THEIVENDRAM Hariharani

VEILLE CEJMA

SOMMAIRE

B1 : Support et mise à disposition des services informatiques

1. Gérer le patrimoine informatique

La gestion de parc informatique consiste à assurer la maintenance, l'administration et la mise à jour des équipements informatiques d'une entreprise. Cela inclut les ordinateurs, les téléphones, les serveurs, les imprimantes et autres périphériques.

La bonne gestion du parc informatique participe au bon fonctionnement de l'organisation et à ses performances. Externaliser peut constituer une option intéressante pour les TPE et PME pour maîtriser ses coûts, disposer de matériel adapté, disposer d'une plus grande flexibilité, avoir une meilleure gestion des risques et se concentrer sur le cœur de son activité.

L'objectif est de garantir la disponibilité et la sécurité des systèmes informatiques tout en réduisant les coûts et en améliorant l'efficacité opérationnelle.

Elle peut inclure :

- L'établissement d'une politique de gestion des actifs informatiques tout au long de leur cycle de vie ;
- La mise en place d'un service d'assistance par exemple au travers d'un outil de gestion des tickets d'incident ;
- Les mises à jour régulières des appareils et logiciels et leur planification, etc..

➔ Lois

Article 544 du Code civil : établit le principe de propriété, qui peut s'appliquer aux biens incorporels, y compris aux actifs informatiques.

Articles 1382 du Code civil : engage la responsabilité civile en cas de dommage causé à autrui. Cela peut s'appliquer en cas de dommage causé par un patrimoine informatique.

Article 5 du RGPD : établit les principes relatifs au traitement des données personnelles, incluant leur licéité, loyauté et transparence. Les entreprises doivent protéger les données personnelles comme faisant partie de leur patrimoine informationnel.

Article 34 de la loi pour la confiance dans l'économie numérique (LCEN) : impose aux prestataires de services de conserver certaines données pendant une durée limitée, en fonction de leur rôle et de leur activité.

1.1. Les acteurs du secteur informatique

Les constructeurs : ces entreprises qui conçoivent et fabriquent le matériel informatique physique, comme les ordinateurs, les serveurs, les périphériques de stockage et le réseautage.

HP, Dell, Lenovo, Apple, Samsung, Cisco,…

Les éditeurs de logiciels : ces entreprises développent et vendent es logiciels, tels que les systèmes d'exploitation, applications logicielles et progiciels.

Microsoft, Oracle, Salesforce, Adobe,…

Les distributeurs et vendeur de solutions : ces entreprises vendent du matériel, des logiciels et des services informatiques à d'autres entreprises. Ils agissent comme intermédiaires entre les fabricants et les revendeurs, en assurant que les produits sont disponibles et livrés aux clients en temps voulu.

L**es intégrateurs** : ces entreprises s'occupent de l'intégration de divers composants matériels et logiciels informatiques pour créer un système complet répondant aux besoins spécifiques d'un client. Ils agissent en tant qu'intermédiaires entre les fabricants de matériel et de logiciels et les utilisateurs finaux, en assurant que tous les composants fonctionnent ensemble de manière transparente.

Les infogérants : un service externalisé qui consiste à confier la gestion et la maintenance d'une partie ou de la totalité du système d'information d'une entreprise à un prestataire externe. Ce prestataire peut prendre en charge divers aspects tes que : le support technique aux utilisateurs, la maintenance du matériel et des logiciels, la sécurité informatique, la gestion des réseaux, le développement et la maintenance d'applications.

Les hébergeurs : ces entreprises mettent à disposition des serveurs et es infrastructures de stockage pour héberger des sites Web, des applications Web, des bases de données et d'autres services informatiques. Les clients de l'hébergeur peuvent être des particuliers, des entreprises, des associations ou des organisations gouvernementales.

OVHcloud , IONOS, Gandi,…

Les FAI : les fournisseurs d'accès à Internet sont des entreprises qui fournissent l'accès à Internet aux particuliers et aux entreprises.

Orange, SFR, Bouygues Telecom, Free,…

Les ESN : entreprises de service numérique, propose des services informatiques à des entreprises clientes. Ces services peuvent inclure : le développement et la maintenance d'applications logicielles, le conseil en informatique, l'intégration de systèmes, l'infogérance, la sécurité en informatique, le cloud computing.

Capgemini, Atos, Sopra Steria, IBM

Les services Cloud : ces entreprises proposent des services de cloud computing, tels que l'infrastructure en tant que service (IaaS), la plateforme en tant que service (PaaS) et le logiciel en tant que service (SaaS).

Amazon -AWS, Cloud – Google, IBM,…

➔ **Lois**

Article 6 de la loi pour la confiance dans l'économie numérique (LCEN) : traite de la responsabilité des fournisseurs de services, y compris les hébergeurs. Il stipule que les hébergeurs ne sont pas responsables des contenus illicites publiés par des tiers, à condition qu'ils agissent promptement pour retirer ces contenus dès qu'ils en ont connaissance.

Article 323-1 du Code pénal : répriment les atteintes aux systèmes de traitement automatisé de données, incluant l'accès frauduleux, l'entrave au fonctionnement, et la détérioration informatique.

Article 5 du RGPD : établit les principes relatifs au traitement des données personnelles, incluant leur licéité, loyauté et transparence. Les entreprises doivent protéger les données personnelles comme faisant partie de leur patrimoine informationnel.

Articles 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : encadre la collecte, le traitement et la conservation des données personnelles. Les acteurs du secteur informatique doivent respecter ces dispositions lorsqu'ils manipulent des données personnelles.

Articles 16 à 18 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) : traitent de la responsabilité des prestataires techniques, notamment en ce qui concerne la conservation et la transmission de données.

1.2. Les enjeux de la gestion

La gestion informatique comporte plusieurs enjeux cruciaux dans le contexte actuel. Voici quelques-uns des principaux :

Sécurité informatique : avec la multiplication des cyberattaques et des menaces en ligne, la sécurité des systèmes et des données est une préoccupation majeure. La gestion informatique doit mettre en place des stratégies et des outils pour protéger les informations sensibles et garantir la confidentialité, l'intégralité et la disponibilité des données.

Gestion des données : la quantité de données générées par les entreprises a explosé ces dernières années. La gestion efficace de ces données, le stockage, leur traitement et leur analyse pour en extraire des informations pertinentes sont des enjeux majeurs pour les organisations.

Infrastructure et technologies émergentes : Les entreprises doivent constamment évaluer et adopter de nouvelles technologies pour rester compétitives. Cela inclut l'infrastructure informatique, les plateformes cloud, l'Internet des objets (IoT), l'intelligence artificielle (IA), la blockchain, etc. La gestion informatique doit s'assurer que ces technologies sont déployées de manière efficace et sécurisée.

Gouvernance et conformité : Les organisations doivent respecter un ensemble de réglementations et de normes en matière de protection des données, de confidentialité, de sécurité et d'autres domaines. La gestion informatique joue un rôle crucial dans la mise en place de politiques de conformité et dans la garantie que les pratiques de l'entreprise respectent ces exigences.

Gestion des risques et continuité des activités : Les interruptions de service, les pannes de systèmes et les catastrophes naturelles peuvent avoir des conséquences désastreuses pour une entreprise. La gestion informatique doit élaborer des plans de gestion des risques et des plans de continuité des activités pour assurer la résilience des systèmes et des opérations en cas d'incident.

Optimisation des coûts et des ressources : La gestion informatique doit s'efforcer d'optimiser l'utilisation des ressources, y compris les infrastructures matérielles et logicielles, pour maximiser l'efficacité opérationnelle tout en minimisant les coûts.

Transformation numérique : Dans un environnement où la technologie évolue rapidement, les entreprises doivent s'adapter et se transformer pour rester compétitives. La gestion informatique joue un rôle clé dans la planification et l'exécution de la transformation numérique, en alignant les technologies sur les objectifs stratégiques de l'entreprise.

En somme, la gestion informatique est au cœur des opérations et de la stratégie des entreprises modernes, et elle doit relever une multitude de défis pour garantir le succès et la pérennité de l'organisation.

→ Lois

Article 1843-4 du Code civil : concerne les obligations des dirigeants en matière de loyauté et de non-concurrence envers leur entreprise. Les dirigeants ont l'obligation d'agir dans l'intérêt de la société et de ne pas exercer d'activités concurrentes.

Article L225-68 du Code de commerce : traite de la responsabilité des administrateurs en cas de préjudice causé par leurs fautes de gestion. Les administrateurs peuvent être tenus responsables sur leurs biens personnels en cas de faute lourde.

1.3. Des actifs informatiques

Les actifs informatiques font référence à tous les éléments de l'infrastructure informatique d'une organisation qui contribuent à la création, au stockage, au traitement et à la transmission des données et des informations. Ces actifs comprennent généralement :

- Matériel informatique
- Logiciels
- Réseaux informatiques
- Données
- Personnel informatique (compétences)
- Politiques, procédures et documentation

Les gestions efficaces des actifs informatiques impliquent leurs surveillances, leur maintenance, leur mise à jour régulière, leur sécurisation et leur alignement sur les objectifs commerciaux de l'organisation. Elle comprend également la gestion des risques liés à ces actifs, notamment les risques de sécurité, de conformité réglementaire, de perte de données et de perturbations des opérations.

➔ **Lois**

Article 323-1 du Code pénal : répriment les atteintes aux systèmes de traitement automatisé de données, incluant l'accès frauduleux, l'entrave au fonctionnement, et la détérioration informatique.

Article 34 LCEN : impose aux prestataires de services de conserver certaines données pendant une durée limitée, en fonction de leur rôle et de leur activité. Cette disposition concerne la gestion et la protection des données informatiques.

Articles 16 à 18 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) : traitent de la responsabilité des prestataires techniques, notamment en ce qui concerne la conservation et la transmission de données.

1.4. Les contrats informatiques

L'expression « contrat informatique », qui ne fait pas l'objet d'une définition légale ou réglementaire ni d'un régime juridique particulier, désigne tout contrat ayant pour objet une **vente, une location et/ou une prestation de services**, relative à un système informatique, ou à un élément intégré ou susceptible d'être intégré dans un tel système :

- Matériel : ordinateurs, périphériques, équipements d'un réseau
- Logiciel : développé par un prestataire pour un client donné ou progiciel standard.

Les contrats le plus fréquents sont :

Contrat de vente ou de location de matériel informatique.

Contrat de licence de logiciel : contrat par lequel l'éditeur d'un logiciel concède à un client le droit de reproduire et d'utiliser ce logiciel dans certains limites (par exemple : limitation du nombre d'utilisateurs, ou du nombre d'installation sur des PCs ou des serveurs, ou du nombre de processeurs du serveur, limitation géographique, etc.) ; le modèle du contrat de licence classique est de plus en plus souvent remplacé par le modèle du contrat SaaS, dans lequel l'utilisation se fait à distance, via Internet au moyen d'un navigateur, sans reproduction du logiciel sur les PC ou des serveurs du client.

Contrat de maintenance de matériel ou de logiciel : contrat par lequel un prestataire informatique s'engage à assurer le maintien du matériel ou du logiciel en condition opérationnelle, en repérant les pannes ou en corrigeant les erreurs, bugs, dysfonctionnements, …

Contrat d'intégration : contrat dans lequel le prestataire informatique (intégrateur) fournit un ensemble de prestations (installation, paramétrage, développements spécifiques, assistance, formation) destinées à permettre l'implémentation d'un logiciel au sein du système

informatique de son client (exemple le plus fréquent, mais il existe de nombreux cas d'intégration).

Contrat de développement de logiciel : contrat par lequel un prestataire informatique s'engage à développer un ensemble de programmes correspondant aux besoins de son clients, exprimés dans un « cahier des charges ».

Contrat d'hébergement de site Web : contrat par lequel le client confie au prestataire le soin d'héberger l'ensemble des données et programmes constituant son site internet (c'est une forme fréquente et parfois minimaliste de contrat d'externalisation).

Ces contrats comportent de nombreuses clauses communes, propres aux contrats informatiques relatives notamment à la propriété intellectuelle des logiciels, de développements et autres créations numériques, à la définition du périmètre technique du contrat, à la « réversibilité », à la protection des données, notamment des données à caractère personnel, …

➔ **Lois**

Article 1101 et suivants du Code civil : établissent les principes généraux applicables aux contrats, y compris les contrats informatiques. Ils abordent des éléments tels que la liberté contractuelle, la formation du contrat, et les obligations des parties.

Article L221-1 et suivants du Code de la consommation : traitent des contrats conclus entre les professionnels et les consommateurs, y compris les contrats de services informatiques. Ces dispositions offrent une protection spécifique aux consommateurs en matière de transparence, d'information et de droit de rétractation.

Article 14 de LCEN : traite de la responsabilité des prestataires de services en ligne, y compris les fournisseurs de services informatiques. Les dispositions de cet article peuvent être intégrées dans les contrats de services informatiques pour définir les obligations et les responsabilités des parties.

Article 28 du RGPD : traite des contrats de traitement de données personnelles entre le responsable du traitement et le sous-traitant. Les prestataires de services informatiques qui traitent des données personnelles doivent conclure un contrat conforme à cet article pour garantir la protection des données personnelles.

1.5. Archivage et preuve

L'archivage est une obligation légale pour les entreprises. Il permet de faire face à de possibles litiges en présentant une pièce à valeur probante, ou encore de justifier les opérations de l'entreprise dans le cas d'un contrôle fiscal.

Les documents se doivent d'être conservés selon une durée prédéterminée par la loi qui varie en fonction de la nature du document (les différents délais de conservations détaillés sur le site de l'administration française). Ainsi, chaque document a son propre « cycle de vie ». Celui-ci va de sa conception jusqu'à sa destruction, soit après la fin du délai de conservation.

L'archivage électronique porte sur la conservation à moyen ou long terme de l'intégrité d'une information ou d'un document. En ce sens, il diffère d'une sauvegarde qui restitue des données à un état antérieur ou encore d'une gestion électronique des documents (GED) qui en facilite l'exploitation. L'archivage électronique permet de recueillir, de classer et de conserver des informations pour que celles-ci puissent être consultées ultérieurement, sans modifications.

➔ **Lois**

Article 1341 du Code civil : stipule que les actes sous seing privé doivent être conservés pendant 5 ans à compter de leur date.

Article L102 B Code général des impôts : stipule que les contribuables doivent conserver pendant 6 ans les documents comptables, fiscaux et sociaux.

Article 5 du RGPD : établit les principes relatifs au traitement des données personnelles, incluant leur conservation. Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Article 6 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : concerne la conservation des données personnelles. Les données personnelles ne doivent pas être conservées au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées.

La preuve

La « preuve numérique » représente toute information numérique pouvant être utilisée comme preuve dans une affaire de type judiciaire. Les entreprises doivent fournir un document électronique qui puisse être retenu comme preuve par les tribunaux. Les outils numériques, tels que les courriels, la signature électronique et les documents numériques, constituent des éléments de preuve nécessaire à la défense d'un professionnel en cas de mise en cause. Se pose alors la question des règles à respecter pour que cette information numérique puisse être considérée comme élément de preuve. Le courrier électronique (recommandé) | La signature électronique

➔ **Lois**

Article 323-3 du Code pénal : punit le fait d'altérer, supprimer, ou rendre inutilisable des données stockées dans un système informatique, ce qui peut avoir des implications sur la validité des preuves électroniques.

Article 5 du RGPD : établit les principes relatifs au traitement des données personnelles, incluant leur exactitude et leur fiabilité. Les données utilisées comme preuve doivent être exactes et fiables pour être acceptées devant les tribunaux.

Article 14 du Loi pour la confiance dans l'économie numérique (LCEN) : traite de la responsabilité des prestataires de services en ligne, y compris en ce qui concerne la conservation et la transmission de données. Les dispositions de cet article peuvent avoir des implications sur la validité des preuves électroniques fournies par les prestataires de services en ligne.

1.6. La charte informatique

Lorsqu'un nouveau salarié est embauché dans l'entreprise, plusieurs étapes doivent être respectées. L'une des premières étapes lors de l'onboarding du salarié est la remise des documents obligatoires. La charte informatique est notamment l'un des documents qui doit être fourni au salarié dès son arrivée dans l'entreprise.

La charte informatique est un document précisant l'utilisation des moyens informatiques et des outils numériques dans l'entreprise. Les bonnes pratiques instaurées via la charte informatique permettent notamment d'éviter tout abus dans l'utilisation des outils informatiques par les salariés.

Ce document juridique permet d'assurer une certaine sécurité numérique au sein de l'entreprise par le respect de règles en matière d'utilisation :

- De la boîte mail ;
- De l'intranet ;
- D'internet ;
- Du matériel informatique.

Cette charte informatique doit :

- Être lisible et compréhensible ;
- Donner des définitions claires et précises ;
- Être signée par les salariés.

Que doit contenir la charte informatique ?

- Son objet et sa portée : rappeler ce sur quoi elle porte ainsi que le fait qu'elle pose les droits et devoirs des utilisateurs.

- Les usages permis des moyens informatiques mis à disposition : rappelle les différents outils et moyens informatiques disponibles en entreprise, les usages que le salarié peut en faire, ainsi que les besoins auxquels le système d'information doit répondre ;
- Les règles de sécurité en vigueur : rappel des bonnes pratiques informatiques.
- Les mesures de contrôle prises par l'employeur : liste des mesures de contrôle, étendue du contrôle et sa conformité avec le droit en vigueur ;
- Les sanctions encourues par l'utilisateur : mentionner une échelle des sanctions auxquelles les salariés peuvent faire l'objet en cas de non-respect de la charte.

➔ **Lois**

Article 323-1 du Code pénal : réprime l'accès frauduleux à un système de traitement automatisé de données. La charte informatique peut inclure des dispositions interdisant l'accès non autorisé aux systèmes d'information de l'entreprise.

Article L1222-1 du Code du travail : impose à l'employeur de prendre les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Une charte informatique peut faire partie des mesures prises par l'employeur pour garantir la sécurité informatique et la protection des données personnelles des salariés.

Article 32 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : impose aux responsables de traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles. Une charte informatique peut détailler ces mesures de sécurité.

Article 32 du RGPD : Il établit l'obligation pour les responsables de traitement et les sous-traitants de mettre en place des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. La charte informatique peut définir les règles et les pratiques à suivre pour assurer la conformité avec cet article.

2. Répondre aux incidents et aux demandes d'assistance et d'évolution

2.1. Accord de niveau de service

Le service-level agreement (SLA) ou « accord de niveau de service » en français, est un document qui définit la qualité de service, prestation prescrite entre un fournisseur de service et un client. Autrement dit, il s'agit de clauses basées sur un contrat définissant les objectifs précis attendus et le niveau de service que souhaite obtenir un client de la part du prestataire et fixe les responsabilités.

Le SLA tend à devenir un outil essentiel aux clients souhaitant bénéficier d'une sécurité élevée sur certains de leurs niveaux de sécurité de stockage ainsi que sur la gestion de leurs données à caractère personnel. De nombreux indicateurs doivent être

définis, analysés et contrôlés afin que la performance proposée par le prestataire soit maximisée.

➔ **Lois**

Article 1103 du Code civil : établit les principes généraux applicables aux contrats, y compris les accords de niveau de service. Cet article stipule que pour qu'il y ait contrat, il faut un consentement, un objet, et une cause. L'accord de niveau de service doit respecter ces principes fondamentaux du droit des contrats.

Article 28 du RGPD : Il traite des contrats de traitement de données personnelles entre le responsable du traitement et le sous-traitant. Si l'accord de niveau de service concerne le traitement de données personnelles, il doit être conforme à cet article pour garantir la protection des données personnelles.

Article 14 de la Loi pour la confiance dans l'économie numérique (LCEN) : traite de la responsabilité des prestataires de services en ligne. Les dispositions de cet article peuvent être intégrées dans les accords de niveau de service pour définir les obligations et les responsabilités des parties en matière de fourniture de services en ligne.

3. Développer la présence en ligne de l'organisation

3.1. E-réputation

La Commission Nationale de l'informatique et des Libertés (CNIL) définit l'e-réputation comme l'image en ligne d'une entreprise ou d'une personne. Cette e-réputation se développe à partir de l'ensemble des informations mises en ligne sur des supports qui ne cessent de croître : site corporate, réseaux sociaux, blogs, forums ou encore plateformes de partage de vidéos. Les informations sont visibles par tous et émanent de sources très variées. Il est donc important d'évaluer sa réputation en ligne, et parfois même d'essayer de la maîtriser.

➔ **Lois :**

Article 9 du code civil : protège le droit à l'image et le respect de la vie privée.

Article 17 du RGPD : stipule le droit de l'individu à obtenir l'effacement de ses données personnelles dans certaines conditions, notamment si ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées.

Article 227-23 du code pénal : sanctionne la diffusion de contenus pornographiques mettant en scène des mineurs.

Article 6-I-2 de la loi pour la confiance dans l'economie numérique (LCEN) : stipule que les hébergeurs ne sont pas responsables des contenus illicites publiées par des tiers, à condition qu'ils agissent promptement pour retirer ces contenus dès qu'ils font connaissance.

3.2. Mentions légales

Les mentions légales sont des informations obligatoires que tout site internet, blog, ou application doit afficher pour être en conformité avec la loi. Elles servent à identifier clairement l'éditeur du site et à informer les utilisateurs sur divers aspects juridiques liés à l'utilisation du site. Ces mentions incluent généralement des informations sur l'identité de l'éditeur, les coordonnées de contact, les conditions générales d'utilisation, ainsi que les informations sur le traitement des données personnelles.

Les mentions légales ont plusieurs objectifs principaux :

- Transparence et identification'
- Protection des droits des utilisateurs
- Conformité juridique
- Responsabilité légale.

➔ **Lois**

Loi pour la Confiance dans l'Économie Numérique (LCEN) : C'est le principal texte qui régit les obligations des éditeurs de sites internet. Les articles clés de cette loi sont :

- Article 6-III : Définit les informations obligatoires à afficher sur un site internet.
- Article 19 : Précise les obligations relatives à la conservation des données des utilisateurs.

Règlement Général sur la Protection des Données (RGPD) : En vigueur depuis mai 2018, ce règlement impose des obligations sur la gestion des données personnelles et renforce les droits des utilisateurs.

- Article 13 et 14 : Informations à fournir aux utilisateurs lors de la collecte de leurs données.

➔ **Actualités :**

- Evolution des mentions légales pour els influenceurs et créateurs de contenu :

Avec la montée en puissance des influenceurs et créateurs de contenu sur les réseaux sociaux, de nouvelles règles encadrent la transparence des partenariats et publicités. Les mentions légales doivent désormais inclure des informations sur les collaborations sponsorisées, sous peine de sanctions pour publicité déguisée.

- Nouvelle obligation pour les sites e-commerce :

Les sites e-commerce doivent désormais inclure des informations plus détaillées sur les avis clients (authenticité, modération), les conditions de retour, et les informations sur les délais de livraison. Ces exigences visent à améliorer la transparence envers les consommateurs.

3.3. Conditions générales d'utilisation d'un site web

Les Conditions Générales d'Utilisation (CGU) sont un document légal qui encadre l'usage d'un site web, d'une application ou d'un service en ligne, définissant les règles et obligations des utilisateurs. Elles visent à informer, limiter la responsabilité du site, encadrer les interactions et protéger les données.

Leurs objectifs incluent :

- Protection juridique
- Clarification des droits et obligations
- Prévention des abus
- Conformité réglementaire

Les CGU évoluent souvent avec la législation et la technologie. Réformes récentes :

- RGPD (2018) : Transparence et consentement sur l'utilisation des données personnelles.
- E-commerce : Renforcement des droits des consommateurs.
- Économie des plateformes : Clarification des responsabilités des plateformes.
- IA et cookies : Règles sur le suivi et le traitement automatisé des données.

3.4. Responsabilité de l'éditeur et de l'hébergeur

L'éditeur est responsable de la gestion du contenu publié en ligne par l'organisation. L'éditeur est responsable du contenu et de sa conformité légale.

Risques en cas de mauvaise gestion :

- Poursuites judiciaires : Non-respect des droits d'auteur, RGPD, ou diffamation.
- Atteinte à la réputation : Contenus erronés ou malveillants nuisant à l'image.

L'hébergeur est chargé de la gestion technique et de la sécurité des infrastructures.

- **Limites de la responsabilité** :
  - L'hébergeur n'est pas responsable des contenus hébergés sauf s'il est informé de leur caractère illégal.
- **Risques en cas de mauvaise gestion** :
  - **Perte de données** : Mauvaise gestion des sauvegardes peut entraîner des pertes importantes.
  - **Failles de sécurité** : Manque de protection peut exposer le site aux attaques.

L'éditeur et l'hébergeur doivent travailler ensemble pour garantir la sécurité et la conformité du site. Les rôles et responsabilités doivent être bien définis pour éviter les litiges en cas de problème technique ou juridique. Une collaboration efficace entre ces deux acteurs est essentielle pour assurer une présence en ligne réussie et conforme aux lois.

➔ **Lois :**
Règlement Général sur la Protection des Données (RGPD)

- **Réglementation** : L'hébergeur est considéré comme un "sous-traitant" dans le cadre du RGPD et doit garantir la sécurité des données personnelles qu'il héberge.
    - **Obligations** : Prendre des mesures techniques pour protéger les données (cryptage, contrôle d'accès, etc.).
- **Sanctions** : En cas de non-respect des obligations, l'hébergeur peut être tenu responsable, avec des sanctions similaires à celles de l'éditeur.

Droit d'auteur et propriété intellectuelle

- Réglementation : L'éditeur doit respecter les droits d'auteur (textes, images, vidéos) en demandant des autorisations pour utiliser des contenus protégés.
- Sanctions : En cas de violation, l'éditeur peut être poursuivi pour contrefaçon.

3.5. Nom de domaine

Un **nom de domaine** est une adresse lisible et mémorable utilisée pour accéder à des sites web sur Internet. Il agit comme un identifiant unique pour des serveurs, sites ou services en ligne, permettant aux utilisateurs d'accéder à un contenu spécifique sans avoir à se souvenir d'une adresse IP complexe.

Par exemple, dans "www.google.com" :

- **"google"** est le domaine de second niveau.
- **".com"** est le domaine de premier niveau.

➔ **Organismes**

CANN (Internet Corporation for Assigned Names and Numbers) : C'est l'organisme international responsable de la coordination des noms de domaine au niveau mondial. L'ICANN supervise le système des noms de domaine, y compris la création de nouvelles extensions (TLD) et la résolution des litiges relatifs aux noms de domaine.

UDRP (Uniform Domain-Name Dispute-Resolution Policy) : Cette politique, établie par l'ICANN, offre un cadre de résolution des litiges concernant les noms de domaine. Elle permet à une partie lésée de demander la suppression ou le transfert d'un nom de domaine si elle peut prouver que le nom a été enregistré de mauvaise foi, ou qu'il enfreint une marque déposée.

➔ **Lois :**

Loi pour la Confiance dans l'Économie Numérique (LCEN) - 2004 : Cette loi encadre la gestion des noms de domaine en France, notamment en ce qui concerne les obligations des hébergeurs et des prestataires de services internet. Elle précise également le rôle des organismes de régulation et les conditions dans lesquelles un nom de domaine peut être suspendu ou supprimé.

➔ **Actualités**

Expansion des extensions de domaines (TLD) : Ces dernières années, l'ICANN a lancé de nombreuses nouvelles extensions de domaines de premier niveau. En plus des traditionnels ".com", ".org", ou ".net", des extensions comme ".tech", ".paris", ".shop" ont vu le jour, offrant aux entreprises et aux particuliers plus de possibilités pour personnaliser leurs adresses web.

P**roblèmes de cybersécurité** : Avec la hausse des activités malveillantes en ligne, la protection des noms de domaine contre les attaques de type **phishing**, **détournement DNS**, et **usurpation d'identité** est devenue une priorité. De nombreux régulateurs et registraires adoptent des mesures pour renforcer la sécurité des noms de domaine, notamment à travers le protocole **DNSSEC** (Domain Name System Security Extensions).

Litiges autour des noms de domaine : Les conflits liés aux noms de domaine continuent de croître, notamment en ce qui concerne les atteintes à la propriété intellectuelle et les cas de cybersquatting. Les procédures UDRP et les jugements de tribunaux nationaux se multiplient dans ces domaines. En 2022 et 2023, certaines grandes entreprises ont récupéré des noms de domaine via des procédures judiciaires ou des règlements à l'amiable, ce qui montre l'importance croissante des noms de domaine comme actifs stratégiques.

B2 : Administration systèmes réseaux & applicative

1. Cahier des charges et ses enjeux numériques

Le **cahier des charges** est un document fondamental dans tout projet, définissant les attentes, exigences, et contraintes liées à la réalisation d'un projet. Dans le domaine du **numérique**, il précise les fonctionnalités, la performance, la sécurité, et les autres caractéristiques techniques d'une solution ou d'un service à développer (site web, logiciel, application, infrastructure IT, etc.). Pour les projets en IT, le cahier des charges permet de détailler les exigences spécifiques en matière de développement logiciel, d'infrastructure réseau ou de cybersécurité.

Enjeux du cahier des charges dans le numérique

Dans le cadre des projets numériques, les enjeux d'un bon cahier des charges sont nombreux :

- **Conformité réglementaire** : Les solutions numériques doivent respecter des normes et des lois spécifiques, notamment en matière de protection des données (RGPD en Europe, par exemple).
- **Sécurité** : La cybersécurité est un enjeu majeur. Le cahier des charges doit détailler les mesures de protection des données (chiffrement, sauvegarde, authentification forte, etc.).
- **Compatibilité et interopérabilité** : Dans un écosystème numérique complexe, la solution doit s'intégrer aux outils existants et respecter des normes de compatibilité.
- **Qualité de l'expérience utilisateur (UX)** : Une mauvaise spécification des exigences UX peut conduire à des interfaces difficiles à utiliser, affectant l'adoption de l'outil.
- **Respect des délais et des coûts** : Un cahier des charges mal défini peut entraîner des dépassements de budget et des retards importants.
- **Sustainability (durabilité)** : L'aspect environnemental devient un enjeu important dans les projets numériques. Le cahier des charges peut inclure des exigences sur l'optimisation des ressources (énergie, matériel), surtout dans un contexte de développement durable.

➔ **Lois :**

Article L111-1 et suivants Code des marchés publiques s'applique aux cahiers des charges des marchés publics.

Non-respect des termes du cahier des charges : Le fournisseur peut voir son contrat rompu ou faire face à des sanctions financières.

➔ **Actualités** :

La numérisation des services publics français a conduit à des révisions des cahiers des charges pour intégrer des exigences de cybersécurité renforcées.

2. Contraintes éthiques et environnementales dans le choix d'une infrastructure réseau

Les infrastructures réseau modernes doivent intégrer des contraintes éthiques et environnementales pour répondre aux exigences sociétales et réglementaires. Sur le plan éthique, il est crucial de s'assurer que les technologies déployées respectent les droits humains, évitent la surveillance excessive, et garantissent la confidentialité des données personnelles. Des mesures peuvent inclure la sélection de fournisseurs responsables ou l'adoption de solutions qui limitent la collecte de données sensibles. Les entreprises doivent également évaluer si leurs infrastructures favorisent une consommation énergétique durable, réduisant ainsi leur empreinte carbone, une exigence de plus en plus demandée par les parties prenantes.

➔ **Lois :**

- Environnement : Loi n° 2021-1104, dite "Loi Climat et Résilience".
- Éthique : Directive européenne 2014/95/UE sur la responsabilité sociale des entreprises.

La violation de ces contraintes peut entraîner des amendes, voire nuire à la réputation des entreprises. Actuellement, les grandes entreprises tech, comme Google et Microsoft, s'efforcent de rendre leurs centres de données et réseaux neutres en carbone, en réponse aux critiques concernant la consommation énergétique massive des infrastructures cloud. Cela illustre l'importance croissante des contraintes éthiques et environnementales dans les décisions technologiques.

➔ **Actualités** :

De grandes entreprises IT comme Microsoft et Google ont annoncé des infrastructures plus écologiques et "sans carbone" pour répondre à la demande croissante de durabilité.

3. Contrat de prestation de services informatiques entre le prestataire et l'organisation cliente et ses clauses spécifiques

Un contrat de prestation de services informatiques encadre les relations entre une entreprise cliente et un prestataire externe qui fournit des services IT. Ce contrat permet de spécifier les attentes, les modalités de service, les droits et les obligations de chaque partie. Les clauses spécifiques incluent généralement les aspects de confidentialité, la sécurité des données, le délai de livraison, les conditions de paiement, ainsi que les responsabilités en cas de manquement aux engagements. Ce type de contrat est particulièrement important pour les entreprises qui sous-traitent des services tels que la maintenance réseau, le support technique ou le développement logiciel. Voici les principales clauses spécifiques du contrat :

1. Objet du contrat : Détaille les services fournis (développement, maintenance, support, etc.).
2. Délai : Fixe la période du contrat et les modalités de renouvellement ou résiliation.
3. Durée Obligations : Précise les responsabilités du prestataire (confidentialité, qualité) et du client (paiements, accès).

4. Tarifs et paiements : Définit le coût des services et les modalités de paiement.
5. Propriété intellectuelle : Indique à qui appartiennent les droits sur les logiciels ou solutions créées.
6. Confidentialité : Garantit la protection des données du client.
7. SLA : Niveaux de service attendus et pénalités en cas de non-respect.
8. Résiliation : Conditions pour mettre fin au contrat.
9. Litiges : Modalités de résolution et juridiction compétente.

Les clauses spécifiques permettent de se prémunir contre les risques potentiels, en définissant, par exemple, les conditions de résiliation en cas de non-respect des engagements. En France, ce type de contrat est soumis au Code civil, notamment pour les aspects de responsabilité, et au RGPD pour les questions de protection des données personnelles. En cas de violation des clauses, des poursuites en responsabilité contractuelle peuvent être engagées. Les récentes évolutions technologiques, telles que le développement du cloud computing, ont également conduit à une complexification des contrats, avec des clauses spécifiques sur la gestion des données dans des infrastructures cloud et les obligations de sécurité.

Ce contrat formalise les engagements et protège les deux parties.

➔ **Lois :**

- Régie par le Code civil (Art. 1101 et suivants) et le RGPD pour les aspects de protection des données.
- Les clauses de non-respect peuvent entraîner des poursuites en responsabilité contractuelle.

➔ **Actualités** :

Avec la montée en puissance du cloud, la rédaction de ces contrats s'est adaptée pour inclure des clauses sur la gestion des données dans des infrastructures externes.

4. Contrat d'entente de niveau de service (ou SLA) déjà étudié dans le bloc

Le contrat d'entente de niveau de service (Service Level Agreement ou SLA) est un accord qui définit les attentes en termes de performances et de disponibilité des services entre un fournisseur de services IT et un client. Ce type de contrat détaille les objectifs de performance (temps de réponse, taux de disponibilité, délai de résolution), les responsabilités respectives, et les mesures de pénalité en cas de non-respect des objectifs. Le SLA est particulièrement courant dans les services de cloud, où la disponibilité et la rapidité des services sont des critères critiques pour les entreprises clientes. Il précise :

1. **Description des services** fournis.
2. **Niveaux de performance** (disponibilité, temps de réponse).
3. **Obligations du prestataire** et du client.

4. **Pénalités** en cas de non-respect.
5. **Procédures d'escalade** pour résoudre les problèmes.

Il assure que les services sont fournis selon les attentes avec des mesures claires et des recours en cas de manquement.

Les SLA n'ont pas de cadre juridique spécifique en France, mais ils sont soumis aux règles générales du Code civil en matière de responsabilité contractuelle. Les SLA incluent souvent des pénalités en cas de non-respect des performances convenues, telles que des réductions de tarifs ou des crédits de service. Ces clauses de service sont devenues plus strictes face à l'augmentation des cyberattaques, ce qui pousse les entreprises à exiger des engagements plus fermes en matière de sécurité et de récupération de données. Le SLA représente donc un engagement mutuel qui protège le client tout en fixant des attentes claires pour le prestataire.

➔ **Lois :**

Aucune réglementation spécifique pour les SLA en France, mais soumis au droit des contrats du Code civil.

En cas de non-respect, des pénalités peuvent être appliquées selon les termes du SLA.

➔ **Actualités :**

En raison de la hausse des cyberattaques, de nombreuses entreprises incluent des SLA plus stricts sur la disponibilité et la sécurité.

5. Des droits et des obligations de l'ASR, l'étendue de sa responsabilité

L'administrateur systèmes et réseaux (ASR) occupe un rôle central dans la gestion de l'infrastructure informatique d'une organisation. Il est chargé de la mise en œuvre, de la maintenance et de la sécurité des réseaux et systèmes, ce qui lui confère un accès privilégié aux données et applications critiques de l'entreprise. Cette responsabilité implique des droits spécifiques, comme l'accès aux données sensibles pour assurer le bon fonctionnement des systèmes, mais elle s'accompagne également de devoirs stricts en matière de protection des données et de confidentialité. L'ASR doit garantir la disponibilité des systèmes, surveiller les anomalies et se conformer aux politiques de cybersécurité.

Sa **responsabilité** porte sur la sécurité, la performance des systèmes et le respect des lois, mais il n'est pas responsable des problèmes externes ou liés à des décisions managériales.

➔ **Lois :**

Code du travail (Art. L1121-1) pour la protection de la vie privée.

RGPD pour les obligations liées à la protection des données personnelles.

Les ASR peuvent être responsables en cas de négligence menant à des pertes de données.

➔ **Actualités :**

Des cas récents ont vu des ASR tenus responsables de violations de sécurité dues à des défauts de maintenance.

6. Contrats spécifiques

Les contrats spécifiques dans les services IT comprennent des accords variés, tels que les contrats de licences logicielles, les contrats de maintenance, le SaaS (Software as a Service), ou encore les prestations de développement sur-mesure. Ces contrats sont essentiels pour définir précisément les droits et obligations de chaque partie, ainsi que les modalités d'utilisation et de répartition des risques. Dans le cadre des licences logicielles, par exemple, le contrat doit inclure les conditions d'exploitation, les limitations d'usage et les obligations de respect de la propriété intellectuelle.

➔ **Lois :**

RGPD pour la protection des données.

Code de la propriété intellectuelle (CPI) pour les droits d'auteur des logiciels.

➔ **Actualités** :

L'évolution des modèles SaaS et PaaS exige une révision régulière des contrats pour intégrer la sécurité et la propriété des données.

7. Cadre juridique spécifique de l'admin systèmes et réseaux

L'administrateur systèmes et réseaux (ASR) dispose d'un cadre juridique spécifique lié à ses missions critiques de gestion et de sécurité des systèmes d'information. En tant que responsable de la bonne marche des infrastructures et des réseaux, l'ASR doit veiller à la protection des données et garantir la disponibilité des systèmes. Il dispose d'un accès privilégié aux données et ressources de l'organisation, mais cet accès est strictement encadré par le droit, notamment le RGPD pour la protection des données personnelles et le Code du travail pour la confidentialité des données des employés.

Toute faute ou négligence de l'ASR, notamment en cas de fuites de données ou d'accès non autorisés, peut engager sa responsabilité civile et, dans certains cas, pénale. Par exemple, une défaillance dans la mise en œuvre des mesures de sécurité peut exposer l'organisation à des violations de données et entraîner des sanctions pour l'administrateur en cas de manquement grave. La jurisprudence montre que les ASR peuvent être tenus responsables pour ne pas avoir correctement exécuté leurs obligations, en particulier face à l'augmentation des cyberattaques et la montée en complexité des infrastructures IT.

8. Les licences

Une **licence en informatique** est un contrat légal qui détermine les conditions d'utilisation, de distribution et de modification d'un logiciel ou d'un code informatique. Ces licences encadrent les droits et obligations des utilisateurs et des développeurs par rapport à un logiciel ou un service. En fonction du type de licence, les utilisateurs peuvent avoir des droits plus ou moins étendus pour utiliser, modifier ou redistribuer le logiciel.

a. Licences propriétaires

Les logiciels sous **licence propriétaire** sont des logiciels dont l'éditeur conserve tous les droits, en limitant l'accès au code source et les droits d'utilisation. Les utilisateurs achètent une licence d'utilisation, mais ils n'ont généralement pas le droit de modifier, distribuer ou copier le logiciel.

Exemples : Microsoft Windows, Adobe Photoshop.

b. Licences libres

Les **licences libres** permettent aux utilisateurs de copier, modifier, et redistribuer le logiciel, souvent à condition de maintenir la même licence sur les versions dérivées. Elles encouragent la collaboration et l'amélioration collective.

Les principaux utiliser :

Linux, Mozilla Firefox.

GPL (General Public License)

Apache License

MIT License

BSD License

c. Licences freemium

Les logiciels freemium sont généralement des logiciels propriétaires qui offrent une version gratuite avec des fonctionnalités limitées et des fonctionnalités supplémentaires payantes.

Exemples : Dropbox, Spotify.

d. Licences open source

Les licences **open source** ressemblent aux licences libres, mais mettent davantage l'accent sur l'accès au code source. Un logiciel open source est accessible à tous, et n'importe qui peut étudier, modifier ou distribuer son code, avec des obligations variables selon les licences.

Exemples : Apache, GPL, MIT.

➔ **Actualités :**

1. **Impact des licences open source dans les grandes entreprises**

En 2023, de nombreuses entreprises, y compris des géants de la technologie comme **Microsoft**, **Google**, et **Amazon**, ont continué à renforcer leur engagement envers l'open source. Cela reflète une tendance croissante dans l'industrie à intégrer des technologies open source pour des raisons de flexibilité, d'innovation rapide, et de réduction des coûts. Les entreprises doivent toutefois s'assurer que leurs produits respectent les termes des licences open source, notamment celles qui imposent des obligations de redistribution (ex. GPL).

2. **Litiges liés aux licences open source**

Les **litiges concernant les licences open source** sont en augmentation. En 2022 et 2023, plusieurs entreprises ont été poursuivies pour avoir violé les termes de la GPL en utilisant du code open source dans leurs produits sans respecter les obligations de redistribution du code source. Ces litiges montrent l'importance croissante du respect des licences open source dans un contexte où de plus en plus de projets numériques s'appuient sur ces technologies.

3. **Réformes des droits d'auteur numériques et des licences**

En réponse à l'évolution des technologies, des réformes du **Digital Millennium Copyright Act (DMCA)** ont été discutées aux États-Unis, cherchant à s'adapter aux nouvelles réalités numériques comme les **NFTs (Non-Fungible Tokens)** et la **blockchain**. De même, l'Union européenne a renforcé son cadre législatif avec la **Directive sur le droit d'auteur dans le marché unique numérique**, qui impacte indirectement les conditions de licence pour les logiciels et les contenus numériques.

9. La protection juridique des productions de solutions applicatives

La protection juridique des solutions applicatives est essentielle pour lutter contre la contrefaçon et le piratage. En cas de violation des droits d'auteur, le producteur de logiciel peut engager des poursuites judiciaires pour obtenir des réparations financières et des injonctions visant à stopper l'usage illégal de son application. La jurisprudence récente en Europe a renforcé ces protections, notamment dans le domaine du logiciel libre, où les licences sont devenues des outils cruciaux pour encadrer l'utilisation, la modification et la distribution de logiciels. Les entreprises doivent donc respecter ces droits pour éviter les litiges, et les développeurs veillent à inclure des clauses spécifiques dans leurs licences pour protéger leurs solutions contre les abus.

➔ **Lois :**

CPI : Art. L122-6 pour la protection des logiciels.

Les violations de licence peuvent entraîner des amendes et des poursuites en contrefaçon.

➔ **Actualités** :

L'essor du logiciel libre a relancé les débats sur les limites des droits d'auteur et les licences ouvertes.

10. La responsabilité civile et pénale

La responsabilité civile et pénale s'applique aux acteurs IT lorsqu'une faute ou négligence entraîne des préjudices, que ce soit pour les utilisateurs, clients, ou tiers. La responsabilité civile vise la réparation des dommages causés à autrui ; elle est engagée si un prestataire ou employé IT manque à ses obligations et cause des dommages matériels ou immatériels. En cas de manquement grave, l'auteur peut être poursuivi pour faute lourde et devra indemniser les victimes, comme en cas de fuite de données personnelles due à une négligence.

La responsabilité pénale intervient si l'infraction est constituée d'une violation de la loi, comme le piratage informatique, la diffusion non autorisée de données, ou la fraude numérique. Selon le Code pénal, ces infractions peuvent entraîner des sanctions allant de l'amende à la peine d'emprisonnement. Dans le contexte de la cybersécurité, les administrateurs et autres responsables IT sont de plus en plus exposés à des poursuites en cas de défaut de protection des systèmes. L'évolution de la législation renforce ainsi les obligations et les sanctions pour encourager une meilleure protection des systèmes d'information et des données personnelles.

➔ **Lois :**

- Code pénal (Art. 226-16 pour les données personnelles).
- Les sanctions incluent des amendes et l'emprisonnement en cas de négligence grave.

➔ **Actualités** :

Les incidents de sécurité récents ont mis en avant les responsabilités des ASR, notamment dans le cadre de la protection des données sensibles.

11. Les données à caractère personnel

Les données à caractère personnel sont définies par le RGPD comme toute information permettant d'identifier directement ou indirectement une personne physique (nom, adresse, numéro de téléphone, etc.). Le RGPD impose aux organisations des règles strictes pour la collecte, le traitement, le stockage et la protection de ces données, exigeant notamment le consentement éclairé de la personne concernée et l'instauration de mesures de sécurité adaptées. Le respect de ces règles est crucial pour assurer la confidentialité et l'intégrité des données et pour limiter les risques de violation.

En cas de non-respect du RGPD, des sanctions financières sévères peuvent être appliquées, pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel de l'entreprise. Les entreprises sont aussi tenues de notifier toute violation des données à caractère personnel dans un délai de 72 heures auprès de la CNIL (en France). L'augmentation des cyberattaques met en lumière les failles de sécurité des données personnelles, et de nombreuses entreprises ont récemment été sanctionnées pour des manquements aux obligations de protection des données, ce qui montre l'importance d'une gestion rigoureuse de ces informations.

➔ **Lois :**

RGPD : Amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel.

➔ **Actualités** :

Depuis sa mise en application, le RGPD a conduit à des centaines de millions d'euros d'amendes pour des entreprises ayant failli à leurs obligations.

12. Les contraintes éthiques et environnementales dans la conception d'une solution

Les contraintes éthiques et environnementales dans la conception d'une solution IT concernent les pratiques durables, l'éthique dans l'usage des données, et la responsabilité sociale des entreprises. D'un point de vue éthique, il s'agit de garantir que les solutions respectent la vie privée, assurent l'équité algorithmique, et évitent toute discrimination ou manipulation des utilisateurs. Les questions de transparence et de respect des droits humains sont centrales, particulièrement pour les entreprises qui manipulent de grandes quantités de données personnelles ou qui développent des intelligences artificielles.

Sur le plan environnemental, la conception durable implique de réduire l'empreinte carbone des solutions, notamment par des choix technologiques économes en énergie, des infrastructures à faible impact environnemental, et une gestion raisonnée des ressources numériques.

➔ **Lois :**

Les lois européennes, comme la directive sur la responsabilité sociale des entreprises **(Directive 2014/95/UE),** imposent de plus en plus aux entreprises de respecter ces contraintes. Aujourd'hui, de grandes entreprises IT s'engagent dans des stratégies de "zéro carbone", cherchant à concilier innovation technologique et développement durable pour limiter l'impact écologique du numérique.

13. Contrat de maintenance applicative (formation, exécution, inexécution)

Un contrat de maintenance applicative encadre les prestations de maintenance logicielle qu'un prestataire effectue pour garantir le bon fonctionnement, la mise à jour et la sécurité d'une application ou d'un logiciel utilisé par un client. Ce type de contrat inclut souvent des clauses sur la formation des utilisateurs ou du personnel technique pour assurer une utilisation optimale de l'application. Les conditions d'exécution précisent les délais de réponse en cas de dysfonctionnement, les procédures de mise à jour et d'assistance, et les modalités de correction des bugs. Le prestataire s'engage à maintenir la solution en état de fonctionnement conformément aux spécifications initiales et aux besoins évolutifs du client.

En cas de manquement, comme une inexécution des prestations de maintenance, le prestataire peut être tenu pour responsable, notamment si cela entraîne une interruption de service préjudiciable pour le client. Les clauses d'inexécution prévoient souvent des pénalités financières ou des réductions de tarif en cas de non-respect des engagements. La jurisprudence considère que le prestataire doit mettre en œuvre tous les moyens raisonnables pour exécuter sa mission, mais en cas de faute lourde ou de négligence, sa responsabilité contractuelle peut être engagée. Le **Code civil** régit les aspects contractuels, et des obligations de sécurité supplémentaires peuvent s'appliquer en vertu du **RGPD** si les applications traitent des données personnelles.

14. Cadre juridique relatif à la conception et à l'exploitation des données de base de données

Le cadre juridique relatif à la conception et à l'exploitation des bases de données a pour objectif de protéger les droits des créateurs et utilisateurs de ces données. Les bases de données sont protégées par le Code de la propriété intellectuelle (CPI) en France, qui offre au producteur un droit spécifique sur la structure de la base et les efforts déployés pour la constituer. En vertu de ce droit, toute extraction ou réutilisation substantielle non autorisée des données d'une base protégée peut être considérée comme une contrefaçon. Par ailleurs, le RGPD impose des obligations strictes de sécurité et de transparence dans la gestion des bases de données contenant des informations personnelles.

Dans l'exploitation d'une base de données, les organisations doivent veiller au respect des droits des utilisateurs, notamment en matière d'accès et de suppression des données personnelles. Des sanctions peuvent être imposées en cas de non-respect de ces obligations, avec des amendes potentielles élevées dans le cadre du **RGPD**. Les récentes affaires de fuite de données ont mis en évidence l'importance du respect des réglementations pour éviter les abus, la surveillance excessive et les violations de la vie privée. Les organisations doivent donc assurer la conformité de leurs pratiques de gestion de données avec les standards légaux pour minimiser les risques juridiques et les atteintes aux droits des utilisateurs.

B3 : Cybersécurité

1. Collecte, traitement et conservation des données à caractère personnel

La **collecte, le traitement et la conservation des données à caractère personnel** concernent toutes les activités impliquant des informations permettant d'identifier directement ou indirectement une personne physique. Ces activités sont cruciales dans le domaine du numérique, car elles touchent à la vie privée et aux droits fondamentaux des individus.

1. Collecte de données à caractères personnel

La collecte des données à caractère personnel désigne l'acquisition ou la réception d'informations concernant un individu. Ces données peuvent inclure :

- Des informations identifiantes (nom, prénom, adresse).
- Des données financières (numéros de carte bancaire).
- Des données comportementales (historique de navigation).
- Des données sensibles (origine, données de santé, opinions politiques).

2. Traitement des données à caractère personnel

Le traitement des données inclut **toute opération ou ensemble d'opérations** effectuées sur les données à caractère personnel. Cela peut inclure :

- La collecte.
- Le stockage.
- L'organisation.
- L'analyse.
- La modification.
- La consultation ou la communication.
- La suppression des données.

3. Conservation des données à caractère personnel

La conservation des données concerne la période pendant laquelle les informations personnelles collectées sont stockées. En principe, les données ne doivent être conservées que pendant la durée nécessaire aux finalités pour lesquelles elles ont été collectées. Les entreprises doivent mettre en place des mesures pour garantir que les données sont sécurisées et que leur durée de conservation respecte les exigences légales.

➔ **Lois**

RGPD :

- **Consentement éclairé** : Les individus doivent donner leur consentement explicite pour le traitement de leurs données.

- **Transparence** : Les entreprises doivent informer clairement les utilisateurs sur la façon dont leurs données sont utilisées.
- **Droit d'accès** : Les utilisateurs ont le droit de consulter les données collectées à leur sujet.
- **Droit à l'oubli** : Les utilisateurs peuvent demander la suppression de leurs données lorsqu'elles ne sont plus nécessaires ou en cas de retrait de consentement.
- **Portabilité des données** : Les utilisateurs peuvent demander la transmission de leurs données d'une entreprise à une autre.
- **Notification de violation** : Les entreprises doivent notifier aux autorités compétentes toute violation de données dans un délai de 72 heures.

➔ **Actualités**

Transfert de données vers les États-Unis : le Privacy Shield remplacé par le Data Privacy Framework

En juillet 2020, la **Cour de Justice de l'Union Européenne** a invalidé l'accord de **Privacy Shield** (Bouclier de Protection des Données) qui permettait le transfert de données personnelles entre l'Union européenne et les États-Unis. Cela a créé un flou juridique pour les entreprises transatlantiques.

En 2023, un nouvel accord, le **Data Privacy Framework**, a été mis en place pour remplacer le Privacy Shield et permettre à nouveau ces transferts tout en garantissant un niveau de protection équivalent à celui du RGPD.

2. Identité numérique de l'organisation

L'**identité numérique d'une entreprise** désigne l'ensemble des informations et des traces qu'une entreprise laisse en ligne. Elle se compose de nombreux éléments qui reflètent l'image et l'existence de l'entreprise dans l'espace numérique, tels que :

- **Nom de domaine** (site web de l'entreprise)
- **Présence sur les réseaux sociaux** (LinkedIn, Twitter, Facebook, Instagram, etc.)
- **Adresses e-mails professionnelles**
- **Contenus publiés en ligne** (articles, blogs, communiqués de presse, newsletters, etc.)
- **Avis et commentaires clients** sur des plateformes dédiées
- **Références et mentions sur d'autres sites ou plateformes** (comme les annuaires professionnels)

L'identité numérique constitue donc l'ensemble des éléments qui permettent de **représenter** l'entreprise dans l'écosystème digital et d'**interagir avec ses clients, partenaires et autres parties prenantes** sur Internet.

Enjeux liés à l'identité numérique :

- Crédibilité et réputation en ligne
- Cybersécurité
- Contrôle de l'image de marque

- Protection des données personnelles
- Marketing numérique et stratégie digitale

➔ **Lois**

Réglementation ePricavy : Cette réglementation, qui complète le RGPD, encadre l'utilisation des cookies, des technologies de suivi et d'autres moyens utilisés par les entreprises pour **collecter des données des utilisateurs** via leurs sites web ou applications. Les entreprises doivent obtenir le consentement explicite des utilisateurs pour l'utilisation des cookies non essentiels.

3. Droit de la preuve électronique

Le droit de la preuve électronique encadre l'admissibilité des documents et échanges numériques comme preuve dans les procédures judiciaires. **La loi française et le Code civil (Art. 1316-1 et suivants**) reconnaissent la validité des documents électroniques sous réserve de leur fiabilité et intégrité. Une signature électronique qualifiée, par exemple, a la même valeur légale qu'une signature manuscrite. Cependant, pour être recevables, les preuves électroniques doivent pouvoir garantir l'authenticité de leur origine et être conservées dans des conditions sécurisées afin d'éviter toute altération.

Les outils comme la blockchain commencent à être explorés pour renforcer la sécurité et l'immutabilité des preuves électroniques. En cas de litige, la charge de la preuve repose souvent sur la capacité à démontrer l'intégrité des fichiers électroniques et des échanges. Les tribunaux s'appuient de plus en plus sur des preuves numériques dans des affaires civiles et commerciales, mais des contestations sur leur validité peuvent survenir si les méthodes de collecte ou de conservation des données ne sont pas conformes aux normes en vigueur. Ce cadre évolue pour mieux répondre aux nouveaux défis posés par les technologies numériques.

4. La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique

Avec l'essor du télétravail et des pratiques BYOD (Bring Your Own Device), la sécurité des équipements personnels utilisés dans un contexte professionnel est devenue une préoccupation majeure. Ces appareils sont souvent plus vulnérables aux cyberattaques que les équipements fournis par l'entreprise (COBO=Company Owned Business Only), car ils ne sont pas toujours protégés par des mesures de sécurité strictes. Les organisations doivent donc déployer des protocoles de sécurité adaptés, incluant des solutions de chiffrement et des logiciels antivirus, pour protéger leurs données sensibles accessibles depuis ces appareils. La charte informatique de l'entreprise joue ici un rôle clé, encadrant les usages permis et imposant des règles de sécurité aux utilisateurs.

Cette charte précise les responsabilités des employés concernant la sécurité de leurs équipements personnels et définit les actions à éviter, comme le stockage de données

professionnelles non sécurisées. En cas de violation des règles de la charte, des sanctions disciplinaires peuvent être appliquées. De plus, si une faille de sécurité due à un équipement personnel conduit à une fuite de données, l'organisation peut engager la responsabilité de l'employé en cas de négligence. Les entreprises doivent ainsi adapter leurs politiques de sécurité pour prendre en compte ces nouvelles modalités de travail et protéger efficacement leurs systèmes d'information.

➔ **Lois :**

Loi n° 2018-493 relative à la cybersécurité.

Les entreprises peuvent limiter ou interdire certains usages pour des raisons de sécurité.

➔ **Actualités :**

Avec le télétravail croissant, de nombreuses organisations ont révisé leurs chartes pour inclure des mesures de cybersécurité renforcées.

5. Les risques économiques et juridiques des cyberattaques pour l'organisation

Les cyberattaques peuvent avoir des conséquences économiques et juridiques désastreuses pour les organisations. Les impacts économiques incluent les pertes financières dues aux interruptions d'activité, les frais de récupération de données, ainsi que les dépenses associées à la réparation des systèmes endommagés. En outre, la perte de données sensibles peut entraîner des répercussions négatives sur la réputation de l'entreprise, ce qui peut se traduire par une baisse de la confiance des clients et une diminution du chiffre d'affaires. Certaines cyberattaques exigent également le paiement de rançons (ransomware), ce qui alourdit encore les coûts pour les organisations touchées.

Les répercussions juridiques d'une cyberattaque peuvent être tout aussi graves, en particulier si l'entreprise ne respecte pas ses obligations légales de sécurité des données. Le **RGPD** impose des obligations de protection des données personnelles et, en cas de violation, des sanctions financières significatives peuvent être infligées par les autorités de régulation. Les entreprises peuvent également faire l'objet de poursuites judiciaires de la part de clients ou partenaires ayant subi un préjudice suite à une cyberattaque. Les incidents récents ont conduit les entreprises à renforcer leurs politiques de cybersécurité pour minimiser ces risques.

➔ **Lois :**

RGPD en cas de fuite de données.

Code pénal pour les infractions liées au piratage et accès illégitime à des données.

➔ **Actualités :**

Les attaques contre des hôpitaux et entreprises du CAC40 ont révélé des lacunes dans la sécurité des infrastructures et relancé les débats sur la protection des infrastructures critiques.

L'attaque récente contre Free, révélée le 26 octobre 2024, a ciblé l'outil de gestion de l'opérateur télécom, menaçant la confidentialité des données personnelles de 19 millions d'abonnés. Bien que les mots de passe, les informations bancaires et le contenu des communications (emails et SMS) n'aient pas été compromis, des informations sensibles telles que les noms, adresses, numéros de téléphone et identifiants abonnés ont été potentiellement exposées. Free a rapidement informé ses clients de cette violation et a renforcé la sécurité de ses systèmes tout en portant plainte auprès des autorités judiciaires françaises pour investigation et notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
CNews | L'Express.

6. La réglementation en matière de lutte contre la fraude numérique

La lutte contre la fraude numérique repose sur un ensemble de régulations et de mesures visant à protéger les systèmes informatiques et les données contre les pratiques frauduleuses. La fraude numérique peut inclure le phishing, les fraudes bancaires en ligne, le détournement d'identité, et d'autres cybercrimes visant à voler ou exploiter illégalement des informations. En France, le Code pénal encadre plusieurs de ces infractions, et des mesures de sensibilisation sont menées pour inciter les entreprises et les particuliers à se protéger contre ces attaques.

Le **RGPD** contribue également à la lutte contre la fraude numérique en imposant des obligations strictes sur la protection des données personnelles. Les organisations doivent donc adopter des politiques de sécurité renforcées, des audits réguliers et des formations pour détecter et prévenir les fraudes numériques. À l'échelle européenne, des initiatives comme le Digital Services Act visent à renforcer les obligations des plateformes numériques pour lutter contre les abus. Le développement rapide des technologies entraîne une augmentation des tentatives de fraude, rendant cruciale l'application de mesures de prévention et de dissuasion adaptées.

➔ **Actualités :**

L'attaque récente contre Free, révélée le 26 octobre 2024, a ciblé l'outil de gestion de l'opérateur télécom, menaçant la confidentialité des données personnelles de 19 millions d'abonnés. Bien que les mots de passe, les informations bancaires et le contenu des communications (emails et SMS) n'aient pas été compromis, des informations sensibles telles que les noms, adresses, numéros de téléphone et identifiants abonnés ont été potentiellement exposées. Free a rapidement informé ses clients de cette violation et a renforcé la sécurité de ses systèmes tout en portant plainte auprès des autorités judiciaires françaises pour investigation et notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
CNews | L'Express

7. Un panorama des organisations de lutte contre la cybercriminalité

Diverses organisations nationales et internationales se mobilisent pour lutter contre la cybercriminalité, protégeant ainsi les réseaux, les données, et les individus contre les cyberattaques. En France, la gendarmerie nationale dispose d'une division spécialisée, le **Centre de lutte contre les criminalités numériques (C3N**), qui collabore avec d'autres institutions, comme **l'ANSSI** (Agence nationale de la sécurité des systèmes d'information) pour protéger les infrastructures critiques. À l'échelle européenne, Europol gère le Centre européen de lutte contre la cybercriminalité (EC3), qui coordonne les efforts des États membres pour lutter contre les cybermenaces transnationales.

Au niveau international, **Interpol** joue un rôle de coordination entre les polices de différents pays pour enquêter sur les cybercrimes. Des collaborations entre agences, telles que celle entre le FBI aux États-Unis et les agences européennes, se développent également pour mieux contrer les attaques mondiales. L'évolution rapide des technologies impose une adaptation continue des stratégies de lutte contre la cybercriminalité, ainsi qu'une coopération accrue entre les acteurs publics et privés pour assurer une protection optimale contre les cyberattaques.

➔ **Actualités** :

Les partenariats entre entreprises et organismes gouvernementaux se sont intensifiés pour lutter contre les cyberattaques, notamment via des collaborations dans le domaine de la cybersécurité.

L'attaque récente contre Free, révélée le 26 octobre 2024, a ciblé l'outil de gestion de l'opérateur télécom, menaçant la confidentialité des données personnelles de 19 millions d'abonnés. Bien que les mots de passe, les informations bancaires et le contenu des communications (emails et SMS) n'aient pas été compromis, des informations sensibles telles que les noms, adresses, numéros de téléphone et identifiants abonnés ont été potentiellement exposées. Free a rapidement informé ses clients de cette violation et a renforcé la sécurité de ses systèmes tout en portant plainte auprès des autorités judiciaires françaises pour investigation et notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
CNews | L'Express

8. Les obligations légales de notification

Les obligations légales de notification imposent aux entreprises de signaler aux autorités compétentes toute violation de données personnelles dans un délai défini, généralement sous 72 heures après la découverte de l'incident. Ces obligations, établies notamment par le RGPD, visent à garantir la transparence vis-à-vis des utilisateurs touchés et à limiter les impacts des fuites de données. Lorsqu'une violation est susceptible de porter atteinte aux droits et libertés des individus, l'organisation doit non seulement informer l'autorité de protection (comme la CNIL en France) mais aussi, dans certains cas, les personnes concernées.

Le non-respect de ces obligations peut entraîner des sanctions financières importantes, pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial de l'entreprise fautive. Ces obligations de notification sont devenues cruciales dans un contexte d'augmentation des

cyberattaques et des risques de fuites de données. Elles permettent de responsabiliser les organisations et de renforcer les pratiques de sécurité pour prévenir de telles violations.

➔ **Actualités :**

L'attaque récente contre Free, révélée le 26 octobre 2024, a ciblé l'outil de gestion de l'opérateur télécom, menaçant la confidentialité des données personnelles de 19 millions d'abonnés. Bien que les mots de passe, les informations bancaires et le contenu des communications (emails et SMS) n'aient pas été compromis, des informations sensibles telles que les noms, adresses, numéros de téléphone et identifiants abonnés ont été potentiellement exposées. Free a rapidement informé ses clients de cette violation et a renforcé la sécurité de ses systèmes tout en portant plainte auprès des autorités judiciaires françaises pour investigation et notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) et l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
CNews | L'Express

9. Responsabilité civile et pénale de l'admin systèmes réseaux

L'administrateur systèmes et réseaux (ASR) assume une responsabilité importante dans la gestion, la protection et la maintenance des infrastructures informatiques de son organisation. Sa responsabilité civile peut être engagée en cas de faute, négligence ou manquement à ses obligations contractuelles ayant causé un dommage à l'entreprise, aux utilisateurs ou aux clients. Par exemple, une mauvaise gestion de la sécurité informatique qui entraîne une fuite de données personnelles pourrait exposer l'ASR à des sanctions civiles et à des demandes d'indemnisation. En règle générale, l'organisation est responsable des actions de ses employés, mais en cas de faute lourde ou de manquement grave, l'ASR peut être tenu personnellement responsable.

➔ **Lois :**

Sur le plan pénal, l'ASR pourrait être poursuivi si son inaction ou sa négligence facilite la **commission de crimes informatiques** ou des violations de la législation, comme la fraude, l'accès non autorisé aux systèmes, ou la diffusion de données confidentielles. Le **Code pénal** prévoit des sanctions pouvant inclure des amendes et des peines de prison pour les infractions graves, en particulier si celles-ci compromettent la sécurité des systèmes d'information ou portent atteinte aux droits des utilisateurs. La **jurisprudence** reconnaît que l'ASR a une obligation de moyens renforcée en matière de sécurité, ce qui implique qu'il doit prendre toutes les précautions nécessaires pour prévenir les incidents informatiques et veiller à la conformité avec les lois de protection des données, telles que le **RGPD**.