DS NEWSLETTER savoir, faire

NEWSLETTER – INFORMATIONS JURIDIQUES PROPOSÉES PAR LE CABINET DS AVOCATS

La charte informatique, un outil privilégié de la sécurité des systèmes d'information de l'entreprise

ASIE

Nombreux sont les articles qui font état de la cybercriminalité et du coût que celle-ci occasionne pour les entreprises (risque de perte de données, atteinte au patrimoine informationnel, risque en termes d'image et de réputation, voire risque pour la continuité de l'activité et la survie de l'entreprise). Sensibilisées depuis plusieurs années sur l'importance de la sécurisation de leurs systèmes d'information, et parfois peu rassurées par les pratiques de leurs sous-traitants voire sous-sous-traitants (dont les défauts de sécurité sont parfois aussi à l'origine de la réussite de certaines attaques), les entreprises sont également l'objet de dispositions légales et réglementaires les obligeant à mettre en œuvre des mesures de sécurité élaborées et parfois contraignantes.

Ainsi, depuis l'entrée en vigueur de la loi Cyber-Sécurité chinoise, le 1er juin 2017, les entreprises, ont vu leurs obligations s'accroitre pour assurer la sécurité de leurs systèmes d'information et celle des informations et données personnelles qui y transitent ou y sont hébergées : mise en place de procédures internes tant pour prévenir que résoudre les incidents de sécurité, notification des incidents aux autorités, voire aux personnes concernées lorsqu'il s'agit d'un incident affectant des données personnelles, hébergement des données personnelles et des « données importantes » sur le sol chinois, etc.

La mise en place d'une politique de sécurité du système d'information (PSSI) est donc essentielle pour fixer le cadre de la cyber-sécurité à mettre en œuvre dans l'entreprise et surtout celui des contrôles. La PSSI décrit les objectifs et mesures générales de l'entreprise, en matière de sécurité du système d'information. Elle vise à assurer un compromis entre les objectifs stratégiques de l'entreprise et le contrôle requis pour la protection de son système d'information.

Mais quid si l'incident de sécurité provient de l'intérieur de l'entreprise ? Par exemple, un système de vidéo-surveillance a permis de détecter les agissements d'un salarié et celui-ci a été sanctionné par l'employeur mais la mise en place du système de surveillance n'avait pas respecté le formalisme du droit du travail et/ou les exigences applicables en matière de protection des données personnelles. **Dans une telle hypothèse, la preuve sera considérée comme irrecevable devant les tribunaux et le salarié indûment sanctionné pourra obtenir indemnisation**. Il faut aussi garder à l'esprit qu'une PSSI n'a qu'un objectif d'organisation interne et ne peut prévoir des règles directement opposables aux salariés et aux prestataires externes. C'est là que la charte informatique entre en action…

QU'EST-CE QU'UNE CHARTE INFORMATIQUE ? A QUOI SERT-ELLE ?

La charte informatique est un document juridique qui a pour objet (i) de fixer les règles d'utilisation des ressources informatiques et des outils de communication de l'entreprise et (ii) de préciser les droits et obligations des utilisateurs (salariés, prestataires externes qui auraient besoin d'accéder au système d'information de l'entreprise) afin d'en assurer la sécurité. L'enjeu consiste à protéger le patrimoine informationnel de l'entreprise. **La charte permet, à ce titre, de valider et de mettre en conformité les modalités de cyber-surveillance et de cyber-protection des salariés ainsi que la collecte licite de preuves électroniques nécessaires en cas de contentieux.**

L'élaboration d'une charte se gère en mode projet et requiert l'intervention de plusieurs directions : sécurité informatique, juridique, RH, etc. Le document doit se fonder sur la PSSI existante et être en cohérence avec celle-ci.

L'employeur peut faire figurer la charte en annexe du contrat de travail mais le plus souvent, la charte informatique sera annexée au règlement intérieur

de l'entreprise, qui est adressé au salarié concomitamment à son contrat de travail. Cela évite ainsi d'avoir à négocier le contrat de travail avec chacun des salariés ou de faire un avenant à celui-ci à chaque mise à jour de la charte.

QUE DOIT CONTENIR UNE CHARTE INFORMATIQUE ?

Le contenu de la charte informatique varie en fonction du contexte, des contraintes, des objectifs et besoins de l'entreprise qui l'impose. Il faut préciser, en outre, qu'il n'y a pas de grands principes ou interprétations qui se dégagent de la jurisprudence des tribunaux chinois en la matière, leur analyse se fait au cas par cas. Aussi, nous recommandons vivement aux entreprises de prévoir les conditions d'utilisation de leurs ressources informatiques et les modalités de contrôle de leurs salariés dans la charte. Dans tous les cas, la charte devra prendre en compte l'équilibre existant entre les intérêts de l'entreprise (besoins de sécurité, pouvoir de direction de l'employeur, etc.) et ceux des salariés. Le contenu de la charte ne doit pas contrevenir aux dispositions légales et réglementaires en vigueur ni imposer des obligations trop contraignantes qui contreviendraient à certaines libertés ou droits dont jouissent les salariés, comme le droit à la vie privée.

La charte devrait au moins comporter les éléments suivants :

1. Le champ d'application de la charte (salariés, intérimaires, stagiaires, prestataires externes, entités concernées, etc.), ainsi que les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'entreprise ;

2. Les moyens d'authentification utilisés par l'entreprise (identifiants/mots de passe, badges, empreintes digitales, reconnaissance faciale, contour de la main, etc.) ;

3. Les règles de sécurité auxquelles les utilisateurs doivent se conformer, telles que notamment de signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ; de ne jamais confier son identifiant/mot de passe à un tiers ; de ne pas installer, copier, modifier, détruire des logiciels sans autorisation ; de ne pas installer de VPN ; de verrouiller son ordinateur dès que l'on quitte son poste de travail ; de ne pas accéder ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ; de respecter les procédures préalablement définies par l'entreprise afin d'encadrer les opérations de copie des données sur des supports amovibles (clé USB, disque externe, etc.), de ne pas consulter certains sites internet, etc. ;

4. Les modalités d'utilisation des outils informatiques et de télécommunications mis à disposition comme :

- le poste de travail (espace de stockage individuel ; possibilité ou non pour le salarié de stocker des fichiers personnels sur son poste ; conditions dans lesquelles l'employeur peut accéder aux fichiers stockés sur le poste d'un salarié, etc.);
- les équipements nomades (notamment dans le cadre du télétravail) ;
- les conditions d'utilisation des dispositifs personnels ;
- l'Internet (ex : usage toléré s'il n'affecte pas la productivité d'un salarié, interdiction de consulter certains sites, interdiction de télécharger des films, jeux vidéo, etc.);
- l'usage des réseaux sociaux (WeChat, Weibo, etc.) et les règles en matière de communication ;
- la messagerie électronique (règles de séparation entre emails professionnels et personnels ; rappel des règles en matière de communication via la messagerie professionnelle de l'entreprise et de gestion des preuves ; usage par le salarié de sa boite e-mail professionnelle à des fins personnelles toléré ou non ; conditions d'accès par l'employeur au contenu des messages reçus et envoyés par un salarié, par exemple en cas de vacances du salarié, etc.) ;
- l'usage des téléphones (à des fins professionnelles exclusivement ou usage personnel également toléré ? l'employeur peut-il lire les SMS reçus ou envoyés par un salarié sur un téléphone portable ?)

1. Les conditions d'administration du système d'information, et l'existence, le cas échéant, des outils de contrôle et de surveillance utilisés (système de traçabilité, géolocalisation, vidéosurveillance, écoutes téléphoniques, etc.)

2. Les responsabilités et sanctions encourues en cas de non-respect de la charte (sanctions disciplinaires, voire poursuites pénales, dans certains cas).

COMMENT RENDRE LA CHARTE OPPOSABLE AUX SALARIÉS ET AUX PRESTATAIRES ET LUI DONNER UNE FORCE CONTRAIGNANTE ?

Pour être opposable aux salariés, la mise en place d'une charte informatique doit respecter un certain formalisme. A défaut, elle n'a pas de valeur contraignante.

Dans les entreprises qui n'ont ni syndicat ni congrès des représentants des employés, le projet de charte devra être soumis pour avis et discussion à l'ensemble des salariés. L'employeur devra tenir compte des commentaires qui lui sont transmis mais n'est pas tenu de tous les accepter. La version finale de la charte sera ensuite adressée à tous les salariés par email avec accusé de réception ou remise contre signature (à des fins de preuve).

Dans les entreprises qui disposent d'un congrès des représentants des employés et/ou d'un syndicat, le projet de charte devra d'abord être soumis au congrès et au syndicat pour avis et discussion. La version finale de la charte sera ensuite adressée à tous les salariés par email avec accusé de réception ou remise contre signature (ici aussi à des fins de preuve).

Concernant les prestataires, pour leur rendre la charte informatique opposable, il conviendra d'annexer celle-ci au contrat de prestations de services qui les lie avec l'entreprise.