Vol de données : la Cnil sanctionne Orange

À la suite du piratage informatique de données ayant touché plus de 1,3 million de clients de l'opérateur en avril 2014, la Cnil a prononcé le 25 août un avertissement public à l'encontre d'Orange après avoir contrôlé cette société et l'un de ses prestataires. La Cnil a relevé des lacunes de sécurité dans leurs relations et souligne notamment la non-réalisation d'audits de sécurité, l'envoi non sécurisé des mises à jour des fichiers clients et l'absence de clause de sécurité et de confidentialité de données imposée au prestataire.

Vidéosurveillance des salariés injustifiée: une société à l'amende

Saisie par l'inspection du travail dénonçant les conditions de mise en œuvre des dispositifs de vidéosurveillance dans des magasins, la Cnil a constaté que la société filmait en continu l'accès au vestiaire et aux salles de repos des salariés. Et a prononcé, le 1er août dernier, une sanction pécuniaire publique en raison de l'atteinte disproportionnée à la vie privée des salariés.

L'Arcep retrouve son pouvoir de sanction

Le pouvoir de sanction de l'Arcep (Autorité de régula- tion des communications électroniques et des postes) lui avait été retiré par une décision du Conseil constitutionnel du 5 juillet 2013 le jugeant non conforme aux principes constitutionnels d'indépendance et d'impartialité. Le décret d'application de l'ordonnance du 12 mars 2014 qui le rétablit vient d'être publié le 1er août au Journal officiel.

Vers un renouveau de la signature électronique ?

LES FAITS

Le Conseil de l'Union européenne a adopté le 23 juillet dernier le règlement « eIDAS » sur l'identification électronique et les services de confiance pour les transactions électroniques qui instaure un espace numérique et juridique sécurisé et commun.

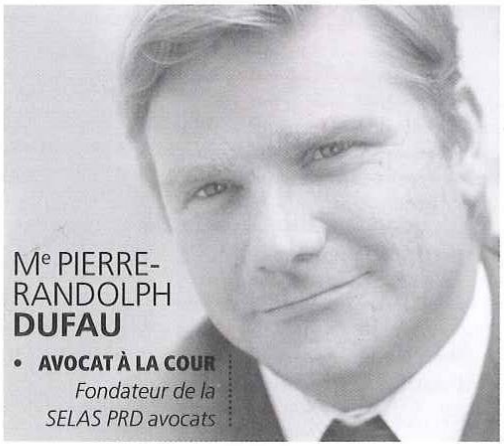
LE CADRE LÉGAL EN VIGUEUR

Le cadre juridique actuel de l'Union européenne sur la signature électronique relève de l'ancienne et presque oubliée directive 1999/93/CE du 13 décembre 1999. Depuis, la signature électronique bénéficie du principe de non-discrimination avec celle manuscrite et ne peut être légalement écartée comme moyen de preuve pour la seule raison de sa forme électronique. Pour autant, la signature électronique s'est avérée être, en pratique, un échec en raison notamment des différences nationales de transposition de cette directive.

En France, elle a été transposée par la loi du 13 mars 2000 et ses décrets d'applications qui instaurent deux catégories de signatures qui se distinguent par leurs exigences techniques et leurs effets juridiques.

La signature électronique avancée est celle qui ne peut être contestée qu'en apportant la preuve de sa non-fiabilité. Selon le décret du 30 mars 2001, la fiabilité est présumée « *lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ». Le décret définit aussi la signature sécurisée comme celle qui est propre au signataire, créée par des moyens que le signataire puisse garder sous son contrôle exclusif et liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

À l'inverse, la signature électronique dite simple est celle qui ne remplit pas l'ensemble de ces critères exigés et qui n'est donc pas présumée fiable jusqu'à preuve du contraire. En cas de contestation, c'est à celui qui entend s'en prévaloir d'apporter la preuve de la fiabilité du système mis en œuvre.



Me PIERRE-RANDOLPH **DUFAU**
- **AVOCAT À LA COUR**
Fondateur de la SELAS PRD avocats

DR

LES APPORTS MAJEURS DU NOUVEAU DISPOSITIF

L'avènement de ce règlement marque une étape importante vers le développement des échanges numériques sécurisés au niveau européen et la création d'une « citoyenneté numérique ». L'adoption d'un règlement et non d'une directive permettra une application directe au sein de tous les États membres sans intervention législative nationale des États. Parmi les nouveautés adoptées, notons principalement la création de la signature ou « cachet » électronique d'une personne morale, auparavant seulement réservée aux personnes physiques. L'apposition de ce cachet permettra de garantir l'origine et l'intégrité de données de la société et ainsi de lutter contre le phishing. Le règlement prévoit également la création d'un troisième niveau de signature électronique dite « qualifiée » plus sécurisé, ayant une valeur juridique supérieure.

CE QU'IL FAUT RETENIR

Le règlement eIDAS fixe un cadre juridique transnational et transectoriel complet de portée générale et obligatoire qui va substantiellement faciliter l'utilisation des services en ligne sécurisés tels que l'identification, l'authentification et la signature électronique, tant pour les entreprises que les particuliers. Applicable au 1er juillet 2016, il va avoir un impact majeur sur le secteur de l'économie numérique qu'il convient d'anticiper dès à présent.