Protection des données de l'entreprise et risques liés
Questions juridiques

Sylvain SAVOLAINEN, Associé fondateur
SAVOLAINEN Avocats, Genève

Club de Réseautage Romand
12 mai 2022

Plan

1. Contexte
2. Définitions
3. Obligations légales en matière de protection des données
4. Responsabilités
    A. Responsabilité contractuelle
    B. Responsabilité délictuelle
    C. Responsabilité des organes de gestion de la société
    D. Responsabilité pénale
5. Conseils pratiques

1. Contexte

- Le risque lié aux **cyberincidents** constitue le **risque d'entreprise le plus important** en 2022 (en augmentation de 44% par rapport à 2021)

- « *Les cyberrisques constituent un risque majeur pour la société en général et pour les entreprises en particulier.* (…) *Si* ***les cyberrisques n'épargnent personne*** *(ni l'État, ni les entreprises, ni les citoyens qui sont tous victimes de cyberincidents et cyberattaques),* ***les PME y sont particulièrement exposées*** » (DE WERRA/BENHAMOU, 2020)

  → Risque pour :

    - Personnes morales (sociétés)
    - Personnes physiques (employeur, administrateur, employé, partenaire d'affaire, etc.)
    - Réputation

- « *Les PME sont particulièrement pénalisées par le fait qu'elles ne disposent pas de service informatique dédié, et que leurs marges bénéficiaires ne leur permettent pas de s'offrir les services coûteux d'experts en cybersécurité* » (Rapport du groupe d'experts concernant le traitement et la sécurité des données, 2018, p. 50)

2. Définitions

- **Cyberrisque :** « *risque de survenance d'un* ***cyberincident****, son ampleur* ***résultant*** *du produit de la probabilité de* ***survenance*** *et de l'****étendue des dommages*** » (art. 3 let. c de l'Ordonnance sur les cyberrisques (OPCy))

- **Cyberincident :** « ***tout évènement nuisant*** *à la* ***confidentialité****, à l'****intégrité****, à la* ***disponibilité*** *ou à la* ***traçabilité des données*** *ou pouvant occasionner des* ***dysfonctionnements****, qu'il soit* ***accidentel ou provoqué intentionnellement*** *par un tiers non autorisé* » (art. 3 let. b OPCy)

- **Dommage :**

  - Le dommage est une **diminution involontaire de patrimoine net**, il est la mesure des conséquences patrimoniales de l'atteinte aux intérêts juridiquement protégés de la victime.

  - Au sens juridique, le dommage est la **différence entre le patrimoine actuel**, mesuré après l'événement dommageable, **et son état hypothétique sans l'événement dommageable**.

3. Obligations légales en matière de protection des données

- Entrée en vigueur de la loi sur la protection des données (LPD) sous sa nouvelle version: 1er septembre 2023

- Protection des données personnelles : « *Les **données personnelles doivent être protégées** contre tout traitement non autorisé **par des mesures organisationnelles et techniques appropriées*** » (art. 7 al. 1 LPD ; *cf*. art. 8-12 OLPD pour le détail des mesures)

- Analyse d'impact relative à la protection des données personnelles: « *Lorsque **le traitement** envisagé est **susceptible d'entraîner** un **risque élevé pour la personnalité** ou les **droits fondamentaux** de la personne concernée, le **responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelle*** » (art. 22 al. 1 nLPD)

- Conseiller à la protection des données: « Les responsables du traitement privés peuvent nommer un conseiller à la protection des données » (art. 10 al. 1 nLPD) ; « *Le conseiller à la protection des données est l'interlocuteur des personnes concernées et des autorités chargées de la protection des données en Suisse. Il a notamment **les tâches suivantes**: a. **former et conseiller le responsable du traitement privé** dans le domaine de la protection des données ; b. **concourir à l'application des prescriptions** relatives à la protection des données* » (art. 10 al. 2 nLPD)

- Obligation d'annonce en cas de violation de la sécurité des données

  « *Le responsable du traitement annonce dans les meilleurs délais au **PFPDT** les **cas de violation de la sécurité des données** entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée* » (art. 24 al. 1 nLPD)

  « *Le responsable du traitement **informe la personne concernée** lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige* » (art. 24 al. 4 nLPD)

4. Responsabilités

A. Responsabilité contractuelle

B. Responsabilité délictuelle

C. Responsabilité des organes de gestion de la société

D. Responsabilité pénale

4/A. Responsabilité contractuelle

- Par exemple vis-à-vis de clients/partenaires lésés:
  - Art. 97 al. 1 CO : « *Lorsque le créancier* ***ne peut obtenir l'exécution de l'obligation*** *ou ne peut l'obtenir qu'****imparfaitement****, le débiteur est* ***tenu de réparer le dommage*** *en résultant,* ***à moins qu'il ne prouve qu'aucune faute ne lui est imputable****.* »
  - Clause exclusive de responsabilité :
    - « *Est nulle toute stipulation tendant à libérer d'avance le débiteur de la responsabilité qu'il encourrait en cas de dol ou de faute grave* » (art. 100 al. 1 CO)
    - « *Les règles particulières du contrat d'assurance demeurent réservées* » (art. 100 al. 3 CO)
  - Responsabilité pour des auxiliaires : « *Celui qui,* ***même d'une manière licite, confie à des auxiliaires*** (…) ***le soin d'exécuter une obligation*** *ou d'exercer un droit dérivant d'une obligation,* ***est responsable*** *envers l'autre partie du dommage qu'ils causent dans l'accomplissement de leur travail* » (art. 101 al. 1 CO)
  - Clause exclusive de responsabilité dérivant du fait des auxiliaires :
  - « *Une convention préalable peut exclure en tout ou en partie la responsabilité dérivant du fait des auxiliaires* » (art. 101 al. 2 CO)
  - Pas d'exclusion valable en cas de clause peu claire tenant en des banalités formulées de manière générale (ATF 124 III 155), ou en cas de clause inhabituelle de conditions générales sans que l'attention de la partie inexpérimentée ait été spécialement attirée (ATF 119 II 443; ATF 135 III 1).

4/A. Responsabilité contractuelle

- Par exemple vis-à-vis d'un employé

  - Art. 328b CO : « *L'employeur ne peut* ***traiter des données concernant le travailleur*** *que dans la mesure où ces données* ***portent sur les aptitudes du travailleur à remplir son emploi*** *ou sont* ***nécessaires à l'exécution du contrat de travail****. En outre les dispositions de la loi sur la protection des données sont applicables* »

    → Concrétise l'**obligation de protéger la personnalité du travailleur** en matière de protection des données.

  - « *Le mot «* ***aptitude*** *» s'interprète de façon* ***large****. Il ne s'agit pas des aptitudes purement professionnelles, attestées par la formation ou l'expérience de l'intéressé, mais, plus largement, des qualités de la personne en regard de l'emploi, lesquelles peuvent inclure, selon les circonstances, le caractère du salarié, sa vision du monde ou ses ambitions. Quant aux informations nécessaires à l'exécution du contrat de travail, elles comprennent avant tout celles dont l'employeur a besoin pour satisfaire à ses obligations légales ou conventionnelles* » (CR-CO, Art. 328b CO)

  - La **LPD est applicable**, notamment les obligations de sécurité (art. 7 LPD *cum* art. 8-12 OLPD)

    → Dès lors, par exemple, l'employeur pourrait engager sa responsabilité contractuelle vis-à-vis d'un employé dont les données personnelles auraient été divulguées suite à un cyberincident.

4/A. Responsabilité contractuelle

- Un fournisseur de services technologiques, par exemple qui serait responsable du préjudice causé en raison des déficiences de cybersécurité des services offerts

  - Devoir de diligence du mandataire (celui à qui le mandat est confié) :

    - « *Le mandataire est responsable envers le mandant de la* ***bonne et fidèle exécution du mandat*** » (art. 398 al. 2 CO)

    - « *Le degré de diligence qui incombe au mandataire ne doit pas se déterminer une fois pour toutes, mais* ***en fonction des capacités, des connaissances techniques et des aptitudes propres de ce dernier que le mandant connaît ou aurait dû connaître*** » (ATF 134 III 534, c. 3.2.2)

    - « *La* ***diligence requise*** *s'apprécie au moyen de critères objectifs ; on cherchera à déterminer comment* ***un mandataire consciencieux, placé dans la même situation, aurait agi en gérant l'affaire en cause*** » (TF 4A_556/2019 du 29 septembre 2020, c. 4.3.1)

  - Responsabilité du fournisseur du fait de ses auxiliaires (art. 101 al. 1 CO)

Attention !

  - Clauses exclusives de responsabilité (art. 100 al. 1 CO ; art. 101 al. 2 CO)

  - Droit applicable au contrat: il se peut que le contrat soit régi par un autre droit que le droit suisse

  - Faute concomitante : « *Le juge peut réduire les dommages-intérêts, ou même n'en point allouer, lorsque la partie lésée a consenti à la lésion ou lorsque des faits dont elle est responsable ont contribué à créer le dommage, à l'augmenter, ou qu'ils ont aggravé la situation du débiteur* » (art. 44 al. 1 CO ; applicable par renvoi de l'art. 99 al. 3 CO)

4/A. Responsabilité contractuelle

- Par exemple d'un employé :

  - Devoir de diligence du travailleur : « *1. Le travailleur exécute avec soin le travail qui lui est confié et sauvegarde fidèlement les intérêts légitimes de l'employeur.*
    2. Il ***est tenu d'utiliser selon les règles en la matière les machines, les instruments de travail, les appareils et les installations techniques*** (…) *et de les traiter avec soin, de même que le matériel mis à sa disposition pour l'exécution de son travail* » (art. 321a CO)

    « *La diligence due se mesure au premier chef en fonction du travail promis par le salarié, lequel est réputé* ***posséder l'instruction les connaissances techniques nécessaires pour accomplir son travail****, à moins que l'employeur n'ait su ou dû savoir que les aptitudes et qualités nécessaires lui faisaient défaut* » (CR-CO, art. 321d CO)

  - Responsabilité du travailleur : « *1. Le* ***travailleur répond du dommage qu'il cause à l'employeur intentionnellement*** *ou par* ***négligence****.*
    2. La mesure de la diligence incombant au travailleur se détermine par le contrat, compte tenu du risque professionnel, de ***l'instruction ou des connaissances techniques nécessaires pour accomplir le travail promis****, ainsi que des* ***aptitudes et qualités du travailleur que l'employeur connaissait ou aurait dû connaitre*** » (art. 321e CO)

Attention !

  - Faute concomitante de l'employeur « *Le juge peut réduire les dommages-intérêts, ou même n'en point allouer, lorsque la partie lésée a consenti à la lésion ou lorsque des faits dont elle est responsable ont contribué à créer le dommage, à l'augmenter, ou qu'ils ont aggravé la situation du débiteur* » (art. 44 al. 1 CO ; applicable par renvoi de l'art. 99 al. 3 CO)

    → Souvent, **une telle faute est reprochée à l'employeur lorsqu'il a mal organisé le travail, n'a pas donné les instructions utiles ou n'en a pas contrôlé l'exécution** (*cf.* art. 321 d CO).

4/B. Responsabilité délictuelle

- **Responsabilité délictuelle**

  - **Art. 41 al. 1 CO :** « *Celui qui cause, d'une manière illicite, un* ***dommage à autrui****, soit* ***intentionnellement****, soit* ***par négligence ou imprudence****, est tenu de le réparer* »

  - **Par exemple, lorsqu'un employé est à l'origine du cyberincident:** « ***L'employeur est responsable du dommage causé par ses travailleurs ou ses autres auxiliaires dans l'accomplissement de leur travail****, s'il ne prouve qu'il a pris tous les soins commandés par les circonstances pour détourner un dommage de ce genre ou que sa diligence n'eût pas empêché le dommage de se produire* » (art. 55 CO)

  - Une entreprise pourrait engager sa responsabilité délictuelle envers des personnes dont elle traiterait les données personnelles qui auraient été atteintes par un cyberincident.

  - En cas de violation de la LPD (en l'absence de base contractuelle), **la PME** (qu'elle agisse comme responsable de traitement sous-traitant) **peut être tenue pour responsable selon le régime de la responsabilité délictuelle pour faute** aux conditions de l'art. 41 CO (faute, dommage, acte illicite, causalité)

  - Si l'incident est due à un tiers avec lequel l'entreprise n'a aucune relation contractuelle, l'entreprise pourra faire valoir des prétentions délictuelles en réparation du préjudice qu'elle aurait subi

  - Cela supposera notamment la commission d'un acte illicite qui pourrait résulter de la commission d'une infraction pénale portant préjudice à l'entreprise

  - Toutefois souvent délicat d'identifier et de poursuivre les auteurs externes d'un cyberincident causant un dommage à une PME, le cyberespace offrant aux auteurs des moyens d'échapper à leur responsabilité

4/C. Responsabilité des organes de gestion de la société

- Art. 754 al. 1 CO : « *Les **membres du conseil d'administration** et **toutes les personnes qui s'occupent de la gestion** ou de la liquidation **répondent** à l'égard de la société, de même qu'envers chaque actionnaire ou créancier social, **du dommage** qu'ils leur causent **en manquant intentionnellement** ou **par négligence** à leurs **devoirs*** »

- Le risque de responsabilité des organes pour cyberincident peut-il être assuré dans le cadre des **polices générales d'assurance des organes dirigeants de sociétés ?**

4/D. Responsabilité pénale

- Dispositions pénales susceptibles de s'appliquer en cas de cyberincident, par exemple:
  - **Soustraction de données** (art. 143 CP)
  - **Accès indu à un système informatique** (art. 143bis al. 1 CP)
  - **Détérioration de données** (art. 144bis al. 1 CP)
  - **Utilisation frauduleuse d'un ordinateur** (art. 147 CP)
  - **Pornographie** (art. 197 CP)
  - **Violation des obligations de renseigner, déclarer et collaborer** (art. 34 LPD)
  - **Violation du devoir de discrétion** (art. 35 LPD)
  - **Violation des obligations d'informer, de renseigner et de collaborer** (art. 60 nLPD)
  - **Violation des devoirs de diligence** (art. 61 nLPD)
  - **Violation du devoir de discrétion** (art. 62 nLPD)
  - **Etc.**

4/D. Responsabilité pénale

- **Par rapport à la LPD en vigueur, la LPD révisée comporte un volet pénal renforcé et prévoit :**
  - De **nouvelles infractions**, notamment la **violation du principe de sécurité**, soit le fait de ne pas respecter les exigences minimales en matière de sécurité des données
  - Des **sanctions plus sévères**
  - Des sanctions applicables également aux **organes responsables**
  - Des sanctions également applicables dans certains cas à **l'entreprise elle-même**

→ D'où l'importance de prendre la question de la protection des données personnelles au sérieux !

4/D. Responsabilité pénale

- **Responsabilité pénale de l'entreprise:** « *Un crime ou un délit qui est commis au sein d'une entreprise dans l'exercice d'activités commerciales conformes à ses buts est imputé à l'entreprise* ***s'il ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise.*** *Dans ce cas,* ***l'entreprise est punie*** *d'une amende de* ***cinq millions de francs au plus*** » (art. 102 al. 1 CP)

- **Responsabilité pénale du chef d'entreprise et de toute autre personne exerçant une fonction dirigeante en cas d'infraction à la LPD commise au sein de l'entreprise** (art. 64 al. 1 nLPD)

- **Aspects procéduraux :**

  - Infractions poursuivies sur plainte (ex : violation du devoir de diligence, art. 61 nLPD) vs. infractions poursuivies d'office (ex: soustraction de données, art. 143 CP)

  - Maxime de l'instruction (art. 6 CPP)

  - Action civile par adhésion au procès pénal (art. 122 CPP)

  - Entraves techniques et juridiques

5. Conseils pratiques

- À l'interne :
  - Se prémunir des risques juridiques par le biais de contrats adaptés (contrat de travail, mandats, etc..)
  - Mettre en place de la formation, notamment juridique, et des directives internes correctement rédigées relatives à la protection des données ainsi qu'à l'utilisation des outils informatiques
  - Organiser correctement le travail, donner les instructions utiles et contrôler de manière adéquate l'exécution des tâches par les collaborateurs
  - Prendre les mesures techniques et organisationnelles en matière de protection des données (*cf.* art. 7 LPD *cum* 8-12 OLPD)
  - Désigner, dans la mesure du possible, un conseiller à la protection des données au sein de l'entreprise
- À l'externe:
  - Contrats adaptés (contrat de travail, mandats, etc..)
  - Prêter attention aux clauses exclusives de responsabilité dans les contrats (art. 100 al. 2 et 101 al. 2 CO)
  - Ne pas sous-estimer la question du droit applicable au contrat

Protection des données de l'entreprise et risques liés

SAVOLAINEN Avocats s'applique à fournir des **services sur mesure** avec **la plus haute exigence** et un soin d'artisan.

Les **intérêts du client** sont placés au centre de la réflexion, de la stratégie et de l'action.

Les maîtres-mots dont l'Étude se réclame : **éthique**, **rigueur**, **créativité**, **engagement** et **humanité**.

SAVOLAINEN Avocats conseille ses clients et les représente en **matière pénale, civile** et **administrative**.

L'Étude est spécialisée en **droit pénal** général, **droit pénal économique**, en matière de **cybercriminalité**, droit pénal international ainsi qu'en **responsabilité de l'entreprise**.

En matière civile, la pratique de l'Étude couvre la **rédaction et le droit des contrats**, la **responsabilité civile** ainsi que le **droit du travail** notamment.

L'Étude jouit d'un réseau étendu de correspondants, tant au niveau national qu'international.

Merci de votre attention

Sylvain Savolainen

SAVOLAINEN Avocats
sylvain.savolainen@savolainen.law
022 320 14 41