CYBERASSURANCE ET DEVOIR D'ANNONCE

FSA JOURNEE DE FORMATION CONTINUE – 14 SEPTEMBRE 2022

Prof. Yaniv Benhamou, avocat
Faculté de droit / Digital Law Center (DLC)

Yaniv.benhamou@unige.ch
Yaniv.benhamou@aegis.ch

CONTEXTE

Statistique policière

83 infractions numériques par jour sont commises en Suisse

Lun 28.03.2022 - 16:41
par René Jaun (traduction/adaptation: ICTjournal)

En 2021, 30 351 délits numériques ont été recensés en Suisse, soit 24% de plus que l'année précédente. Les escroqueries en ligne ont connu la plus forte augmentation. Il s'agit le plus souvent de marchandises payées puis non livrées ou d'usurpation d'identité.

THURSDAY 10 MARCH 2022 6:51 PM

UK data watchdog fines Tuckers Solicitors £98,000 after hacker leaked legal papers onto dark web

"The first thing we do, let's hack all the lawyers"

Episode 416 of the Cyberlaw Podcast

STEWART BAKER | 7.11.2022 8:54 PM

CYBERASSURANCE (MESURE PREVENTIVE)

- **COUVERTURE DES CYBERRISQUES**
  - Distinctions (sélection)
    - Couverture expresse *vs* implicite (*silent cyber risk*)
    - Dommage propre subi par l'assuré (*Eigenschaden*) *vs* dommage à des tiers (*Drittschaden*)
    - Couverture des cyberrisques *vs* autres prestations (p.ex. protection des données personnelles, telle que perte de données, amendes ou peines pécuniaires, *ransomware*)
  - Difficultés pratiques
    - Hausse des cyberattaques = hausse des exigences
    - Diversité des clauses sur les cyberrisques et difficultés d'interprétation des clauses

- **ASSURABILITE DES AMENDES?**
  - Clauses spécifiques pour les amendes RGPD (exemples)
    - sont exclues « *Les prétentions relatives à des indemnités à caractère pénal (par ex. les amendes) » ; D.2.2 sont couvertes « Les amendes en raison de dispositions en matière de protection des données.* » (*cf.* Bâloise, B4.3)
    - sont exclues « *les prétentions pour des indemnités à caractère pénal, tels que les amendes. Cette exclusion ne s'applique pas aux peines et amendes du RGPD*. » (*cf.* Zurich, Art. 5)
  - Une amende est de nature strictement personnelle et toute convention visant à la faire supporter par un tiers est nulle (CO 20 al. 2) (ATF 86 II 71, cons. 4)
    - Amendes LPD 60 ss: non réparables (*cf.* ATF 134 III 59)
    - Amendes RGPD "administratives": non réparables (*NB*: pour la part de nature pénale, la part réparatrice pouvant être réparable, *cf.* double nature des amendes fiscales, TF 2C_916/2014)

- **ASSURABILITE DES RANSOMWARE?**
  - Clauses spécifiques pour le paiement de ransomware (exemples)
    - sont couvertes « *(pour autant que la couverture soit convenue) les paiements de rançons effectués sur accord écrit préalable de la Bâloise*. » (*cf.* Bâloise D4.2)
    - sont couvertes les indemnités « *jusqu'à 25% au maximum de la somme d'assurance en cas de ransomware*. » (*cf.* Zurich, art. 104)
  - Un tel paiement pourrait être contraire aux principes généraux de droit civil / aux bonnes mœurs (CO 19-20) (Bracher; de Werra / Benhamou).
  - Un tel paiement pourrait-il être contraire aux règles de lutte contre le blanchiment d'argent et le financement du terrorisme?
    - Le paiement ne peut pas constituer un acte de blanchiment (CP 305bis) (*cf.* NCSC, p. 25; HCJP 2022, p. 24)
    - Attention aux personnes placées sous sanctions (cf. FAC 2021) et aux exigences préalables pour ces cyberrisques (p.ex. confidentialité, mesures de sécurité) (*cf.* BaFin 1998 et 2017)

DEVOIR D’ANNONCE (MESURE CURATIVE)

- **PRINCIPE**
  - Devoir d'annonce en cas de **violation de la sécurité des données** (*data breach*) entraînant de manière accidentelle ou illicite la *perte* de données personnelles, leur *modification*, leur *effacement* ou leur *destruction*, leur *divulgation* ou un *accès non autorisés* à ces données (nLPD 5 let. h).
    - **Perte**: disponibilité des données (p.ex. vol/perte d'un support)
    - **Modification** : altération ou effacement (p.ex. intégrité, suppression accidentelle de données)
    - **Divulgation ou accès non autorisés** : confidentialité des données (p.ex. envoi d'un e-mail à un mauvais destinataire, mauvaise gestion des droits d'accès au sein de l'entreprise
  - **Risque** concret / mise en danger des données

- **MODALITES (DESTINATAIRES ET DELAIS)**
  - aux **autorités de protection des données**
    - **PFPDT** sans délai en cas de "*violation de la sécurité des données*" (si risque élevé) (nLPD 24 et 5 let. g).
    - **Autorités étrangères de protection des données**, p.ex. européennes dans les 72h en cas de "*violation de données à caractère personnel*" (sauf si pas de risque) (RGPD 33 et 4 ch. 12). Cf. "*Le seuil d'annonce en vertu du droit européen est plus bas, puisqu'il s'applique déjà à un risque simple*" (PFPDT, Actualité 05.03.2021), pas de violation de CP 271 en cas d'annonce aux autorités européennes (DFJP, Note, 04.09.2018)
    - Autres régulateurs selon les réglementations spécifiques, p.ex. FINMA dans les 24 heures en cas de cyberattaques à des **actifs d'importance critique** (LFINMA 29 al. 2, Communication FINMA // art. 14 Directive NIS)
  - à la **personne concernée** dans certains cas (nLPD 24 al. 4, RGPD 34)
  - à d'**autres personnes** selon les obligations contractuelles (p.ex. clients)

- **ARTICULATION AVEC LE PRINCIPE DE SECURITE**
  - Principe de sécurité des données: obligation d'assurer la sécurité des données par des mesures techniques et organisationnelles (approche fondée sur les risques) (nLPD 8, nOPDo 1 ss).
  - Même avec le respect du principe de sécurité, il peut y avoir un devoir d'annonce en raison d'une perte accidentelle ou illicite (*cf.* CNIL, mise en demeure, 8 juillet 2022).
- **INFORMATIONS CONTENUES DANS LE RAPPORT D'ANNONCE**
  - Informations non réutilisables dans une procédure pénale contre la personne tenue d'annoncer sans son consentement (*nemo tenetur*) (LPD 24 al. 6)
- **SECRET PROFESSIONNEL (P.EX. CABINET D'AVOCAT)**
  - Au PFPDT: ne pas révéler l'identité des clients (cf. formulaire Luxembourg)
  - Aux personnes visées: client √ (= maître du secret), partie adverse √ (si déjà au courant, sinon levée)

REFERENCES (SELECTION)

- Bundesaufsichtsamt für das Versicherungswesen (BaFin), BaFin erlaubt Bündelung mit Versicherung gegen Cyberrisiken, septembre 2017
- Benhamou Yaniv, Wang Louise, Cyberattaque et ransomware: quels risques juridiques à payer? (à paraître)
- Bracher Nicholas, Rechtliche Stolpersteine bei der Versicherung von Cyberrisiken, 2017, p.185 ss
- De Werra Jacques, Benhamou Yaniv, Cyberassurance : instrument utile pour la cybersécurité des entreprises ?, *Jusletter 24/*2020
- HCJP, Rapport sur l'assurabilité des risques cyber, janvier 2022
- NCSC, Rapport semestriel 2021, Novembre 2021
- OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (cité : Updated Advisory), septembre 2021

Merci de votre attention

Prof. Yaniv Benhamou, avocat
Faculté de droit / Digital Law Center (DLC)

Yaniv.benhamou@unige.ch
Yaniv.benhamou@aegis.ch