Revue d'actualité juridique de la Sécurité des systèmes d'information

Raphaël PEUCHOT

Avocat associé, Fourmann & Peuchot

9 décembre 2020, Covid An 1

1. **Marchés publics: cahier des clauses simplifiées de cybersécurité**
2. **Protection des données personnelles : une profusion de nouveautés**
3. **Cybersurveillance des salariés**
4. **Incident de sécurité et effets contractuels collatéraux**

1.

Marchés publics:
Cahier des clauses simplifiées de cybersécurité

Rappel : l'Etat a défini une « Politique générale de sécurité des systèmes d'information pour les ministères économiques et financiers » en 2016

Arrêté du 18 sept. 2018 portant approbation du Cahier des clauses simplifiées de cybersécurité

- définit les conditions auxquelles les soumissionnaires (candidats aux marchés publics) doivent se soumettre pour prendre en compte les exigences SSI des personnes publiques

- s'applique prioritairement aux machés à objet technologique,

- concerne le titulaire du marché, mais également ses sous-traitants pour l'exécution du marché

- peut être complété par un CCP, et un PAS

Respect des PSSI des personnes publiques

- annexes techniques
- RGS (téléservices)
- PSSI d'Etat

Contrôles et audits

- fourniture, prestations, moyens, services, y compris des sous-traitants
- sans accord préalable, sous réserve de respect des conventions techniques d'usage

Documentations

- revue formelle de sécurité (homologation) portant sur les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience
- à première demande, fourniture de la documentation attestation de la sécurisation de la fourniture et des services, de la conformité au RGPD, des flux échangés

Maintien en condition de sécurité

- services et composants à jour des correctifs de faille
- idem pour les sous-traitants du marché

Signalements de sécurité

- fils publics (flux RSS, liste de diffusion)
- respect des conventions d'usage en cybersécurité (security.txt)
- identification, analyse, partage des failles détectées, puis notification aux autorités compétentes (CERT, CNIL, ANSSI)

Hébergement de données

- identification des sous-traitants

Sous-traitances

- les clauses du Cahier des clauses de cybersécurité s'appliquent à tous les sous-traitants du marché

Etats de l'art

- obligation du prestataire de se conformer aux standards techniques
- cf. référentiels du gouvernement pour : interfaces web, services de courriels, appareils connectés, sauvegardes de données, administration de SI

2.

Protection des données personnelles : une profusion de nouveautés

2.

Protection des données personnelles : une profusion de nouveautés

- Biométrie
- Privacy Shield
- Sanctions CNIL
- Cookies
- Droit au déréférencement

1. Biométrie : règlement-type de la CNIL du 10 janv. 2019

- la biométrie traite, par nature, des données personnelles sensibles

- « règlement-type » : norme contraignante s'imposant aux organisations mettant en œuvre des outils de biométrie

- finalités du traitement : contrôle d'accès aux locaux limitativement énumérés, aux appareils et applications informatiques

- établir la nécessité de recourir à la biométrie plutôt qu'à des systèmes de badges et autres systèmes de contrôle d'accès

- limitation des données : identité, vie professionnelle, locaux, outils

- données générées : journalisation des accès

- personnes habilitées à traiter les données : limitation des personnes habilitées à gérer l'enrôlement, les gabarits, les profils d'accès

- personnes habilitées à traiter les données collectées : qui gèrent la sécurité des locaux

- choix des gabarits utilisés : par défaut, gabarit sous contrôle de la personne concernée

- durée de conservation :
  - données brutes d'enregistrement : aucune durée
  - données dérivées sur gabarit :durée d'habilitation de la personne concernée;
  - données de journalisation : six mois glissants à compter de la date d'enregistrement

- mesures diverses : traitement des données, organisation, matériels, logiciels, canaux informatiques

- obligation de réaliser une analyse d'impact préalable (PIA)

2. Invalidation du Privacy shield - CJUE 16/07/2020

- après invalidation du Safe Harbor le 6/10/2015

- critique de l'absence de protection réelle des DCP aux USA

- la CJUE considère qu'aucune garantie ne peut être données puisqu'en vertu des règles sur la sécurité intérieure, les acteurs américains sont susceptibles de révéler la teneur de leurs traitements de DCP en provenance d'Europe, sans recours juridictionnel possible.

- le recours aux clauses-type est cependant possible (le contrat RT/ST doit alors s'inspirer des clauses définies par la C° européenne)

- l'export de DCP vers les USA n'est donc légal qu'en présence de contrats RT/ST conformes et si les conditions de sécurité des DCP sont réunies (confidentialité, intégrité, accessibilité)

Mais ces clauses permettent-elles la protection des DCP à l'égard des autorités US ? Le RGPD impose des « garanties appropriées » à rechercher dans les offres contractuelles des prestataires américains.

3. Sanction CNIL du 18/07/2020 « Active Assurances »

- activité d'assurance automobile pour les particuliers
- vente directe de produits d'assurance ou par le site web
- dénonciation à la CNIL d'un accès libre à des données d'assurés à partir d'une simple connexion au site web
- contrôle en ligne par la CNIL (…)
- « *la société Active Assurances n'a placé la sécurité des données de ses clients au cœur de ses préoccupations qu'après l'intervention des services de la Commission* ».
- sanction de 180.000 € / publication nominative

4. Lignes directrices et recommandations CNIL sur les cookies du 17/09/2020

• Rappel chronologique

• **Lignes directrices :**

- la seule navigation en ligne ne constitue pas un accord univoque aux cookies et autres traceurs
- les informations doivent être claires et simples (cf. § 24)
- le consentement donné par l'internaute doit pouvoir être prouvé
- le retrait du consentement doit pouvoir être rendu possible, à tout moment
- « cookies wall » : initialement prohibés, puis rectification du Conseil d'Etat

• **Recommandations :**

- à chaque type de cookies: une finalité décrite (en synthèse, puis en détail)
- un consentement spécifique recueilli,
- le consentement peut cependant être recueilli de façon globale, si les finalités sont préalablement présentées de manière détaillée
- le consentement ou le refus doivent être recueillis aussi facilement

5. Exercice du droit au déréférencement

« Déférencement » (ou désindexation)

- **absolu :** suppression totale de la donnée du réseau internet et des moteurs de recherche,

- **géographique**: limitation des accès à la donnée depuis certaines zones géographiques (cf. Affaire Yahoo! , TGI Paris référé 22 mai 2000),

- **relatif** : suppression de certaines indexations, reléguant en position éloignée le résultat d'une recherche comportant la donnée.

- **« Droit à l'effacement »** (ou droit à l'oubli)

Droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant.

Le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais (art. 17 RGPD).

- **Cour de cassation, Civ. 1, 27 nov. 2019**

« Il s'ensuit que, lorsqu'une juridiction est saisie d'une ***demande de déréférencement*** *portant sur un lien vers une page internet sur laquelle des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté sont publiées, elle doit, pour porter une appréciation sur son bien-fondé, vérifier, de façon concrète, si l'inclusion du lien litigieux dans la liste des résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, répond à un motif d'intérêt public important, tel que le droit à l'information du public, et si elle est strictement nécessaire pour assurer la préservation de cet intérêt. »*

- **Conseil d'Etat, 6 déc. 2019**

« Eu égard à la nature et au contenu des informations litigieuses, à leur source, au rôle qu'a joué et continue de jouer dans la vie publique M. X et au contexte dans lequel ont été tenus les propos rapportés dans les articles vers lesquels mènent les liens litigieux, la CNIL a pu légalement estimer que le maintien des liens permettant d'avoir accès à ces informations à partir d'une recherche effectuée sur le nom de M. X était strictement nécessaire à l'information du public. »

3.

Cybersurveillance des salariés

1. Surveillance du réseau

Arrêt Cour d'appel Aix-en-Provence 31 oct. 2019

- Faits : - surveillance déloyale d'un salarié et de l'usage fait du réseau
  - illicéité des preuves
  - licenciement jugé sans cause réelle et sérieuse, faute de preuve

- Article L. 1222-4 Code du travail:

« *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.* »

- Enseignement : préciser dans la charte informatique les mesures de surveillance habituelle et leur finalité.

1. Surveillance du réseau

Arrêt Cour d'appel de Paris 20 mai 2020

- Faits : - demandes de remboursement de frais excessifs et injustifiés
  - vérifications approfondies par DSI : agendas électroniques, effacement en grand nombre de données Outlook
  - licenciement pour faute grave confirmé par le juge

- Article L. 1222-4 Code du travail:

« *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.* »

- Enseignement : préciser dans la charte informatique la faculté de la DSI de procéder à des audits internes.

1. Surveillance du réseau

Arrêt Conseil d'Etat 2 mars 2020

• Faits : - différend d'ordre privé entre un employé de banque, salarié protégé, et un client de la banque

- menaces de l'employé à l'aide de relevés bancaires sur de prétendus mouvements de fonds suspects

- sur signalement, l'employé fait l'objet d'une enquête interne, qui conduit l'employeur à consulter les comptes bancaires personnels de l'employé et à requérir son licenciement à l'inspecteur du travail

- refus d'autorisation de l'inspecteur du travail, puis annulation par le Ministre du travail

• Article L. 1121-1 Code du travail :

« *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* »

• Conseil d'Etat : « *lorsqu'un employeur diligente une enquête interne …les investigations doivent être justifiées et proportionnées par rapport aux faits* »

2. Utilisation excessive du réseau

Arrêt Cour d'appel de Paris 12 sept. 2019

- Faits : - utilisation excessive du réseau par deux salariés
  - licenciement pour faute grave

Article L. 1121-1 Code du travail :

« *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* »

- Charte informatique : l'employeur peut suspendre les accès à internet en cas d'abus.

- Licenciement validé

4.

Incident de sécurité
et
effets contractuels collatéraux

Cas d'école :

- HR Acess est un logiciel de gestion RH (édition de paie)
- HR Access est accessible en mode Saas

- l'éditeur (Sopra Steria) subit une attaque majeure le 21/10/2020

- incident de sécurité (*cryptolocker*) chez un utilisateur d'HR Access
- l'éditeur bloque tout accès à son Saas tant que son client ne justifie pas une remédiation complète

Questions : un incident de sécurité chez le client utilisateur peut-il justifier une suspension de service côté éditeur ?

- quelles mesures correctives exigibles ?
- quelles autorisations contractuelles stipuler ?
- quelle action judiciaire engager ?

Merci pour votre attention !