dposystem

(In)sécurité du système d'information : Panorama des responsabilités

Face à un problème de sécurité du système d'information dont ils ont la charge, les professionnels de l'informatique, et en particulier les DSI et les RSSI, connaissent souvent mal leur responsabilité juridique. L'appréciation de la faute du DSI ou RSSI et donc la sanction seront d'autant plus sévères que sa mission induit de grandes facilités d'accès et de contrôle d'informations à caractère confidentiel. dposystem fait le point avec vous !

Quelle responsabilité pour le DSI/RSSI[1] ?

Il existe deux types de responsabilités auxquelles peuvent être confrontées les équipes DSI : la responsabilité civile et la responsabilité pénale. Il est important de bien distinguer les deux avant d'aller plus loin.

Responsabilité civile

Vise une réparation pécuniaire du préjudice subi

En **responsabilité civile**, le DSI ou le RSSI pourra être tenu responsable suite à une faille de sécurité des systèmes d'information en cas d'inexécution d'une obligation contractuelle ou de faute, intentionnelle ou non, commise par le DSI/RSSI ou par une personne dépendant du DSI/RSSI.

Responsabilité pénale

Tente d'obtenir la punition du justiciable

La **responsabilité pénale** est une **responsabilité personnelle**. L'infraction se mesure selon trois éléments constitutifs :

- Élément légal : étape de qualification de l'infraction
- Élément matériel : identification des actes de l'infraction
- Élément intentionnel : volonté (consciente et libre) de l'auteur

Il peut arriver que le RSSI soit confronté à un ordre hiérarchique d'enfreindre la loi. Même dans ce cas, sa propre responsabilité peut être engagée. La jurisprudence considère que « l'ordre reçu d'un supérieur hiérarchique ne constitue pas, pour l'auteur d'une infraction, une cause d'irresponsabilité pénale ».

A fortiori, la responsabilité au sein d'une entreprise, qu'elle soit civile ou pénale, incombe au chef d'entreprise. Néanmoins, ce dernier peut déléguer son pouvoir à ses équipes (ici DSI/RSSI) et donc les responsabilités associées aux risques corrélés.

FOCUS : la délégation de pouvoir

A pour objet et pour effet d'opérer un transfert des responsabilités civile et pénale du chef d'entreprise vers le préposé délégataire, DSI ou RSSI.

Trois éléments caractérisent la délégation de pouvoir :

1. autorité : la personne investie de la délégation doit avoir un pouvoir de commandement tel que les salariés appliquent ses directives.
2. compétences : la personne investie de la délégation doit avoir les compétences techniques et la maîtrise des textes légaux dont elle aura la charge de contrôler l'application ;
3. moyens : la personne investie de la délégation doit disposer d'un budget suffisant pour mettre en œuvre les mesures nécessaires et maîtriser les risques identifiés de l'entreprise.

A noter que la délégation de pouvoir doit être précise, permanente et que le chef d'entreprise a obligation d'informer le salarié des conséquences juridiques de cette délégation.

[1] http://www.feral-avocats.com/fr/publication/rssi-quelles-responsabilites/

Quelle responsabilité civile en cas d'agissements répréhensibles d'un salarié ?[2]
En effet, la responsabilité civile de l'entreprise ou de l'employeur peut être mise en cause si une faute a été commise par un salarié, sauf s'il est possible de démontrer qu'il y a abus de fonction.

Exemple avec l'affaire Escota : Un employé de l'entreprise a tenu des propos diffamatoires à l'encontre d'une société concurrente sur un blog satirique. Le blog, bien qu'hébergé par un tiers, est administré par le salarié à son domicile, le soir, au moyen de l'ordinateur portable mis à sa disposition par l'entreprise. Ce cas a fait jurisprudence, les juges ont déclaré l'employeur du créateur du blog responsable de contrefaçon car ils ont jugé que c'est dans l'exercice de ses fonctions que le salarié a trouvé « l'occasion et les moyens de sa faute ». Le site a été réalisé sur le lieu de travail grâce aux moyens fournis par l'entreprise d'une part et la création de sites internet ou de fournitures d'informations sur des pages personnelles n'étaient pas spécifiquement interdites d'autre part.
Ce cas permet de souligner l'importance que revêt **l'interprétation des chartes de bon usage des ressources informatiques de l'entreprise**. Ces documents, qui sont autant de véritables guides comportementaux, doivent en particulier permettre de dessiner très précisément les contours de l'usage à des fins privés toléré par l'entreprise, lequel comportera par exemple les critères de définition suivants :

- un usage non susceptible d'amoindrir les conditions d'accès professionnel
- ne mettant pas en cause la productivité de l'utilisateur
- ne portant pas atteinte aux intérêts ou la réputation de l'entreprise
- ni de nature à causer un quelconque préjudice à un tiers.

Quelle responsabilité pénale du fait d'un comportement délictueux d'un salarié ?
En cas de téléchargement illégal au travail : Le salarié a commis une infraction pénalement répréhensible dans le cadre de son emploi, en téléchargeant des fichiers pirates (audios, vidéos ou logiciels contrefaits) ou des images pédophiles par exemple depuis le système d'information de son entreprise.
La responsabilité pénale du chef d'entreprise ou du DSI/ RSSI en cas de délégation de pouvoir, peut tout à fait être engagée pour toute infraction causée dans l'entreprise par un préposé dans la mesure où le chef d'entreprise est tenu d'une obligation de surveillance et de contrôle sur le fonctionnement de l'entreprise. Cependant, les cas de condamnation du dirigeant sur ce fondement sont très rares. En effet, pour pouvoir être retenue, la responsabilité pénale de l'employeur nécessiterait de démontrer sa participation intentionnelle à la commission de l'infraction, scénario qui serait plutôt exceptionnel par rapport à l'hypothèse la plus courante qui est que le salarié agit à l'insu de cet employeur.
Ainsi, dans un jugement rendu par le Tribunal correctionnel du Mans le 16 février 1998 où des images pédophiles avaient été téléchargées par un salarié sur l'Internet, la responsabilité du dirigeant n'a pas été recherchée sur le plan pénal.
Toutefois, il en aurait très certainement été autrement s'il avait été démontré que le dirigeant avait été informé du comportement délictueux sans rien faire pour le faire cesser. Il est donc fortement recommandé de veiller à dénoncer les faits auprès des autorités de police. L'abstention ou le silence « en connaissance de cause » étant alors susceptible de se transformer en aide ou assistance à la commission du délit.
En conclusion, le RSSI doit affirmer son rôle d'organisateur de la gestion des risques, à défaut de quoi il peut apparaitre comme le bouc émissaire du premier incident d'ampleur. Les évolutions réglementaires exigent que les organisations mènent des démarches de mises en conformité. Celles-ci contribuent à la compréhension des enjeux de la gestion des risques et du rôle de RSSI. C'est un élément fondamental de l'évolution du métier du RSSI.

Une question ?
Prenez contact avec nous !
https://dpo.netsystem.fr/#contactez-nous

[2] https://actes.sstic.org/SSTIC06/RSSI_droits_et_responsabilites/SSTIC06-article-Barel-RSSI_droits_et_responsabilites.pdf