DROITS RÉSERVÉS

RAYNALD WAUTERS (Ai. 184) est le fondateur d'eMana [1], éditeur français, basé à Aix-en-Provence, d'une solution de messagerie «intelligente», à la fois boîte aux courriels, armoire de classement et outil de travail collaboratif. Le Gadzarts a travaillé chez Capgemini et Orange. Expert de la souveraineté, la sécurité et la diffusion des données, il a participé au développement des systèmes d'information et de commandement pour l'état-major de l'armée de terre.

[1] https://www.emana.io

POURQUOI FAUT-IL PROTÉGER SES DONNÉES

Ce n'est pas un film d'anticipation : il y a quatre ans, le Congrès américain a voté une loi autorisant les États-Unis à saisir les données informatiques émises à l'étranger. Il ne s'agit donc pas de cyberpiraterie à proprement parler. Mais savez-vous qui a le droit d'accéder aux données de votre entreprise ? Quels risques courez-vous ? Réponses par Raynald Wauters (Ai. 184), fondateur de l'éditeur de messagerie élaborée eMana.

Petit préambule sur deux lois que tout oppose de part et d'autre de l'Atlantique. Côté européen, le règlement général sur la protection des données (RGPD) a été adopté en avril 2016 par l'Union en vue de protéger davantage les données informatiques de sa population. Chaque entreprise européenne est à présent obligée de décrire sa politique quant aux données qu'elle récupère. Côté américain, le «Cloud Act», loi fédérale de mars 2018, permet aux agences de renseignement d'obtenir toutes les informations stockées sur leurs serveurs «cloud» — que ces données émanent des États-Unis ou d'ailleurs. En février 2019, «l'Usine nouvelle» résumait : «Le "Cloud Act" est un passe-droit sur les données pour les autorités américaines.»

ALERTES RÉPÉTÉES DE LA CNIL

Remontons le temps. En avril 2016, le «Privacy Shield», bouclier de protection des données confidentielles, imposait aux entreprises américaines d'appliquer le RGPD européen. C'était un accord juridique entre l'Union européenne et les États-Unis d'Amérique. Toutefois, en contradiction avec l'esprit du RGPD, les données européennes pouvaient être transférées vers les États-Unis ! Voilà pourquoi le «Privacy Shield» a été invalidé en juillet 2020 par la Cour de justice de l'Union européenne. Depuis, plusieurs alertes ont été émises. Ainsi, le 31 mai 2021, la Cnil demande aux professionnels de l'enseignement supérieur et de la recherche de ne plus utiliser Google Docs et d'opter pour des solutions européennes. Le 15 septembre 2021, sur une note du Premier ministre, la direction interministérielle du Numérique interdit le déploiement d'Office 365, suite logicielle de Microsoft, dans les ministères. Plus récemment, en janvier, l'armée suisse a interdit à ses soldats d'utiliser la messagerie WhatsApp, de Meta (Facebook), qui, parce qu'elle est «soumise au "Cloud Act", permet aux Américains d'accéder aux données même si les serveurs sont en dehors des États-Unis». En février, la Cnil a mis en demeure un gestionnaire de site web pour utilisation de Google Analytics, à la suite d'une plainte pour transfert de données vers les États-Unis, en violation du RGPD.

RISQUES D'ESPIONNAGE INDUSTRIEL

De façon concrète, tout ce qui se trouve sur les ordinateurs d'une entreprise est passé par messagerie de courriels («e-mails»), messagerie instantanée, gestionnaire de la relation avec la clientèle (CRM) ou progiciel de gestion intégrée (ERP). Ces données contiennent le savoir-faire de l'entreprise, sa stratégie ainsi que des infos personnelles. Si l'entreprise utilise un logiciel américain en mode web, le «Cloud Act» s'applique : les États-Unis ont la main dessus.

Nos métiers d'ingénieur nous amènent à mesurer nos risques professionnels et personnels. Sans dresser un tableau trop noir, plusieurs risques liés au «Cloud Act» et au non-respect du RGPD sont envisageables. D'un point de vue stratégique, l'accès aux données de l'entreprise peut se retourner contre elle et ses dirigeants. Les Européens sont de plus en plus soucieux à propos de la sécurisation et de la protection de leurs données. En France, au début des années 2000, on enregistrait 4 000 plaintes par an à la Cnil. En 2019, après le RGPD, plus de 14 000 plaintes ont été déposées.

La surveillance est à considérer. Il ne suffit plus de dire que les données sont localisées en Europe pour échapper à l'extraterritorialité de la loi américaine [1]. Tous les fournisseurs de services «cloud» américains, de Microsoft à IBM en passant par Amazon et autres éditeurs de services SaaS [2] ayant des liens capitalistiques avec une société américaine, doivent, s'ils en reçoivent l'injonction, fournir aux autorités américaines les données stockées sur leurs serveurs, et ce, quel que soit l'emplacement de ces derniers.

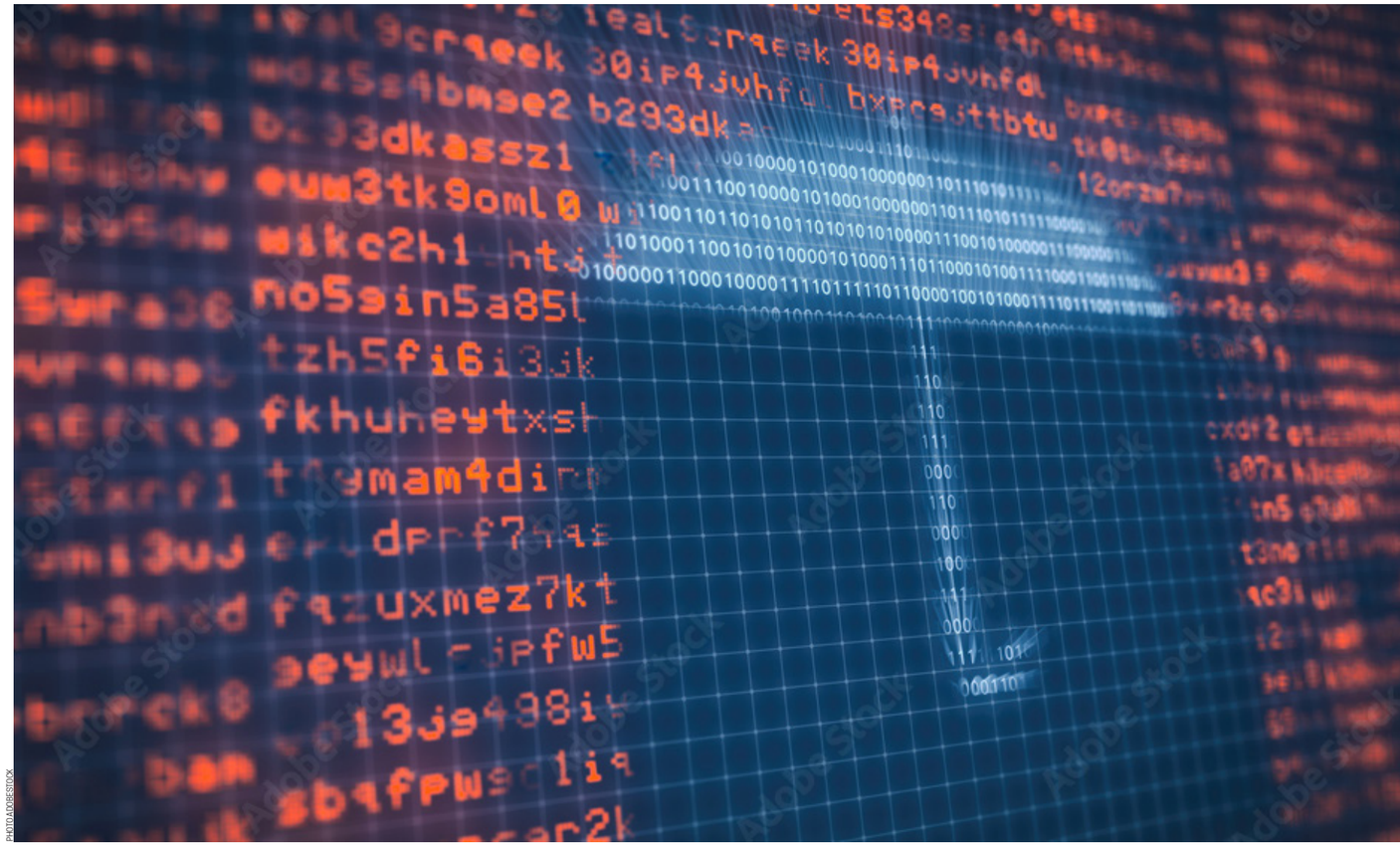

PHOTO ADOBESTOCK

DANGERS LÉGAUX ET FINANCIERS

La majorité des directeurs des systèmes d'information des sociétés du Cac 40 et du top 100 sont préoccupés par le «Cloud Act» et les désormais possibles indiscrétions de leurs prestataires. Toujours dans le cadre de l'extraterritorialité des lois américaines, un dirigeant européen peut être poursuivi par la justice des États-Unis. Les données de son entreprise sont alors saisies sans même qu'il en soit informé. L'exemple de la Royal Bank of Scotland est édifiant. La banque a accepté de payer 4,9 milliards de dollars pour une faute de fait. Le bureau du procureur américain a énoncé les faits détaillés en s'appuyant sur sa lecture des courriels des dirigeants de la banque.

Si les données de l'entreprise sont transférées sans cadre légal, celle-ci risque une amende pouvant aller jusqu'à 4 % du chiffre d'affaires mondial. Les 5 300 entreprises américaines qui s'appuyaient sur le «Privacy Shield» sont elles-mêmes contraintes d'ajuster leurs pratiques pour demeurer dans la légalité. Et donc, les milliers d'organisations européennes qui utilisent leurs solutions sont passibles d'amendes. Les sous-traitants ne sont pas à l'abri non plus. Il y a un an, en janvier 2021, la Cnil a indiqué avoir non seulement sanctionné un responsable de traitement des données mais également son sous-traitant pour un manquement à leur obligation découlant de l'application du RGPD. Quelles solutions pour les entreprises européennes ? Le plus simple reste de passer par des services hébergés en Europe dès que possible pour limiter les risques juridiques.

Raynald Wauters (Ai. 184)

[1] Lire aussi en p. 20 de ce numéro.

[2] Le «software as a service», ou logiciel exploité comme un service, est un modèle commercial : le plus souvent payé par abonnement, le logiciel est installé sur un serveur éloigné, et non plus sur l'ordinateur du client.

Quelques parades

La direction interministérielle du Numérique, organisme d'État, a dressé une liste d'éditeurs français : **https://catalogue.numerique.gouv.fr/catalogue**

Le collectif PlayFrance.Digital se mobilise pour une action nationale et collective pour une Europe forte du numérique : **https://www.lesacteursdunumerique.fr**

Une liste des acteurs français du numérique, à utiliser à la place de solutions américaines, est disponible sur Solainn : **https://solainn.digital**