Secret des affaires et données personnelles : la sécurité numérique en question

les faits **À l'heure du big data et du tout numérique, nombreux sont les textes qui protègent les entreprises contre le piratage de leurs données stratégiques. Dans le même temps, leurs obligations en matière de sécurité numérique ne cessent de croître, imposant la mise en œuvre de mesures organisationnelles de protection de plus en plus sophistiquées.**

Accès frauduleux à un système de données, entrave au fonctionnement des systèmes d'information, protection sui generis du producteur de bases de données : l'arsenal juridique visant à protéger les informations stratégiques des entreprises s'étoffe constamment. Derniers en date, la proposition de loi sur le secret des affaires adoptée par le Sénat le 18 avril 2018 qui sanctionne l'usage illicite d'informations secrètes, ou le Règlement européen sur la protection des données personnelles (RGPD), entrant en vigueur le 25 mai prochain. Cependant, qu'elles visent l'activité économique d'une société (secrets industriels, procédés de fabrication, informations financières) ou qu'elles revêtent un caractère personnel (données clients, fournisseurs et collaborateurs), les données des entreprises doivent être gouvernées par des règles de sécurité numérique, qui peuvent conditionner leur protection. C'est ainsi qu'une information sera protégée au titre du secret des affaires notamment si elle a fait l'objet « *de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret* ». À la lecture des discussions ayant entouré le vote de ce texte, ces mesures de protection « raisonnables » pourraient aller de la

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS
PRD avocats

simple mention explicite du caractère confidentiel d'une information à l'adoption de réelles mesures techniques et organisationnelles intégrées par les entreprises. Ces démarches ne sont pas sans rappeler les obligations fixées par le RGPD relatives à la sécurité des données personnelles dont il convient de s'inspirer. En effet, ces deux textes tendent tous deux à responsabiliser les entreprises face à la gestion de leurs données et aux cyber-menaces. Les dispositions du RGPD imposent l'intégration de la protection des données dès la conception d'un service et la mise en place d'une politique, de mesures et d'outils internes garantissant une protection optimale des données (« privacy by design », études d'impact, évaluation des risques, notification de failles de sécurité). À la lumière de ce texte, la protection des secrets d'affaires pourrait alors également impliquer, en fonction de la nature des informations à protéger et au-delà d'une sécurisation des réseaux informatiques, l'intégration d'une politique et de procédures internes organisant et encadrant strictement la protection des données financières, commerciales et industrielles de l'entreprise, comme la mise en place d'accords de confidentialité, de procédures de formations internes et l'adoption de restrictions d'accès physiques et électroniques adaptées au contenu des informations protégées. ■

ce qu'il faut retenir **La protection des secrets d'affaires et celle des données personnelles convergent vers un enjeu commun : l'instauration d'un cadre juridique permettant une sécurisation numérique optimale. Dans un souci de rationalisation de temps et des coûts, les entreprises ont tout intérêt à appréhender conjointement ces deux problématiques.**

Responsabilité des internautes négligents

Un client avait reçu plusieurs e-mails portant le logo imité de sa banque, l'invitant à renseigner ses données personnelles et ayant conduit à la soustraction frauduleuse de plus 7 000 € sur son compte. Par un arrêt du 28 mars 2018, la Cour de cassation retient pourtant la négligence fautive du client pour casser la décision de la Cour d'appel et exclure la garantie de sa banque en considérant qu'un utilisateur normalement attentif aurait dû se douter qu'il s'agissait de hameçonnage.

Facebook condamnée à transmettre les données d'un utilisateur

Une page Facebook usurpait l'identité d'un boulanger en jetant le discrédit sur son activité commerciale par la publication de photos représentant les locaux de la boulangerie dans un état déplorable. Les demandes formulées pour faire supprimer cette page s'étant révélées infructueuses, la victime a assigné Facebook en référé et a obtenu du juge que cette dernière lui communique les données de nature à identifier l'usurpateur.

Intelligence artificielle et conditions de travail

La Cour de cassation a considéré, dans un arrêt du 12 avril 2018, que l'introduction auprès de chargés de clientèle d'une société d'un programme informatique reposant sur l'intelligence artificielle, conçu dans le seul but d'aider les salariés à traiter les nombreux courriels reçus en les triant par ordre de priorité, n'avait pas de conséquences majeures sur les conditions de travail de ces derniers nécessitant une expertise du CHSCT.