L'action de l'Union européenne en matière de sécurité internationale et européenne – Ecole d'automne
(Université Laval, Québec, 31 octobre 2018)

Le cadre juridique européen de la cybersécurité

Bertrand Warusfel,
Professeur à l'Université Paris 8
bertrand.warusfel@univ-paris8.fr

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Pourquoi l'Union européenne construit un cadre juridique de cybersécurité ?

- L'UE soutient et encourage le développement d'une société européenne de l'information (économie de la connaissance, services de la société de l'information, …)

- La sécurité et la défense sont devenus des enjeux majeurs de la politique européenne (lutte contre le terrorisme, coopération policière, espace de liberté, sécurité et justice, politique commune de sécurité et de défense, …)

- Des pratiques non harmonisées de sécurité numérique pourraient constituer un obstacle à la libre circulation des données

- La sécurité des données est un des principes essentiels du nouveau règlement général RGPD (art. 32-34)

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Principaux textes de l'Union européenne sur la cybersécurité

- Règlement n°526/2013 du 21 mai 2013 définissant le statut de l'agence européenne pour la sécurité des réseaux et des systèmes d'information (ENISA)
- Directive n°2013/40 du 12 Août 2013 sur les attaques aux systèmes d'information
- Règlement n°910/2014 sur l'identification électronique et les services de confiance (eIDAS)
- Directive n° 2016/1148 du 6 Juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (NIS directive)

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Directive n° 2013/40 du 12 Août 2013 relative aux attaques contre les systèmes d'information

- « La présente directive fixe des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information. Elle vise également à faciliter la prévention de ces infractions et à améliorer la coopération entre les autorités judiciaires et les autres autorités compétentes » (art. 1er)
- accès illégal (art. 3)
- atteinte à l'intégrité d'un système (art. 4)
- atteinte à l'intégrité des données (art. 5)
- interception illégale (art. 6)
- instruments utilisés pour commettre les infractions numériques (art. 7)
- (infractions précédemment définies par la Convention Cybercriminalité du Conseil de l'Europe, novembre 2011)

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

eIDAS : une coopération public/privé pour la sécurité numérique

En vue d'assurer le bon fonctionnement du marché intérieur tout en visant à atteindre un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance, le présent règlement :

a) fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;

b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques; et

c) instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envoi recommandé électronique et les services de certificats pour l'authentification de site internet.
(art. 1er)

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Du côté de l'initiative privée

- Signature électronique (art. 25)
- Sceaux électroniques (art. 35)
- certificat pour l'authentification des sites webs (art. 45)
- service d'envoi recommandé électronique (art. 43)
- services de conservation (signature ou sceaux) (art. 34 et 40)

basés sur l'usage

- de certificat électroniques qualifiés délivrés
- par des fournisseurs de services de confiance
- qualifiés et contrôlés par les autorités nationales de sécurité

Du côté du secteur public :

- Reconnaissance mutuelle des moyens d'identification électronique utilisés par les services publics en ligne

- Utilisation de services de confiance par les organismes publics (notamment signature électronique …)

- + contrôle et supervision des fournisseurs de services de confiance par chaque autorité nationale de sécurité

Directive n° 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (NSI directive)

« les États membres peuvent adopter ou maintenir des dispositions en vue de parvenir à un niveau de sécurité plus élevé des réseaux et des systèmes d'information » (art. 3)

Désignation d'une autorité nationale compétente dans chaque Etat-membre,
+ création d'un centre d'alerte et de réponse aux incidents de sécurité numérique

« Les critères d'identification des opérateurs de services essentiels visés à l'article 4, point 4), sont les suivants:

- une entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques;
- la fourniture de ce service est tributaire des réseaux et des systèmes d'information;
- et un incident aurait un effet disruptif important sur la fourniture dudit service » (art. 5.2).

Les États membres

- « veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances » (art. 14)
- « Les États membres veillent à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III, et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer » et
- « veillent à ce que les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services visés à l'annexe III qui sont offerts dans l'Union, de manière à garantir la continuité de ces services » (art. 16)

Nouvelles étapes prévues (Conseil UE 18 octobre 2018)

Le Conseil européen a préconisé des mesures pour mettre en place une cyber-sécurité solide au sein de l'Union européenne :

- la mise en place d'une **agence de l'UE pour la cybersécurité dotée de compétences plus étendues**
- l'instauration d'un **système de certification de cybersécurité à l'échelle de l'UE** (projet de nouvel « Acte sur la cybersécurité »)
- la mise en œuvre rapide de la directive NSI

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS