PROTÉGER VOS BASES DE DONNÉES

HISCOX

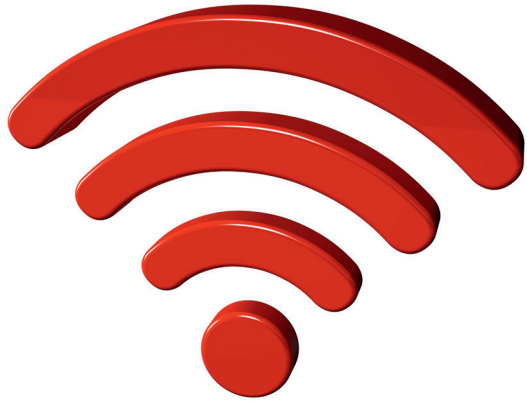
Préambule

La base de données est définie par l'article L.112-3 du Code de la propriété intellectuelle comme un "recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen".

Les **bases de données sensibles, et surtout personnelles** (données clients, salariés, partenaires, savoir-faire, produits, etc.), constituent aujourd'hui des **actifs stratégiques** pour toutes les entreprises. Ceci leur donne une valeur économique essentielle et fait de leur protection une **préoccupation cruciale** pour les dirigeants, qui doivent aujourd'hui gérer les vulnérabilités de leur système d'information face aux menaces de cyber-attaques, de vol ou d'extraction par des tiers de leurs données.

C'est pourquoi les entreprises disposent aujourd'hui d'un arsenal de mesures techniques et juridiques à mettre en place pour protéger :

- Les investissements réalisés pour constituer et faire fonctionner leurs bases de données,
- Le contenu de ces bases de données, particulièrement quand il concerne des tiers.



I. Comment protéger les investissements relatifs à vos bases de données ?

Objectif du régime spécifique dédié à la protection des producteurs de bases de données : empêcher l'extraction ou la réutilisation substantielle ou systématique de vos bases de données par des tiers, notamment par les méta-moteurs de recherche, lorsque la constitution et/ou le fonctionnement de ces bases reposent sur des investissements conséquents (financiers, humains, matériels, organisationnels, etc.).

Le producteur de base de données est celui qui "prend l'initiative et le risque des investissements correspondants". Il bénéficie d'une protection du contenu de sa base "lorsque la constitution, la vérification ou la présentation de celle-ci atteste d'un investissement financier, matériel et humain substantiel" (article L.341-1 du Code de la propriété intellectuelle).

a. Quelques mesures juridiques à mettre en place

- **Documenter vos investissements** liés à la constitution de vos bases de données (architecture, processus de collecte des données, etc.) et à leur fonctionnement (mises à jour, vérifications, upgrades, etc.) – attention, les investissements relatifs à la création des contenus ne sont pas pris en compte.
- Prévoir dans vos conditions générales d'utilisation une **limitation de l'accès par des tiers** (clients, partenaires, etc.) à vos bases de données, dans le temps, l'espace, les supports, etc.
- **Faire des constats d'huissier** à plusieurs reprises, en cas d'extraction non autorisée de données par des tiers qui les rendent ensuite disponibles sur internet.

b. Quelques conseils techniques pour vous protéger

- **Contrôler les accès à la base de données** (nombre réduit d'utilisateurs, identifiants et mot de passe forts, politique active de contrôle des accès, accès uniques ou en durée limitée, etc.).
- **Créer des coquilles** ou informations fictives dans la base pour permettre une identification de l'origine des données.
- **Intégrer dans votre base de données des adresses mails qui vous appartiennent**, de manière à recevoir les mailings qui feraient suite à une utilisation non autorisée.

II. Comment protéger juridiquement les données personnelles ?

Définition d'une donnée à caractère personnel au sens de la Loi Informatique & Libertés : information permettant, directement ou non, l'identification de personnes physiques.
Par exemple : nom, immatriculation, téléphone, photo, compte bancaire – figurant dans des fichiers salariés / clients / prospects / fournisseurs, badge d'accès, appareil mobile, intranet, etc.

a. Déclarer le traitement de données personnelles à la CNIL

Dans leur grande majorité, les traitements de données personnelles sont **soumis à déclaration à la CNIL** (Commission nationale de l'informatique et des libertés) ou **autorisation de celle-ci**. Le non-respect de cette obligation est passible de sanctions pénales. En outre, la CNIL peut infliger des amendes **allant jusqu'à 150 000 €, et, en cas de récidive, jusqu'à 300 000 €**. Ces sanctions peuvent être rendues publiques, et / ou accompagner d'une insertion de la décision de la CNIL dans la presse, aux frais de l'organisme sanctionné.

De surcroît, tout fichier de données personnelles **non déclaré à la CNIL est dit "hors commerce"** : il ne peut être ni vendu, ni cédé, ni loué, etc., parce qu'il est illicite (Cour de Cassation, arrêt du 25 juin 2013). Cela constitue donc une protection de la base.

Depuis la loi du 17 mars 2014, **la CNIL peut, en direct et sans information préalable, procéder à des contrôles en ligne** des sites internet et / ou fichiers disponibles en ligne, constater à distance les failles de sécurité, puis engager des poursuites et prononcer des sanctions.

En complément, la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes) est également habilitée lors de ses contrôles à recueillir les informations concernant d'éventuelles violations de la loi Informatique et Libertés, et à les transmettre à la CNIL pour action.

b. Respecter les critères de collecte et de traitement des données personnelles

Pour répondre aux critères de la Loi Informatique et Libertés, la collecte et le traitement de données à caractère personnel dans le cadre de bases de données internes ou externes doivent être faits dans les conditions suivantes (sauf cas particuliers) :

- Le producteur de base de données **doit informer les personnes dont les données sont collectées / traitées et, dans certains cas, obtenir leur consentement**,

- Le traitement et la collecte doivent être effectués proportionnellement à un **but précis et légitime**,
- La collecte des données doit être **loyale et licite**,
- Les données doivent être **exactes et à jour**,
- Les données doivent être **conservées pendant une durée limitée** au regard du but recherché (c'est le principe consacré du droit à l'oubli),
- Des **mesures de sécurité** doivent être mises en place pour lutter contre les risques de destruction, perte, diffusion ou accès non autorisé aux données.

Exemples de cas sanctionnés par la CNIL :

- Absence sur votre site internet d'un formulaire de recueil du consentement des internautes concernant les cookies,
- Impact d'une cyber-attaque qui a mis en libre accès sur internet les données personnelles dont vous êtes responsable.

Enfin, le transfert des fichiers de données personnelles en dehors de l'Union Européenne (UE) n'est autorisé que sous réserve de garanties particulières. Pour simplifier leurs procédures, les entreprises avec des filiales hors de l'UE ont la possibilité d'adopter un **code de conduite appelé BCR** (Binding Corporate Rules) : le respect de ce code à l'intérieur de l'entreprise permet le transfert des données partout dans le monde entre les entités qui la composent.

Pour en savoir plus : http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/

Parmi les évolutions réglementaires à venir, nous pouvons citer une proposition de règlement européen qui impose, entre autres, une **étude d'impact préalable à certains traitements de données personnelles** présentant des risques spécifiques pour les droits et libertés des personnes.

Conclusion

Le cyber-risque fait désormais partie des menaces que les dirigeants d'entreprises doivent impérativement appréhender et anticiper. Afin de préserver la confiance des investisseurs, des partenaires et des clients, les entreprises doivent donc faire évoluer régulièrement leur politique de sécurité IT, mettre en place des plans de réponse avec l'aide d'experts, et **transférer à un assureur spécialiste le risque financier** que représente une cyber-attaque ou une perte de données.

À propos de Hiscox

Fondé en 1901, Hiscox est un groupe international d'assurances spécialisées coté sur le London Stock Exchange (HSX). Hiscox a trois principales composantes : Hiscox London Market, Hiscox Re et Hiscox Retail regroupant plus de 1 500 collaborateurs.

Hiscox est présent depuis 25 ans dans le secteur des métiers de l'informatique (20000 clients IT en Europe dont 7500 en France), et depuis plus de cinq ans dans le domaine de la cybercriminalité, avec 30 souscripteurs dédiés aux risques technologies-médias-télécoms.

En se spécialisant dans des secteurs bien définis et en plaçant l'assuré au cœur de ses préoccupations, Hiscox a mis au point des solutions sur mesure pour garantir les professionnels contre les conséquences en cas de perte/vol de données.

En France, Hiscox dispose de bureaux à Paris, Lyon et Bordeaux. Hiscox France s'appuie sur ses 110 collaborateurs pour proposer une large gamme d'assurances conçues pour répondre aux besoins des particuliers, des professionnels et des collectivités.

Pour plus d'informations : www.hiscox.fr

À propos de Bird & Bird

Le cabinet Bird & Bird a été fondé à Londres en 1846 et dès ses débuts s'est investi dans la protection des idées et innovations de son temps. Aujourd'hui, Bird & Bird est un cabinet d'avocats international avec 26 bureaux répartis en Europe, Asie et Moyen-Orient. Avec plus de 1100 professionnels du droit, le cabinet couvre la plupart des domaines du droit privé et public des affaires et de la fiscalité.

Un des atouts du cabinet est sa connaissance approfondie de secteurs clés de l'économie tels que l'aviation, l'énergie, les services financiers et l'assurance, les technologies de l'information, les communications électroniques ou encore les sciences de la vie.

En France, le cabinet est présent à Paris et à Lyon et rassemble plus de 90 avocats dont 22 associés. Depuis de nombreuses années, Bird & Bird France a acquis une position de leader dans les secteurs des technologies de l'information, de la protection des données personnelles, de l'aviation, des communications électroniques et des médias. Il est également l'un des acteurs incontournables en propriété intellectuelle (marques, noms de domaines, droits d'auteur et brevets).

HISCOX

19 rue Louis Le Grand 75002 Paris
T 0810 50 20 10
F 0810 00 71 02
E hiscox.info@hiscox.fr

www.hiscox.fr

En partenariat avec

Bird & Bird

Bird & Bird AARPI
Centre d'Affaires Edouard VII
3 square Edouard VII 75009 Paris

www.twobirds.com