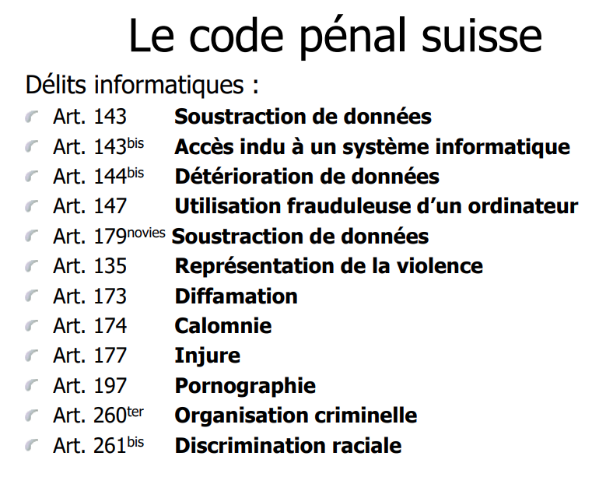
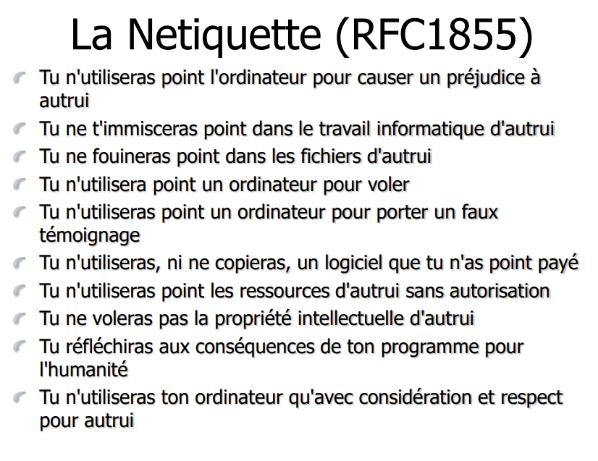
# Aspects légaux

4 textes incontournables: LPD = Loi fédérale sur la protection des données, LDA = Loi sur le droit d'auteur et droits voisins, Code pénal, Code des obligations

LPD : La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l’objet d’un traitement de données

LDA : Loi sur le droit d'auteur et droits voisins a.la protection des auteurs d'œuvres littéraires et artistiques b.la protection des artistes interprètes, des producteurs de phonogrammes ou de vidéogrammes ainsi que des organismes de diffusion c.la surveillance fédérale des sociétés de gestion.



**Virus** : programmes capables de modifier une application pour se loger à l'intérieur et contenant une routine d'autoreproduction **Les familles** : VIRUS DE FICHIER, LE RÉSIDANT, LE COMPAGNON, LE FURTIF, LE CRYPTÉ, LE MUTANT, LE PIÈGE, LE RÉTROVIRUS, LE POLYMORPHE, LE MACROVIRUS, ... **Programmes destructeurs** : LE CHEVAL DE TROIE, LA BOMBE LOGIQUE et LE VER **Les canulars** : Message électronique largement diffusé qui vous annonce une menace imminente (Hoax en anglais) Pour vérifier : www.hoaxbuster.com 

Déni de service (rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs) Buffer Overflow (dépassement ou débordement de tampon) Root compromise (acquisition des privilèges les plus élevés d’un serveur) Cross Site Scripting (attaque à l'internaute via une faille au niveau d'un serveur) IP Spoofing (usurpation d'adresse IP) WEB Spoofing (remplacement d’un site par une version pirate du même site)

Freeware (graticiel) : Logiciel "à libre usage", réellement gratuit, par opposition au logiciel contributif : il bénéficie bien de la protection des droits d'auteur, mais l'on a pourtant le droit (en général par l'intermédiaire d'utilisateurs privés) de le copier, de le distribuer et de l'utiliser librement. Shareware (partagiciel) : Programme commercial, qui s'appuie sur un concept de distribution particulier : on peut copier gratuitement ces programmes et les tester autant que l'on veut avant de les acheter. Mais pour en obtenir une version plus complète, il faut s'enregistrer et acquitter un droit d'utilisation (licence). Licence GNU / Logiciel libre : Les licences d'utilisation de la plupart des programmes sont définies pour limiter ou supprimer toute liberté à l'utilisateur. À l'inverse, les Licences Publiques Générales GNU (GNU General Public Licenses) sont destinées à vous garantir la liberté de partager et de modifier les logiciels libres, et de s'assurer que ces logiciels sont effectivement accessibles à tout utilisateur. Liberté des logiciels ne signifie pas nécessairement gratuité. Les Licences Publiques Générales sont conçues pour assurer la liberté de distribuer des copies des programmes, gratuitement ou non, de recevoir le code source ou de pouvoir l'obtenir, de modifier les programmes ou d'en utiliser des éléments dans de nouveaux programmes libres, en sachant que vous y êtes autorisé.

**Une bonne stratégie de sécurité suppose de** : Sécuriser l’ordinateur ou le réseau Vacciner l’ordinateur contre les virus, Maintenir la sécurité physique, Se préparer à affronter une catastrophe, Assurer un contrôle et une maintenance en permanence

**LPD** : *But* : La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l’objet d’un traitement de données., *Champ d'application* : C'est l'énumération des personnes concernées, *Définitions*: Définition des différents termes juridique, *Exactitude des données* : Cet article dit que la personne traitante les données doit s'assurer que celles-ci sont correcte, *Sécurité des données* : Les personnes qui gardent les données doivent les sécuriser.

**CP articles Info**: 1, 8, 143, 143bis, 144, 144bis, 147, 148, 150, 150bis, 151, 160, 173, 179-153, 179-154, 179-156, 197-179, 261, 261bis

**Sécurité des données Responsabilités**

*L’enjeu de la sécurité des informations :* **Confidentialité** L’information n’est pas rendue disponible ni divulguée à des personnes, entités, ou des processus non autorisés. **Intégrité** Exactitude et complétude (exhaustivité) de l’information. **Disponibilité** L’information est accessible et utilisable à la demande par une entité autorisée. **Traçabilité** Si les données sont altérées, possibilité de garder une trace de toutes les modifications à des fin d’analyse et de remédiation de la faille de sécurité

*Les rôles* **Le Maitre du fichier** Entité qui décide du but et du contenu du fichier **SI** Service de l'Informatique **PPDT** Préposé à la protection des données et à la transparence.

**Sauvegarde informatique**

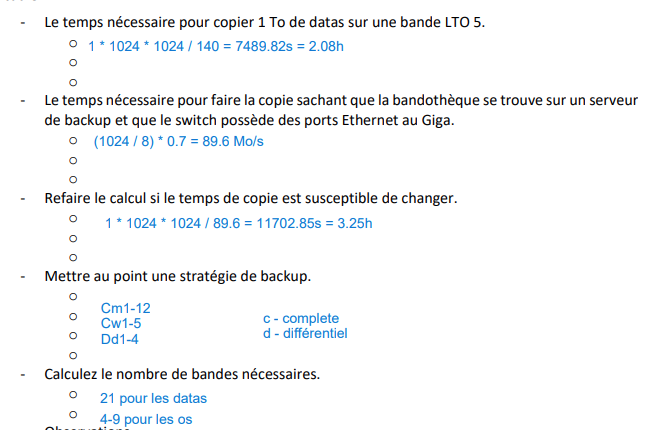
**Avantages** La sauvegarde informatique en continue est devenue une stratégie d’entreprise inévitable, car elle permet de protéger des données importantes pour ne pas les perdre définitivement au cas où un mauvais incident se produirait. En effet, la disparition définitive de toutes ces informations pourrait conduire une société à la faillite. Dans le cas contraire, elle pourrait mettre des années à se reconstruire. Le **back-up** est donc une tactique de prévention indispensable.

Une fois que vous avez une bonne compréhension de la taille et de l’étendue des données que vous devez sauvegarder, vous devez commencer par développer un plan de sauvegarde réel. Votre plan de sauvegarde doit conserver **au moins une ou deux copies** de vos données **stocker** sur différents supports de stockage, **dont une copie sera située hors site**. Cette règle permet de créer à la fois une redondance dans les sauvegardes et une diversité des emplacements de stockage et des supports.

**Règles** 1) Planifiez votre stratégie de sauvegarde. 2) Développez un plan de sauvegarde écrit qui vous indique: - Ce qui est sauvegardé. - Où il est sauvegardé. - Fréquence des sauvegardes. - Quel type de sauvegardes est effectuée. - Qui peut accéder aux sauvegardes et comment les contacter. - Qui est chargé d’effectuer les sauvegardes. - Qui est chargé de surveiller le succès de ces sauvegardes. - Accordez la plus haute priorité aux données cruciales. - Garantie qu’il existe des copies de la sauvegarde et qu’elles ne se trouvent pas au même emplacement que les données d’origine. - Testez vos sauvegardes avant d’en avoir besoin. Restauration en bac à sable pour connaître les temps nécessaires à la reconstruction du système.

**Types Sauvegardes complètes** Une sauvegarde complète est exactement ce que son nom indique, il s’agit d’une copie complète de l’ensemble de vos données. Bien que les sauvegardes complètes offrent sans doute la meilleure protection, la plupart des organisations ne les utilisent que périodiquement car elles prennent du temps et nécessitent souvent beaucoup de capacité de disque ou de bande. Parce que toutes les organisations n’ont pas le temps ou l’espace de stockage pour des sauvegardes complètes fréquentes, d’autres types sont souvent nécessaires. **Sauvegardes incrémentielles** Les sauvegardes incrémentielles ont été introduites pour réduire le temps et l’espace de stockage nécessaires à l’exécution d’une sauvegarde complète. Les sauvegardes incrémentielles ne sauvegardent que les données modifiées depuis la dernière sauvegarde (bit archive à 1). La sauvegarde incrémentielle se base sur le bit archive pour copier ses fichiers. Ce bit archive est automatiquement mis à 1 lors de la création ou de la modification d’un fichier. La sauvegarde incrémentielle remet le bit archive à 0. **Sauvegardes différentielles** Une sauvegarde différentielle est similaire à une sauvegarde incrémentielle, en effet, elle commence par une sauvegarde complète et les sauvegardes suivantes contiennent uniquement les données qui ont changées. La sauvegarde différentielle sauvegarde les fichiers dont le bit archive est à 1, elle laisse le bit archive à 1 après sauvegarde. Une sauvegarde différentielle contient toutes les données qui ont changé depuis la dernière sauvegarde complète. La sauvegarde différentielle présente l’avantage d’un temps de restauration plus court. Dans un scénario de sinistre, le temps de reprise d’activité est généralement critique, une restauration rapide limitera au maximum cet impact temps

Copie image disque (Ghost) peut être utilisé comme moyen de sauvegarde.

Le 0.7 dans le deuxième calcule est la perde durant le transfert internet causé par les headers etc…

Mb -> Mo / 8 dans le deuxième calcule

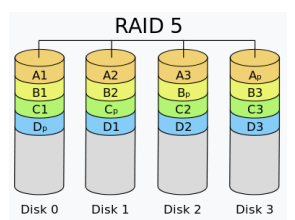
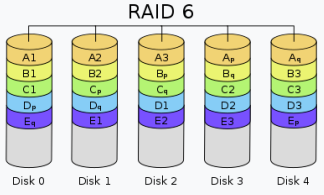
1To x 1024 = 1024 Go x 1024 => Mo

Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement1Go/s = 1Gb/s x 1024 => 1024 Mb/s / 8 => Mo/s x 0.7

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Une image contenant texte, cylindre, capture d’écran

Description générée automatiquementUne image contenant cylindre, texte

Description générée automatiquementUne image contenant cylindre, texte

Description générée automatiquementUne image contenant cylindre, texte

Description générée automatiquementLa technologie JBOD permet de regrouper plusieurs disques durs en une seule partition. JBOD est l'acronyme de l'expression Just a Bunch Of Disks. Avec cette technique, on attend qu'un disque dur soit rempli pour commencer à entamer le suivant. Les capacités totales des disques durs s'additionnent. Il est parfaitement possible d'utiliser des disques durs de tailles différentes.   
Avec le **RAID 0, (disk stripping, agrégat par bande)** des données consécutives sont réparties sur des disques durs différents. Là encore, le système RAID contient plusieurs disques durs, mais est reconnu comme une seule et unique partition par le système d'exploitation. La capacité totale du RAID 0 est égale à la somme des capacités de chaque disque dur, comme avec le JBOD. La différence avec le JBOD tient dans le fait que les données d'un même fichier étant systématiquement réparties sur plusieurs HDDs, ce que ne faisait pas le JBOD. Cela permet une amélioration des performances lors de l'accès à des données consécutives, celles-ci étant lues/écrites depuis plusieurs disques durs en parallèle.   
   
   
   
Avec le **RAID 1 (disk mirroring, disque en miroir)**, les données sont copiées à l'identique sur tous les disques durs. Chaque disque dur est ainsi une copie de tous les autres, chaque disque dur ayant exactement le même contenu. L'avantage de cette technique réside dans la résistance aux pannes : cela permet de résister à une panne qui touche un grand nombre de disque dur, tant qu'au moins un disque dur est épargné. Cependant, cette technique ne permet pas de gagner en espace disque : l'ensemble des disques durs est vu comme un unique disque de même capacité qu'un disque individuel. Des gains en performances sont possibles, vu que des données consécutives peuvent être lues depuis plusieurs disques durs. Mais cette optimisation entraine une baisse des performances en écriture, ce qui fait que peu de contrôleurs RAID l'utilisent.   
Les **RAID 2, 3 et 4** peuvent être vu comme une sorte de RAID 0 amélioré. Il est amélioré dans le sens où on ajoute un disque pour les données de parité à un RAID 0. L'idée est simplement de calculer, pour tous les secteurs ayant la même adresse, un secteur de parité. Les octets des différents disques du RAID 0 seront utilisés pour calculer un octet de parité, qui sera enregistré sur un disque de parité à part. Il faut noter que certaines formes améliorées du RAID 4 dupliquent les disques de parité, ce qui permet de résister à plus d'une panne de disque dur (autant qu'il y a de disques de parité). Mais ces améliorations ne font pas partie des niveaux de RAID standard.   
Le **RAID 5** est similaire au RAID 4, mais les secteurs de parité sont répartis sur les différents disques dur, afin de gagner en performances.  
Le **RAID 6** est une amélioration du RAID 5 où les données de parité sont elles-mêmes dupliquées en plusieurs exemplaires. Cela permet de résister à la défaillance de plus d'un HDD.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Il est possible de combiner des disques durs en utilisant diverses techniques de RAID. Par exemple, on peut utiliser un RAID1 de disques en RAID 0 : on parle alors de RAID 01. Il est aussi possible d'utiliser un RAID 0 de disques en RAID 1 : on parle alors de RAID 10. De même, utiliser un RAID 0 de RAID 3, 4, 5 ou 6 est possible : on parle respectivement de RAID 30, 40, 50, 60.

Une image contenant texte, cylindre, Approvisionnement général, bouteille

Description générée automatiquementUne image contenant texte, capture d’écran

Description générée automatiquement

**Bit d’archivages** : Dans les systèmes d’exploitation se basant sur cet attribut, chaque fichier dispose d’un bit particulier dit « d’archivage ». Lorsque le fichier est créé ou modifié puis refermé, le système d’exploitation positionne ce bit à 1 pour indiquer qu’il a été créé ou modifié depuis la dernière sauvegarde. Le bit d’archivage permet aussi aux logiciels de sauvegarde d’identifier les fichiers à enregistrer, puis de repositionner le bit à 0 une fois la sauvegarde effectuée. Pour les systèmes d’exploitation qui s’appuient sur la date des fichiers, le principe est beaucoup plus simple. Tous les fichiers possèdent une date de création et une date de dernière modification, ce qui permet au système de sauvegarde de les comparer à celle de la dernière sauvegarde. Les différents attributs de fichiers, dont les dates, sont stockés dans les inodes (index et nodes). Le système de sauvegarde va donc comparer cette date à celle de la dernière sauvegarde. Si elle est antérieure à la date de modification du fichier alors il enregistrera le fichier, sinon il sera ignoré lors de la sauvegarde.

**Pour restaurer l’ensemble des données, il faut se munir de la dernière sauvegarde complète (la base différentielle) puis de la dernière sauvegarde différentielle.**

**Pour restaurer l’intégralité des données, il faut donc se munir de la dernière sauvegarde complète ainsi que toutes les sauvegardes incrémentales effectuées depuis.**

**Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement**