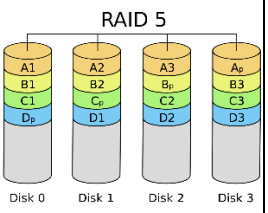
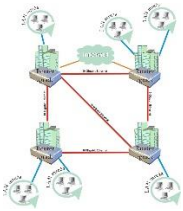
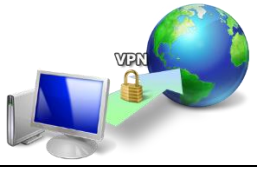
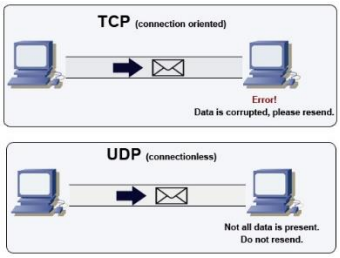
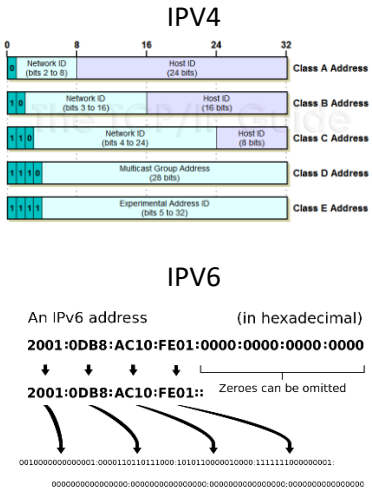
FICHE RESSOURCE – STRUCTURE DU RÉSEAU – PROTOCOLES – ÉLÉMENTS PHYSIQUES & LOGICIELS - SÉCURITÉ

Les tableaux synthétiques ci-dessous vous présentent les informations essentielles à retenir pour la GSI.

	Rôle	
Matériel de connexion		
- **Prise Ethernet (RJ45)**	Elément physique du réseau qui est positionné à proximité d'un ordinateur fixe et qui est relié au réseau de l'entreprise. Le débit maximum est de l'ordre du Gigabit mais il est soumis à des perturbations électromagnétiques.	
- **Borne Wifi**	Elément physique du réseau qui est positionné à proximité des ordinateurs de l'entreprise et qui propose une connexion sans fil. Elle est reliée elle-même au réseau de l'entreprise par une connexion Ethernet.	
- **Câble Ethernet**	Elément physique du réseau qui connecte la carte réseau de l'ordinateur fixe à la prise Ethernet du réseau de l'entreprise. La distance est limitée à 100 mètres (voire 70 mètres)	
- **Répéteur**	Matériel qui permet de répéter le signal qui emprunte le câble Ethernet afin de réduire la perte de qualité	
- **Carte réseau Ethernet**	Elément physique de l'ordinateur qui permet de le relier au réseau de l'entreprise par l'intermédiaire d'un câble Ethernet.	
- **Carte réseau wifi**	Elément physique de l'ordinateur qui permet de le relier au réseau de l'entreprise par un l'intermédiaire d'une borne wifi (reliée elle-même au réseau de l'entreprise).	
- **Câble optique (jarretière optique)**	Elément physique d'interconnexion de différents segments d'un réseau local séparés par des espaces ouverts ou soumis à perturbation électromagnétique. Les câbles optiques relient généralement les commutateurs des différents segments. Le débit est de l'ordre du Gigabit.	
- **Commutateur**	Elément physique d'interconnexion de l'ensemble des matériels actifs d'un réseau (ordinateurs, serveurs, imprimantes, bornes wifi, etc.). Sa taille, son coût varie selon les besoins d'interconnexion. Une prise est à prévoir par matériel à raccorder. Il réduit le traffic sur le réseau car il sait n'envoyer le message (trame) qu'au seul bon ordinateur concerné.	
- **Bridge**	Elément matériel qui relie deux réseaux en acheminant au bon endroit les informations d'un réseau vers un autre réseau.	
- **Routeur**	Elément matériel qui permet de relier deux réseaux différents. Il peut gérer en plus la sécurité en limitant les accès de part et d'autre des réseaux.	
- **Boîtiers ADSL des FAI**	Ils jouent à la fois le rôle de switch, de borne wifi et de routeur. Ils permettent de relier le LAN (réseau local) et le WAN (réseau internet)	

FICHE RESSOURCE – STRUCTURE DU RÉSEAU – PROTOCOLES – ÉLÉMENTS PHYSIQUES & LOGICIELS - SÉCURITÉ

Matériel de protection physique		
- **Onduleur**	Elément matériel qui protègent les matériels actifs (ordinateurs, serveurs, commutateurs, routeurs) des surtensions. L'onduleur est branché sur le réseau électrique et les matériels sont branchés sur le onduleur.	
- **Branchement RAID**	Pratique qui consiste à dédoubler (redondance) le nombre de disques durs sur un serveur afin de garantir la sécurité des données. Selon la configuration, la panne mécanique d'un disque dur garantie le maintien de la donnée sauvegardée. L'organisation RAID standard proposée sur les serveurs est du RAID 5 avec 4 disques durs. Pour le serveur, il n'existe qu'un seul disque dur. L'information est recopiée sur chaque disque.	
- **Protection incendie**	Ensemble des éléments qui garantissent la sécurité contre les risques d'incendie (alarme, extincteurs spécifiques, portes coupe-feu).	
Solutions de protection logicielle		
- **Antivirus**	Solution logicielle qui garantit la sécurité des données locales (ordinateurs ou serveurs) contre les virus (programmes malveillants) qui peuvent prendre le contrôle, crypter les données, etc.	
- **Antispyware**	Solution logicielle qui permet de protéger la confidentialité de l'activité d'un utilisateur	
- **Firewall**	Solution logicielle (ou matérielle) qui permet de protéger un ordinateur (logicielle) ou l'ensemble d'un réseau (matérielle) contre les tentatives d'intrusion extérieure.	
Typologie des réseaux		
- **LAN (Local Area Network)**	Réseau local qui peut être organisé en Poste à Poste (A - Peer to Peer) ou en Client / Serveur (B). Dans le mode Peer to Peer, chaque ordinateur est à la fois client et serveur des autres. Dans le mode Client / Serveur, un ordinateur central joue le rôle de Serveur (fournit des services) et les autres ordinateurs jouent le rôle de client (utilisent les services). C'est le mode le plus répandu aujourd'hui.	 (A)  (B)
- **MAN (Metropolitan Area Network)**	Le MAN interconnecte plusieurs LAN proches de quelques dizaines de kilomètres par des liaisons fibre (ex : FTTH sur Dunkerque, Saint-Pol-sur-mer, Cappelle-la-Grande et Coudekerque-Branche). Il permet la création d'un immense réseau local. Il permet pour certaines entreprises de relier différents sites par des Fibres Noires et de créer un réseau LOCAL à l'échelle d'une ville.	
- **WAN (Wide Area Network)**	Le WAN interconnecte les LAN séparés par de grandes distances en utilisant des solutions spécifiques afin de garantir les débits et vitesses de connexion. Internet est un exemple du WAN.	
- **VPN (Réseau Privé Virtuel)**	Solution matérielle et logicielle qui permet de relier deux entités géographiquement distantes par une solution internet tout en garantissant la sécurité de la transmission des données.	

	Les deux entités reliées par une solution VPN sont placées dans une structure de réseau local.	
Protocole		
- **TCP**	**Transmission Control Protocol**. Protocole qui permet de vérifier que l'information est bien arrivée à destination. Plus fiable que UDP, il est aussi plus lent.	
- **UDP**	**User Datagram Protocol** (**UDP**, en français protocole de datagramme utilisateur). Il est utilisé dans les protocoles de transfert de données sans contrôle des erreurs. Plus rapide, il est moins fiable. Utilisé notamment dans les flux vidéos en streaming.	
- **IP**	**Internet Protocol** Protocole qui permet de créer une identification **UNIQUE** sur un réseau pour un matériel actif (ordinateur, serveur, imprimante, etc.). **IPV4 – Procotole IP** sur 4 octets. Chaque octet peut prendre les valeurs entières entre 0 et 255. Exemple : 192.168.120.14 4,3 milliards d'adresses possibles **IPV6 – Procotole IP** sur 8 groupes de 4 caractères (chiffres et lettres) Exemple : 2001 :0db8 :0000 :85a3 :0000 :0001 :ac1f :8001 667 millions de milliards d'adresses disponibles. Internet des objets	
- **IP privée / IP publique**	**IP privée :** Adresse IP attribuée à un matériel actif dans le cadre du LAN ET non utilisable sur l'internet. Les matériels actifs du réseau local n'ont qu'une adresse IP privée. **IP publique** : Adresse IP attribuée à un routeur par le FAI ET utilisable sur l'internet. Le routeur de l'entreprise peuvent avoir une ou plusieurs adresses privées et éventuellement une adresse publique.	
- **Masque de sous-réseau**	**Il permet de fixer la taille du réseau et le nombre d'hôtes disponibles sur le réseau :** **Masque** / **Net ID** / **Host ID** **255.0.0.0** / **Octet 1** / **Octets 2-3-4** **255.255.0.0** / **Octets 1 - 2** / **Octets 3 - 4** **255.255.255.0** / **Octets 1 – 2 – 3** / **Octet 4**	
- **Adresse Passerelle**	**Adresse IP attribuée au routeur (dans le réseau local) afin de pouvoir communiquer avec l'extérieur. Chaque matériel actif, pour avoir accès à internet, doit connaître l'adresse passerelle.**	
- **WINS**	**WINDOWS INTERNET NAME SERVICE** Service installé sur un serveur qui permet de transformer les adresses IP locales en nom et inversement. Service dépassé et remplacé par le service d'annuaire AD de Windows et le DNS dynamique	
- **DNS**	**Domain Name System** Service essentiel à internet car il permet de transformer les adresses IP publiques en noms de domaine et inversement. Généralement, on utilise le DNS du FAI. Si le DNS	

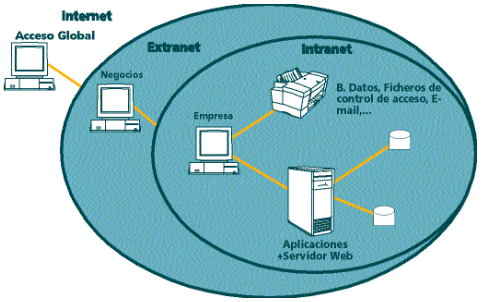
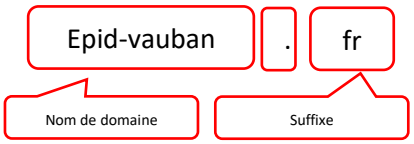
<table>
<tr><td></td><td>est en panne, le navigateur ne pourra pas afficher le site web via son nom mais via son adresse ip.</td></tr>
<tr><td>- Protocole DHCP</td><td>Dynamic Host Control Protocol. Protocole qui permet à un ordinateur central d'attribuer à la demande (des autres matériels) une adresse IP unique dans un pool d'adresses fixées par l'administrateur.
Cela permet d'automatiser la gestion des adresses IP pour chaque matériel (donc de gagner du temps) et d'éviter les erreurs d'attribution (doublons possibles).</td></tr>
<tr><td colspan="2">Les différents types de serveur</td></tr>
<tr><td>- D'applications</td><td>Il centralise les applications utilisées sur les postes clients tandis que les interfaces hommes-machines sont installées sur les postes clients. Il permet de mieux contrôler les utilisations des applications.</td></tr>
<tr><td>- De données ou de fichiers (NAS)</td><td>Il stocke les fichiers informatiques et notamment les données partagées (agendas partagés, messagerie, base de données). Les applications clientes du réseau y accèdent pour charger les fichiers.</td></tr>
<tr><td>- D'impression</td><td>Il permet de partager une imprimante entre les différents postes reliés au réseau. Il centralise les impressions, la file d'attente et lance les éditions.</td></tr>
<tr><td>- Web</td><td>Relié à internet, il peut héberger le site internet de l'entreprise et gère les requêtes des internautes. Il peut aussi stocker les documents internes et jouer le même rôle sur l'intranet de la société.</td></tr>
<tr><td>- SMTP et POP</td><td>Le serveur SMTP (simple Mail Transfert Protocol) gère les mails sortants et le serveur POP (Post Office Protocol) gère les mails entrants.</td></tr>
<tr><td>- IMAP</td><td>Interactive Message Access Protocol
Protocole qui permet d'accéder à sa messagerie via un navigateur.</td></tr>
<tr><td>- HTTP</td><td>Hypertext Transfer Protocol permet de gérer les communications client/serveur sur l'internet. On l'utilise à travers les navigateurs web</td></tr>
<tr><td>- HTTPS</td><td>S pour sécurisé. Le protocole HTTPS crypte les données entre le serveur web et le client. Il assure donc une meilleure sécurité et confidentialité des données transmises sur l'internet.</td></tr>
<tr><td>- FTP</td><td>File Transfert Protocol permet de transférer (déposer ou récupérer) des fichiers sur des serveurs de stockage en ligne. On utilise un logiciel spécifique pour récupérer et déposer des dossiers sur le serveur à distance (filezilla). Le navigateur internet permet d'accéder uniquement en téléchargement aux fichiers disponibles à distance.</td></tr>
<tr><td colspan="2">Les droits des utilisateurs sur les fichiers, les logiciels et matériels</td></tr>
<tr><td>- Droits standards d'accès aux données</td><td>Pour protéger la confidentialité, l'accès à certaines données peut être limité.
Un utilisateur (ou un groupe d'utilisateurs) peut avoir les droits suivants :

<table>
<tr><th>Droit</th><th>Explication</th></tr>
<tr><td>Lecture</td><td>Peut ouvrir un fichier sans le modifier</td></tr>
<tr><td>Ecriture</td><td>Peut déposer/créer un fichier à un emplacement</td></tr>
<tr><td>Modification</td><td>Peut ouvrir un fichier et le modifier sans pouvoir le supprimer.</td></tr>
<tr><td>Suppression</td><td>Peut supprimer un fichier.</td></tr>
<tr><td>Exécuter</td><td>Peut lancer une application</td></tr>
<tr><td>Lister</td><td>Peut lire le contenu d'un dossier sans pouvoir ouvrir les fichiers ou dossiers.</td></tr>
<tr><td>Contrôle total</td><td>Peut tout faire et modifier les règles de sécurité pour les autres utilisateurs.</td></tr>
</table>
</td></tr>
<tr><td>- Droits liés aux logiciels</td><td>Certains logiciels (ou PGI) permettent d'accorder ou non certains droits aux utilisateurs. Ils imposent généralement l'obligation de s'authentifier (PGI).
Certaines applications peuvent être protégées par un mot de passe (Excel, Word) et en lecture seule sur la structure du fichier.</td></tr>
</table>

Les risques et leur(s) solution(s)		
Type	Explication	Solution
- **Virus**	Fichier exécutable qui permet de prendre le contrôle, de crypter les données, d'espionner le comportement de l'utilisateur. Souvent associé en pièce jointe d'un mail. Virus de boot (prend le contrôle de l'ordinateur) Virus d'application (infecte un progiciel ou s'exécute à son lancement) Macro virus (infecte les macro-commandes des documents bureautiques)	Antivirus (protection en temps réel)
- **Ver (Worm)**	Virus spécifique au réseau. Il récupère les adresses des contacts de l'utilisateur et envoie des copies à tous les destinataires qui seront aussi infectés.	Antivirus
- **Cheval de Troie (Trojan)**	Programme caché qui ouvre un port internet de l'ordinateur pour le rendre accessible à des pirates extérieurs. Il facilite l'espionnage ou la prise de contrôle de l'ordinateur.	Firewall
- **Spyware**	Programme mouchard qui recueille des informations sur les habitudes de l'ordinateur puis les envoie à un tiers qui l'utilise pour dresser un profil (profilage)	Antispyware
- **Cookie**	Fichier stocké sur le disque dur de l'ordinateur pendant la consultation de sites web. Stocke des informations sur votre profil. Lors d'une nouvelle connexion, ce fichier est utilisé pour proposer une offre personnalisée.	Interdire les cookies dans le navigateur. Attention, certains sites peuvent ne pas fonctionner correctement.
- **Pourriel**	SPAM (courrier indésirable) envoyé en masse à des fins publicitaires. 75% des messages.	Anti-spam sur le réseau ou sur chaque ordinateur
- **Hameçonnage**	Phishing qui consiste à afficher une page identique à celle d'un site de confiance (banque, administration, etc.) pour soutirer des informations confidentielles (login, mot de passe, numéro carte de crédit, etc.)	Filtre anti hameçonnage (souvent avec anti-spam)
- **Hacker, Cracker, espionnage**	Hacker : casse les codes d'accès aux ordinateurs ou réseaux pour pénétrer un système informatique (par jeu ou malveillance).	Solution logicielle : protection par mots de passe Solution matérielle : accès physique limité, protection par cryptage
- **Vol et sabotage**	Vol de données, casse intentionnelle du matériel	Protection par assurances Limitation des accès aux données et matériels sensibles
- **Piratage des réseaux sans fil**	La récupération des informations qui transitent via ces réseaux est possible	Crypter les données transmises par un protocole spécifique (clé WEP-WPA)
- **Chantage numérique**	Ransomware. Technique qui consiste à rendre les fichiers voir les ordinateurs illisibles par cryptographie et de	Protéger le réseau (éviter les mails

	proposer un échange de rançon contre un code de déblocage à la victime.	douteurs). Si en action, aucune solution.
- **Canular (Hoax)**	Messages qui colportent des mensonges ou rumeurs (chaînes de solidarité, théories conspirationnistes) destinés à utiliser la crédulité des internautes.	Regard critique sur l'information et contrôler les sources.
Les sauvegardes informatiques		
- **Sauvegarde complète**	Manuelle ou automatique. Elle consiste à copier périodiquement (tous les mois, toutes les semaines) l'intégralité des données d'un disque sur un support externe.	Inconvénients : -Risques d'oubli -Longueur de la sauvegarde -Modifications entre 2 sauvegardes sont perdues
- **Sauvegarde incrémentale**	Sauvegarde automatique après une première sauvegarde complète. Seuls les fichiers modifiés ou ajoutés depuis la dernière sauvegarde sont sauvegardés.	Avantage : -Réduction du besoin de stockage Inconvénient : -Avoir toutes les sauvegardes incrémentales pour reconstituer la sauvegarde complète
- **Sauvegarde différentielle**	Sauvegarde automatique après une première sauvegarde complète. Seuls les fichiers modifiés ou ajoutés depuis la dernière sauvegarde complète sont sauvegardés.	Avantage : -Fiabilité Inconvénient : -Sauvegarde plus lente et plus coûteuse en espace de stockage
- **Modes de restauration des sauvegardes**	Débuter par la dernière sauvegarde Si incrémentale : restauration chronologique Si différentielle : restauration de la sauvegarde la plus récente	
Les mots de passe		
- **Méthodes d'attaque**	- **Ingénierie sociale** : deviner le mot de passe selon le profil du propriétaire (nom, prénom, date de naissance) - **Attaque brute** : génération de mots de passe aléatoires.	Pas de solution miracle. Avoir un mot de passe long et complexe ralenti le succès du piratage.
- **Conseils mots de passe forts**	- 8 à 10 caractères - Minuscules, majuscules, lettres, chiffres, caractères spéciaux - Pas de lien avec soi - Unique (un par accès) - Modifié régulièrement - Ne pas être enregistré - Ne pas être noté dans un fichier de l'ordinateur - Nombre de tentatives d'accès limité	Méthodes pour retenir un mot de passe complexe : **Phonétique** : « J'ai acheté 3 CD pour cent euros cet après midi » ➔ Ght3cdp%E7am **Premières lettres** : « La vie vaut-elle d'être vecue mon amour ? » ➔ LVVEDEVMA

FICHE RESSOURCE – STRUCTURE DU RÉSEAU – PROTOCOLES – ÉLÉMENTS PHYSIQUES & LOGICIELS - SÉCURITÉ

<table>
<tr><th colspan="3">Intranet, extranet et internet</th></tr>
<tr><td>- Intranet</td><td>Réseau informatique interne de l'entreprise réservé aux seuls membres de l'entreprise. Il est fermé et protégé.</td><td rowspan="3"> 
</td></tr>
<tr><td>- Extranet</td><td>Réseau informatique ouvert et contrôlé à des partenaires extérieurs à l'entreprise. Réseau privé et protégé interconnectant plusieurs intranets d'entreprises.</td></tr>
<tr><td>- Internet</td><td>Réseau informatique mondial, ouvert et non protégé.</td></tr>
<tr><th colspan="3">Noms de domaine, utilisation</th></tr>
<tr><td>- Nom de domaine</td><td>Remplace l'adresse IP sur l'internet.
Facilement identifiable sur l'internet, son accès est payant et chaque nom de domaine est unique.
On peut l'acheter auprès de prestataires (quelques euros à quelques centaines) auprès de l'ICANN.
Nom de domaine : en rapport avec l'activité de l'entreprise
Suffixe :
- Code pays : (fr, eu, de, uk)
- Domaine activité (org, com, net, asso, gouv)</td><td> 
</td></tr>
<tr><th colspan="3">Sécurité et nouvelles pratiques informatiques</th></tr>
<tr><td>- BYOD</td><td>Bring your own device
Les salariés utilisent leur propre matériel</td><td rowspan="3">Le BYOD Génère une image positive mais créé des nouveaux risques.

Obligation de sécuriser les appareils (CYOD ou COPE) et de développer des opérations de sensibilisation aux bonnes pratiques pour se protéger tout en respectant les salariés et en les préservant de systèmes trop contraignants.</td></tr>
<tr><td>- CYOD</td><td>Choose your own device
Les salariés choisissent leur appareil ou l'un des appareils proposés par l'entreprise</td></tr>
<tr><td>- COPE</td><td>Corporate owned personnally enabled
Les salariés utilisent du matériel appartenant à l'entreprise dans le cadre du travail mais aussi pour un usage personnel</td></tr>
<tr><th colspan="3">Licences logiciels et droits du numérique</th></tr>
<tr><td>- Contrat CLUF</td><td colspan="2">Contrat de licence Utilisateur final
- Simple droit d'utilisation d'un logiciel.
- Nombre d'installations limité
- Une seule copie de sécurité
- Acceptation globale et non partielle
Interdiction d'installation sur un autre matériel, etc.</td></tr>
<tr><td>- Licence GNU GPL ou Créative Commons (CC)</td><td colspan="2">Lié aux logiciels libres en réaction à la situation de Microsoft.
- Programme librement copiable, diffusable, installable et utilisable.
- Le code source est public et toute modification doit être accessible librement.
Obligation plus éthique que juridique</td></tr>
<tr><td>- RGPD ou GDPR</td><td colspan="2">La GDPR (General Data Protection Regulation) est un nouveau règlement européen qui introduit une série de mesures fixant le cadre juridique relatif à la protection des données personnelles au sein de l'Union européenne. Il s'agit de renforcer les droits des citoyens de l'UE et leur accorder plus de contrôle sur leurs données personnelles.</td></tr>
</table>

Ce règlement s'appliquera à toute entreprise amenée à collecter et manipuler les données de ses clients. Les multinationales, mais aussi les PME, les TPE ou les artisans gérant un fichier client.

Quel est le principe ?

Le point majeur concerne le principe du consentement à la collecte et à la conservation des données, une notion qui constitue l'une des spécificités du droit européen. Les données personnelles appartiennent aux citoyens et les entreprises, et notamment les géants américains (Facebook, Google, Apple, Amazon, Microsoft et consorts), ne pourront donc plus arguer d'une présomption de consentement pour justifier de l'utilisation des infos de leurs clients et usagers.

Concrètement, que prévoit la GDPR ?

Les entreprises devront désormais fournir des informations précises sur leur pratique de collecte et de conservation des données personnelles. Des informations qui devront en outre être formulées de manière claire et précise dans un souci de transparence.

Les obligations imposées aux entreprises

- Respect de la protection des données dès la conception (article 25 §1)
- Obligation de sécurité par défaut (article 25 §2)
- Obligation de documentation (article 24);
- Étude d'impact avant la mise en œuvre de certains traitements (article 35);
- Obligation de nommer un délégué à la protection des données ou "Data Protection Officer" (article 37), garant des moyens mis en œuvre par l'entreprise.

Que faire en cas d'incident touchant les données clients ?

Tout incident susceptible d'avoir compromis l'intégrité de données des clients de l'entreprise doit être déclaré officiellement à la CNIL dans un délai de 72 heures. Cette tâche incombe au Data Protection Officer désigné par l'entreprise.

Quelles sanctions en cas d'infraction ?

Un arsenal de sanctions administratives en cas de non-respect de la réglementation, peut aller du simple avertissement à une amende d'un montant pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise.

- **CNIL**

Commission Nationale Informatique et Libertés (1978) est chargée de veiller à ce que l'informatique ne porte pas atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Les entreprises doivent déclarer leurs fichiers nominatifs dès qu'ils contiennent des données personnelles sur un individu (nom, prénom, date de naissance, etc.). Toute entreprise doit avoir un référent numérique CNIL.

Mentions obligatoires sur un site web :

Si l'exploitant est une personne physique	Le nom du directeur de publication Le nom du responsable de la rédaction Noms et prénoms et numéros de téléphone, le numéro RCS ou celui fournir par la chambre des métiers
Si l'exploitant est une personne morale	Le nom du directeur de la publication nommée par la personne morale Le numéro RCS donné lors de l'inscription sur le registre ou le numéro donné par la chambre des métiers en cas d'inscription La dénomination ou la raison sociale et le siège social, le numéro de téléphone, le capital social, l'adresse du siège social ;