Focus sur les « Chartes IT », des instruments toujours plus indispensables pour renforcer la cybersécurité des entreprises

François COUPEZ
Avocat à la cour
Associé et fondateur de Level Up Legal
Senior advisor du CyberCercle

Le législateur fait "level up" face aux cyber-risques

Il est aujourd'hui devenu évident que les entreprises sont confrontées à des cyber-risques de plus en plus nombreux et dangereux, qui peuvent affecter leurs données, leurs systèmes, leur réputation et leur activité. Pour se protéger et assurer leur cybersécurité, elles doivent se doter d'outils, de procédures et de logiciels efficaces et adaptés. Elles doivent aussi respecter le contexte réglementaire, qui impose des exigences de plus en plus nombreuses et strictes, qu'elles soient générales ou spécifiques à leur secteur d'activité.

La loi du 6 janvier 1978 dite "Informatique et libertés" a été la première à imposer une sécurisation des données personnelles en fonction des risques que leur traitement peut entraîner pour les personnes concernées. Depuis, d'autres réglementations sectorielles ont vu le jour, pour encadrer les secteurs sensibles comme la finance, l'énergie, la santé, les télécommunications, etc.

Plus globalement, le législateur a souhaité imposer des exigences de cybersécurité strictes aux opérateurs considérés comme d'importance vitale (les OIV, via la Loi de programmation militaire de 2013), c'est-à-dire nécessaires à la survie de la Nation dans les cas les plus graves. Au niveau européen, ces réflexions ont conduit à l'adoption notamment de la directive NIS (pour Network Information Security) le 6 juillet 2016 et des obligations spécifiques pour les Opérateurs de Services essentiels d'une part et les Fournisseurs de Services Numériques de l'autre. D'autres textes ont suivi ces dernières années (directive CER, projet de règlement CRA, règlement DORA, etc.) aboutissant à un cadre réglementaire de plus en plus dense et, il faut le dire, complexe.

Ainsi, la directive européenne NIS 2, qui annule et remplace NIS 1 et entrera en vigueur le 18 octobre 2024, renforce à la fois le volume des obligations et le périmètre des acteurs concernés. En fonction de la transposition à venir en 2024 par le Parlement français (a priori au 3ème trimestre), ce sont en effet près de 15 000 entreprises françaises qui pourraient être directement concernées, sans compter l'effet halo dont nous reparlerons à une prochaine occasion.

L'ANSSI, la CNIL, ISO 27001 ou encore NIS 2 : tous unis pour des chartes opposables et efficaces

LIL, RGPD, NIS 1 et 2, DORA, etc. : toutes ces réglementations ont en commun le fait d'être fondées sur des analyses de risques liées à chaque

activité, et exigent des mesures de sécurité appropriées. Mais, au-delà de la "simple" mise en œuvre effective de ces mesures, tant les régulateurs (ANSSI, CNIL[1], etc.) que les normes techniques reconnues (ISO 27001[2]) imposent de s'assurer que ces règles sont effectivement connues des personnels internes et surtout peuvent leur être effectivement opposables en cas de non-respect.

En pratique, ces règles se retrouvent dans des chartes informatiques, aussi appelées chartes IT, chartes d'usage des outils numériques, ou autre titre similaire. Celles-ci se déclinent en fonction des règles qu'elles prévoient et des personnes à qui elles s'adressent, afin là encore que ces règles soient opposables à tous, quelle que soit leur situation :

- Les chartes destinées aux utilisateurs salariés forment la grande majorité des chartes en question, et sont annexées au règlement intérieur de l'entreprise pour être rendues opposables aux salariés (ou via des notes de service pour les entreprises de taille réduite n'en disposant pas) ;

- C'est également le cas des chartes dédiées aux « administrateurs systèmes » techniques (chargés d'assurer le bon fonctionnement et/ou la cybersécurité des systèmes d'information), ou encore fonctionnels disposant de droits privilégiés sur les systèmes leur permettant notamment de gérer les accès à des bases métiers spécifiques ;

- Si des clauses spécifiques ne sont pas prévues dans les documents précédents, il peut exister également des chartes encadrant l'usage des réseaux sociaux ou encore de l'acceptation des terminaux personnels dans l'entreprise (le « *Bring your Own Device* », BYOD francisé en AVEC[3]) ;

- Le cas des prestataires externes est quant à lui réglé via des clauses spécifiques insérées dans le contrat de prestation ;

- Enfin l'encadrement de l'usage des outils IT par les instances représentatives du personnel s'opère via des accords d'entreprise.

A cet égard , si l'article 21 i) de la directive NIS 2 concernant les "*Mesures de gestion des risques en matière de cybersécurité*" ne mentionne que "*la sécurité des ressources humaines*", les projets de règles opérationnelles, dont discute actuellement l'ANSSI à l'occasion des travaux de transposition, envisagent clairement d'imposer à l'ensemble des acteurs concernés par NIS 2 la définition et la mise en œuvre d'une charte d'usage des systèmes d'information, opposable à chaque utilisateur du système d'information.

Comment rédiger une charte efficace ?

Composante majeure des règles de sécurité organisationnelle, ces chartes sont des documents hybrides, aussi bien techniques que juridiques. Constituant la colonne vertébrale de l'application des règles internes et le pendant de la Politique de Sécurité des Systèmes d'Information (PSSI), elles doivent être rédigées avec grand soin. Le comité de rédaction associe ainsi fréquemment au minimum la direction juridique, celle en charge de la cybersécurité, la direction des ressources humaines ou encore le DPO.

Leur caractère dual, technico-juridique, complique leur rédaction, qui s'avère être un véritable « champ de mines » juridique.

[1] Cf. Guide de la sécurité des données personnelles (CNIL, 2023) soulignant la nécessité de « *Rédiger une charte informatique et de lui donner une force contraignante (ex. : annexion au règlement intérieur)* ».

[2] Cf. le 6.4 de la norme ISO 27001 qui impose la formalisation d'un « *processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information* ».

[3] Cf. notamment les travaux du Forum des compétence, le cercle d'échange entre banques et assurances sur les sujets It et risques, sur le sujet, avec le livre blanc « Terminaux personnels en entreprise ».

Une jurisprudence très casuistique... et qui a beaucoup évolué avec le temps

La jurisprudence, patiemment construite depuis l'arrêt Nikon du 2 octobre 2001[4], peut ainsi évoluer drastiquement avec le temps et s'avérer extrêmement complexe car directement liée à chaque type de cas envisagé.

Concernant l'évolution jurisprudentielle, nous sommes ainsi passés en vingt ans :

- D'une protection absolue des messages privés/extra-professionnels (au visa de la Convention Européenne des Droits de l'Homme !) à une présomption de caractère professionnel généralisée rendant leur contenu accessible à l'employeur. Par exemple, au terme de la jurisprudence la plus actuelle, l'employeur peut légitimement contrôler tout matériel ou système d'information privé se connectant au système d'information de l'entreprise et, à cet égard, présumé professionnel (document ou message électronique généré sur un ordinateur professionnel y compris les messages WhatsApp ou SMS émis depuis un téléphone professionnel, etc.) ;

- D'un système où la preuve d'une faute du salarié, recueillie de façon non conforme aux règles de droit du travail ou de protection des données personnelles, était nulle devant les tribunaux à un système où elle devient acceptable sous conditions, sous l'impulsion de la jurisprudence de la Cour Européenne des Droits de l'Homme.

De plus, toute formulation doit être très soigneusement choisie, car pouvant impacter les mesures de sécurité internes ou restreindre de façon drastique les contrôles que l'employeur serait en droit de faire, comme l'histoire a pu le montrer[5].

Sa rédaction doit donc être l'objet de toutes les attentions et pesée à l'aune des centaines de décisions de justice qui la guide.

Un environnement réglementaire et technique toujours plus foisonnant à prendre en compte

D'autant que doivent également être intégrés dans la réflexion et considérés dans le processus de rédaction :

- Un certain nombre de règles juridiques « classiques » de droit du travail (sur le contrôle, sur l'information des salariés, le formalisme d'adoption du règlement intérieur, etc.), mais aussi les interactions à prévoir avec les règles applicables en matière de télétravail, de droit à la déconnexion, de droit à la vie privée, de droit de la cybersécurité ou encore avec la protection des données personnelles, qu'elles soient d'origine européenne (RGPD) ou purement franco-française (spécificités de la loi du 6 janvier 1978). Sans oublier les conséquences de faits parfois tragiques pouvant intervenir dans l'entreprise, comme à l'occasion de la disparition d'un salarié (Quid de l'accès à sa messagerie et ses fichiers par exemple[6] ?) ;

- Les évolutions en matière de cybersécurité et les mesures de sécurité qui en découlent : historiquement, le déchiffrement des flux TLS (imposant une analyse d'Impact relative à la protection des données ou *PIA* [7] préalable), encadrement des pratiques de *Data Leak Prevention*,

[4] Cass. Soc. 2 octobre 2001, 99-42.942.

[5] Cf. Cass. Soc. 26 juin 2012 : indépendamment de la jurisprudence en matière d'accès aux courriels professionnels adressés ou reçus par le salarié, le « *règlement intérieur peut toutefois contenir des dispositions restreignant le pouvoir de consultation de l'employeur, en le soumettant à d'autres conditions* ». Dans ces cas « *celles-ci prévaudront sur les critères issus de la jurisprudence* ». Or, dans cette affaire, le règlement intérieur prévoyait « *que les messageries électroniques des salariés ne pouvaient être consultées par la direction qu'en présence du salarié* », ce qui empêche l'employeur de se prévaloir des règles de contrôle habituellement reconnues par la jurisprudence et donc, *in fine*, de mener des opérations de contrôle efficaces.

[6] Notamment au regard des spécificités de la loi française sur les données personnelles des personnes décédées, dérogatoire au droit de la dévolution successorale.

[7] Pour *Privacy Impact Assessment*, ou Analyse d'impact à la protection des données (AIPD).

plus récemment approche de type « *0 trust* » (conduisant à réaliser l'analyse comportementale des salariés se connectant au SI et donc imposant là aussi la réalisation d'un *PIA* préalable), etc. ;

- Les évolutions d'usage des outils numériques au sein de l'entreprise et l'intégration d'un cadre au regard des risques (outils cloud, shadow IT, usage des outils d'IA générative, etc.) ;

- La rédaction de l'encadrement spécifique aux « administrateurs systèmes » techniques ou fonctionnels, compte tenu des droits d'accès privilégiés, dérogatoires, dont ils sont amenés à disposer ;

- Ou encore la coordination de ces règles avec celles applicables aux prestataires intervenant sur le système d'information - ces dernières étant dérivées des chartes, avec une adaptation nécessaire de leur contenu et de leur vecteur d'opposabilité.

Dans sa fiche 2 de son Guide de la sécurité des données personnelles, intitulée "Sécurité : Définir un cadre pour les utilisateurs" et publiée sur son site le 14 mars 2024, la CNIL liste les quelques thématiques qu'elle estime absolument nécessaires à inclure dans un tel document.

Elle précise surtout à cette occasion ce qu'il convient de ne surtout pas faire :

- Ne pas donner de force contraignante à la charte ou ne pas l'appliquer et la faire appliquer en cas de manquement.

- Ne pas tenir compte des pratiques réelles des usagers, de leurs attentes et de leurs besoins en définissant les règles d'usage des moyens informatiques : l'informatique fantôme (ou « shadow IT » en anglais) révèle parfois des besoins essentiels non pourvus par l'organisme ou un dysfonctionnement structurel.

- Ne pas accompagner les usagers dans leurs pratiques.

"Une synthèse complexe, mais possible"

Bien rédigée, exhaustive, rendue opposable et prenant en compte l'ensemble des comportements numériques au sein de l'entreprise dont ceux des titulaires de comptes à privilèges, la charte est un atout essentiel pour assurer la cybersécurité de l'entreprise.

Elle doit toutefois interagir avec un ensemble documentaire plus vaste, dans lequel figurent également des règles destinées cette fois-ci aux prestataires intervenant sur le système d'information de l'entreprise, ces impératifs étant, là également, imposés autant par ISO 27001 que par le RGPD ou encore le projet de transposition en droit français de la directive NIS 2. En pratique, reprenant l'essentiel des règles de la charte tout en prévoyant des règles propres (concernant l'usage privé, etc.), celles-ci s'intègrent en annexe aux contrats de prestation et doivent être rédigées de façon précise et exhaustive. Alors que tous les regards se portent sur la cybersécurité des prestataires IT et, plus globalement, la gestion des risques fournisseurs (avec des exigences fortes autant de l'ANSSI que de la CNIL[8] notamment), ces règles ne doivent surtout pas être négligées !

[8] Cf. la décision de sanction de la CNIL du 16 mars 2023 : « *La formation restreinte considère également que la clause "Security ", qui prévoit que le sous-traitant met en place des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque* », devrait être plus précise. « *Ici, seuls les objectifs de sécurité à atteindre sont décrits, sans précision sur les moyens d'y parvenir, tels qu'une description des processus ou mécanismes développés dans des annexes au contrat. En l'absence de précision sur les moyens pour remplir l'obligation de mettre en place des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque, la formation restreinte considère que le contrat ne répond pas aux exigences du RGPD* ».

Les points clefs :

- Il est impératif de disposer de règles opposables et efficaces en matière de cybersécurité, insérées dans le règlement intérieur de l'entreprise (charte) afin d'être rendues opposables aux salariés utilisant le système d'information ;

- La charte guide les bons comportements en matière de cybersécurité et permet une répression efficace des violations de sécurité qui peuvent se produire en interne ;

- C'est un atout de l'entreprise face aux risques endogènes de cybersécurité ;

- Déchiffrement TLS, DLP, 0 trust, droit à la déconnexion, télétravail, usage de l'IA générative, impact du décès d'un salarié, comptes à privilèges, etc. sont autant de sujets à prévoir ;
- La rédaction de ce texte, colonne vertébrale de l'application des règles internes au contenu aussi bien technique que juridique, est d'une complexité croissante ;

- Ces chartes doivent être déclinées dans une version spécifique applicable aux prestataires externes intervenant sur le système d'information de l'entreprise, et utilisant cette fois le contrat de prestation comme vecteur afin d'être opposable à leur société de prestation.

L'auteur remercie Me Anne-Laure Pons Poline et Me Loane Da Silva de Level Up Legal pour leur relecture attentive.