Club de la sécurité de l'information français

CLUSIF

Numérique et droit : les dernières évolutions législatives

Myriam QUEMENER, Magistrat, docteur en droit

Plan d'intervention

- Un rappel sur le RGPD
- L'adaptation du droit actuel : l'exemple de la loi pour la République numérique
- Directive NIS : des OIV aux les organismes d'importance essentielle; quelles évolutions
- Les perspectives d'évolution : « paquet cyber», objets connectés, I.A.

Loi pour la République numérique : les dispositions phares

- **En matière d'open data :** Mention explicite de l'utilisation d'un traitement algorithmique dans le cadre d'une décision administrative et possibilité pour l'usager d'en demander les principales règles. (Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique)

- **Loyauté des plateformes** (transparence de l'information pour les consommateurs et régulation des avis en ligne) : les trois projets de décret ont fait l'objet d'une longue concertation avec les acteurs concernés et d'une notification à la Commission européenne qui est en voie d'achèvement.

Loi pour la République numérique

- **La multiplication par 20 du plafond des sanctions que peut prononcer la Commission nationale informatique et libertés**, qui passe de 150 000 euros à 3 millions d'euros

- **La protection des citoyens détecteurs de faille informatique**, ou « hackers blancs », afin de les inciter à révéler ces failles à l'Agence nationale pour la sécurité des systèmes d'information, sans encourir de risque pénal pour cette action (art. L.232164 du Code de la défense)

Quelques rappels sur le RGPD

- *Le RGPD s'appliquera dès lors qu'un responsable du traitement ou un sous-traitant est établi sur le territoire de l'UE ou qu'un résident européen est directement visé par un traitement de données.*
- Désignation d'un délégué à la protection des données
- Violation de données personnelles (obligation de notification à la CNIL)
- Réalisation d'analyses d'impact relatives à la protection des données
- Droit à l'oubli consacré
- Droit à la portabilité des données personnelles
- Transferts de données hors Union européenne
- Amendes administratives et sanctions (*La violation des dispositions du RGPD fait l'objet d'amendes*
  administratives pouvant s'élever jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent)

Objets connectés et fondements juridiques de la responsabilité

- Droit de la consommation

- Droit des contrats

- Le règlement européen développe deux autres principes :
  - Le **« Privacy by design »** : la question de la protection et de la confidentialité des données doit être abordée dès la conception de l'objet. Une réflexion doit être menée en amont sur la nécessité des données et leur durée de conservation.
  - Le **« Privacy by default »** : par défaut, le service proposé doit demander le minimum d'informations nécessaires, pour offrir le niveau de sécurité le plus protecteur pour le consommateur.

Directive NIS / Les acteurs visés

1) Les fournisseurs de service numérique

- Les moteurs de recherche en ligne ;
- Les places de marchés en ligne ;
- Les services de cloud

2) Les OSE

- Santé : concerne tout établissement de soins de santé, y compris les hôpitaux et cliniques privées ;
- Fourniture et distribution d'eau potable ;
- Energie : concerne les sous-secteurs de l'électricité, du pétrole et du gaz ;
- Transports : concerne les sous-secteurs des transports aérien, ferroviaire, routier, et par voie d'eau ;
- Banques : la directive désigne ainsi les établissements de crédit, entendu comme « une entreprise dont l'activité consiste à recevoir du public des dépôts ou d'autres fonds remboursables et à octroyer des crédits pour son propre compte »;
- Infrastructures de marchés financiers : concerne tout autant les exploitants de plate-forme de négociation que les contreparties centrales ;
- Infrastructures numériques : il s'agit des IXP (Internet eXchange Point ou « points d'échange internet»), définis comme « une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange

Directive NIS

Structurée autour de quatre axes, la directive prévoit

- Le renforcement des capacités nationales de cybersécurité. Les Etat membres devront notamment se doter d'autorités nationales compétentes en matière de cybersécurité, d'équipes nationales de réponse aux incidents informatiques (CSIRT) et de stratégies nationales de cybersécurité.
  - Respectivement en France, l'ANSSI, le CERT-FR et la stratégie nationale pour la sécurité du numérique ;

- l'établissement d'un cadre de coopération volontaire entre Etats membres de l'UE via la création de
  - un « groupe de coopération » des Etats membres sur les aspects politiques de la cybersécurité ;
  - un « réseau européen des CSIRT » des Etats membres. Ce dernier visera notamment à faciliter le partage d'informations techniques sur les risques, vulnérabilités

- le renforcement par chaque Etat de la cybersécurité d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société par
  - la définition au niveau national de règles de cybersécurité auxquels ces derniers devront se conformer ;
  - l'obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels.

- l'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne.

Paquet cyber

Transformation de l'ENISA en agence européenne de cybersécurité

Cette nouvelle agence disposerait d'un mandat permanent permettant d'aider les Etats membres à gérer les cyberattaques. Elle superviserait en outre la mise en œuvre de la directive sur la sécurité des réseaux et des systèmes d'information, entrée en vigueur en août 2016, et obligeant les entreprises ainsi que les organisations à signaler les incidents informatiques dont elles sont victimes.

Création d'un label européen pour les entreprises

Cet "étiquetage" des dispositifs informatiques permettrait de garantir aux consommateurs la fiabilité des systèmes qui pilotent de nombreuses infrastructures clés (réseaux d'énergies, voitures connectées, etc.), et ce dans tous les Etats membres.

Investissements dans l'innovation technologique

Lutte renforcée contre la fraude aux moyens de paiement...

Paquet cyber

Nouvelle directive contre la fraude et la contrefaçon des moyens de paiement autres que les espèces

- Il s'agit d'une source de revenus importante pour la criminalité organisée :
- 1,44 milliard d'euros par an selon la Banque centrale européenne, juste pour la fraude aux cartes de paiement. Europol estime que cette manne financière sert en partie à financer d'autres activités criminelles comme le terrorisme, le trafic de drogues et la traite d'être humains.
- La nouvelle directive vise donc à adapter la législation à l'utilisation croissante des paiements mobile, des monnaies virtuelles et autres nouveaux instruments de paiement issus des évolutions technologiques. Notamment sur la question de la territorialité - un cybercriminel agissant depuis un pays A pour escroquer dans un pays B -, qui permet à de nombreux escrocs de passer entre les mailles du filet.

Un droit des robots

Dans une proposition de résolution contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103 INL), le Parlement européen s'est prononcé en faveur de la reconnaissance d'une personnalité juridique spéciale pour les robots, pour

« qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques dotées de droits et de devoirs bien précis y compris celui de réparer tout dommage causé à un tiers »

Avis du CESE

- Dans un avis publié le 31 mai 2017, le Conseil économique social et européen
- (CESE) a annoncé être défavorable à la création d'une personnalité juridique pour les robots dotés d'intelligence artificielle.
- En revanche, dans un avis publié le 31 mai 2017, le Conseil économique social et européen (CESE) s'y est opposé, préférant plutôt une approche « **human in command** », de l'intelligence artificielle, dans laquelle « *les machines restent des machines que les hommes ne cessent jamais de contrôler* » comme l'a déclaré la rapporteur Catelijne Muller, ce pour des raisons compréhensibles de développement responsable, sûr et utile de l'intelligence artificielle.

Une reconnaissance européenne des enjeux de la robotique : une réflexion non aboutie

- Dans une proposition de résolution contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103 (INL), le Parlement européen s'est prononcé en faveur de la reconnaissance d'une personnalité juridique spéciale pour les robots, pour « *qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques dotées de droits et de devoirs bien précis y compris celui de réparer tout dommage causé à un tiers* ».

Merci de votre attention

Pour aller plus loin :

Quéméner M. « La directive NIS, un texte majeur en matière de cybersécurité », *Sécurité et stratégie*, 2016/3 (23), p. 50-56.