Les enjeux des données RH pour les DSI

les faits **Un an après l'entrée en vigueur du RGPD, les pléthoriques implications en matière RH soulèvent encore des interrogations. Le référentiel de la Cnil sur la gestion des ressources humaines, issu de la consultation publique achevée le 31 mai, est attendu avec intérêt. Un sujet qui exige une coopération étroite entre DRH et DSI afin d'appréhender avec justesse les enjeux tant managériaux que juridiques et contentieux spécifiques à cette matière.**

La confidentialité doit être d'autant plus renforcée en RH qu'il s'agit de données dites «à risque», comme le numéro de Sécurité sociale, voire de données «sensibles» dont le traitement est en principe interdit, comme par exemple les informations tenant à la santé du salarié. Pour cette raison, la gestion des données RH est encadrée aussi bien par le Code du travail que par le RGPD. Un ensemble normatif complexe que connaît le DRH, mais qui pèse en partie sur le DSI, chargé de définir les habilitations et de mettre en place les mesures de sécurité. La gestion des données RH nécessite de bien identifier la diversité des intervenants, parfois extérieurs à l'entreprise. Un principe est fondamental : on ne peut accéder qu'aux données personnelles nécessaires à l'exercice de ses fonctions. Les documents accessibles doivent donc être différents pour un recruteur (diplômes…), un employé de gestion du personnel (maladie, retraite, mutuelle…) ou un supérieur hiérarchique (évaluation, rémunération…). Il incombe au DSI, en harmonie avec le DRH, de définir des profils d'habilitation en conséquence, associés à des identifiants individuels et des mots de passe robustes, et de tracer les accès et prévoir un système de journalisation. Pour une meilleure efficacité, cette politique d'accès doit tout d'abord être formalisée dans une charte informatique opposable et contraignante.

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

Des dispositions spécifiques doivent également être intégrées dans les contrats de travail des salariés et notamment ceux en charge de la gestion des données de leurs collègues. Il serait aussi souhaitable de régulariser des accords avec le CSE (Comité social et économique) sur la transmission de données personnelles. Les sous-traitants ne doivent pas être oubliés et il convient dès à présent d'inclure les clauses contractuelles sur le traitement de ces données. À cet encadrement de la confidentialité doit s'ajouter une réflexion approfondie sur les délais de conservation desdites données, lesquels sont particulièrement disparates et emportent de lourdes conséquences en cas de litige sur la prescription et la charge de la preuve. En effet, si la majorité des données d'un salarié doit être conservée le temps de son parcours dans l'entreprise, les exceptions résultant des obligations et contraintes particulières de l'employeur s'avèrent nombreuses et difficilement conciliables avec le principe de minimisation. Entre autres, les dossiers de candidats non retenus ne peuvent être conservés plus de deux ans après le dernier contact. Que dire des bulletins de paie qui doivent être conservés cinq ans après leur émission alors qu'un procès en discrimination peut porter sur plusieurs dizaines d'années ? Il appartient à chaque entreprise d'établir son propre référentiel de délais de conservation des données et de l'implémenter au terme d'un échange continu entre le service des RH, qui exécute les mesures au quotidien, et le DSI, qui met en place un ensemble de processus automatisés : archivage intermédiaire pour les données conservées en cas de contentieux, anonymisation des données statistiques, relance automatique des candidats qui n'ont pas été contactés depuis deux ans, etc.

ce qu'il faut retenir **Les enjeux des données RH sont nombreux, transverses et durables. Leur exacte et complète appréhension est essentielle puisqu'ils peuvent devenir une source de désorganisation et même de déstabilisation en matière contentieuse.**

Confirmation de la proportionnalité d'une sanction de la Cnil

Le Conseil d'État a retenu par une décision du 17 avril 2019 que la sanction de 75 000 € infligée par la Cnil à l'Association pour le développement des foyers (Adef) en juin 2018 était proportionnée à la gravité de ses manquements. L'association avait fait preuve d'un défaut de sécurité élémentaire «*qu'il aurait été facile de prévenir*», permettant l'accès de tiers non autorisés aux données (bulletins de salaire, avis d'imposition…) des personnes sollicitant son aide.

Pas de concurrence déloyale entre deux sites au design banal

Par un arrêt du 11 mars 2019, le Tribunal de commerce de Paris a jugé qu'il n'y avait pas d'acte de concurrence déloyale entre deux sites de voyage ressemblants, mais aux couleurs et au design couramment utilisés sur Internet par des sites d'agences de voyage, ne pouvant ainsi être considérés comme de véritables signatures visuelles. Le Tribunal a donc considéré, eu égard à la banalité des sujets traités que ces ressemblances n'engendraient aucun risque de confusion.

Perte de données : réparation limitée du préjudice

Le Tribunal de commerce de Nanterre a limité, dans un jugement du 23 avril 2019, l'indemnisation du préjudice subi par une entreprise suite à une perte de données fautive de son prestataire. En l'absence de faute grave de ce dernier, les dommages et intérêts alloués au client lésé ont ainsi été limités à la contrepartie financière du coût de la reconstitution des fichiers perdus nécessaires à la poursuite de son activité.