A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Nouveaux règlements Data & règlement IA Européens

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Maître André MEILLASSOUX est avocat et vice-président de l'association française du droit de l'informatique et de la télécommunication (AFDIT). Il présentera un exposé sur les règlements européens qui concernent les données personnelles. Pierre DELORT, président de l'ANDSI, s'attachera à sa suite à rendre compte des enjeux, pour les entreprises et leurs DSI, de l'AI Act.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Pierre DELORT introduit la conférence en pointant l'intérêt sur les data de l'UE, en premier pour protéger notre intimité (RGPD) puis ensuite pour stimuler l'économie (Data Governance Act et surtout Data Act).

Les règlements européens à la suite du RGPD

André MEILLASSOUX indique qu'en matière de protection des données personnelles, l'UE favorise désormais l'adoption de règlements plutôt que de directives. En effet, ils ont pour avantage d'être d'application immédiate dans les vingt-sept États membres. En outre, ils permettent de contrôler efficacement les grandes entreprises américaines du secteur.

E-privacy

Le règlement e-privacy porte sur la protection de la vie privée et des échanges d'informations dans les communications électroniques, à l'exemple des courriels ou des messageries WhatsApp ou Messenger. Il propose des règles concernant le stockage des données. Bien qu'approuvé, le texte est complexe à appliquer, et son entrée en vigueur a donc été mise en attente.

Loi sur les services numériques (DSA)

Les sanctions prévues par le DSA, supérieures à celles prévues par le RGPD, peuvent atteindre 6 % du chiffre d'affaires mondial. En imposant des règles aux grandes plateformes, le DSA vise à ce que les comportements illégaux ne restent plus impunis sur internet. Les règlements tels que le DSA, le DMA, le data Act et l'AI Act répondent à un principe téléologique, c'est-à-dire qu'ils fixent les objectifs et non les moyens pour les atteindre. Il peut ainsi s'agir de tracer les vendeurs de produits et de services, de réaliser des audits internes, de protéger les mineurs et d'établir un rapport annuel sur les risques systémiques. Afin d'en garantir l'application, une autorité indépendante doit être mise en place dans chaque État membre dans le cadre d'une coopération européenne.

Int : Si une entreprise conteste la sanction, l'autorité indépendante a-t-elle le pouvoir d'imposer le paiement ?
AM : Oui, elle le peut.

Int : Cette réglementation ne risque-t-elle pas de compromettre le développement des futurs champions européens ?
AM : Le RGPD constitue une garantie démocratique essentielle. En la matière, l'UE a joué un rôle précurseur qui a inspiré les législations du monde entier.

Règlement sur les marchés numériques (DMA)

Le DMA entend lutter contre les pratiques anticoncurrentielles des acteurs dits « contrôleurs d'accès » qui imposent aux autres entreprises de faire appel à eux pour obtenir l'accès à certains services. Des règles et des sanctions fortes sont nécessaires pour éviter les positions dominantes sur le marché, par exemple, celle de Google qui bénéficie d'un quasi-monopole en Europe. L'objectif est de favoriser une concurrence loyale qui protège les petites et moyennes entreprises. Les amendes prévues pour les contrevenants peuvent atteindre 10 % du chiffre d'affaires mondial, et 20 % en cas de récidive. En outre, le démantèlement de certaines activités peut être imposé.

Règlement sur la gouvernance des données

Le data gouvernance Act, entré en vigueur en septembre 2023, organise le partage de la valeur issue de la captation des données. La mise en disponibilité de ces dernières permet de nourrir les systèmes d'intelligence artificielle (IA) et d'en ouvrir l'accès aux services publics.

L'*open data* promue par la France permet de favoriser la croissance des start-ups. Les entreprises du numérique européennes souffrent en effet d'un retard technologique, et leur croissance est freinée par la place prépondérante des grands acteurs historiques. Ce règlement entrera en vigueur en 2025. Ses défenseurs mettent en avant la fixation d'un cadre relativement souple doté d'un contrôle *ex ante*, c'est-à-dire préalable.

La jurisprudence du Conseil d'État a statué que les données étaient dépourvues de statut juridique, afin que les citoyens ne puissent pas en disposer comme des biens. En conséquence, une donnée technique n'est pas protégeable en soi. En revanche, les bases de données peuvent être protégées.

Pour conclure, un effort considérable a été consenti en matière de réglementation des données comme en atteste le succès du RGPD. La Commission européenne a su faire preuve d'inventivité et nouer le dialogue avec les GAFAM. Aujourd'hui, les données personnelles des citoyens sont efficacement protégées, les contenus illicites ont été interdits, et un cadre a été donné aux données industrielles pour garantir un traitement équitable entre les entreprises et favoriser une concurrence loyale.

AI Act

Pierre DELORT indique que l'AI Act a fait l'objet d'une proposition en avril 2021 d'un accord provisoire entre le Parlement européen et le Conseil de l'UE le 9/12/2023, qui ont ensuite trouvé un *accord provisoire* sur ce texte le 2/02/2024 dans l'attente d'une adoption formelle par le Parlement en 2024, en session plénière. La définition prise de l'Intelligence Artificielle n'est pas celle, peu satisfaisante, de la France (JO 2018 imitation des mécanismes de la cognition et de la réflexion…) mais est basée sur les technologies ;

- IA inductive ; apprentissage automatique (supervisé, non supervisé, renforcement…) ;
- IA déductive ou symbolique ; moteurs d'inférence et de déduction, systèmes experts….
- Approches statistiques ; estimations baysiennes…

Les objectifs de l'AI Act sont ;

1. veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur relative aux droits fondamentaux et aux valeurs de l'Union ;
2. garantir la sécurité juridique pour faciliter l'investissement et l'innovation dans l'IA ;
3. améliorer la gouvernance et l'application efficace de la législation existante sur les droits fondamentaux et les exigences de sécurité applicables aux systèmes d'IA ;
4. faciliter le développement d'un marché unique pour les applications d'IA licites, sûres et dignes de confiance et prévenir la fragmentation du marché.

Son approche se fonde sur la prévention des risques et la fixation d'objectifs. La réglementation est fonction des risques d'application de l'IA, sériés en :

- inacceptables : ils contreviennent aux valeurs de l'UE en violant les droits fondamentaux des citoyens (dont la notation sociale et l'identification biométrique en temps réel…) ; l'utilisation de L'IA y est interdite.
- élevés : 8 catégories sont distinguées (gestion des infrastructures critiques, gestion des migrations, accès à l'emploi ou l'éducation…) ils requièrent la réalisation d'un dossier technique (démonstration de conformité, plan post-Market de surveillance…), avec enregistrement du Système d'Intelligence Artificielle – SIA- dans une BdD EU, accessible par le public, logs automatiques conservés 6 mois….
- risques faibles ou minimaux ; amélioration d'une activité humaine déjà réalisée, effectuer une tâche procédurale limitée… ; pas de contrainte règlementaire exprimée.

Un bac à sable réglementaire pourra être mis en œuvre afin de permettre aux fournisseurs de SIA de proposer des innovations et les citoyens de l'UE pourront ;

- déposer des plaintes concernant les SIAs ;
- recevoir des explications sur les décisions basées sur des SIAs et ayant une incidence sur leurs droits.

Si nécessaire pour la détection des biais, l'utilisation de données personnelles est possible, sous réserve de garanties incluant les limites techniques de pseudonymisation (réidentification…).

Les pénalités pour les risques inacceptables ont été portées à 35 millions d'euros ou 7% du CA Annuel, ainsi que pour les SIA à haut risque si les données d'entrainement ne respectent pas des règles (pertinence, annotation, nettoyage, agrégation, complétude, absence de biais…) et pour IA autres qu'inductive si Data Management & Gouvernance ne sont pas appropriés
Pour les autre infractions 15m€-7% du CA Mondial en amendes, fortement réduites pour les administrations.
La fourniture d'informations fausses ou incomplètes aux autorités de contrôle est punissable de 7m€ ou 1% du CA Mondial.

Pour les DSI, il apparait, à la lecture du règlement, important de bien détourer la notion d'« utilisateur » et de « déployeur » (personne physique ou morale utilisant un SIA sous son autorité sauf si utilisation pour activité personnelle non professionnelle - Art. 3) et s'assurer que l'utilisation du SIA ne se situe pas dans la zone dangereuse (cf. points inacceptable & hauts risques).
Si elle se situe en zone à hauts risques préparer le dossier technique ; description technique, process de développement (spécifications, data avec origine & sélection, entrainement, test & validation), logs, monitoring, gestion des risques… ainsi que la déclaration.
Si un LLM modifié (par fine tuning, RAG…) est utilisé, évaluer si la règle applicable aux General-purpose AI à risque systémique (Annexe IX) s'applique, dont la fourniture d'informations spécifiques (architecture, nombre de paramètres, nombre de flops utilisés à l'entrainement….)

Débat

Int : En matière de transparence des algorithmes, les administrations seront-elles concernées ? Je prends pour exemples les admissions postbac et la détection des fraudes fiscales.
AM : Le DMA porte sur le droit de la concurrence et concerne donc plutôt les acteurs économiques. L'accessibilité des algorithmes doit permettre une concurrence saine.
Int : Leur divulgation ne risque-t-elle pas de décourager l'innovation ?
AM : Le DMA ne concerne que les grandes plateformes. En pratique, l'accès aux algorithmes n'est pas ouvert à tous. À l'exemple des procédures du droit de la concurrence, il ne devrait être permis qu'à ceux qui peuvent se prévaloir d'un intérêt légitime après avoir saisi l'autorité administrative indépendante. En la matière, si les décisions peuvent être publiées, le détail des procédures demeure confidentiel.

AM : Le président Obama s'était opposé aux règlements européens. Le président Trump, quant à lui, avait menacé de supprimer les services gratuits aux acteurs européens. Or en unissant leurs forces, les vingt-sept États membres sont parvenus à adopter des textes qui sont devenus des standards mondiaux en matière de système de protection des données. L'« effet Bruxelles » a ainsi rendu obsolètes les législations antérieures.
Int : Le but est-il vraiment atteint ou, au contraire, l'émergence au sein de l'Union européenne d'acteurs majeurs du secteur n'est-elle pas ralentie là où les GAFAM mettent au point des stratégies de contournement ?
AM : Le consensus autour du RGPD a été obtenu grâce à un eurodéputé du parti pirate qui a démontré que la surveillance généralisée rendait impossible l'existence d'une démocratie. Eu égard à l'enjeu politique de la protection des données, les inconvénients demeurent acceptables.
Int : Le RGPD est contourné, car les plateformes imposent la collecte de données pour des services essentiels pour les utilisateurs.
AM : La règle dispose qu'il doit être aussi facile de l'accepter que de la refuser.

Int : La présence d'un délégué à la protection des données au sein des entreprises et des administrations pose le principe salutaire selon lequel les informaticiens ne sont pas propriétaires de celles-ci.
Int : Cette réglementation répond à un principe démocratique, mais la protection des données de l'individu se heurte aux limites de l'intérêt collectif, si bien que nous pouvons nous demander si nous ne sommes pas trop protégés.
AM : Le RGPD intègre des exceptions en matière de recherche scientifique, de prévention des risques ou des épidémies. Cependant, les moyens doivent être proportionnés aux objectifs. Le principe de minimisation de la collecte de données est sain pour la collectivité publique.

Int : Dans l'industrie automobile, nous récupérons les données mises à disposition par le constructeur de la machine. Les contrats ne mentionnent pas un quelconque droit de propriété, mais le service d'accès aux données est payant.
AM : Si la donnée n'est pas protégeable, la base de données est protégée afin de rétribuer l'investissement que constitue sa réalisation.
PDT : Le monde agricole est un peu précurseur dans la promotion de contrats d'échange de données, par exemple la production par parcelle d'une ferme entre fermier, propriétaire terrien, fabricant de machines, d'engrais..., acheteur des produits agricoles… Le but du Data Act est de favoriser l'utilisation des données par les acteurs de l'*espace*, et ce faisant de stimuler l'économie.

Présentation des orateurs

André Meillassoux est avocat à ATM Avocats, Vice Président de l'Association Française du Droit de l'Informatique et de la Télécommunication (AFDIT) après en avoir été Président durant des années. Il enseigne le droit dans différents établissements d'enseignement supérieur (CentraleSupelec….).

Pierre Delort est DSI et Président de l'Andsi. Après la direction d'un projet de Workflow-BPM dans l'assurance, sujet de son PhD aux Mines, il a dirigé plusieurs DSI, créé le cours de Data au corps des Mines puis est devenu Professeur Invité à Telecom Paris. Il a publié « Le Big Data » dans la collection *Que Sais-je* ?, plusieurs éditions.