Olfeo

LIVRE BLANC

Les chartes IT en entreprise

Cybersécurité

EN PARTENARIAT AVEC ERIC BARBRY – CABINET D'AVOCAT RACINE

racine AVOCATS

RACINE est un cabinet d'avocats français indépendant de droit des affaires qui réunit près de 270 avocats et juristes, répartis au sein de 7 bureaux : Paris, Bordeaux, Lyon, Marseille, Nantes, Strasbourg et Bruxelles. RACINE se caractérise par une approche « full service » en droit des affaires en conseil et contentieux. Ses avocats, impliqués et pragmatiques, accompagnent les clients en leur apportant des solutions innovantes dans leur activité au quotidien, l'accompagnement des projets stratégiques et la gestion des crises. Ils s'attachent à la construction de relations de partenariats solides et durables avec les clients. RACINE intervient pour des entreprises, issues de différents secteurs de l'industrie et des services, des organisations professionnelles et interprofessionnelles ainsi que des collectivités publiques. Le cabinet a développé une expertise particulière des secteurs que sont le luxe, les médias, l'immobilier, l'agroalimentaire et la distribution. RACINE est membre du réseau international d'avocats Multilaw, ainsi que d'OMNIA. Le cabinet entretient par ailleurs d'étroites relations avec de nombreux cabinets étrangers.

SOMMAIRE

Le terme « en entreprise » du titre de ce livre blanc doit être pris au sens large. Il peut viser des entreprises mais aussi des acteurs publics ou des établissements à but non lucratif.

Propos introductif

Aujourd'hui, la sécurité de l'information ne se limite pas aux contrats de travail et au règlement intérieur. Bien que ceux-ci soient importants, ils ne suffisent pas à eux seuls pour garantir la sécurité. En effet, la sécurisation des systèmes d'information (SI) implique plusieurs niveaux, dont les audits de sécurité et la gestion des contrats avec les prestataires de sécurité (tests intrusifs). Cependant, l'utilisateur reste le maillon faible du système. Il est difficile de le surveiller en permanence et l'analyse de ses logs intervient souvent trop tard. Ainsi, la maîtrise de la sécurité des SI passe par l'information, la formation et la régulation.

Le premier élément est la sensibilisation. Sensibiliser les utilisateurs est crucial pour la réussite des politiques de sécurité. Cette sensibilisation peut prendre différentes formes, telles que le e-learning ou les MOOC, et doit être adaptée à la taille de l'entreprise et au niveau de risque. Par exemple, le risque est faible dans un contexte B2B mais beaucoup plus élevé en B2C, où des réglementations comme le RGPD s'appliquent. L'objectif est de développer une culture de la sécurité au sein de l'entreprise.

Ensuite, la formation des utilisateurs est essentielle. Cette formation doit être plus approfondie et adaptée aux différents profils au sein de l'entreprise. En effet, les utilisateurs n'ont pas les mêmes besoins ni les mêmes responsabilités que les administrateurs ou les personnes ayant des droits étendus. Certains utilisateurs ont accès à des données sensibles, d'autres non, et leur formation doit refléter ces différences. La sécurité doit donc être abordée métier par métier, avec des formations spécifiques (MOOC, e-learning) adaptées à chaque fonction. Par exemple, les ressources humaines et les services informatiques ne seront pas formés de la même manière.

Enfin, la régulation est nécessaire. Il est important de réguler les usages, de se donner le droit de contrôler ces usages et, si besoin, de sanctionner les mauvais comportements.

LES CHARTES IT, BONNE PRATIQUE OU RESPECT DE LA LOI ?

Même s'ils sont de moins en moins nombreux, certains s'interrogent encore sur la pertinence des chartes en entreprise. Ils considèrent en effet que le droit et les contrats (notamment les contrats de travail) suffisent au bonheur des employeurs.

C'est méconnaitre plusieurs réalités :

- des réalités légales ;
- des réalités jurisprudentielles ;
- des réalité normatives ;
- des réalités liées à des recommandations d'autorités compétentes.

Réalités légales – Rappelons tout d'abord que pour les entreprises (et les EPIC) employant au moins 50 salariés le règlement intérieur est obligatoire. Or ce règlement est destiné à fixer certaines règles dans l'entreprise dont « les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur ».

Lorsqu'il s'impose le règlement intérieur doit donc comprendre les mesures relatives aux règles de discipline à respecter. Or la mise à disposition de matériel, logiciel et services numériques aux salariés impose de fixer des règles communes à tous.

C'est pour cette raison que par principe le règlement intérieur doit traiter des conditions d'usage des outils IT. Cependant pour des raisons de confort la plupart des entreprises ont décidé d'adopter des « charte informatique »[1] qu'elles ont annexées à leur règlement intérieur.

Les deux formules (all inclusive ou document séparé) sont justes sur un plan juridique. Mais lorsque la charte est annexe au règlement intérieur elle doit suivre le même processus d'adhésion que le règlement intérieur lui-même notamment avec le CSE (Comité social et économique).

1 Ou toute autre formulation

Pour les établissements publics la règle est sensiblement la même mais l'on parlera de « comité social » et non de CSE.

Réalité jurisprudentielle – La jurisprudence reconnaît une valeur juridique à part entière à ces chartes, dont la violation peut aboutir à une sanction du salarié voire, selon les hypothèses, justifier son licenciement.

La Cour de cassation a eu l'occasion de reconnaître la force contraignante d'une charte. Ainsi elle a considéré, par un arrêt du 21 décembre 2006[2] , que la tentative de connexion sur le poste informatique du directeur de la société, par emprunt du mot de passe d'un autre salarié, constituait « un comportement contraire à l'obligation de respect de la charte des systèmes d'information en vigueur dans l'entreprise, rendait impossible son maintien dans l'entreprise pendant la durée du préavis et constituait une faute grave ».

Dans un arrêt rendu le 15 décembre 2010[3] , la Chambre sociale de la Cour de cassation a affirmé que le fait de recevoir, envoyer et détenir sur un disque dur professionnel 480 fichiers pornographiques constituait un manquement à l'interdiction posée par la charte des systèmes d'information de l'entreprise, ce qui justifiait le licenciement pour faute grave d'un salarié.

Enfin, dans un arrêt du 5 juillet 2011[4] , la même juridiction a considéré comme justifié le licenciement d'un salarié ayant prêté à un collègue son code d'accès pour télécharger des informations confidentielles alors que ce dernier n'y était pas habilité, ce qui constituait un comportement prohibé par la charte informatique de l'entreprise.

A contrario, l'absence de charte informatique peut empêcher de qualifier une faute du salarié. Selon la chambre sociale de la Cour de cassation, la suppression et le transfert de mails professionnels ne constituent pas une faute grave à défaut de charte informatique et à défaut de pièces permettant d'apprécier l'ampleur du préjudice subi par l'employeur dès lors que les emails transitaient également via l'adresse email d'une assistante de direction et avaient été restaurés par l'employeur. Il incombe donc à l'employeur de mettre en œuvre une charte informatique permettant de définir les obligations des parties et les conditions d'utilisation du matériel informatique mis à disposition. La définition claire et précise des droits et obligations des utilisateurs – spécialement les comportements prohibés comme la suppression et les transferts de courriers électroniques professionnels vers la boîte personnelle ou autres – au sein d'une charte

2 Cass soc. 21 déc. 2006, n41165-05°.
3 Cass. soc. 15 déc. 2010, n° 42691-09.
4 Cass. Soc. 5 juil. 2011, n14685-10°

informatique, dès lors qu'elle était opposable, aurait évité à l'employeur de devoir rapporter la preuve de son préjudice [5].

Depuis on ne compte plus le nombre de décisions de la Cour de cassation qui encouragent l'élaboration de tels documents.

En dehors des cas clairement illicites (pédopornographie, terrorisme, détournement de fond, …) le juge vérifiera pour toute sanction si le salarié ou l'agent a été clairement informé de ses obligations et des limites imposées en termes d'usage des outils et services. En ce sens l'absence de charte sera un risque important pour l'entreprise de voir la sanction annulée ou limitée.

Au-delà des règles et sanctions les tribunaux sont attentifs à la manière dont certains droits du salariés/agents sont protégés et notamment leur droit à la vie privée résiduelle.

Réalité normative – La norme ISO 27001 (et ses déclinaison), établit les exigences pour la mise en place, la mise en œuvre, le maintien et l'amélioration d'un système de management de la sécurité de l'information (SMSI) au sein d'une organisation. Parmi les nombreux aspects abordés par cette norme, une attention particulière est accordée à l'élaboration de chartes de sécurité de l'information. Ces chartes constituent des documents essentiels définissant les principes, les politiques et les procédures de sécurité de l'information au sein de l'entreprise. Elles servent de cadre pour garantir la cohérence des pratiques de sécurité, en définissant les responsabilités, les autorisations d'accès, les procédures de gestion des incidents, et autres directives pertinentes.

Se conformer à la norme ISO 27001, même en l'absence d'adhésion formelle ou de certification, revêt plusieurs avantages significatifs. Tout d'abord, adopter les principes et les recommandations de cette norme permet de bénéficier d'un cadre structuré et reconnu pour la gestion de la sécurité de l'information. En suivant les lignes directrices de l'ISO 27001, une entreprise peut renforcer sa posture de sécurité, réduire les risques liés aux failles de sécurité et améliorer sa capacité à se conformer aux réglementations en vigueur, telles que le RGPD. De plus, même sans une certification formelle, l'adoption des bonnes pratiques de sécurité énoncées dans la norme peut renforcer la confiance des clients, des partenaires commerciaux et des parties prenantes dans la capacité de l'entreprise à protéger leurs données sensibles. Enfin, la conformité à l'ISO 27001 démontre l'engagement de l'entreprise envers la sécurité de l'information, ce qui peut avoir un impact positif sur son image de marque et sa réputation

5 Cass. soc., 7 déc. 2022, n° 11.206-21

sur le marché. En somme, même sans certification officielle, se conformer aux principes de l'ISO 27001 représente un investissement judicieux pour renforcer la sécurité et la fiabilité des opérations informatiques d'une entreprise.

Réalité recommandations et avis – En matière de sécurité et de données deux autorités se partagent le devant de la scène : l'Anssi et la Cnil. Pour l'Anssi disposer d'une charte d'utilisation des moyens informatiques et des outils numériques est un atout pour vous protéger des risques cyber. Dès 2017 l'Anssi publiait un guide pour la rédaction d'une « charte d'utilisation des moyens informatique et outils numériques » pour les PME et ETI. Dans le cadre de ses 42 mesures dites « hygiène informatique » l'Anssi précise : « Pour renforcer ces mesures, l'élaboration et la signature d'une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs peut être envisagée. ».

- La Cnil quant à elle, qui est la gardienne des mesures prises pour protéger les données personnelles au sein des établissements publics ou privés, insiste également sur la nécessité de rédiger ce qu'elle appelle une « charte informatique ».[6] La Cnil indique notamment que « Les utilisateurs ont un usage souvent quotidien de l'outil informatique. Leurs pratiques peuvent avoir un impact direct sur la sécurité des données personnelles et doivent donc être encadrées. ». Elle précise quels sont les grands thèmes à ne pas oublier dans la rédaction d'une charte à savoir : les règles de sécurité auxquelles les utilisateurs doivent se conformer, les moyens d'authentification utilisés par l'organisme et la politique de mots de passe que l'utilisateur doit respecter et les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme.

6 https://www.cnil.fr/fr/securite-definir-un-cadre-pour-les-utilisateurs

Les chartes quelle que soit leur nom (informatique, des système d'information, moyens informatiques ou outils numériques) ne sont pas seulement des « bonnes pratiques » mais s'inscrivent dans le respect de la loi.

En pratique, il faut savoir distinguer différentes situations et donc différentes chartes. Sans vouloir multiplier les chartes à outrances plusieurs chartes doivent, ou peuvent selon les cas, s'imposer.

Titre	Personnes visées	Objet
Charte des systèmes d'information	Ensemble des salariés / agents	Définir les conditions d'utilisation des outils informatiques et numériques par l'ensemble des personnels autorisés
Charte administrateur	Administrateur (ASR, système, réseau, sécurité, …)	Définir les droits et obligations des personnels disposant de droit étendus
Charte télétravail	Tous les salariés autorisés à télétravail	S'impose à défaut d'accord dans l'entreprise
Charte IA	Tous les salariés ou les salariés autorisés à utiliser des outils d'IA	Définir le cas particulier de l'usage des outils d'IA (nouvelle tendance)

La charte des systèmes d'information, mode d'emploi

Règle 1 – Taille de la charte - Une charte n'est ni courte ni longue : elle doit être efficace. Par exemple, une start-up opérant dans un domaine sensible pourrait avoir une charte informatique (IT) très détaillée, tandis qu'une grande entreprise (GE) avec une infrastructure IT limitée pourrait se contenter d'une charte plus légère.

Règle 2 – Lutter contre le risque d'obsolescence programmé. Les technologies se développent bien plus vite que le droit. De fait le risque majeur pour une charte est de vite être dépassée par une évolution des pratiques de l'entreprise et la mise à disposition de nouveaux outils.

Le secret d'une « bonne » charte est donc de lutter contre la « techno captivité ». En résumé le rédacteur de la charte devrait tout faire pour s'éloigner des contraintes opérationnelles et fixer des règles qui seront capables d'évoluer.

Si l'on prend l'exemple des règles d'identification et d'authentification, la plupart des chartes actuelles expliquent comment créer, utiliser et changer un login mot de passe. Mais cette technologie est déjà dépassée par le MFA ou d'autres technologies ou solutions plus robustes.

Ainsi si le rédacteur de la charte indique que le mot de passe est de 8 caractères, qu'il doit être changé tous les X et qu'il ne faut pas utiliser de mots de passes triviaux, il figera sa charte à l'instant T de la technologie mise en œuvre.

S'il a une approche plus large et moins techno alors il abordera cette même disposition d'une autre manière. Il n'indiquera pas si c'est la technologie A ou la B qui est utilisée mais définira des règles telles que : l'obligation d'utiliser l'ID et le moyen d'authentification fourni par l'entreprise, que ces outils sont personnels et ne doivent en aucun cas être partagés, que leur usage présume que c'est bien le salarié en question qui s'est connecté et enfin que si ledit salarié ne fait pas savoir que ses ID et moyens

d'authentification ont été compromis sa responsabilité est engagée.

Il est toujours possible pour des raisons opérationnelles et d'information de prévoir les conditions d'utilisation dans d'autres documents comme des fiches pratiques ou un guide pratique.

Il doit en être de même de tous les thèmes traités dans la charte.

Règle 3 – organiser l'usage privé des outils professionnels. Comme cela a été rappelé par la Cour de cassation dans un célèbre arrêt Nikon de 2001 l'entreprise (ou l'acteur public) ne peut interdire un usage privé raisonnable des outils professionnels mis à sa disposition (mel, matériel, fichier, …).

Il est donc primordial de bien définir et encadre cet usage qui peut vite être source de difficulté.

Il faudra pour ce faire que l'entreprise fixe des règles comme : le nommage des fichiers/mails, les outils qui par exception ne pourront pas faire l'objet d'un usage privé s'il y en a, les conditions d'accès à ces documents/mails privés conformément aux prescriptions de la Cour de cassation (il est en effet possible d'accéder à des mails ou fichiers privés dans des conditions exceptionnelles).

Règle 4 – Définir les règles d'absence et/ou de départ du collaborateur et notamment le sort de ces dossiers et mel professionnelle. Il est toujours bon de rappeler que ces fichiers et mels appartiennent à l'employeur et certainement pas au salariés/agents !

Règle 5 – Il convient de rappeler que l'entreprise se réserve le droit de procéder à des contrôles individuels ou collectifs. Il ne s'agit pas ici de détailler les mesures prises qui ne regardent que l'entreprise et la DSI mais de rappeler que les contrôles sont effectifs et peuvent conduire à des restrictions d'usage ou des sanctions de nature RH.

Quant à la mise en œuvre de la charte, si elle suit le processus d'adoption du règlement intérieur alors la charte ne doit pas être validée ou signée par les salariés/agents. Elle doit simplement être portée à leur connaissance et affichée selon les règles légales en vigueur.

Il est possible de prévoir que le salarié devra prendre connaissance de la charte et toute modification lors de l'ouverture d'une session informatique. Pour les personnels qui n'auraient pas accès à des outils numériques l'affichage apparait suffisant mais il n'est pas interdit de leur adresser par courrier postal.

La charte administrateur, un document de toute autre nature

Rappelons tout d'abord que comme la Charte SI, la charte administrateur est fortement préconisée par l'Anssi, la Cnil, l'ISO, …

En page 10 de son Guide pratique RGPD sécurité des données personnelles version 2024[1] la Cnil indique qu'il faut « Prévoir une charte spécifique pour les administrateurs qui détaille les exigences complémentaires que cette population particulièrement à risque doit respecter. »

La norme ISO 27001 et les recommandations de la CNIL soulignent l'importance d'établir une relation claire entre l'employeur et l'administrateur, souvent formalisée par un avenant au contrat de travail.

Par ailleurs la responsabilité des administrateurs a déjà fait l'objet de débats judiciaires.

La charte administrateur est d'une toute autre nature que la charte des systèmes d'information par son objet, son contenu et sa mise en œuvre.

L'objet de cette charte est de définir les droits et obligations d'une catégorie particulière de salariés ou d'agents. Ils peuvent être des administrateurs statutaires ou des personnes disposant de droits plus étendus que le commun des salariés.

Dans la mesure où ces personnes peuvent réaliser des opérations que les autres salariés ne peuvent pas faire et qu'ils peuvent accéder à des données et fichiers auxquels les salariés lambdas ne peuvent pas accéder cette catégorie de personne est à la fois source de risque et en état de risque.

1 https://www.cnil.fr/sites/cnil/files/03-2024/cnil_guide_securite_personnelle_2024.pdf

Elle est source de risque car elle peut facilement accéder à des contenus de tiers et pourquoi pas des contenus privés. Elle peut aussi être exposée si par exemple l'employeur leur demande de réaliser des opérations illicites (prendre connaissance de mails privés sans une des rares raisons prévues par la Cour de cassation).

Les administrateurs doivent respecter des obligations renforcées de confidentialité, ne divulguer aucune information sensible et assurer la sécurité des systèmes et des données. Ils sont tenus de n'utiliser que les moyens informatiques fournis par l'entreprise et de documenter toute action en dehors des procédures internes. La charte stipule également le respect des droits de propriété intellectuelle et de la vie privée des utilisateurs. Toute violation des règles peut entraîner des sanctions disciplinaires et des poursuites judiciaires. La charte est régulièrement mise à jour pour s'adapter aux évolutions technologiques et aux besoins de l'entreprise.

Comme la charte administrateur n'affecte pas l'ensemble des collaborateurs, elle ne suit pas le même régime notamment devant le CSE ou le CS, même s'il n'est pas interdit de porter à la connaissance de ces instances l'existence de ces chartes.

Elles devront donc faire l'objet d'une adhésion par chacune des personnes concernées.

La charte IA, une route vers le furtur présent

En matière d'IA on ne peut plus vraiment parler de « futur » … Tous les salariés ou agents utilisent de manière plus ou moins autorisé des outils d'IA comme ChatGPT ou MistralAI.

La question se pose donc de définir ou non leurs conditions d'utilisation.

Il est important de relever que l'introduction de l'intelligence artificielle soulève d'importantes questions de confidentialité en raison de la quantité massive de données personnelles et sensibles traitées par ces systèmes. Ainsi, les collaborateurs peuvent être soumis à des impératifs légaux, contractuels ou déontologiques de confidentialité : pourtant, le partage de données confidentielles en input dans un système d'IA peut violer ces principes. En particulier, les données dont disposent certains collaborateurs peuvent être confidentielles au titre de :

- D'un niveau Diffusion Restreinte[1] ou d'une classification de défense[2];
- Des travaux de recherche relevant de la Protection du potentiel scientifique et technique de la nation[3] ;
- De données contractuelles, juridiques ou financières de l'entreprise ;
- Des secrets informatiques, comme des mots de passe ou des jetons d'authentification (clés d'API) ; ou encore

1 L'instruction interministérielle no 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 définit les exigences organisationnelles et techniques applicables aux systèmes d'information amenés à traiter des informations sensibles, dont celles portant la mention de protection Diffusion Restreinte. L›II 901 s›applique également aux systèmes d›information amenés à traiter d›informations classifiées de l›OTAN de niveau NATO Restricted / Restreint OTAN. L›II 901 s›applique également aux systèmes d›information amenés à traiter d›informations classifiées de l›UE de niveau EU Restricted / Restreint UE.

2 Consécutive au décret n1271-2019° du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale, l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale (IGI 1300) détermine les rôles et responsabilités ainsi que les exigences liées à la gestion du cycle de vie d'une information ou d'un support classifié. À travers ses différentes versions, dont la précédente est entrée en vigueur le 30 novembre 2011, cette instruction renforce la prise en compte de l'information classifiée dématérialisée. Ainsi, la nouvelle IGI 1300 précise les exigences applicables aux informations classifiées dématérialisées ainsi qu'aux systèmes d'information amenés à les traiter.

3 La protection contre l'espionnage technologique est l'objectif premier du dispositif de protection du potentiel scientifique et technique de la nation (PPST). Il a pour but de protéger, au sein des établissements publics et prives, les savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qu'ils détiennent. Cette règlementation offre une protection juridique et administrative fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues.

Au sujet de la manipulation des données personnelles, la confidentialité est un sujet majeur. Les collaborateurs d'une entreprise ne sont pas des responsables de traitement de données à caractère personnel au sens du RGPD lorsqu'ils traitent de ces données : la responsabilité est portée par l'employeur. Ainsi, l'employeur doit sensibiliser et former ses salariés afin que toutes les données à caractère personnel qu'ils manipulent le soient dans le respect de la réglementation. Or, nourrir un système d'IA de données personnelles peut être une violation du principe de sécurité des données et constituer un nouveau traitement de données qui doit être documenté. Ce traitement peut même être qualifié de flux de données en dehors de l'Union européenne et les garanties appropriées doivent alors être fournies par le responsable de traitement. Pour toutes ces raisons, les entreprises peuvent sensibiliser leurs salariés sur ces risques notamment via la Charte IA.

L'IA pose également des défis significatifs en matière de propriété intellectuelle (PI) dans les entreprises. Les algorithmes et les systèmes d'IA peuvent générer des outputs protégeables au titre du droit d'auteur ou au contraire qui constituent en tant que telle une contrefaçon d'une œuvre constituant sa base de données. L'output peut alors recevoir la qualification d'œuvre dérivée ou de contrefaçon selon les cas. En outre, certaines règles spéciales peuvent être prévues dans les conditions générales accompagnant le système d'IA concernant les droits d'auteur, la contrefaçon et les garanties associées.

Là encore, les entreprises peuvent sensibiliser leurs salariés sur ces risques notamment via la Charte IA et définir des règles du jeu.

Le règlement IA[4] du 13 juin 2024 précise dans son article 4 intitulé « Maitrise de l'IA » que :

4 Règlement (UE) 1689/2024 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 2008/300, (UE) n° 2013/167, (UE) n° 2013/168, (UE) 858/2018, (UE) 1139/2018 et (UE) 2144/2019 et les directives 90/2014/UE, (UE) 797/2016 et (UE) 1828/2020 (règlement sur l'intelligence artificielle) (Texte présentant de l›intérêt pour l›EEE)

> Les fournisseurs et **les déployeurs[1] de systèmes d'IA prennent des mesures** pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés.
>
> 1 Les déployer sont les établissement qui utilisent l'IA

En avril 2024, l'ANSSI a publié ses recommandations de sécurité pour un système d'IA générative. Parmi ces recommandation, l'ANSSI recommande aux entités clientes d'IA génératives tierces telles que ChatGPT, Gemini ou même DeepL de proscrire l'utilisation d'outils d'IA générative sur Internet pour un usage professionnel impliquant des données sensibles. Ainsi, l'employeur n'ayant pas la maîtrise du service d'IA générative, il n'est pas possible pour lui de s'assurer que la protection en confidentialité des données soumises en entrée respecte les besoins de sécurité de son entreprise. Par mesure de précaution, il est donc obligatoire de ne jamais intégrer de données sensibles de l'entité dans les requêtes des utilisateurs-salariés[5]. Cette proscription passe nécessairement par l'adoption d'une Charte IA en interne.

Par ailleurs, la CNIL évoque aussi indirectement la mise en place d'une telle charte, en en faisant mention comme l'un de ses points prioritaires de contrôle :

5 ANSSI, Recommandations de sécurité pour un système d'IA générative, 29 avril 2024, n°ANSSI-PA102-, p. 29 : https://bit.ly/3WfANVT

CNIL, Intelligence artificielle : le plan d'action de la CNIL, 16 mai 2023

« La CNIL sera particulièrement attentive à ce que les acteurs traitant des données personnelles afin de développer, d'entraîner ou d'utiliser des systèmes d'intelligence artificielle aient :

- réalisé une analyse d'impact relative à la protection des données (AIPD) pour documenter les risques et pris des mesures permettant de les diminuer ;
- pris des mesures d'information des personnes ;
- prévu des mesures d'exercice des droits des personnes adaptées à ce contexte particulier. »

La nouvelle norme ISO/IEC 42001, publiée en décembre 2023, établit un « système de management pour l'intelligence artificielle » (SMIA) destiné aux organismes qui fournissent ou utilisent des systèmes d'IA. Cette norme fournit un cadre certifiable visant à améliorer la qualité, la sécurité, la traçabilité, la transparence et la fiabilité des applications de l'IA. Elle aide les entreprises à respecter les exigences réglementaires et les attentes des parties prenantes, tout en renforçant la confiance dans les systèmes d'IA. Le SMIA couvre l'établissement, la mise en œuvre, le maintien et l'amélioration continue de la gestion de l'IA dans les organisations.

Certains réagissent déjà en disant « une charte de plus » !

Oui c'est vrai, une charte de plus, mais pour un objectif bien défini.

Rappelons d'abord que l'établissement peut décider d'intégrer les éléments relatifs à l'IA dans sa charte SI en la modifiant et n'est donc pas obligé d'éditer une charte IA autonome.

La réalité veut que les établissements qui se sont lancés dans cette opération ont préféré passer par la voie d'une charte autonome pour deux raisons essentielles : agilité & déploiement.

Au titre de l'agilité, une charte autonome permet de ne se concentrer que sur la seule question de l'IA et ne pas remettre en cause les règles déjà établies et logiquement suivies par les collaborateurs.

Au titre du déploiement une charte autonome présente le mérite de ne pas avoir à représenter une charte SI complète au CSE ou au CS. Il ne faut pas oublier en effet que même si la charte SI n'était modifiée que sur la partie IA, le fait de la (re)présenter au CSE ou CS donne compétence à ces organismes pour réaliser 100% de la charte y compris les dispositions déjà adoptées dans la version antérieur…

Quant aux contenus de cette charte elle doit se concentrer exclusivement sur l'IA.

Il existe trois situations possibles :

- Situation 1 : l'interdiction. L'établissement est parfaitement fondé à interdire tout usage d'un outil d'IA. Cette situation est très rare mais peut s'entendre dans des secteurs d'activités hautement stratégiques (défense par exemple).

- Situation 2 : l'autorisation contrôlée. L'établissement accepte que les collaborateurs utilisent des outils d'IA gratuit (ou payant si accord de l'employeur) et fixe les règles d'usages : quel type d'outil, pourquoi faire, confidentialité, propriété intellectuelle, contrôle par l'entreprise, transparence, …

- Situation 3 – L'IA imposée. L'entreprise peut tout aussi bien imposer un outil d'IA développé par lui ou pour lui. Dans ce cas l'entreprise devra fixer les conditions d'utilisation de cette IA et interdire l'usage des autres.

Dans certaines professions comme celle des avocats le déploiement de charte IT ou autre document est vivement recommandé.

Sécurisez les accès internet contre les cyber attaques.

Olfeo est le leader français de la sécurisation des accès Internet, depuis 20 ans, avec 36 % de part de marché et 1 milliard de requêtes web traitées par jour.

Nos solutions de passerelles de sécurité offrent le plus haut niveau de protection grâce à notre approche Internet Zero Trust.

Elles combinent des fonctions de proxy, de déchiffrement TLS , de filtrage d'urls, d'antimalware et de filtrage DNS, … Elles sont disponibles en Saas et en on-premise.

L'augmentation du nombre des attaques réussies montrent que les organisations sont encore mal protégées par des solutions généralistes qui ne se sont pas adaptées aux nouvelles menaces.

Cet échec vient premièrement de l'explosion du nombre des urls malicieuses qui hébergent les menaces et deuxièmement du facteur humain exploité par les hackers à travers les attaques par ingénierie sociale (phishing, …).

Nous pensons que le web, principal vecteur d'attaques, est devenu trop dangereux pour laisser n'importe quel utilisateur aller sur n'importe quel site avec n'importe quel équipement.

C'est pourquoi nos solutions reposent sur la technologie exclusive Trust-Centric qui offre le plus haut niveau de protection :

Les solutions de sécurité historiques sont basées sur la reconnaissance et le blocage des menaces. Or avec l'explosion de leur nombre : 13 millions d'urls malicieuses créées chaque mois, ces solutions ne peuvent plus les suivre et sont débordées. Elles sont devenues obsolètes.

La technologie exclusive Trust-Centric d'Olfeo, basée sur la confiance, offre une bien meilleure protection car elle limite l'accès aux seuls contenus légitimes vérifiés par Olfeo.

Illustration : Dans une attaque par ransomware, le hacker créé

des domaines éphémères quelques minutes avant l'attaque. Votre équipement historique ne pourra pas les reconnaître car ils sont inconnus et donc laissera passer l'attaque.

La technologie Trust-Centric, elle, bloquera ces contenus car ils n'auront pas été validés par Olfeo.

Cette approche est rendue possible grâce à l'exhaustivité et la qualité de la base de données d'urls d'Olfeo qui reconnaît des centaines de millions d'URLs et couvre plus de 99% des requêtes en France et Europe.

Disponible dans le cloud souverain, la solution Saas est simple et elle se met en œuvre en moins d'1 heure. Nous mettons nos clients à l'abri du Cloud Act et sommes pleinement conforme au RGPD et d'ailleurs la CNIL est un de nos clients.

Contactez-nous

contact@olfeo.com

www.olfeo.com

Olfeo