BIANCHISCHWALD

NEWS

CYBERSÉCURITÉ ET COVID-19 :

La crise du COVID-19 a forcé les entreprises à prendre des mesures importantes dans des délais très courts. Beaucoup se sont tournées vers le télétravail, ce qui a eu pour effet d'accroître leur dépendance aux technologies. Les attaques cybercriminelles entraîneraient dans ce contexte des dégâts encore plus importants. Une attention particulière doit être accordée dans ce contexte aux questions juridiques.

Une partie du problème vient du fait que les entreprises ont choisi leur infrastructure informatique (*hardware*, logiciels) sans procéder à une analyse approfondie et sans former et sensibiliser leurs employés aux risques induits par l'utilisation de cette infrastructure.

Qu'entend-on par cybersécurité ?
La cybersécurité désigne la protection des systèmes informatiques, qui se composent du *hardware*, des logiciels et des données qui y sont contenues. Ces systèmes sont exposés à des menaces nombreuses et variées. L'exemple classique est celui du cybercriminel qui s'introduit sans autorisation dans un système informatique, par exemple pour prendre connaissance d'informations secrètes, ou pour paralyser ou rendre hors d'usage l'infrastructure informatique de la victime. Les cas de rançongiciel (*ransomware*) ont causé des dégâts importants ces dernières années et ont fait l'objet d'une attention médiatique particulière. Ces attaques ont pour effet de rendre inexploitables les données de la victime, cette dernière devant verser une rançon (de l'argent, des cryptomonnaies) pour récupérer ses données. Même des modifications apparemment mineures de l'infrastructure informatique peuvent entraîner des risques importants qui ne seront pas nécessairement détectés à temps. Citons à titre d'exemple le cas des employés qui se connectent à leur WiFi privé plutôt qu'au réseau interne de l'entreprise ; de nombreux autres points d'attaque sont ainsi créés, contre lesquels le responsable de la cybersécurité ne pourra généralement pas agir. Le fait que le serveur ne soit accessible que par le biais d'une connexion sécurisée (par exemple un VPN) n'y change rien.

Tout aussi courantes sont les attaques dites de *Social Engineering*, qui cherchent à exploiter les faiblesses psychologiques, sociales ou organisationnelles des victimes en conduisant ces dernières à adopter un comportement voulu. Les attaques de phishing en sont un exemple bien connu. L'agresseur se fait passer pour un tiers de confiance afin d'inciter la victime à révéler des informations secrètes (mots de passe, données bancaires ou de carte de crédit, etc.) ou à effectuer des paiements. Le recours aux méthodes de travail décentralisées rend les entreprises beaucoup plus vulnérables à de telles attaques. D'un seul coup, les interactions quotidiennes n'ont plus lieu au travers d'échanges personnels, mais par des moyens de communication électroniques, ce qui peut constituer une nouvelle cible pour les cybercriminels.

Quelles sont les questions juridiques qui se posent en matière de cybersécurité ?
La cybersécurité ne se limite pas aux risques opérationnels et financiers ou aux éventuelles atteintes à la réputation. Elle place également l'entreprise face à certaines obligations légales. La question de savoir quelles obligations doivent être respectées dans chaque cas est une question clé. Le droit suisse ne contient aucune base légale imposant de manière générale de protéger l'intégrité des systèmes informatiques. Par contre, ce devoir de protection découle explicitement ou implicitement de diverses lois règlementant des domaines particuliers du droit.

Droit pénal
Il importe en premier lieu d'examiner les règles dont la violation peut avoir des conséquences pénales. La protection des secrets professionnel, de fabrication, commercial ou du secret bancaire en sont des exemples bien connus. Il est par contre moins évident qu'une sécurité insuffisante des systèmes informatiques peut également constituer une infraction pénale (concurrence déloyale), ou encore que la violation de certaines règles en matière de protection des données est punissable.

Ces dispositions pénales ne sanctionnent en principe cependant que les infractions commises intentionnellement, et ne sont poursuivables que sur plainte. Rares seront donc les cas qui donneront lieu à une condamnation pénale. Il n'en

demeure pas moins qu'une analyse juridique doit à chaque fois être conduite, compte tenu des conséquences importantes qui pourraient trouver application.

Droit civil et droit administratif

De nombreuses dispositions de droit civil et de droit administratif doivent conduire la grande majorité des entreprises suisses à mettre en place une protection adéquate de leurs systèmes informatiques.

Tel est en particulier le cas de la législation sur la protection des données, à savoir de la Loi fédérale sur la protection des données (LPD), ainsi que de son ordonnance d'exécution. Il s'agit d'une source de droit importante en matière de protection des systèmes informatiques. La LPD prévoit par exemple expressément que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques appropriées.

En raison de la définition large de la notion de « données personnelles », cette obligation s'applique presque sans exception à toutes les entreprises, quelle que soit leur forme juridique.

L'Ordonnance concernant la tenue et la conservation des livres de comptes (Olico) prévoit pour sa part un certain nombre de règles en matière de conservation électronique de documents. En termes de cybersécurité, l'intégrité (authenticité et infalsifiabilité) et la disponibilité des documents doivent ainsi être garanties. Cette obligation doit être respectée par toutes les entreprises soumises à l'obligation de tenir une comptabilité. Il y a lieu de rappeler que l'obligation de conserver les documents découle également de dispositions légales applicables en matière fiscale et de sécurité sociale.

A cela s'ajoutent diverses normes techniques et industrielles, ainsi que des standards de bonnes pratiques (*best-practice*). Il s'agit, en particulier, de la règlementation applicable aux institutions financières, ainsi que des normes de certification ISO, qui offrent un niveau de détail plus poussé s'agissant de la mise en œuvre des diverses règles applicables, notamment en matière de protection des données. Enfin, des organismes privés prévoient de leur côté, par voie d'autorégulation, des obligations plus étendues (par exemple, des obligations de confidentialité).

Sur un autre plan, les contrats conclus par les entreprises avec leurs contreparties pourront imposer de garantir la sécurité des systèmes informatiques. Il s'agit en premier lieu des accords de non-divulgation ou de confidentialité, ainsi que de la clause accessoire de confidentialité figurant dans de nombreux contrats. D'autres clauses contractuelles peuvent également, de manière moins évidente, entraîner des obligations en matière de sécurité des systèmes informatiques. Il en est par exemple ainsi de l'obligation de rendre compte prévue par ou applicable à certains contrats, qui ne pourra être observée que si la documentation électronique produite dans ce cadre est conservée de manière sécurisée.

Le principal risque découlant de la violation des normes de droit civil est l'éventuelle obligation de réparer les dommages ainsi causés. Le montant des dommages-intérêts versés correspond au préjudice causé suite à la violation de la base légale ou de la clause contractuelle applicable. Certains contrats contiennent en outre une clause pénale, dont le montant devra être versé en sus.

La responsabilité personnelle des administrateurs (pour les SA) et des gérants (pour les Sàrl) pourrait par ailleurs être engagée en cas de manquement à l'obligation de sécurisation des systèmes informatiques. Ces personnes sont soumises à un strict devoir de diligence et doivent sauvegarder de bonne foi les intérêts de l'entreprise. Lorsqu'ils délèguent la gestion opérationnelle, les administrateurs et gérants doivent exercer la haute surveillance sur les personnes chargées de la gestion.

Autres questions juridiques

Les méthodes de travail décentralisées et le recours accru à la technologie posent d'autres questions juridiques qui vont au-delà de la cybersécurité :

- Les appareils électroniques privés des employés (ordinateur portable, téléphone mobile) peuvent-ils être utilisés à des fins professionnelles ? A quoi faut-il faire attention ? Les employés doivent-ils être indemnisés ?
- Est-il possible de placer des documents dans le « *cloud* » ? A quoi faut-il faire attention ? Une copie papier doit-elle, dans tous les cas, être conservée ?
- Un document peut-il être légalement signé sans signature manuscrite ?

De nombreux fournisseurs envisagent de proposer leurs produits et services au travers de nouveaux canaux de distribution, en particulier via Internet. La création d'une boutique en ligne en Suisse suppose le respect de diverses exigences légales (voir pour les détails la Newsletter BianchiSchwald sur le commerce électronique).

BIANCHISCHWALD

Que faut-il faire ?
Les systèmes informatiques font régulièrement l'objet d'évolutions importantes. Les menaces potentielles changent donc de manière très dynamique. Il y a par conséquent lieu d'exercer un contrôle permanent des mesures de protection des systèmes informatiques. C'est l'analyse des obligations légales en matière de cybersécurité qui permet aux entreprises de définir les mesures appropriées. Cette analyse constitue ainsi un aspect important de toute stratégie de cybersécurité. Elle doit être conduite régulièrement pour s'assurer qu'elle reste à jour et que les ajustements nécessaires sont introduits à temps.

Le recours accru au travail à distance du fait du COVID-19 constitue un motif important de réexamen de la stratégie en matière de cybersécurité. Les entreprises doivent ainsi examiner dans quelle mesure les différentes dispositions qu'elles prennent sur le plan technologique doivent être accompagnées d'intervention en matière de cybersécurité. Les questions suivantes sont utiles à se poser dans ce contexte :

- L'entreprise a-t-elle adopté un nouveau système informatique qui touche à un de ses processus essentiels ou qui revêt de toute autre manière pour elle une fonction importante ?
- Les employés ont-ils été suffisamment formés à l'utilisation du nouveau système informatique ?
- Est-ce que tous les employés sont informés des risques supplémentaires entraînés pour la sécurité des systèmes informatiques ?
- Est-il prévu de tester l'efficacité des mesures de protection des systèmes informatiques ?

Dans le contexte actuel qui voit les entreprises adapter leur organisation en réponse à une crise, il est particulièrement important d'identifier à un stade précoce les éventuels problèmes juridiques et d'adopter les solutions adéquates.

En cas de questions, veuillez vous adresser à votre personne de contact au sein de BianchiSchwald.

CHRISTOPH GASSER
Avocat, Dr. iur.
LL.M. University of Michigan
Juge suppléant au Tribunal fédéral des brevets
Associé

ADRIAN TRUTMANN
Avocat, MLaw
Collaborateur

THIERRY BURNENS
Avocat, M.A. HSG
CIPP/E
Collaborateur

BIANCHISCHWALD SARL
mail@bianchischwald.ch
bianchischwald.ch

GENÈVE
5, rue Jacques-Balmat
Case postale 5839
1211 Genève 11, Suisse
T +41 58 220 36 00
F +41 58 220 36 01

ZURICH
St. Annagasse 9
Case postale 1162
8021 Zurich, Suisse
T +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
Case postale 5410
1002 Lausanne, Suisse
T +41 58 220 36 70
F +41 58 220 36 71

BERNE
Elfenstrasse 19
Case postale 133
3000 Berne 15, Suisse
T +41 58 220 37 70
F +41 58 220 37 71