06.02.19

Obligations légales et réglementaires en matière de sécurité numérique et vidéo

Olivier Sanviti // Avocat Associé // Responsable du Département Venture M&A

ASTON SOCIETE D'AVOCATS EN QUELQUES CHIFFRES

2012

LE 140

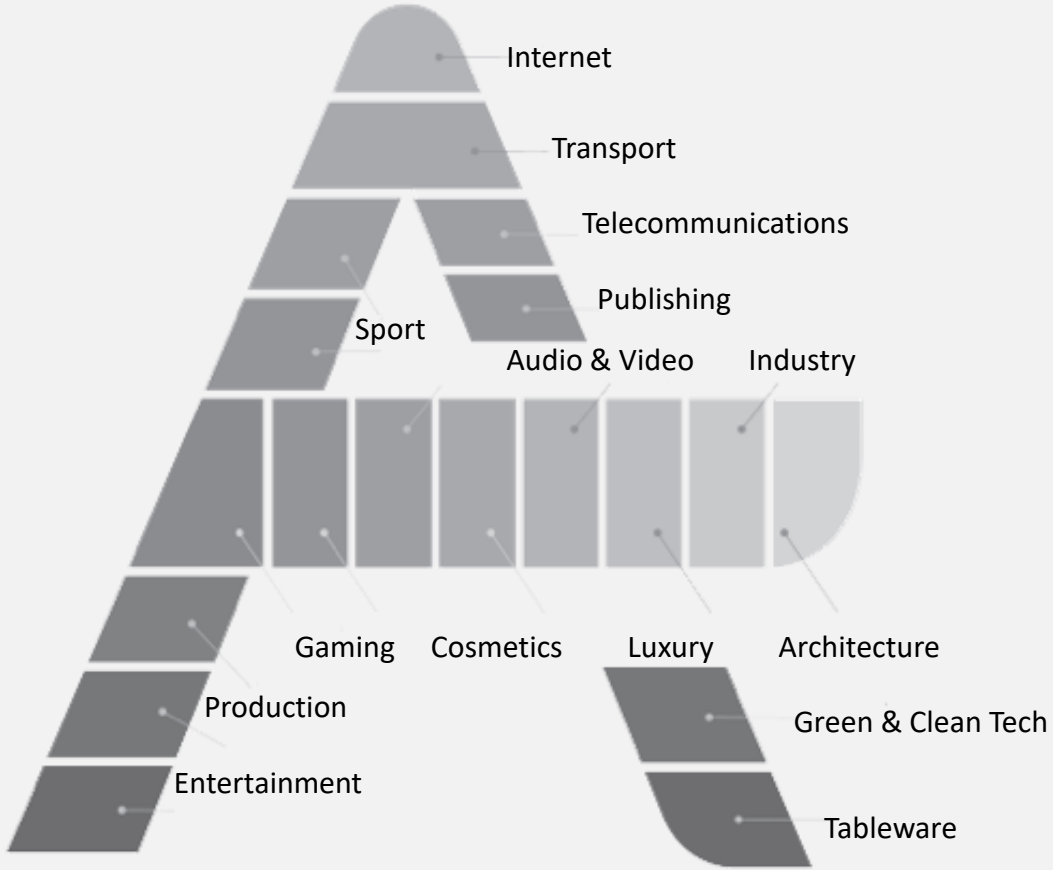
15

46 pays

NOS DOMAINES D'EXPERTISE

TECHNOLOGY - IP
SOCIAL
CONTENTIEUX D'AFFAIRES
VENTURE - M&A - RESTRUCTURING - TAX
MEDIA, SPORT & ENTERTAINMENT

NOS SECTEURS D'INTERVENTION



SOMMAIRE

1. LE DROIT AU SERVICE DE LA CYBERSÉCURITÉ

1. LE DROIT AU SERVICE DE LA CYBERSÉCURITÉ

- En 2018 :
  - 21.643.946 logiciels malveillants distincts ont été détectés attaquants 1 ordinateur sur 3 ;
  - 4.000 attaques quotidiennes par *« rançongiciel ».*

- Création d'un cadre juridique national et européen permettant de sécuriser le numérique et de défendre les libertés fondamentales :
  - Dispositions du Code pénal protégeant la vie privée des dispositifs techniques intrusifs ;
  - Règlements européens encadrant la protection des données personnelles et renforçant la coopération entre les Etats membres.

- Lundi 28 janvier 2019, journée européenne de la protection des données :
  - Constat : plus de 2,5 milliards d'octets de données sont crées chaque jour ;
  - Conclusion : les acteurs se voyant confier des données ont pour première obligation celle de les défendre et de les protéger, notion primordiale de confiance des consommateurs.

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2.1. Loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025

- Nombreuses attaques en 2017 par des logiciels malveillants tels que WannaCry et NotPetya => réaction étatique par la Loi :
  - Fait des opérateurs de communications électroniques des collaborateurs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : objectif d'identification et de blocage rapide en cas d'attaques ;
  - Ouvre la possibilité pour les opérateurs de communications électroniques d'installer des dispositifs sur leurs réseaux pour détecter les évènements affectant la sécurité des usagers.

- Distinction entre les opérateurs :
  - *« systèmes d'information standards »* (particuliers, entreprises…) :
    - Possibilité d'installer des marqueurs techniques pour détecter les événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés ;
    - Conservation des données : 6 mois ;
  - *« opérateurs d'importance vitale » (OIV)* (autorités publiques et opérateurs publics ou privés d'importance capitale pour la Nation → domaines de la guerre, de l'économie, de la sécurité, du nucléaire…) :
    - Possibilité identique avec en plus exploitation des données aux seules fins de prévention et de caractérisation de la menace ;
    - Conservation des données : 10 ans.

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2.2. Transposition du *« Paquet Numérique »* européen

2.2.1. Entrée en vigueur le 25 mai 2018 du Règlement général sur la protection des données *(RGPD)*

- 80% des entreprises ne sont pas en règles avec les nouvelles obligations issues du RGPD *(sondage BFM Business)*

- Le RGPD précise et renforce les mesures de l'ancienne Directive et consacre de nouvelles dispositions, notamment :
  - Augmente les pouvoirs des acteurs de la protection des personnes par une possibilité de sanctions administratives pouvant aller jusqu'à 10.000.000 € ou 2 % du CA annuel total mondial ;
  - Reconnait de nouveaux droits à l'effacement et à la portabilité des données ;
  - Introduit de nouvelles obligations au responsable du traitement et au sous-traitant : exemple de la sanction de Darty par la CNIL pour une faille sur un module développé par un sous-traitant *(Délibération du 8 janv. 2018 : sanction de 100.000€)*.

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2.2. Transposition du *« Paquet Numérique »* européen

2.2.2. DPO *(Data Privacy Officer)* ou DPD *(Délégué à la Protection des Données)*, fonction nouvelle dans l'entreprise

- Nouveauté issue du RGPD, nomination obligatoire pour toute entreprise traitant des données personnelles.

- Mise en place nécessite une réelle (ré)organisation et implication des entreprises → processus spécifique :
  - Désigner un pilote, le DPO (mission d'information, de conseil et de contrôle en interne) ;
  - Cartographier les traitements des données personnelles (recensement précis des traitements internes) ;
  - Prioriser les actions à mener (identifier les actions pour être conforme aux obligations au regard des risques) ;
  - Gérer les risques (et procéder à une analyse d'impact) ;
  - Organiser les processus internes (en prenant en compte l'ensemble des évènements qui peuvent survenir au cours de la vie d'un traitement => faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire…) ;
  - Documenter la conformité (pour la prouver lors de contrôles et assurer une protection continue).

2.2. Transposition du *« Paquet Numérique »* européen

2.2.3. Loi du 26 février 2018 transposant la directive NIS *(Network and Information Security)*

- Objectif d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne : *« renforcement des capacités nationales de cybersécurité ».*

- Les Etats membres doivent se doter d'autorités nationales compétentes en matière de cybersécurité, d'équipes nationales de réponse aux incidents informatiques et de stratégies nationales → ANSSI pour la France.

- La Loi étend le contrôle des OIV à deux nouveaux types d'acteurs :
  - Les *« opérateurs de services essentiels » (OSE)* → entreprises dans les domaines de l'énergie, de la banque et des marchés financiers, de la fourniture numérique, des transports, de la santé et de l'eau ;
  - Les *« fournisseurs de services numériques » (FSN)* → places de marché, moteurs de recherche et opérateurs *Cloud.*

- Les OSE et FSN doivent désormais publier les attaques dont ils auraient été l'objet, subir des audits de leurs systèmes d'information et être sanctionnés pécuniairement jusqu'à 100.000 € par infraction.

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2.3. Décrets du 30 mai 2018 et du 5 octobre 2018 pris en application de la *« Loi pour une République numérique »*

- Mise en œuvre du *« coffre-fort numérique »* à destination des entreprises leur permettant de stocker en ligne des documents et données sous format numérique avec assurance d'une sécurité élevée :
  - Documents administratifs : statuts, contrats d'assurances ;
  - Documents RH : contrats, fiches de paie ;
  - Documents R&D : projets, brevets ;
  - Documents comptables : factures, bilans, relevés bancaires ;
  - Mots de passe...

- Objectifs :
  - Protection contre les failles de sécurité ;
  - Archiver des documents sans perdre leur valeur juridique ;
  - Gagner en temps et en productivité (automatisation de certaines tâches, facilité de recherche et d'accès aux documents…)

2. DISPOSITIFS DE PROTECTION NUMÉRIQUE APPLICABLES A L'ENTREPRISE

2.3. Décrets du 30 mai 2018 et du 5 octobre 2018 pris en application de la *« Loi pour une République numérique »*

- Garanties :
  - Intégrité des documents (une empreinte numérique est créée lors du dépôt) ;
  - Pérennité des documents (contrôles périodiques et duplication du stockage pour prévenir toute perte) ;
  - Confidentialité (grâce au cryptage et au contrôle d'accès) ;
  - Traçabilité (grâce à un historique des utilisateurs).

- Pour s'assurer de la conformité d'un coffre fort numérique, les entreprises peuvent se référer à trois repères :
  - La norme NF Logiciel « composant coffre fort numérique » de l'AFNOR ;
  - Le label « Coffre fort électronique » de la Fédération des Tiers de confiance ;
  - La Certification de la CNIL.

- Chiffres clés :
  - 15% des entreprises en utilise un ;
  - 92% des entreprises utilisatrices s'en servent comme réceptacle numérique des documents RH.

3. LES MOYENS DE PROTECTION VIDÉO MIS À LA DISPOSITION DE L'ENTREPRISE

3. LES MOYENS DE PROTECTION VIDÉO MIS À LA DISPOSITION DE L'ENTREPRISE

3.1. Vidéosurveillance

- Chiffres clés :
  - En 2018 : plus d'1 millions de caméras en France ;
  - Moyenne de 3 caméras par entreprises dont 80% utilisées à l'intérieur ;
  - Enregistrement 24h/24 mais seules 10% permettent d'intervenir en cas de problème => utilisation préventive.

- Droits et devoirs de l'entreprise :
  - Pouvoir de direction de l'employeur lui autorise à surveiller l'activité des salariés par un système de caméra ;
  - Limites du dispositif quant au respect des libertés individuelles et collectives (Art L.1121-1 du Code du travail codifié par l'ordonnance du 13 mars 2007) : droit au respect de la vie privée, secret des correspondances, liberté d'opinion, liberté syndicale…

- Arrêt portant sur l'utilisation licite d'un système de vidéosurveillance dans un magasin *(Cass. Soc., 7 nov. 2018)* : des affiches informaient le public aux entrées du magasin que le site était sous vidéoprotection, un arrêté préfectoral autorisait ce dispositif, ce système avait donné lieu à information et approbation de la CNIL et des IRP, et l'utilisation de l'enregistrement était en l'espèce licite.

3. LES MOYENS DE PROTECTION VIDÉO MIS À LA DISPOSITION DE L'ENTREPRISE

3.2. Télésurveillance

- Chiffres clés :
  - En 2018 : plus de 70.000 cambriolages dont 44% dans des locaux professionnels ;
  - Environ 445.000 systèmes d'alarmes reliés à une télésurveillance ;
  - En 2018 : 11% de croissance annuelle moyenne du CA des entreprises de télésurveillance (= 7 milliards d'€).

- Condamnation par la CNIL d'une société de télésurveillance ayant mis en œuvre illégalement un système biométrique à des fins de contrôle des horaires des salariés *(CNIL, 20 sept. 2018).*

- Engage sa responsabilité quasi-délictuelle envers le commissionnaire, le sous-dépositaire qui manque à ses obligations contractuelles en ne sécurisant pas suffisamment le site où l'envoi était entreposé. A défaut d'avoir satisfait aux règles de prévention, portant notamment sur la souscription d'un contrat de télésurveillance, le dépositaire ne bénéficie pas de la garantie de son assureur RC *(CA Rouen, 26 avril 2018).*

4. LA TECHNOLOGIE *BLOCKCHAIN*

4. LA TECHNOLOGIE *BLOCKCHAIN*

- Chiffres clés :
  - ➢ Selon une étude du cabinet IDC :
    - 1,5 milliard de $ ont été investis dans cette technologie en 2018 ;
    - 11,7 milliards de $ devraient être investis d'ici à 2022.

  - ➢ Potentiel du marché *Blockchain* et crypto-devises d'ici 15 ans (étude de la Royal Bank of Canada) : 10.000 milliards de $.

- Initialement connue pour le *Bitcoin*, cette nouvelle technologie infiltre tous les secteurs d'activité et entreprises.

- Permet de transmettre des informations regroupées en « chaînes de blocks » avec une degré élevé de sécurité, grâce à des méthodes de cryptage et à des protocoles de transmission.

- Le législateur français a choisi l'approche règlementaire et de la proportionnalité en partenariat avec les régulateurs :
  - ➢ Expérimentation de la technologie du registre distribué avec les *« minibons »* (= bons de caisse dématérialisés pouvant être échangés sur des plateformes internet de financement participatif).

4. LA TECHNOLOGIE *BLOCKCHAIN*

- Saisine du CE le 16 mai 2018 d'un projet de Loi relatif à la croissance et la transformation des entreprises (PACTE) :
  - Idée de création d'un régime des offres au public de *« jetons »* ;
  - Idée de proposer aux émetteurs d'ICO *(Initial Coin Offerings)* un visa préalable de l'AMF pour garantir leur offre et prévenir des abus.

- Projet de Loi PACTE adopté par l'AN le 9 octobre 2018 et adopté en partie par le Sénat le 31 janvier 2019 :
  - Reprise de la proposition de l'AMF d'offrir un visa optionnel pour les ICO (Article 26 de la Loi PACTE) ;
  - Dote la France d'un cadre juridique souple pour encadrer le financement des entreprises par l'émission d'ICO.

5. VISION PROSPECTIVE

5. VISION PROSPECTIVE

Transformation numérique : bilan 2018 et perspectives 2019

- Selon Syntec Numérique, la transformation numérique en 2018 des entreprises a représenté 56,3 milliards d'€.
- Les entreprises de cybersécurité et d'intelligence artificielle ont augmenté leur CA de 66%.
- La croissance des SMACS pour 2019 *(Social-Mobility-Analytics-Cloud & Security)* est estimée à 14,7%.
- *« Soyons tous connectés, tous impliqués, tous responsables »* : c'est l'appel que lance l'ANSSI pour 2019