaire européenne en charge de la justice de l'époque, Viviane Reding, a présenté le projet de loi tant attendu. Depuis lors, le Parlement européen et le Conseil des États membres (Conseil des ministres) ont travaillé pour parvenir à une version du texte législatif qui puisse être acceptée par les deux instances. Les travaux réalisés au Parlement européen sont placés sous la direction de Jan Philipp Albrecht, spécialiste de la protection des données issu du groupe des Verts. La présidence du Conseil est assurée à tour de rôle par un État membre différent, qui change tous les six mois.

La réforme de la protection des données poursuit trois objectifs: renforcer et mieux faire respecter nos droits; faciliter le respect des règles européennes pour les entreprises; faire en sorte que les systèmes informatiques respectueux de la confidentialité des données deviennent la norme.

1) Afin de mieux faire respecter nos droits, des amendes élevées sont prévues, ainsi que les mêmes instruments prévus pour la protection des consommateurs comme les actions collectives (possibilités pour les associations représentantes de la protection des données, de la protection des consommateurs ou d'autres causes d'utilité publique d'engager des actions en justice). Dans le même temps, le couplage des données est interdit (c'est-à-dire que la fourniture d'un service ne peut pas être subordonnée à la collecte de plus de données que nécessaire). Les personnes concernées ont le droit de consulter leurs données sous forme électronique et de pouvoir les réutiliser pour d'autres services. Des symboles standardisés doivent permettre de comprendre instantanément la façon dont les données sont utilisées, à l'instar des labels pour l'alimentation biologique.

2) Pour faciliter la tâche des entreprises, l'ancienne directive sera remplacée par un règlement européen qui entrera immédiatement en vigueur. Cela permettra d'instaurer un droit uniforme pour l'ensemble de l'Union européenne et de remplacer le patchwork des 28 législations nationales distinctes des États membres qui s'appliquaient jusqu'à présent. De plus, les obligations bureaucratiques seront également simplifiées ou supprimées.

3) À l'avenir, la protection technologique des données devrait veiller davantage à limiter la quantité de données produites dès le départ, à restreindre le stockage des données aux seules informations qui sont véritablement nécessaires pour la fourniture d'un service et à offrir la possibilité d'utiliser des services de façon anonyme ou sous pseudonyme. Pour ce faire, de nouvelles règles promouvront le respect de la confidentialité des données (prise en compte du respect de la vie privée dès la conception, « privacy by design ») et des paramètres par défaut qui impliquent moins de données (respect de la vie privée par défaut, « privacy by default »). Le droit de prendre nos données aux autres prestataires dans un format lisible par machine facilitera la concurrence.

Les défis liés à la
PROTECTION DES DONNÉES

Une quantité croissantes de données sur chacun de nous sont stockées et traitées.

Les consommateurs allemands utilisent désormais 100 millions de cartes de fidélité comme Payback ou Happy Digit lorqu'ils font leurs achats, offrant aux entreprises des informations détaillées sur les habitudes de consommation quotidiennes des gens.

Grâce à l'utilisation de plugins sociaux, comme le bouton « J'aime », le réseau social Facebook peut suivre les activités des utilisateurs d'Internet, même sur d'autres sites web en dehors de sa propre infrastructure. La fonction « Retrouver des amis » fournit à l'entreprise américaine un large aperçu de l'environnement social des utilisateurs d'Internet. De cette façon, même les utilisateurs qui n'ont pas de compte Facebook finissent dans ses bases de données. Tout comme Facebook, les administrateurs des pages fan sur Facebook peuvent eux aussi voir ces données et les communiquer à des annonceurs.

En utilisant les techniques de big data, les entreprises peuvent analyser et exploiter des quantités de données sans précédent. L'exemple de l'application pour smartphone Uber révèle quel type d'informations intimes les entreprises cherchent à extraire de ces montagnes de données : le fournisseur de cette application analysait les données de déplacement de ses clients pour déterminer si ceux-ci utilisaient le service Uber pour avoir une aventure d'un soir. En dehors de ce genre d'exemple extrême, les entreprises utilisent généralement les données dans l'intérêt mutuel des parties, pour diffuser des publicités de façon ciblée et améliorer leurs produits. Le fait de disposer de davantage d'informations leur permet cependant aussi de réduire les risques inhérents à leur modèle économique, au détriment des consommateurs. Un exemple, les décisions pour les paiements échelonnés : les individus qui, selon les prévisions statistiques, seraient plus susceptibles de prendre du retard dans leurs versements paient ainsi des intérêts plus élevés, même s'il s'agit de personnes en réalité tout à fait fiables individuellement. Les possibilités des entreprises dans ce domaine vont continuer à s'étendre rapidement dans les prochaines années. Le « Cloud », l' « Internet des objets » et les accessoires vestimentaires connectés, tels que les montres, les télévisions, les commandes de chauffage, les voitures et les frigos intelligents, vont tous permettre à des systèmes informatiques avides de données d'envahir encore davantage notre quotidien que les ordinateurs et les smartphones auxquels nous sommes aujourd'hui habitués. Cela signifie que des profils beaucoup plus précis seront rapprochés. Le fait d'assurer qu'à l'avenir, chacun soit conscient de ce que les autres savent sur lui dans cet environnement numérique, constitue l'un des grands défis de notre époque. La réforme de la protection des données vise à cela.

Les applications de big data permettent aux entreprises d'évaluer et d'exploiter des quantités de données sans précédent. L'exemple de l'application pour smartphone Uber révèle quel type d'informations intimes les entreprises cherchent à extraire de ces amas de données. Le fournisseur de cette application analysait les données de déplacement de ses clients pour déterminer si ceux-ci utilisaient le service Uber pour avoir une aventure d'un soir potentielle. En dehors de ces exemples extrêmes, les entreprises utilisent généralement les données dans l'intérêt mutuel des parties, pour diffuser des publicités de façon ciblée et améliorer leurs produits. Le fait de disposer de davantage d'informations leur permet cependant aussi de réduire les risques inhérents à leur modèle économique au détriment de leurs clients, par exemple en ce qui concerne les décisions pour les achats à crédit: les individus qui, selon les prévisions statistiques, seraient plus susceptibles de prendre du retard dans le remboursement de leurs mensualités paient ainsi des intérêts plus élevés, même s'il s'agit de personnes en réalité tout à fait fiables. Au cours des prochaines années, les entreprises continueront à voir s'ouvrir de nombreuses possibilités dans ce domaine. Le «Cloud», l'»Internet des objets» et les dispositifs «portables», tels que les montres, les télévisions, les commandes de chauffage, les voitures et les frigos intelligents, autorisent des systèmes informatiques avides de données à envahir encore davantage notre quotidien que les ordinateurs et les smartphones auxquels nous sommes aujourd'hui habitués. Ces technologies définissent des profils beaucoup plus précis pour chaque individu. Le fait de permettre à l'avenir à chacun d'avoir un droit de regard sur ce que les autres savent sur lui dans cet environnement numérique constitue l'un des grands défis de notre époque, que la réforme de la protection des données devrait contribuer à relever.

LA MISE EN VENTE DE NOS DONNÉES

Les empreintes dans la neige finissent par disparaître, pas celles que nous laissons dans le monde numérique. Google et Facebook suivent même les visiteurs d'autres sites web pendant des mois. Les deux géants américains enregistrent ainsi le comportement des gens sur internet, qu'il s'agisse ou non d'utilisateurs de leurs services. Les gestionnaires de données traditionnels, comme la filiale de Bertelsmann Arvato Infoscore, collaborent avec les collecteurs de données numériques, et le leader du marché américain, Acxiom, a maintenant des fichiers sur près de 700 millions de personnes, comprenant jusqu'à 3 000 informations par personne. Les données enregistrées incluent des informations sur leur formation, leur logement, leur emploi, leurs finances, leurs centres d'intérêt et leur santé. Acxiom compte déjà 44 millions d'Allemands dans ses dossiers, soit plus de la moitié de la population. Les interfaces numériques prennent également de plus en plus d'importance au quotidien. Les Allemands possèdent plus de 100 millions de cartes de fidélité, qui, combinées avec les informations de paiement provenant des cartes de débit et de crédit, fournissent aux entreprises un aperçu détaillé des habitudes d'achat et de paiement des consommateurs.

Les traces laissées par nos données permettent de prévoir notre comportement : en analysant ces données, les sociétés d'assurance et les banques peuvent réduire les risques inhérents à leurs activités au détriment de leurs consommateurs. La firme hambourgeoise Kreditech utilise les données de localisation et des réseaux sociaux Facebook, Xing et LinkdIn pour fournir des taux de crédits. La société d'assurance-vie Aviva étudie pour sa part des modèles qui s'appuient sur les habitudes de consommation, le style de vie et le revenu pour prévoir qui va développer du diabète, de l'hypertension ou une dépression, et devra alors payer des cotisations plus élevées. L'assureur Generali veut encourager les clients de ses assurances maladie à rassembler des informations sur leur alimentation, leur condition physique, leur santé et leur mode de vie au moyen de leur smartphone en leur offrant en échange des bons d'achat ou des réductions sur leurs cotisations. À l'avenir, les personnes qui refuseront de participer à de tels systèmes pourraient se voir imposer des cotisations plus élevées. La société Allianz a des projets semblables : en collaboration avec des constructeurs automobiles, cette entreprise travaille à l'élaboration de programmes de primes pour ses assurances véhicule incluant des GPS embarqués qui enregistrent automatiquement les comportements au volant. Parallèlement, les entreprises peuvent utiliser les données de consommation de leurs clients pour en tirer des conclusions sur leur vie. La chaîne de supermarchés américains Target, par exemple, utilise ces données pour établir la probabilité que ses clientes soient enceintes : l'entreprise vise les futurs parents aux alentours de la date de naissance présumée, car leurs habitudes de consommation changent énormément à cette période et ils sont particulièrement sensibles à la publicité. L'analyse des données permet également aux entreprises de désavantager certains consommateurs ciblés lorsqu'ils établissent leurs prix : après avoir obtenu les informations de navigation de ses visiteurs, le portail de voyage en ligne Orbitz est par exemple parvenu à soutirer aux utilisateurs de produits Apple des prix jusqu'à 13 % plus élevés pour une même chambre d'hôtel, car ces utilisateurs avaient été classés dans la catégorie des clients aisés.

Dans ce contexte, chacun peut être victime des statistiques. Les fournisseurs de services de notation font des erreurs lorsqu'ils collectent et interprètent les données et aucune probabilité statistique ne peut être strictement équivalente aux personnes concernés. Les développements qui ont été détaillés ici discriminent principalement ceux qui ne rentrent pas dans la grille statistique. Cela est aussi vrai pour les personnes qui souhaitent éviter d'être ainsi sous surveillance : elles sont de plus en plus souvent confrontées à des prix plus élevés, car même l'absence d'informations à leur sujet représente un risque pour les entreprises, qui réagissent en augmentant les tarifs. Les consommateurs sont donc soumis à une pression de plus en plus forte pour livrer davantage d'informations. Le droit à la protection des données devient ainsi un privilège qui se paie cher.

LA SOCIÉTÉ DE SURVEILLANCE

Les révélations sans précédent d'Edward Snowden ont montré avec quelle ampleur les services secrets américains et britanniques surveillent les citoyens du monde entier à leur insu, en collaboration avec leurs homologues canadiens, néo-zélandais et australiens. Dans le cadre du programme Prism, les autorités des États-Unis exploitent massivement les informations des centres de données des grands fournisseurs de services informatiques américains, tels que Microsoft, Google, Yahoo et Amazon. Le GCHQ, le service de renseignement électronique britannique, utilise le programme Tempora pour puiser dans les flux transatlantiques de données majeurs, intercepter une grande partie du trafic international de données et analyser ces informations. Le GCHQ est également parvenu à avoir accès aux courriels des journalistes travaillant pour les médias internationaux. Il a également infiltré les infrastructures de l'opérateur de télécommunications belge Belgacom, utilisées par les députés européens et les membres d'autres institutions européennes. Tout comme le GCHQ, la NSA, l'agence américaine de surveillance, a également ciblé les gouvernements : parmi les 122 chefs d'État du monde entier placés sur écoute figuraient même des alliés comme la chancelière allemande, Angela Merkel, dont le téléphone portable avait été infiltré par les services secrets. Bien que la réforme européenne de la protection des données ne s'appuie pas sur les révélations d'Edward Snowden en tant que telles, elles ont tout de même considérablement influencé la législation. Elles ont permis d'orienter le débat politique sur les enjeux de la société de surveillance et donc de la protection des données.

La surveillance massive et non maîtrisée exercée par les services secrets ne représente pas seulement un danger pour les droits fondamentaux des citoyens : elle menace également les entreprises, car celles-ci utilisent généralement des logiciels et du matériel informatique provenant de sociétés américaines. Ces sociétés accordent à leurs services secrets nationaux, de façon plus ou moins volontaire, un large accès à des données parfois extrêmement sensibles.

Face aux menaces posées par le terrorisme et le crime organisé international, les appels aux niveaux européens et nationaux pour le renforcement des instruments de surveillance publique se font de plus en plus pressants : la reconnaissance automatique des plaques d'immatriculation, le logiciel espion allemand «Bundestrojaner» (« cheval de Troie fédéral »), l'accord SWIFT relatif à l'échange international des données bancaires et avant tout la collecte des informations personnelles des passagers aériens et la conservation des données ne sont que quelques-uns des grands sujets actuellement débattus. Les jugements de la Cour de justice de l'Union européenne et de la Cour constitutionnelle fédérale allemande sur la conservation des données montrent que, dans son désir pressant de plus de sécurité, le législateur risque de compromettre les libertés et les droits fondamentaux des citoyens. Dans ces arrêts majeurs, les deux instances judiciaires ont démontré que le stockage injustifié des données est contraire aux droits fondamentaux européens et allemands.

Il incombe dès lors au législateur d'imaginer des solutions moins simplistes pour relever les défis de la lutte contre le terrorisme et des services de police modernes, avec des réponses qui ne considèrent pas la sécurité collective comme incompatible avec les libertés individuelles. Les autorités gouvernementales doivent également protéger efficacement leurs citoyens contre la surveillance par les services secrets.

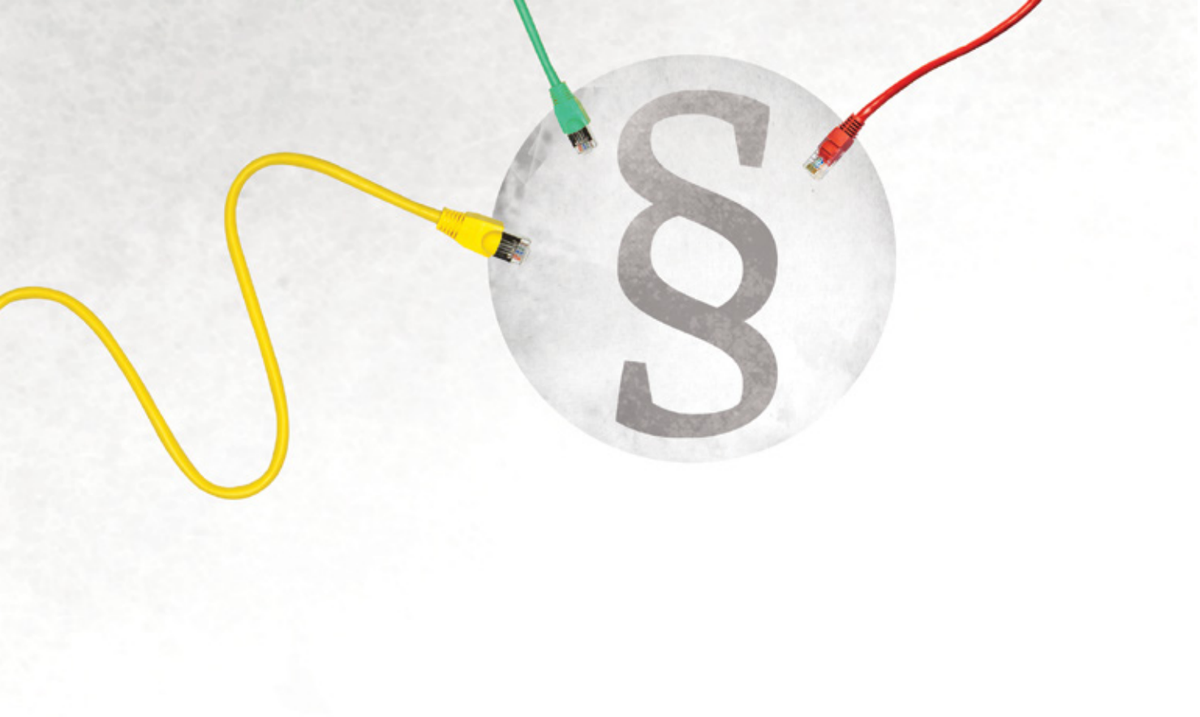
FAQ

1. À qui s'applique réellement le règlement sur la protection des données ?

A l'origine de la réforme européenne de la protection des données, la question était « pourquoi » : pourquoi est-il nécessaire de réformer le cadre réglementaire de la directive européenne de 1995, et même d'aller plus loin en adoptant une législation européenne unique en matière de protection des données, qui serait le règlement européen sur la protection des données ? La réponse à cette question est a priori très simple : parce que, contrairement aux marchandises traditionnelles, les données peuvent franchir les frontières en quelques millisecondes et qu'il devient de plus en plus difficile de déterminer l'endroit exact où nos données sont stockées. Pour les entreprises dont l'activité tire profit des données, il est donc très facile de déclarer « vos lois allemandes sur la protection des données ne s'appliquent absolument pas à nous, puisque nous traitons vos données en Irlande ou aux États-Unis ». Il y a là un paradoxe, particulièrement vis-à-vis de l'Union européenne : les entreprises établies dans un État membre de l'Union peuvent offrir leurs services en ligne sur l'ensemble du marché intérieur européen. Cependant, si ces entreprises ne respectent pas la législation des autres États membres de l'Union, les autorités de ces États ne peuvent l'obliger à s'y conformer, seules les autorités du territoire où se trouve le siège de l'entreprise ayant ce droit. Un ensemble commun de règles applicables à l'ensemble du marché de l'Union européenne est donc nécessaire. L'idée est un règlement européen prévoyant, conformément au principe du « lieu où se tient le marché » (lex loci solutionis), que toutes les entreprises du monde doivent respecter les règles uniformes établies par ce règlement dès lors qu'elles proposent leurs biens et services sur le marché européen. En cas de non-respect, les entreprises s'exposeront à de sévères sanctions identiques dans toute l'Europe, pouvant être appliquées partout dans le monde. Néanmoins, une telle approche n'est possible que si les 28 États membres de l'Union parviennent à s'accorder sur un standard de protection des données uniforme et juridiquement solide. Le Parlement européen y est d'ores et déjà parvenu, mais un accord avec le Conseil des ministres doit encore être trouvé.

Bien entendu, un tel projet d'harmonisation nécessite de tenir compte du fait qu'il existe certains domaines particuliers dans lesquels les règles et les cultures juridiques des Etats membres diffèrent encore considérablement. Dans une proposition de janvier 2012, la Commission avait par exemple déjà prévu d'autoriser l'adoption de règles particulières au niveau national en ce qui concerne la liberté de la presse, la recherche, les églises, les métiers soumis au secret professionnel et les droits des travailleurs. Le Parlement européen a étendu cette exception à d'autres secteurs, comme la sécurité sociale publique et les archives. La réforme comprend également un aspect important mais souvent source de malentendus : le nouveau règlement sur la protection des données doit en effet également s'appliquer aussi à la façon dont les administrations publiques traitent les données, afin de permettre, par exemple, aux personnes concernées de s'assurer que les administrations respectent leurs demandes en matière d'information et de suppression des données. Cependant, ce règlement prévoit explicitement que le traitement des données par les administrations publiques doit toujours (!) faire l'objet d'une loi nationale qui définit clairement l'ampleur et les conditions de la collecte et du traitement de données par les autorités publiques. Ce règlement ne restreindra donc nullement ni ne se substituera aux règles des administrations gouvernementales en matière de protection des données. Dans son avis, le Parlement européen à une nouvelle fois insisté clairement sur cette marge de manœuvre accordée aux législateurs nationaux.

> Toutes les entreprises du monde doivent respecter les règles uniformes établies dans ce règlement dès lors qu'elles proposent leurs biens et services sur le marché européen.



2. Une telle loi est-elle vraiment adaptée à Internet?

Une législation applicable au marché unique du numérique, et non une réglementation concrète de la technologie : L'un des arguments souvent avancés pour justifier la nécessité de remplacer la directive européenne de 1995 sur la protection des données actuellement en vigueur est que cette législation a été adoptée avant que l'usage d'Internet ne se massifie : c'est exact. Le règlement sur la protection des données devrait avant tout instaurer un cadre juridique uniforme pour le marché unique numérique européen qui est apparu. Cette loi a aussi pour but de garantir l'application de la législation aux entreprises établies en dehors de l'Union européenne qui proposent des services sur le marché européen, c'est-à-dire sur Internet. Cependant, il ne s'agit en aucun cas de réglementer des technologies particulières comme Internet ou les services en ligne. En effet, une telle loi deviendrait très rapidement obsolète. Il ne serait guère possible pour le législateur d'établir de nouvelles règles pour toutes les nouvelles innovations technologiques, telles que les réseaux intelligents d'énergie, l'Internet des objets ou les voitures connectées.

Principes fondamentaux du droit établi en matière de protection des données : Les principes fondamentaux ne seront pas altérés : l'autorisation de la collecte et du traitement des données personnelles uniquement si les personnes concernées y consentent librement ou sont, a minima en mesure de l'assumer sur la base des déclarations de confidentialité, des dispositions légales ou l'existence d'une relation avec l'opérateur chargé du traitement des données ; droit d'accès, de rectification et de suppression ; l'obligation que les données soient collectées dans un but précis ; minimisation des données. L'application spécifique de ces principes aux différentes technologies et aux différents modèles d'activités relève des autorités nationales chargées de la protection des données. Malheureusement, le Parlement européen et le Conseil des ministres prennent des positions très différentes même en ce qui concerne ces principes fondamentaux. Le Parlement européen a, par exemple, restreint les « intérêts légitimes » de l'opérateur traitant les données – qui permet de traiter des données sans l'accord de la personne concernée – à ce qui peut être raisonnablement attendu. Les clients d'une entreprise, par exemple, peuvent s'attendre à ce que celle-ci leur envoie de temps en temps ses dernières offres s'ils ne s'y opposent pas ; par contre, ils ne s'attendent pas à ce que cette entreprise revende leurs données à d'autres sociétés. De leur côté, les États membres débattent pour décider s'il convient d'autoriser le traitement des données à des fins entièrement différentes de celles présentées lors de la collecte initiale des données, y compris par des tiers inconnus. De telles dispositions affaibliraient cependant les droits des personnes concernées à un niveau nettement inférieur à celui proposé par la Commission, et même inférieur au niveau actuel de protection des données.

Des définitions pérennes dans le temps : Toutes les informations susceptibles d'être associées à une personne, de façon directe ou indirecte, sont protégées comme des données à caractère personnel. Il s'agit d'une notion particulièrement importante à l'époque des « big data », où de plus en plus de séries de données peuvent être réunies, combinées et exploitées. Il devrait donc exister des mesures d'incitation pour encourager l'utilisation de données sous forme pseudonyme, qui ne peuvent pas être mises en relation avec d'autres données sur la personne concernée. Le Parlement a également clairement établi que les données ne doivent pas nécessairement permettre de déterminer l'identité d'une personne (même de façon indirecte) pour pouvoir bénéficier d'une protection ; il suffit qu'elles permettent de reconnaître une personne parmi d'autres individus. Ces mesures ne sont toutefois pas dirigées contre les « big data » : bon nombre de nouvelles applications qui traitent de grandes quantités de données n'ont pas besoin de données personnelles, des données anonymes peuvent être utilisées afin de ne pas permettre d'identifier des individus. Ces applications ne sont donc pas bridées par le droit sur la protection des données.

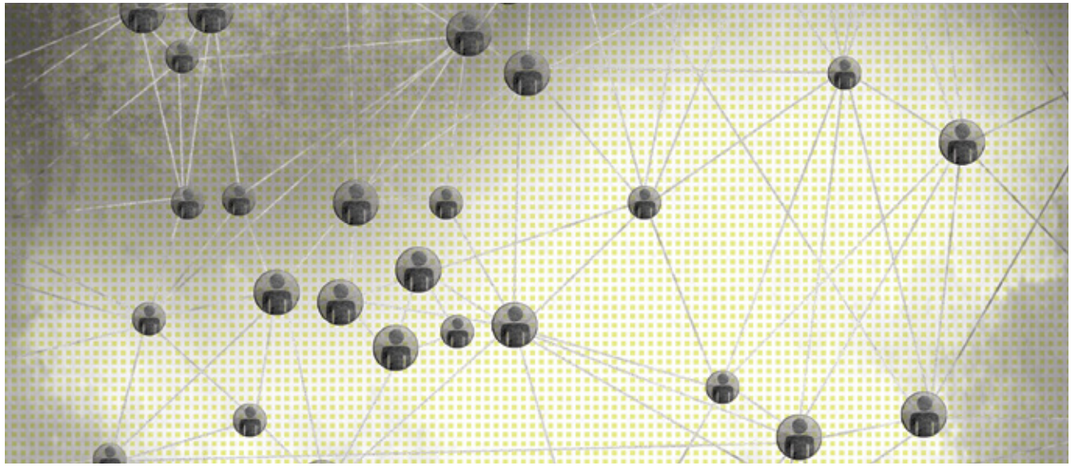
Le consentement éclairé comme pierre angulaire : les utilisateurs doivent être informés de ce qui advient de leurs données et doivent en principe donner leur accord pour tout traitement de leurs données, ou pouvoir s'y opposer. Tandis que le Parlement euro-

péen tient à la notion de « consentement explicite », telle que proposée par la Commission européenne, le Conseil des ministres préfère la formulation « consentement clair », beaucoup plus vague. Une telle formulation laisserait aux opérateurs chargés de traiter les données la possibilité de ne pas avoir à obtenir le consentement des utilisateurs, dans la mesure où ils pourraient déclarer que l'utilisation d'un service en ligne constitue déjà un « consentement clair » pour le traitement des données. Facebook a notamment agi de la sorte à plusieurs reprises, en interprétant la simple inscription sur son site comme une acceptation de ses conditions générales, modifiées depuis. Le Parlement européen entend de plus compléter les longues conditions générales d'utilisation et déclarations de confidentialité par des symboles facilement reconnaissables, afin de permettre aux utilisateurs de comprendre d'un seul coup d'œil les éléments principaux concernant le traitement de leurs données. Ces symboles devraient également être proposés sous une forme lisible par machine dans le cadre des services en ligne et être ainsi reconnus par les plugins des navigateurs, par exemple. De cette façon, chaque ordinateur pourrait, en se basant sur les réglages prédéfinis par l'utilisateur, décider automatiquement quelles pages web sont fiables et lesquelles ne le sont pas.

Des réglementations techniques peu nombreuses, mais fondamentales : le règlement comportera également plusieurs règles techniques, mais suffisamment générales pour pouvoir être applicables de façon globale. Elles incluront la possibilité d'une certification paneuropéenne pour les normes techniques conformes aux standards de la protection des données, comme la fonctionnalité « Do Not Track », ou la restriction de la création automatique de profils, c'est-à-dire de l'évaluation électronique d'un comportement par laquelle un ordinateur détermine les opportunités de participation sociale d'un individu. En outre les entreprises devront également être capable de remettre, sur demande, les données des utilisateurs rapidement et gratuitement dans un format numérique standard réutilisable ou les transférer directement vers d'autres plateformes. Au XXIe siècle, il n'est plus logique de fournir un ensemble de données dans un document papier ou dans un format PDF pratiquement inutilisable.

Concepts de « prise en compte du respect de la vie privée dès la conception » et du « respect de la vie privée par défaut » : les opérateurs traitant les données et les fabricants de systèmes informatiques doivent concevoir leurs systèmes de sorte à réduire au minimum la quantité de données traitées et les proposer avec des réglages prédéfinis pour respecter la confidentialité des données. Un principe strict de limitation de la finalité s'applique dans ce domaine. Cela signifie que seules les données réellement nécessaires pour fournir le service peuvent être collectées. Une application pour smartphone qui n'offre qu'une fonctionnalité de lampe de poche ne pourra donc plus transférer les informations de mon carnet d'adresses à la firme qui l'a vendue. À cette fin, le Parlement européen a explicitement prévu une disposition interdisant les couplages : celle-ci devrait empêcher des services de collecter des quantités excessives de données après avoir obtenu un simple et unique consentement de la part de l'utilisateur. De plus, il doit égalemenrt être possible d'utiliser des services de façon anonyme ou sous pseudonyme.

Le droit à l'oubli numérique : Toute personne souhaitant obtenir la suppression de ses données personnelles doit pouvoir faire valoir ce « droit à l'effacement



des données » établi de longue date à l'encontre des opérateurs qui traitent des données. Ceux-ci doivent aussi transmettre la demande de suppression aux tiers auxquels ils ont fourni les données concernées. Le Parlement européen a restreint ce « droit à l'oubli numérique », très controversé : seuls les opérateurs qui ont publié illégalement les données d'une personne doivent aussi s'assurer que toutes les copies de ces données sont supprimées. Tandis que le Parlement européen considère que le « droit à la non-indexation » invoqué dans le jugement rendu en mai 2014 par la Cour européenne de justice, dans l'affaire opposant Google à l'Espagne, est déjà inscrit dans la législation, les États membres s'interrogent encore quant à la nécessité d'ajouter des clauses particulières à ce sujet. Le législateur européen dispose cependant d'une marge de manœuvre réduite, car l'Union n'est pas habilitée à adopter des législations relatives à la liberté d'expression et d'information, les États membres étant les seuls compétents dans ce domaine. Le règlement demande donc aux États membres de trouver un juste équilibre entre, d'une part, la liberté d'expression et d'information et, d'autre part, la protection des données à caractère personnel. Il importe en particulier d'éviter qu'une société privée, comme Google, ne puisse définir cet équilibre des droits fondamentaux en dernière instance par l'intermédiaire d'un comité consultatif auto-désigné. Cette tâche doit continuer à incomber aux autorités chargées de la protection des données et aux tribunaux.

Autodétermination et règles de conduite sur internet : Un argument contre la protection des données souvent cité est que les jeunes souhaitent étaler toute leur vie sur Internet. Personne n'a l'intention d'interdire à quiconque d'agir de la sorte, mais ceux qui ne veulent pas tout révéler d'eux-mêmes doivent aussi avoir le droit et la possibilité de le faire. De la même façon, qui que ce soit qui souhaite livrer beaucoup d'informations à son sujet doit pouvoir s'attendre à ce que les services en ligne et les gestionnaires de données respectent des règles équitables.

3. Les nouvelles règles de protection des données génèrent-elles plus de bureaucratie ?

On entend régulièrement dire que le règlement sur la protection des données va entraîner une augmentation des formalités administratives pour les entreprises. En réalité, c'est le contraire. Le nouveau règlement européen signifierait que les 28 différentes lois des Etats membres seraient remplacées par une seule et unique réglementation paneuropéenne. Étant donné que la plupart des entreprises proposent déjà aujourd'hui leurs produits dans plus d'un seul pays de l'Union, une uniformisation de la réglementation entraînerait une réduction des formalités administratives pour tous. En outre, dans sa résolution sur la réforme de la protection des données, le Parlement européen a restreint les obstacles bureaucratiques imposés aux opérateurs chargés du traitement des données au strict minimum requis pour assurer le respect des droits des personnes concernées, et a introduit de nombreux dispositions de facilitation pour les petites et moyennes entreprises. Il est donc clair que le règlement sur la protection des données ne fera peser aucune charge administrative supplémentaire sur la majorité des entreprises. Par exemple, le Parlement européen n'impose de recruter obligatoirement un responsable de la protection des données que lorsqu'il est question de traiter de très grandes quantités de données ou des données sensibles. Dans ces cas, il n'est cependant pas nécessaire de créer un emploi spécialement consacré à cette fonction. Selon l'échelle du traitement des données réalisé dans l'entreprise, il est également possible de libérer juste quelques heures de travail pour confier cette tâche à des collaborateurs, ou bien de déléguer cette mission à des profesionnels de la protection des données externes. En Allemagne, contrairement à beaucoup d'autres Etats membres, ces pratiques sont déjà courantes. Le règlement soulagerait particulièrement les entreprises allemandes dans la concurrence qui les oppose à d'autres sociétés sur le marché européen.

Dans tous les cas, ce règlement offre aux entreprises des États membres de l'Union de grandes opportunités, qui dépassent de loin d'éventuels coûts d'adaptation. L'instauration d'une égalité de traitement absolue entre toutes les entreprises par un cadre juridique uniforme sur la protection des données éliminerait les désavantages de la concurrence internationale qui existent depuis des années. Cela signifie que les entreprises en Allemagne et dans d'autres États membres de l'Union européenne ne peuvent simplement pas tirer avantage du fait d'être bien établies et, comme c'est le cas habituellement, de taille moyenne pour passer à un autre pays européen pour y exploiter les avantages présumés d'une réglementation plus faible en matière de protection des données. À l'inverse, les grands groupes Internet de la Silicon Valley, comme Google, Facebook ou Amazon, jouissent, eux, d'un choix relativement libre du lieu où s'établir dans l'Union européenne. Ils ont un énorme pouvoir de levier dans le choix de leur lieu d'établissement, qu'ils peuvent utiliser pour accroître la pression sur les pays visés pour que ceux-ci adoptent une attitude plus laxiste en matière de contrôle de la protection des données ou d'imposition des sociétés. Pour ces sociétés, pour s'établir, une simple boîte aux lettres et un accès correct à Internet suffisent, et cela détermine finalement le standard de protection des données pour plus de 500 millions de citoyens de l'Union européenne. Cette situation équivaut à une subvention déguisée aux grandes entreprises américaines d'internet. L'adoption du règlement européen sur la protection des données serait l'étape la plus significative pour apporter un soutien adéquat à l'économie européenne du secteur informatique.

Le nouveau règlement soulagerait particulièrement les entreprises allemandes dans la concurrence qui les oppose à d'autres sociétés sur le marché européen.

4. Comment puis-je faire valoir mes droits dans l'UE?

Un interlocuteur unique pour toute l'Europe : Un guichet unique signifie que les citoyens de toute l'Union n'ont besoin de s'adresser qu'à une seule autorité chargée de la protection des données par pays. Les personnes concernées peuvent adresser leurs plaintes à l'autorité chargée de la protection des données de leur État membre, peu importe où l'usage abusif des données a été commis. De la même façon, les entreprises ne doivent plus coopérer qu'avec l'autorité chargée de la protection des données de l'État membre où se trouve leur siège principal.

Actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations qui s'engagent en faveur de la protection des données, des consommateurs ou d'autres causes d'utilité publique semblables auront à l'avenir, elles aussi, la possibilité d'introduire des recours.

Une application uniforme de la législation : Un comité européen de la protection des données, composé des autorités de surveillance nationales, doit veiller à l'application uniforme du droit sur la protection des données et peut également prendre des décisions contraignantes dans les cas à portée européenne, tout comme dans les domaines du droit de la concurrence et de la surveillance bancaire. Cela permettra d'éviter à l'avenir tout nivellement par le bas dans les États membres appliquant la législation moins strictement.

Le Parlement européen et le Conseil des ministres sont d'accord sur le principe de cette approche et ne souhaitent pas laisser le dernier mot à la Commission européenne, ce qui permet de préserver l'indépendance des autorités chargées de la protection des données. Un régime commun de la protection des données signifie également que les autorités chargées de la protection des données ont besoin de davantage de ressources et de personnel.

Des sanctions efficaces : Les violations des règles établies ne sont pas des infractions mineures, et les sanctions doivent être sévères. Jusqu'à présent, cet aspect faisait largement défaut aux autorités chargées de la protection des données en Europe. La Commission avait proposé de fixer des pénalités pouvant aller jusqu'à deux pour cent du chiffre d'affaires global annuel pour les cas graves, et les États membres semblent vouloir s'en tenir à ce montant. Le Parlement européen voudrait relever ce niveau maximal à cinq pour cent du chiffre d'affaires annuel, ou à 100 millions d'euros. De telles sanctions permettront de garantir que les entreprises n'envisageront pas à la légère d'enfreindre les règles sur la protection des données. Bien entendu, les pénalités doivent toujours être proportionnées. Les petites entreprises ne doivent donc pas craindre d'être acculées à la faillite pour des infractions mineures.

5. La protection des données nuit-elle à la presse, à la science et aux services d'archives ?

La protection des données est un droit fondamental et est consacrée en tant que telle dans la Charte des droits fondamentaux de l'Union européenne. Néanmoins, comme tous les droits fondamentaux, elle ne constitue pas un droit absolu ou supérieur aux autres. La liberté d'expression, la liberté de recherche, la liberté de la presse et d'autres droits fondamentaux doivent être pris au sérieux et protégés. Lorsque ces différents droits entrent en conflit les uns avec les autres, il incombe toujours au législateur - et, en dernière instance, à la justice - d'établir un équilibre juste et équitable.

En ce qui concerne la liberté de la presse, il est évident que les médias peuvent fournir des informations sur des personnalités publiques, même contre leur volonté. Certains Etats membres de l'Union ont déjà des lois faisant cette distinction. L'Allemagne, par exemple, distingue les personnalités « absolues » des personnalités « relatives ». Une personnalité absolue de l'histoire contemporaine, comme par exemple la chancelière, doit dans le doute accepter que des informations sur sa vie privée soient publiées et que ces informations soient organisées et stockées là où elles peuvent facilement être récupérées ; elle ne pourrait pas les faire supprimer en invoquant le droit à la protection des données. Par contre, quand il s'agit d'une personnalité relative de l'histoire contemporaine, seules des informations liées à l'événement couvert par la presse (comme une élection locale) peuvent être publiées. Tous ces aspects sont d'ores et déjà régis par la législation sur la presse et le droit général de la personnalité des différents États membres de l'Union et la réforme de la protection des données ne modifiera pas ces règles. Cela serait de toute façon impossible, car l'Union européenne ne possède aucune compétence législative dans ce domaine. C'est pour cette raison que le règlement sur la protection des données demande expressément aux États membres d'établir un équilibre approprié entre le droit à la protection des données et la liberté de la presse et la liberté d'expression.

En général, toute personne souhaitant utiliser des données personnelles à des fins de recherche doit préalablement en demander l'autorisation aux personnes concernées. Cette exigence ne s'applique pas que par le principe de la protection des données, mais aussi par les principes éthiques de presque toutes les associations scientifiques. La Commission avait prévu de larges exceptions, qui, en fin de compte auraient même autorisé la publication potentielle de données médicales, particulièrement sensibles, à des fins de recherche. Le Parlement européen a renforcé la protection en faveur des personnes concernées et supprimé ces dispositions aberrantes. Dans le même temps, il a clairement indiqué qu'en cas de recherches présentant un grand intérêt public, il sera possible de traiter des données personnelles, y compris des informations médicales, sans avoir préalablement obtenu l'accord des personnes concernées. Cette disposition permet de garantir que le contrôle des maladies ou les registres des cancers, par exemple, ne soient pas affectés à l'avenir. De plus le Parlement européen a introduit la possibilité de donner également son consentement pour le traitement de données pour le futur, comme pour des projets de recherche imprévus. Ici aussi, les États membres peuvent ajuster les détails dans leur législation nationale, puisqu'il peut notamment exister des interprétations sociales et historiques différentes de l'« intérêt public ».

Les archives historiques et scientifiques sont, elles aussi, partiellement exemptées des règles sur la protection des données. Il ne sera pas possible, même à l'avenir, d'invoquer le droit à la suppression des données à caractère personnel pour réécrire l'histoire ou falsifier des archives historiques. Là aussi, les États membres ont la possibilité de fixer eux-mêmes les détails de la réglementation. Les archives étaient déjà exemptées de ces règles vis-à-vis de la recherche historique dans le projet présenté par la Commission. Cependant, au vu des fréquents malentendus, le Parlement européen a ajouté au texte un article spécialement consacré aux archives pour clarifier la situation.

Il importe de garder à l'esprit que toutes ces règles ne s'appliquent qu'aux données à caractère personnel. La recherche et l'archivage portant sur des données anonymisées, qui ne peuvent plus être reliées aux personnes concernées, ne relèvent pas du droit sur la protection des données et ne sont soumis à aucune restriction.

6. Que se passe-t-il si les données sortent de l'UE?

Les citoyens de l'Union s'inquiètent de plus en plus de savoir où leurs données personnelles atterrissent, notamment depuis les révélations d'Edward Snowden. Le nouveau règlement européen sur la protection des données peut partiellement contribuer à restaurer le contrôle sur nos données. Il ne définit toutefois pas ce que les procureurs ou les services secrets sont autorisés à faire avec : les premiers font l'objet d'une directive européenne à part actuellement en négociation en parallèle, tandis que l'Union n'est pas habilitée à adopter des lois concernant les seconds. Le règlement sur la protection des données réglemente cependant la collecte de données par les entreprises, et moins de données sont obtenues, moins de données peuvent être interceptées par les services secrets. Le transfert de données personnelles vers des États en dehors de l'UE est également encadré.

Le Parlement européen tient à ce que les entreprises européennes ne puissent pas transmettre des données directement aux autorités des États extérieurs à l'Union Européenne. Ce type de transfert ne doit être autorisé qu'en concordance avec le droit européen et les éventuels accords d'entraide judiciaire fondés sur ce droit. Cette protection contre l'accès de pays étrangers aux données européennes figurait déjà dans le projet initial de la Commission, mais avait été retiré après de lourdes pressions exercées par le gouvernement américain. Le Parlement l'a une nouvelle fois intégré dans le règlement à la suite des révélations d'Edward Snowden. Bien que cette approche ne figure pas dans le texte proposé par les États membres, ils semblent y être favorables. Entretemps, le Congrès américain a déposé un projet de loi, le LEADS Act (« Law Enforcement Access to Data Stored Abroad »), qui respecterait les règles européennes.

En principe, les données personnelles ne peuvent être transférées vers des États en dehors de l'Union Européenne pour y être traitées de façon plus approfondie qu'uniquement si ces États appliquent un niveau de protection des données adéquat, par exemple avec une législation nationale sur la protection des données. Décider quels États satisfaisaient aux critères européens en matière de protection des données relevait jusqu'à présent de la Commission européenne. Le Parlement européen souhaite obtenir un droit de veto dans cette décision lourde de conséquences, comme c'est le cas dans le cadre de la plupart des autres accords conclus avec des États tiers.

Puisque les États-Unis ne disposent d'aucune législation complète en matière de protection des données et ne peuvent donc pas offrir de niveau de protection des données satisfaisant, en 2000, la Commission européenne et le ministère du commerce américain ont rusé. Les entreprises américaines peuvent certifier elles-mêmes qu'elles se conforment aux règles en matière de protection des données et se présenter comme des « zones sûres », et être autorisées à traiter des données européennes. À l'époque, le Parlement européen avait déjà jugé cette solution inappropriée et l'a donc constamment rejetée depuis lors. Outre le problème du respect des droits fondamentaux, ce dispositif de « zones sûres » offre de facto un avantage concurrentiel aux entreprises américaines, qui sont soumises à des obligations bien moins strictes que les entreprises établies dans l'Union européenne.

Le Parlement européen refuse également d'autoriser les sous-traitants chargés du traitement des données à envoyer celles-ci aux quatre coins du monde. Si c'était autorisé, ni les personnes concernées par les données, ni les services chargés de leur traitement n'auraient la moindre idée de l'endroit où ces données sont effectivement traitées.

L'Union européenne et les États-Unis sont en conflit dans les négociations des accords de libre-échange internationaux TTIP (Transtlantic Trade and Investment Partnership) et TISA (Trade in Services Agreement). Tandis que la Commission européenne a reçu un mandat de négociation clair excluant des discussions la protection européenne des données, les négociateurs américains veulent pour leur part prohiber toute restriction à la libre circulation des données (y compris des données à caractère personnel). Cela signifierait que toute tentative de l'Union Européenne pour se protéger par exemple de la surveillance massive des services secrets américains, la NSA, en mettant un terme au système des « zones sûres », serait alors un obstacle au commerce et donc interdite. Il doit être clair que la protection des données est un droit fondamental et non négociable.

Comment les lois européennes comme le règlement **SUR LA PROTECTION DES DONNÉES** sont-elles élaborées?

Bien des processus de discussions, rédactions et formulations ont lieu avant qu'une législation n'entre en vigueur dans l'Union européenne. De nombreuses parties prenantes sont impliquées dans ce processus.

Dans la procédure législative dite « ordinaire », qui est la principale procédure législative de l'Union européenne, la Commission européenne dispose d'un droit d'initiative exclusif : elle est donc la seule à pouvoir soumettre une proposition législative. Cette proposition découle d'un vaste processus de consultation. Cela signifie que les associations et les parties concernées sont invitées à exprimer leurs avis et positions sur les travaux préliminaires de la Commission. Dans le cas du règlement sur la protection des données, la Commission a recueilli des avis et positions pendant un an et demi, avant de présenter sa proposition législative en janvier 2012.

Une fois que la Commission a déposé une proposition, le texte est envoyé au Conseil des ministres et au Parlement européen. Le Parlement européen désigne alors une commission compétente ainsi qu'un « rapporteur » pour l'examiner. La commission discute des modifications à apporter au texte de la Commission.

Pour le règlement sur la protection des données, la commission compétente est la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE), et le rapporteur est l'eurodéputé vert Jan Philipp Albrecht. En sa qualité de rapporteur, Jan Philipp Albrecht a étudié en détail la proposition de la Commission et présenté son rapport, c'est-à-dire ses propositions de modification du texte législatif, en janvier 2013. Aux côtés de Jan Philipp Albrecht se tiennent les eurodéputés désignés par les autres groupes politiques pour suivre la procédure, les « rapporteurs fictifs ». Pendant la phase d'examen en commission, tout député européen peut déposer des amendements. La commission trouve ensuite un accord sur le rapport et quelques amendements. En octobre 2013, les membres de la commission LIBE se sont mis d'accord sur un texte de compromis élaboré sur la base de 4 000 amendements ! Les députés européens sont l'une des cibles privilégiées des actions de lobbying : l'ampleur des efforts déployés par les groupes de lobby et les associations pour influencer le règlement sur la protection des données se reflète dans le fait que les amendements déposés reprenaient bien souvent mot pour mot le contenu de positions formulées par des entreprises (voir www.lobbyplag.eu).

Après le vote en commission, le Parlement vote en plénière la proposition : ce vote suit généralement celui de la commission. C'est ainsi que les choses se sont passées pour le règlement sur la protection des données. En mars 2014, l'assemblée plénière a adopté presque à l'unanimité le texte négocié par Jan Philipp Albrecht en tant que position du Parlement européen. La position du Parlement a ensuite été transmise au Conseil des ministres. Ce dernier formule, lui aussi une position, au sujet du texte proposé par la Commission européenne.

Les travaux au sein du Conseil sont menés parallèlement à ceux du Parlement. Le règlement sur la protection des données donne du fil à retordre au Conseil des ministres. Depuis que le Parlement avait adopté un compromis, en mars 2014, le Conseil était au pied du mur et n'est parvenu que progressivement à commencer à trouver un accord. Comme pour le Parlement, il n'y a pas de limite de temps pour parvenir à un accord en première lecture.

La position du Conseil est élaborée par les représentations permanentes des États membres à Bruxelles et les experts de leurs capitales. Ces ambassades et les gouvernements des États membres sont, eux aussi, la cible des lobbies.

Lorsque le Parlement européen et le Conseil des ministres ont tous deux adopté leurs positions respectives, ils entrent dans des négociations tripartites avec la Commission européenne, le « trilogue ». Les trilogues doivent permettre de trouver un équilibre entre les intérêts des trois institutions. La plupart du temps, bon nombre de réunions, de compromis et de concessions sont nécessaires. La Commission européenne agit généralement comme intermédiaire entre le Parlement et le Conseil lors de ces négociations. Cependant, en dernier recours, elle peut cependant aussi retirer sa proposition ou soumettre une version amendée du texte législatif.

La procédure est terminée une fois qu'un accord a été dégagé sur le texte législatif définitif et que le Parlement et le Conseil l'ont tous deux officiellement approuvé. Après avoir été publié au Journal Officiel de l'Union Européenne, le règlement sur la protection des données entrera en vigueur et s'appliquera dans tous les États membres de l'UE après une période de transition de deux ans.

LE LOBBYING

et le règlement sur la protection des données

Les hommes et les femmes politiques doivent s'appuyer sur de l'expertise pour pouvoir prendre des décisions dans des domaines extrêmement larges. Or, la frontière qui sépare la simple mise à disposition de connaissances de la tentative d'influence est floue. La nouvelle réglementation européenne sur la protection des données est l'une des initiatives législatives les plus ambitieuses dans l'histoire de l'Union européenne. Cela se reflète dans l'importance du lobbying dont cette réforme a fait l'objet. Dans le mille-feuilles du système institutionnel européen, les groupes de pression et les associations ont de nombreuses possibilités d'avoir de l'influence : au cours du processus de consultation qui précède la publication d'une nouvelle proposition de la Commission, en contactant des eurodéputés occupant des positions clés ou en entretenant de bonnes relations avec les représentations permanentes, c'est-à-dire les ambassades des États membres auprès de l'Union européenne.

D'un côté, l'expertise et les connaissances spécialisées peuvent aider les députés dans leurs travaux parlementaires. Puisque les législations touchent souvent à des intérêts extrêmement divers, le lobbying peut également être considéré comme une sorte de réponse sur les intérêts des différents groupes sociaux. De l'autre côté, les politiques doivent aussi être en mesure d'examiner et d'évaluer les propositions des groupes de pression. Le fait de reprendre des formulations écrites par des parties extérieures sans même y réfléchir jette le doute sur l'indépendance des décisions politiques. Les informations transmises peuvent être volontairement fallacieuses, incomplètes ou sélectionnées. Les études fabriquées de toutes pièces ne sont pas rares, à l'instar de l'étude « The economic importance of getting data protection right » (« L'importance économique d'établir une protection des données correcte ») de la chambre de commerce américaine. Cette étude affirmait que le droit à l'oubli existant, renforcé par la réforme, coûterait 3 512 euros à chaque ménage. En outre, un déséquilibre clair apparaît dans l'exercice de l'influence : les intérêts économiques prédominent, car les groupes de pression qui représentent les intérêts sociaux et écologiques ont moins de moyens pour faire passer leurs points de vues.

Le règlement sur la protection des données est en bon exemple pour montrer à quel point une législation peut devenir le jouet des intérêts économiques. La plateforme participative www.lobbyplag.eu permet de mesurer l'influence exercée par les groupes de pression : le projet Open Data City, lancé à Berlin, montre quels amendements ont été proposés par des groupes de pression et soumis directement comme tels par différents députés européens. En tant que rapporteur, Jan Philipp Albrecht a rendu publiques ses rencontres avec des entreprises et des associations. La prédominance des groupes de pression par des demandes incessantes de rendez-vous, invitations et réunions montre très clairement l'ampleur des tentatives pour influencer le processus de prise de décision politique. Ces informations peuvent être vérifiées à cette adresse (uniquement en allemand) : https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyismus-zur-eu-datenschutzreform.html

Pour savoir exactement quels textes ont été soumis par chaque eurodéputé comme amendements au règlement sur la protection des données, le lien suivant fournit une liste des amendements déposés évalués du point de vue de la protection des données : http://lobbyplag.eu/map

Il est possible de vérifier quels passages formulés par des groupes de pression ont été repris tels quels par les eurodéputés à l'adresse suivante : http://lobbyplag.eu/influence

La brochure intitulée « Activist guide to the Brussels Maze » (« Un guide du labyrinthe bruxellois »), publiée par l'association EDRi (European Digital Rights), est une bonne base pour les activistes cherchant à gagner de l'influence (en anglais) : https://edri.org/files/activist_guide_to_the_EU_2012.pdf

La plateforme LobbyCloud veut remédier au manque d'information et de transparence qui caractérise le processus législatif. Elle permet de télécharger de façon anonyme des documents provenant de groupes de pression et de les rendre publics. Les parties intéressées peuvent l'utiliser pour voir qui a influencé qui : https://lobbycloud.eu

Comment protéger **ma vie privée** sur Internet ?

Les mots de passe efficaces sont des combinaisons aléatoires de lettres, de chiffres et de symboles, d'une longueur de douze caractères minimum, qui n'incluent ni le nom de la personne concernée, ni de son animal de compagnie ou de ses meilleurs amis. Les mots de passe ne doivent jamais être communiqués à d'autres personnes et doivent être régulièrement modifiés. Il est conseillé de ne pas utiliser un même mot de passe ou des mots de passe similaires pour différents comptes. Les gestionnaires de mots de passe, comme le logiciel libre et gratuit KeePass, enregistrent tous les mots de passe dans une base de données cryptée.

Messagerie électronique privée : Les fournisseurs européens comme posteo.de ou mailbox.org proposent des services de messagerie électronique sans publicité. Le contenu des courriels n'est pas analysé à des fins publicitaires.

Cryptage : Le programme Pretty Good Privacy (PGP) et sa version libre, GNU Privacy Guard (GnuPG), sont leaders en matière de cryptage de courriels. Le plugin Enigmail pour les programmes de messagerie électronique comme Thunderbird facilite le chiffrement et le déchiffrement, ainsi que la gestion des clés.

Messagerie instantanée : Pour les messageries instantanées libres, il est recommandé d'utiliser des services décentralisés comme Jabber (XMPP), qui fonctionnent aussi bien sur ordinateur que sur smartphone, idéalement chiffrés à l'aide du protocole OTR. Il existe une application Jabber pour Android, Chatsecure. Les SMS peuvent par exemple être chiffrés au moyen de Textsecure. Les programmes Surespot ou Threema (payant) sont d'autres solutions possibles.

Masquer l'adresse IP : Le logiciel libre TOR (The Onion Router) permet de masquer les adresses IP, afin d'empêcher les services en ligne de déterminer l'identité ou la localisation de l'utilisateur. Attention : Tor dissimule seulement l'origine, et non le contenu des données. Un protocole crypté en HTTPS est souhaitable lorsqu'on introduit des données de connexion par exemple.

Utiliser HTTPS : HTTPS est la variante chiffrée du protocole Internet HTTP. L'extension HTTPS-Everywhere pour Firefox et Chrome permet aux utilisateurs de naviguer sur les sites avec une connexion HTTPS chaque fois que c'est possible.

Navigation anonyme avancée : Tails (« The Amnesic Incognito Live System ») est un système d'exploitation libre qui permet de naviguer sur Internet de la façon la plus anonyme possible. Tails peut être lancé à partir d'une clé USB, d'un DVD ou d'une carte SD sur n'importe quel ordinateur, indépendamment du système d'exploitation utilisé. Les données ne sont pas enregistrées sur le disque dur de l'ordinateur, mais seulement dans la mémoire vive, qui est effacée de l'appareil une fois éteint. Le guide de l'utilisateur et la dernière version sont disponibles en téléchargement sur tails.boum.org.

Hébergement de fichiers : Dropbox est un service de cloud populaire. Cependant, ce service a des pratiques discutables en matière de protection des données : les données non cryptées sont facilement transmises aux autorités américaines. D'autres solutions existent, comme le système Teamdrive, conçu à Hambourg, ou les services Pulse, Wuala et SpiderOak. Les plus ambitieux peuvent même créer leur propre service d'hébergement en ligne avec le projet libre OwnCloud.

Moteurs de recherche : Google n'est pas le seul service disponible. Il existe de nombreux autres moteurs de recherche qui respectent davantage la confidentialité des données personnelles : ixquick, DuckDuckGo, yandex.com ou YaCy par exemple.

Conditions d'utilisation : La plateforme bénévole Terms of Service ; Didn't Read analyse les clauses en petits caractères. Les conditions générales de vente sont ensuite décomposées en indications facilement compréhensibles. Des symboles colorés permettent d'identifier immédiatement les inconvénients de chaque service. Il existe également un module Firefox pour cette fonctionnalité. La campagne de sensibilisation biggestlie.com explique pourquoi des conditions d'utilisation concises et compréhensibles sont si importantes.

Cookies de navigateur : Les cookies sont pratiques, mais révèlent également beaucoup d'informations sur nos habitudes de navigation. Il est difficile de renoncer complètement aux cookies, car bon nombre d'offres ne peuvent être utilisées que si l'utilisateur active les cookies. Avec l'extension de navigateur Self-Destructing Cookies (sur Firefox), les cookies soient automatiquement supprimés lorsque l'utilisateur quitte une page web.

Pour plus d'information :
https://securityinabox.org
https://myshadow.org
https://digitalcourage.de/adventskalender

Jan Philipp Albrecht, MdEP
Platz der Republik 1
UDL 50 – 2113
11011 Berlin
Allemagne

jan.albrecht@europarl.europa.eu
www.janalbrecht.eu
twitter.com/janalbrecht
youtube.com/ JPAforMEP

Cette brochure peut être commandée à info@gef.eu.

Les Verts | ALE
au Parlement européen

GEF
GREEN EUROPEAN FOUNDATION