Club de la sécurité de l'information français

LPM, Directive NIS et RGPD : quelles influences de l'un à l'autre ?

Par Maître Olivier ITEANU,
Avocat

De quoi parle-t-on ?

- Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale dite *LPM*
  - Institue un cadre légal en matière de cybersécurité des OIV (Opérateurs d'Importance Vitale)
- Directive (UE) 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 dite *Directive NIS (Network and Information System)*
  - Institue un cadre commun aux États membres en matière de cybersécurité des OSE (Opérateurs de Services Essentiels)
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit *RGPD (Règlement Général sur la Protection des Données)*
  - Institue un cadre commun aux États membres en matière de protection des données personnelles

Des dispositifs nécessaires

Exemple de la cyberattaque « Wannacry » des 12 et 13 mai 2017

- 300 000 systèmes d'information affectés en quelques jours
- En Europe, plusieurs services « essentiels » affectés :
  - Un opérateur téléphonique espagnol
  - Des hôpitaux britanniques
  - Des compagnies de transport allemandes

La Directive NIS, héritière de la LPM

Des concepts voisins

Directive NIS	LPM
« Opérateurs de services essentiels » (articles 4 et 5) : *« entité publique ou privée dont le type figure à l'annexe II et qui répond aux critères »* 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 »* - *« un incident aurait un effet disruptif important sur la fourniture dudit service »*	**Opérateurs *« d'importance vitale »*** (article 22 LPM) : *« opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et […] opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation »*

La Directive NIS, héritière de la LPM

Des obligations similaires

	Directive NIS	LPM
Obligation de sécurisation	Les OSE doivent **prendre des mesures pour *« gérer les risques qui menacent la sécurité*** *des réseaux et systèmes d'information qu'ils utilisent »* (article 14)	Possibilité d'imposer aux OIV (article 22): • qu'ils *« mettent en œuvre des **systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité** de leurs systèmes d'information »* • qu'ils *« soumettent leurs systèmes d'information à des **contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité** »*
Obligation de notification	Les OSE doivent **notifier** *« à l'autorité compétente ou au CSIRT, sans retard injustifié, les **incidents** qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent »* (article 14)	Les OIV *« **informent** sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité »* des SIIV (article 22)

Focus sur l'obligation de notification

	• Directive NIS (articles 14 et 16) • LPM (article 22)	RGPD (Article 33)
Objet de la notification	• *« les incidents »* qui ont *« un impact significatif »* sur la *« fourniture »* ou la *« continuité »* d'un service • Les *« incidents affectant le fonctionnement ou la sécurité »* d'un service	Une *« violation de données à caractère personnel »*
Personnes devant notifier	• Les OSE et les FSN • Les OIV	• Les responsables de traitement • Les sous-traitants
Autorité à qui l'on doit notifier	• L'autorité compétente ou le CSIRT (donc l'ANSSI) • Le Premier ministre	• L'autorité de contrôle compétente (la CNIL) quand la violation est constatée par le responsable de traitement • Le responsable de traitement quand la violation est constatée par le sous-traitant
Délai de la notification	• *« sans retard injustifié »* • *« sans délai »*	• *« 72 heures au plus tard après en avoir pris connaissance »* pour le responsable de traitement • *« dans les meilleurs délais après en avoir pris connaissance »* pour le sous-traitant
Sanction en cas de non respect de l'obligation notification	• Des sanctions *« effectives, proportionnées et dissuasives »* (article 21 de la Directive NIS) • 150 000 € d'amende pénale	Amende administrative pouvant s'élever jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel de l'entreprise (article 83)

Conclusion

- Le taux d'élucidation des cyberattaques par les autorités policières et judiciaires est très faible (Wannacry : Où est l'auteur du malware ? Où sont les premiers diffuseurs ?)
- Une coopération policière et judiciaire insuffisante, que la Directive NIS et le RGPD visent à renforcer
- Conséquence : une lame de fond réglementaire, tous cybercriminels !
- On est tous responsables les uns des autres :
  - Des OIV (de l'ordre de 250) aux OSE et aux FSN (de l'ordre de « plusieurs milliers »)
  - De Responsable de traitement à Responsable de tous traitements et sous-traitants
  - On peut être victime et responsable en même temps
- Un mouvement d'ampleur mondial :
  - De la LPM à la Directive NIS
  - La loi sur la cybercriminalité en Chine est une copie de la LPM