

*TechnofuturTIC*

# Droit de l'informatique

HELHA Tournai – 11 octobre 2019

**Didier GOBERT**

Conseiller-Juriste au SPF Economie

Consultant en droit de l'informatique

[didier.gobert@dgober.be](mailto:didier.gobert@dgober.be)

## Plan de l'exposé

- **Vie privée (RGPD et cybersurveillance)**
- Publicité/marketing et gestionnaire réseau
- Questions relatives à la preuve
- Questions relatives à la propriété intellectuelle
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- Criminalité informatique et obligation de collaboration
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Quelques questions pour se mettre en jambe !

- Comment réagir si :
  - Le patron vous demande de fournir la liste de toutes les adresses emails des employés de l'entreprise ou de l'administration à son frère... qui est mandataire politique... ?
  - Un employé sur le départ... vous demande de lui faire une copie du listing clients ?
  - Le service communication vous demande d'afficher sur le site web la photo des tous les employés ou agents... qui avait été prise initialement pour le badge de pointage ?
  - Un chef de service demande le listing de tous les pointages à la pointeuse ?
  - Le DPO/DPD de l'organisation vous demande de collaborer ?
  - Gestion des accès aux données sur le serveurs de l'entreprise ?
  - Limitation en fonction du profil de fonction ? Traçabilité ?

Copyright Didier Gobert 2000-2019



The screenshot shows the Facebook homepage with the following elements:

- Header:** Facebook logo, links for "Garder ma session ouverte" and "Mot de passe oublié ?", and a "Connexion" button.
- Navigation:** "Adresse électronique" and "Mot de passe" input fields.
- Main Content:**
  - Left Column:** Text "Facebook vous permet de rester en contact et d'échanger avec les personnes qui vous entourent." and a world map with user avatars.
  - Right Column:** "Inscription" section with the text "Le site est gratuit et ouvert à tous." and a registration form with fields for "Prénom", "Nom de famille", "Votre adresse électronique", "Nouveau mot de passe", "Sexe", "Date de naissance" (with day, month, and year dropdowns), and a "Mot de passe" field. A green "Inscription" button is at the bottom.
- Footer:** Language selection (Français (France), English (US), Español, Português (Brasil), Deutsch, Italiano, العربية, हिन्दी, 中文(简体)), copyright notice "Facebook © 2009", and links for "À propos de", "Publicité", "Développeurs", "Emplois", "Conditions", "Blog", "Widgets", "Rechercher des amis", "Confidentialité", "Mobile", and "Aide".

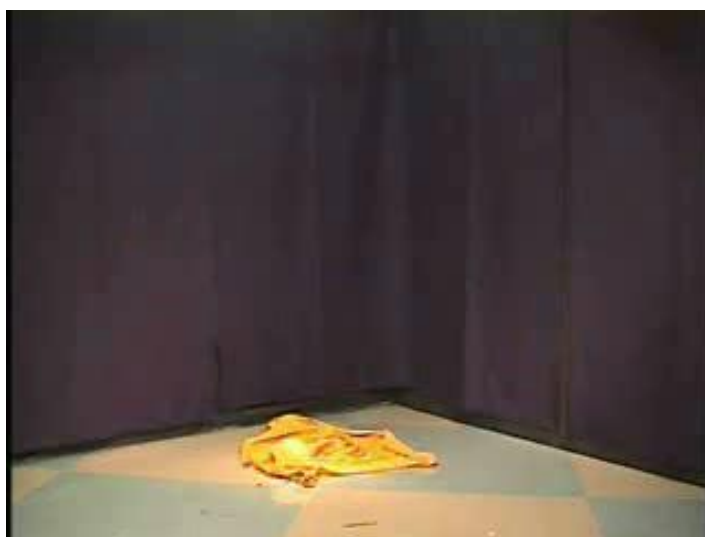
Copyright Didier Gobert 2000-2019

## Les mésaventures de Star Wars Kid



Copyright Didier Gobert 2000-2019

## Les mésaventures de Star Wars Kid



## Les mésaventures de Star Wars Kid



Febelfin – Dave le voyant !

[http://www.youtube.com/watch?v=spopho\\_wJOU](http://www.youtube.com/watch?v=spopho_wJOU)

## Introduction

- Réseaux sociaux :
  - CA lié à l'exploitations commerciales des données à caractère personnel... données par vous et vos connaissances !
  - Exploitations limitées aux informations annoncées dans leur politique vie privée ?
- Bourgmestre d'Alost : droit à suppression de vidéo sur Internet mais en pratique...
- Responsables RH valident votre CV en consultant internet : les données qui y trainent reflètent-elles votre personnalité/expérience ?
- Sur Internet : important de divulguer des données personnelles avec « parcimonie » car outil redoutable => risque de perte de la maîtrise de sa personnalité.

Copyright Didier Gobert 2000-2019

## Introduction

- Le développement de l'informatisation, l'automatisation du traitement et l'interconnexion des bases de données défient la protection de la vie privée => on est tous « fiché » !
- Pas un problème en soi mais risque d'abus
- Traitement pas interdit mais consécration d'un droit de savoir et d'agir (à certaines conditions) au profit de la personne concernée
- Les réseaux ont amplifié ce phénomène de « fichage » et augmenté le niveau de risque/préjudice
- Si non respect des règles vie privée => Fondement juridique aisé pour réclamer un préjudice + **sanctions lourdes RGPD** !

Copyright Didier Gobert 2000-2019

## Introduction

- 2017-2018 : année importante de transition => de la directive 95/46 au RGPD 2016/679 (application au 25 mai 2018)
- Renforcement de la protection des données à caractère personnel des personnes physiques (précision et nouveaux droits, + de pouvoir à l'autorité, sanctions lourdes,...)
- Prise en compte de l'environnement numérique
- Responsabilisation plus poussée du responsable de traitement et du sous-traitant (charge de la preuve, registre des activités de traitement, AIPD, DPO, ...)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Définitions

## Principes généraux

### Définitions

- **Le RGPD s'applique dès lors que (art. 2.1.) :**
    - Traitement de données à caractère personnel automatisé en tout ou en partie
- => toujours le cas si consultation, enregistrement, ... des données relatives aux employés sur le réseau de l'entreprise ou publication de données sur Internet

Copyright Didier Gobert 2000-2019

## Principes généraux

### Définitions

- **Donnée à caractère personnel (art.4.1.)**

« toute information se rapportant à une *personne physique identifiée ou identifiable*; est réputée être une *«personne physique identifiable»* une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, *tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »

Copyright Didier Gobert 2000-2019

## Principes généraux

### Définitions

- **Donnée à caractère personnel** (art.4.1.)

- *Exemples* : nom, adresses physique et électronique, n° de téléphone, de sécurité sociale, de registre national, d'entreprise, immatriculation véhicule, données bibliographiques, données professionnelles ou non, etc.

=> notion très large : donnée à caractère personnel dès que l'on peut associer la donnée (directement ou par recoupement) à une **personne physique** !

- Données collectées sur internaute :

- Volontairement : formulaire, participation à jeu ou concours, demande d'accès à internet ...
- A son insu : cookies, adresse IP

Copyright Didier Gobert 2000-2019

## Principes généraux

### Définitions

- **Traitement** (art. 4.2.)

*« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*

=> notion très large (implique le « profilage » art. 4.4.) !

Copyright Didier Gobert 2000-2019



## Principes généraux

### Définitions

- **Responsable du traitement** (art. 4.7.)

« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, *détermine les finalités et les moyens du traitement* (...) »

=> personne sur laquelle repose la charge de la plupart des obligations de la loi (informer, RAT, AIPD,...), **mais RGPD renforce obligations du sous-traitant**

=> pour un même traitement, il peut y avoir plusieurs responsables (**art.26 => accord obligatoire**)

=> **Conseil** : toujours demander des instructions

Copyright Didier Gobert 2000-2019

## Principes généraux

### Champ d'application matériel et personnel

- **Principe** : art. 2.1. (cfr. *supra*)

- **Exceptions** :

- Un exemple (art.2.2.c): exception pour « *traitement effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique* »

- Illustration : arrêt CJCE du 6 novembre 2003 => *un site web – même personnel – doit respecter la loi sur les données à caractère personnel et ne bénéficie donc pas de cette exception*

- RGPD s'applique uniquement aux **pers. physiques**

Copyright Didier Gobert 2000-2019

## Principes généraux

### Champ d'application matériel et personnel

- **Exception** pour « activités exclusivement personnelles ou domestiques » : applicable au réseaux sociaux ? Avis Groupe 29
  - Non pour fournisseurs de SRS et applications
  - Oui *généralement* pour utilisateurs ! Sauf si :
    - Pas activité purement personnelle et domestique (utilisation du profil à des fins associatives, commerciales, politiques, etc.)
    - Profil ouvert (informations accessibles en tout ou en partie à tous les membres voire aux non membres, et pas uniq. à son carnet)
    - Profil fermé mais « Nombre élevé de contacts peut indiquer qu'on dépasse l'activité exclusivement personnelle ou domestique »
    - Traitement de données sensibles ou image de tiers (sans consent.)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

## Principes généraux

### Conditions légales du traitement (art.5)

- Principe de **licéité, loyauté et transparence** (incluant finalités déterminées, explicites et légitimes ET info aisément accessible et facile à comprendre)
- Principe de **minimisation des données** (adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités)
- Principe de **d'exactitude** (exactes et tenues à jour => droit d'accès et rectification)
- Principe de **limitation de durée** (suppression si plus nécessaire à la réalisation des finalités des traitements)
- Principe de **sécurité/intégrité et confidentialité**
- Principe de **responsabilité** (garantir et démontrer respect RGPD => intérêt du registre, AIPD, DPO)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Conditions de licéité** (art. 5 et 6)
  - Traduction : « *Je dois dire ce que je fais avec les données et je ne peux pas faire plus que ce que je dis* »
  - Principe de finalité des traitements :
    - Le traitement doit poursuivre une **finalité déterminée, explicite et légitime** (art. 5.1.b.)
    - Le traitement doit être effectué dans une des **hypothèses de l'article 6** (présomption de légitimité du traitement) : par ex., consentement ou nécessaire à l'exécution du contrat.

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Finalité déterminée, explicite et légitime**

Les données doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* ».

=> « *finalités déterminées et explicites* » = nécessité de définir précisément et d'afficher clairement les objectifs du traitement (application du principe de transparence : art.12 à 14)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Finalité déterminée et explicite**

=> nécessité d'assurer la **compatibilité** des traitements avec ces finalités annoncées

=> la personne concernée doit toujours connaître (ou raisonnabl. prévoir) les utilisations faites de ses données

Illustration : Appel Anvers => condamnation d'une banque pour avoir utilisé à des fins publicitaires pour des produits d'assurance des données relatives à sa clientèle communiquées dans le cadre d'ordres de paiement => exploiter les données de virements bancaires en vue de proposer des produits d'assurance excède les « prévisions raisonnables » du client (non informé de cette finalité)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Finalité déterminée et explicite**

*Illustration* : l'administration qui communique à des fins commerciales des données recueillies initialement en vertu d'une obligation légale et/ou en vue de bénéficier d'un service public

=> traitement (communication à des tiers) incompatible avec la finalité annoncée au départ (bénéficiaire d'un service public)

=> aurait dû en principe être envisagé comme un nouveau traitement, dont la finalité (tirer un profit économique de ces données) aurait dû être déterminée, explicite et légitime et dont le traitement aurait dû répondre aux autres conditions de licéité.

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- « **Finalité légitime** »

- Un équilibre doit exister entre l'intérêt du responsable du traitement et les intérêts des personnes sur qui portent les données traitées => l'appréciation de la légitimité suppose une mise en balance des intérêts en présence

- Le fait de se prévaloir d'une des hypothèses (obligatoires) de l'article 6 crée une présomption de légitimité

=> l'équilibre des intérêts en présence est *a priori* atteint !

=> présomption réfractive : un contrôle du juge est toujours possible

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**
  - *Consentement* de la personne concernée => **RGPD renforce les conditions du consentement** (cons. tacite plus possible => voir slides suivants)
  - Nécessaire à la *négociation ou l'exécution d'un contrat*
  - Nécessaire au *respect d'obligations légales*
  - Nécessaire pour *sauvegarde de l'intérêt vital*
  - *Mission d'intérêt public/autorité publique*

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**
  - **Consentement** (art. 4.11.) : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, **par une déclaration ou par un acte positif clair**, que des données à caractère personnel la concernant fassent l'objet d'un traitement* » => **fin du consentement tacite** (absence d'opposition ou silence même circonstancié)
  - **Conditions** (art.7) :
    - Consentement dilué dans des conditions générales ne suffit pas
    - Droit de retirer à tt moment et aussi simplement (+ info préalable)
    - Charge de la preuve pour le responsable de traitement (archiver)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**
  - *Consentement des enfants pour SSI (art.8)* : si offre directe d'un SSI (vente en ligne, inscription à Facebook, Instagram, Snapchat, Whatsapp,...), consentement au traitement des données est valable si :
    - Enfant = ou > à 16 ans (ou 13 ans si EM décide)
    - Parent quand enfant < à 16 ans (ou 13 ans si EM décide)
  - En pratique : vérification de l'âge de l'enfant **pas facile à mettre en œuvre** (à un prix raisonnable dans un environnement international) vu les moyens technologiques actuels et leur interopérabilité
  - Mais rappel : **charge de la preuve** sur responsable !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**
  - *En principe, interdiction du traitement des « données sensibles » (art. 9.1.)* : « données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »
  - *SAUF si exception (art. 9.2.) => Consentement « explicite » pour traitement (art. 9.2.a.)* : quelle différence avec le consentement classique (art. 4.11.) ? Possibilité pour un EM de supprimer cette exception !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**

- nécessaire aux fins d'un *intérêt légitime du responsable ou d'un tiers*, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (particulièrement si c'est un enfant)

Illustration : Affaire DATASSUR

=> le juge considère que les intérêts de DATASSUR sont légitimes et proportionnés et que les données traitées sont minimales et nécessaires à la finalité (appréciation du risque)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Conditions légales du traitement

- **Justification du traitement : art. 6**

Illustration : CPVP (avis n°34)

=> la CPVP considère que la collecte d'adresses e-mail à *l'insu de l'individu* et leurs utilisation à des fins de marketing direct n'est pas proportionnée (intérêt de l'individu prévaut)

=> seul moyen de légitimer le traitement : obtenir le consentement préalable au traitement des données à cette fin de marketing direct

=> *ex. de collecte à l'insu* : automatique sur Internet, dans des espaces de discussion, par le biais d'une connaissance, obtenu d'un tiers sans information, ...

Copyright Didier Gobert 2000-2019



## Principes généraux

### Conditions légales du traitement

- Quid des photos et du respect de la vie privée ?
  - La photo d'un individu est une donnée à caractère personnel => permet de l'identifier
  - Publier une telle photo sur un site web, blog, etc = **traitement de donnée à caractère personnel** => RGPD applicable !
  - Pour légitimer ce traitement :
    - **consentement** de la personne, ou d'un parent si mineur sans capacité de discernement (< 13-16 ans au regard du RGPD)
    - consentement doit être **libre** (exercé sans pression ou contre-partie), **spécifique** (respecter le contexte de publication défini) et **informé** => une autorisation générale ne suffit pas => définir le type de photo publiée, le contexte, le but, etc.... et se limiter à cela !
    - nécessiter en principe d'une déclaration à la CPVP
  - **Attention** : accepter de se faire prendre en photo ne présume pas accepter la publication de sa photo !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

## Principes généraux

### Droits de la personne concernée

- **Droits consacrés par les articles 12 à 23 :**
  - Transparence et modalités
  - Droit à l'information
  - Droits d'accès et de rectification
  - Droit à l'effacement (« droit à l'oubli »)
  - Droit à la limitation du traitement
  - Droit à la portabilité des données
  - Droit d'opposition (conditionné)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Transparence et modalités (art. 12)**
  - Information ou communication doit être **concise, transparente, compréhensible et aisément accessible**, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.
  - **Forme** : libre mais écrit (papier ou électronique) conseillé pour questions de preuve => *sur site web : prévoir une « Politique vie privée », avec lien à partir de toutes les pages, surtout page collectant information*
  - Responsable doit donner suite à toute demande de la personne dans les **meilleurs délais** (maximum un mois, prolongeable 2 mois si complexe et/ou nombreuses demandes, moyennant info préalable)
  - Information et communication **gratuite** (sauf si manifestement infondé ou excessif ou répétitif => refus ou paiement de frais raisonnables acceptés)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droit à l'information** (RGPD allonge la liste des infos à fournir) :
    - Soit responsable du traitement collecte les données **auprès de la personne concernée** (art. 13)
    - Soit responsable du traitement collecte les données **auprès d'un tiers** (art. 14) : généralement auprès d'un autre responsable de traitement, pas exemple dans le cas de la transmission de données (vente, location...)
- => il faut aussi informer dans ce cas => ce traitement ne peut se faire à l'insu !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droit à l'information** (art. 13)
  - **Informations minimales obligatoires** :
    - Identité et coordonnées du responsable du traitement
    - Coordonnées du DPO (si il y en a un)
    - Finalités du traitement ET base juridique (+ intérêts légitimes poursuivis si base = art. 6.1.f.)
    - (Catégories de) Destinataires des données (si transfert)
    - Le cas échéant, l'intention d'effectuer un transfert de données vers un pays tiers (+ infos supplémentaires)
    - Existence du droit de s'opposer au traitement à des fins de marketing direct
  - **Informations supplémentaires** (si nécessaires pour garantir un traitement « équitable et transparent » ! => laissé à l'appréciation du responsable !) => art. 13.2.

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droit à l'information (art. 14)**
  - **Informations minimales obligatoires :**
    - Identité et coordonnées du responsable du traitement
    - Coordonnées du DPO (si il y en a un)
    - Finalités du traitement ET base juridique
    - Catégories de données concernées
    - (Catégories de) Destinataires des données (si transfert)
    - Le cas échéant, l'intention d'effectuer un transfert de données vers un pays tiers (+ infos supplémentaires)
    - Existence du droit de s'opposer au traitement à des fins de marketing direct
  - **Informations supplémentaires** (si nécessaires pour garantir un traitement « équitable et transparent » ! => laissé à l'appréciation du responsable !) => art. 14.2.

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droit à l'information (art. 13 et 14)**
  - **Quand fournir l'information ?**
    - Au moment de la collecte si données collectées auprès de la personne concernée (art. 13)
    - Au moment de la communication auprès de la personne si pas de collecte directement auprès de la personne, ou à défaut « dans un délai raisonnable » (max. 1 mois) (art. 14)
  - **Exception à l'obligation d'information :**
    - La personne dispose déjà des infos (art. 13 et 14)
    - Fourniture impossible ou exige des efforts disproportionnés (art.14)
    - Données frappées par secret professionnel (art.14)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits d'accès** (art. 15) : droit d'obtenir du responsable du traitement confirmation que données sont ou non traitées. Si oui, infos à fournir (notamment) :
  - l'accès et/ou une copie des données + catégories de données
  - les finalités de traitement
  - les destinataires éventuels
  - la durée de conservation envisagée
  - l'existence du droit de rectification, effacement ou limitation
  - le droit d'introduire une réclamation auprès de l'autorité de contrôle
  - toute information sur l'origine/source des données
  - Si profilage => logique sous-jacente et conséquences du traitement=> Si fourniture électronique : format d'usage courant.

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits de rectification** (art. 16) : droit d'obtenir du responsable du traitement rectification des données inexactes ou incomplètes => constat possible après exercice du droit d'accès
- Droits d'accès, rectification, effacement (et autres) nécessitent la mise en place de *moyens humains et organisationnels* chez le responsable de traitement => **à ne pas sous-estimer !**

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits à l'effacement – « droit à l'oubli »** (art. 17) : droit d'obtenir du responsable du traitement l'effacement des données traitées si :
  - elles ne sont plus nécessaires au regard des finalités
  - la personne retire le consentement (et seule base légale)
  - exercice du droit d'opposition (au marketing direct par exemple)
  - les données sont traitées illicitement
  - elles ont été collectées dans le cadre de l'offre d'un SSI à un enfant sans respecter l'article 8
- **Si effacement** : et que responsable avait rendu public les données (par ex., sur internet) => informer tous les autres responsables par moyens technologiques pour rendre efficace cette demande d'effacement (=> oubli numérique : suppression des liens ou des données reproduites en ligne sur d'autres sites) => illusoire en pratique ?

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droit à l'effacement - droit à l'oubli !** (arrêt CJUE, 13 mai 2014, Google Spain)
  - Moteur de recherche = Responsable de traitement car référencement automatique de données publiées sur les pages web de tiers = traitement
  - Si intérêt légitime, et après pondération des intérêts (notamment celle du public à recevoir l'information), une personne peut demander de « supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne », et cela même si les infos restent publiées sur les pages des tiers => moteur de recherche démultiplie le risque à la VP

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits à la limitation (art. 18) :** droit d'obtenir du responsable du traitement la limitation du traitement si :
  - contestation quant à l'exactitude des données (le temps de vérifier)
  - le traitement est illicite ou contestation sur motifs légitimes, et la personne privilégie la limitation plutôt que effacement des données (par exemple car encore nécessaires pour agir en justice)
- **Si limitation :**
  - le responsable doit se limiter à conserver les données (seul traitement possible), sauf si consentement de la personne pour autres traitements ou nécessaires pour agir en justice
  - en pratique : déplacement ou verrouillage des données, retrait temporaire sur internet, etc.
- **Si fin de la limitation :** le responsable doit en informer au préalable la personne concernée

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Obligation de notification si rectification, effacement ou limitation (art.20) :**
  - Si le responsable de traitement a communiqué des données à des tiers, il doit notifier à ces destinataires les rectifications ou effacements de données effectuées ou les limitations de traitement effectués (pour que ceux-ci les répercutent) SAUF si notification impossible ou exige des efforts disproportionnés (en pratique, souvent difficile à mettre en œuvre et à gérer)
  - La personne peut demander au responsable des infos sur ces destinataires

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits à la portabilité des données (art. 20)**
  - Les personnes concernées ont le droit de recevoir, ou demander la transmission à un autre responsable, des données qu'elles ont fournies au responsable du traitement initial, dans un format structuré, couramment utilisé et lisible par machine, lorsque:
    - le traitement est fondé sur le consentement ou sur un contrat; **ET**
    - Le traitement est effectué à l'aide de procédé automatisé (presque systématiquement le cas aujourd'hui)
  - Exemples : changement d'opérateur télécoms => transfert de toutes les données administratives ; transfert de toutes les données comptables d'un indépendant
  - Vise pas données fournies par des tiers. Quid données générées par responsable (facturation, localisation, trafic) ?

Copyright Didier Gobert 2000-2019

## Principes généraux

### Droits de la personne concernée

- **Droits d'opposition (art. 21)**
  - sans justification et gratuitement, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant **à des fins de prospection**, y compris au profilage dans la mesure où il est lié à une telle prospection
  - la personne doit être informée de ce droit de **manière claire et séparée** de toute autre information, au plus tard au moment de la première communication
  - Pas oublier : on peut retirer consentement à tout moment

Copyright Didier Gobert 2000-2019



# Principes généraux

## Obligations du responsable de traitement ET sous-traitant

# Principes généraux

## Obligations respons. traitem. ET sous-traitant

- **Obligations consacrées par les articles 24 à 43:**
  - Responsabilité plus poussée (fin déclaration !)
  - Registre des activités de traitement (RAT)
  - Analyse d'impact relative à la protec. données (AIPD)
  - Désignation délégué protection données (DPO-DPD)
  - Notification si « data breaches »
  - Protection des données dès conception et par défaut
  - Liens avec et obligations du sous-traitant
  - Sécurité du traitement
  - Coopération avec autorité de contrôle

Copyright Didier Gobert 2000-2019

## Principes généraux

### Fin de la déclaration à la CPVP

- **Avant :**  
préalablement à tout traitement, le responsable du futur traitement (entièrement ou partiellement automatisé) doit – *sauf exception* - faire une déclaration à la Commission de la protection de la vie privée => *déclaration formelle (assez administrative) préalable, sans réel contrôle (mais consultable par registre public) => peu efficace !*
- **Maintenant :**  
responsabilisation plus poussée et charge de la preuve (*pour tous traitements sans exception !*): tout mettre en œuvre pour assurer le respect du règlement ET pouvoir le démontrer (charge de la preuve) => *travail de réflexion, d'analyse et de documentation a priori (pour pouvoir prouver) et éventuel contrôle a posteriori*

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Responsabilité du responsable (art. 24):**
    - Le responsable du traitement doit mettre en œuvre des *mesures techniques et organisationnelles appropriées (voire des politiques internes)* **pour s'assurer ET être en mesure de démontrer** (charge de la preuve) que le traitement est effectué conformément au RGPD
    - **Paramètres pour déterminer les mesures :** le type de données (sensibles ou pas) ; la nature, la portée et le contexte du traitement ; les finalités du traitement ; les risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie
    - Ces mesures sont **réexaminées et actualisées** si nécessaire.
- => *certainement pas moins lourd et coûteux que la déclaration*  
=> *plus efficace si autorité a les moyens de contrôle ! (sanctions lourdes)*  
=> *RAT, AIPD, DPO aident à mettre en œuvre cette obligation*  
=> *Nécessité d'une coordination entre tous les services (IT, law, RH, market.)*

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Registre des activités de traitement – RAT (art. 30):**
  - **Obligation** pour responsable traitement ET sous-traitant (traitements pour le compte du responsable)
  - **Exception** : facultatif si < 250 employés (mais conseillé pour questions de preuve) SAUF si traitement :
    - présente un risque pour droits et libertés de la personne (subjectif !)
    - est habituel
    - porte sur des « données sensibles »
  - **Contenu** du registre :
    - Responsable (art. 30.1.) : coordonnées, finalités, description catégories de personnes et données, catégories de destinataires, transfert vers pays tiers ?, délais prévus pour effacement et description générale mesures de sécurité techniques et organisationnelles (dans mesure du possible !)
    - Sous-traitant (art. 30.2.) : coordonnées, catégories traitement, ...
  - **Forme** : écrite (électronique ou non) => à disposition de autorité !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Analyse d'Impact Protection des Données – AIPD (art. 35):**
  - **Obligation** pour responsable – préalable au traitement – s'il présente un « risque élevé pour les droits et libertés des personnes concernées », en particulier par le recours aux nouvelles technologies (=> *subjectif !* : *discrimination, usurpation identité, atteinte réputation, perte financière importante, viol secret professionnel, etc.*)
  - **Toujours obligatoire SI** (liste + ou - « complétable » par autorité) :
    - l'évaluation systématique et approfondie d'aspects personnels, qui est fondée sur un traitement automatisé, y compris le profilage, sur base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire
    - traitement à grande échelle de données sensibles ou condamnations pénales
    - surveillance systématique à grande échelle d'une zone accessible au public
  - Si DPO, il **doit être consulté** pour conseil lors de l'AIPD

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Analyse d'Impact Protection des Données – AIPD (art. 35):**
  - **Objectif :** *évaluer* la probabilité et la gravité du risque afin de déterminer, à partir du résultat de l'évaluation, les *mesures appropriées à prendre* afin de démontrer que le traitement des données à caractère personnel est conforme au RGPD
  - **Contenu de l'AIPD :**
    - description systématique des traitements envisagés et des finalités
    - évaluation de la nécessité et de la proportionnalité des traitements au regard des finalités
    - évaluation des risques pour les droits et libertés des personnes concernées
    - mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer et à apporter la preuve du respect du RGPD
  - **Consultation de l'autorité de contrôle préalable** au traitement si AIPD indique que traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque (art. 36)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Désignation délégué protection données (art. 37-39) :**
  - **Obligation** pour responsable traitement ET sous-traitant si :
    - traitement effectué par une autorité publique, à l'exception des juridictions
    - activités de base consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées
    - activités de base consistent en un traitement à grande échelle de catégories particulières de données sensibles ou condamnations pénales
  - Dans les autres cas : **facultatif** mais conseillé car spécialiste-expert en protection des données qui va aider et conseiller en vue du respect du RGPD
  - Il **doit être associé**, de manière appropriée et en temps utile, à toutes questions relatives à la protection des données => il **doit disposer** des ressources nécessaires pour exercer ses missions, accéder aux données et aux traitements et se former

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Désignation délégué protection données (art. 37-39) :**
  - Le DPO peut être membre de l'organisation ou consultant extérieur MAIS **doit être indépendant** (ne peut recevoir aucune instruction ou être pénalisé du fait de ses missions), **éviter conflits d'intérêts** et tenu au **secret professionnel**
  - Il fait **directement rapport au niveau le plus élevé** de la direction
  - Ses **coordonnées** doivent être **publiées et communiquées** à l'autorité de contrôle => « point de contact » pour l'autorité de contrôle ET la personnes concernée (par ex., pour le droit d'accès)
  - **Missions :**
    - **Informier et conseiller** le RT et SS-Traitant, notamment dans le cadre de l'AIPD et du RAT, ET leurs employés qui procèdent aux traitements sur le plan opérationnel
    - **Contrôler le respect du RGPD** (sensibilisation, formation, audit, avis, etc.)
    - **Coopérer** avec l'autorité de contrôle

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Notification si « violation de données » (art. 33-34) :**
  - Obligation pour RT de **notifier à l'autorité de contrôle** « dans les meilleurs délais » (si possible max.72 heures après prise de connaissance) SAUF si « pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques » (*subjectif !*)
  - **Obligation du sous-trait.** de notifier au RT « dans les meilleurs délais »
  - **Informations** minimales à fournir (art.33.3.) ET nécessité de **documenter** la violation (faits, effets, mesures prises)
  - Si « **risque élevé** » pour les droits et libertés d'une pers. phys. (*subjectif !*) => obligation de **communiquer la violation à cette personne** « dans les meilleurs délais » et la décrire en termes clairs et simples
  - **Exemptions possibles** (art. 34.3.)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Protection « dès la conception » et « par défaut » (art. 25) :**
  - *Data protection by design* (25.1.) : le RT **met en œuvre**, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, **des mesures techniques et organisationnelles** appropriées, en vue d'assurer le **respect des principes du RGPD** de façon effective et à assortir le traitement des garanties nécessaires
  - *Data protection by default* (25.2.) : le RT **met en œuvre les mesures techniques et organisationnelles** appropriées pour **garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées**. Cela s'applique à la quantité de données traitées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.

=> Tous les métiers de l'organisation sont impliqués !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Si recours à un sous-traitant (art. 28-29) :**
  - Le RT doit veiller à ce qu'il offre des « **garanties suffisantes** » quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour respecter le RGPD
  - Obligation de **conclure un contrat écrit** entre RT et ss-traitant => contenu bien précis quant aux questions à régler (28.3.) => attente du développement de clauses contractuelles « types » (par COM et/ou autorité de contrôle)
  - Un sous-traitant **ne peut pas sous-traiter sans l'accord préalable** du RT => le cas échéant, « **back to back** » au niveau du contrat
  - Sauf obligation légale, le sous-traitant qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur **instruction du responsable du traitement** (29 et 32.4.)

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Sécurité du traitement (art. 32) :**
  - Le RT ET le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées **afin de garantir un niveau de sécurité adapté au risque** (ex. : pseudonymisation, chiffrement, moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes (sorte de « reset ») des systèmes et des services de traitement, procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement, etc.)
  - Les résultats de l'AIPD seront très utiles **pour évaluer le risque et déterminer les mesures « appropriées » à prendre**
  - Nécessité d'une **discussion et compréhension mutuelle** entre technicien (informaticien, analyste, etc), juriste et DPO !

Copyright Didier Gobert 2000-2019

## Principes généraux

### Obligations respons. traitem. ET sous-traitant

- **Coopération avec autorité de contrôle (art. 31) :**
  - Le responsable du traitement ET le sous-traitant **coopèrent** avec l'autorité de contrôle, **à la demande de celle-ci**, dans l'exécution de ses missions => le RGPD a clairement renforcé les pouvoirs de l'autorité de contrôle (=> gros changement en BE)
  - Si un agent de la CPVP vous contacte ou débarque au sein de votre organisation : **réservez lui un bon accueil !**

Copyright Didier Gobert 2000-2019

# Cybersurveillance des travailleurs

## Introduction

- La cybersurveillance consiste à contrôler l'usage des moyens de communication en ligne (Internet visant à la fois le mail, le web, le FTP, le chat, ..., la téléphonie au sens large, le téléfax) ainsi que ses utilisateurs (notamment à l'aide de la vidéosurveillance, de cookies, de logiciels espions ou de gestion de travail, de boîtes e-mail, etc.).
- Sur le lieu de travail, il faut concilier :
  - Besoin pour l'entreprise d'assurer la sécurité, la rentabilité et de vérifier la bonne exécution du contrat de travail par l'employé
  - ET**
  - Droit du travailleur au respect de sa vie privée, même sur le lieu de travail

=> Équilibre parfois difficile à trouver

Copyright Didier Gobert 2000-2019



## Cybersurveillance

### Cadre juridique

- **Convention européenne des droits de l'homme**

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

*Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui » (art. 8)*

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Cour européenne des droits de l'homme**

*Affaire Niemitz (27/05/1997) : application de l'article 8 sur le lieu de travail*

=> la notion de vie privée ne peut être limitée à un « *cercle intime où chacun peut mener sa vie personnelle à sa guise* » et écarter le monde extérieur

=> la Cour refuse par conséquent d'exclure les activités professionnelles ou commerciales du concept de vie privée, soulignant que c'est « *dans leur lieu de travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur* »

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Constitution belge**

- L'article 22 de la Constitution dispose que « *Chacun a droit au respect de sa vie privée et familiale, sauf dans les conditions fixées par la loi* ».
- L'article 29, quant à lui, indique que « *Le secret des lettres est inviolable* ».

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Loi du 8 décembre 1992 (maintenant RGPD)**

- Pas de dispositions spécifiques à la cybersurveillance
- Mais principes généraux applicables dès que traitement de données à caractère personnel => généralement le cas dans le contexte de la cybersurveillance
- Avis de la CPVP du 3 avril 2000 : interprète l'application des principes de la loi du 8 décembre 1992 au contexte de la surveillance par l'employeur de l'utilisation de l'outil informatique sur le lieu de travail
- D'autres avis interprètent la loi à la vidéosurveillance

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Article 314bis du Code pénal**

*« Est puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications »*

⇒ protège le contenu des communications privées

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Article 314bis du Code pénal**

*Qu'est-ce qu'une communication privée ?*

⇒ Est privé « ce qui n'est pas destiné à être entendu par d'autres que les participants à la communication. Il ne s'agit donc pas de savoir si la communication est professionnelle ou non »

⇒ « Une communication professionnelle, mais non destinée à être entendue par d'autres personnes que les partenaires à la conversation, est une communication privée au sens de la loi »

⇒ Le fait qu'une communication (téléphonique, par e-mail, par fax, etc.) soit qualifiée de professionnelle ou a été passée à partir du lieu de travail ne permet pas d'en déduire automatiquement qu'elle n'est pas privée.

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Article 124 de la loi du 13 juin 2005**

« Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers (...) de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne ».

=> Protection comparable à l'art. 314bis (protection du contenu), mais vise en plus les **données de trafic** (tel numéro ou adresse e-mail appelant et appelé, heure d'appel ou d'envoi, localisation de l'appelant, taille du fichier, type de fichier attaché, etc.)

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Cadre juridique

- **Articles 314bis et 124**

- **Principe** : interdiction pour le gestionnaire de réseau de prendre connaissance du contenu ainsi que des données de trafic des communications privées
- **Exceptions** : l'interdiction est levée si
  - Le gestionnaire obtient l'accord de toutes les parties à la communication => un consentement individuel et explicite est requis => à prévoir dans contrat de travail mais attention aux tiers à la communication !
  - La loi permet la prise de connaissance (art. 125) => **CCT n°81**
  - Actes nécessaires pour vérifier le bon fonctionnement du réseau (art. 125)
  - Actes nécessaires pour prévenir ou interrompre une infraction d'une extrême gravité => prudence : faire appel FCCU

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### Jurisprudence

- Le cadre juridique *de l'époque* était « plutôt favorable » à l'employé : sauf exception, le contrôle des communications des travailleurs par l'employeur est en principe impossible
- Dans ce contexte, les juges ont eu à connaître du licenciement de travailleur suite à l'utilisation (abusives) de nouvelles technologies (courrier électronique, accès à Internet)
- La jurisprudence est divergente : elle donne tantôt raison à l'employeur, tantôt à l'employé, en fonction de l'importance respective que le juge accorde soit à la protection de la vie privée, soit à la lutte contre les abus au sein de l'entreprise

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### Convention collective de travail n° 81 : contrôle des communications électroniques

## Cybersurveillance des travailleurs

### CCT n° 81 : préliminaires

- Vu le cadre juridique strict et la jurisprudence divergente  
=> **urgent** d'adopter un texte consacrant un **équilibre**  
entre les droits de chacun (vie privée >< contrôle pour  
assurer bon fonctionn. entreprise !)
- **Texte négocié** : CCT n° 81 « relative à la protection de la  
vie privée des travailleurs à l'égard du contrôle des  
données de communication électronique en réseau » (AR  
12/06/2002)

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : préliminaires

- Terrain de concession (art. 3) :
  - travailleurs reconnaissent à l'employeur un **droit de contrôle** sur l'utilisation des moyens de télécommunications mis à leur disposition par l'employeur, que ceux-ci soient utilisés à des fins professionnelles ou à des fins privées
  - employeurs reconnaissent le respect du **droit à la vie privée** des travailleurs dans le cadre de leur relation de travail
- CCT ne remplace pas mais **s'intègre dans le cadre juridique existant** (Const., 124, 314bis...) !

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : champ d'application

- La CCT ne **règle pas** les modalités d'accès et/ou d'utilisation des moyens de communication électroniques (art. 1, § 2) => prérogative de l'employeur (peut interdire accès à certains sites, l'envoi d'image par e-mail, etc.)
- La CCT n'autorise que la **prise de connaissance des données de communication électronique** en réseau (la prise de connaissance du contenu reste interdite en principe)  
=> données de communication (art. 2) =
  - Données de trafic (expéditeur, destinataire, date, heure, ...)
  - Nature et taille du fichier attaché (txt, image, audio, exe, ...)
  - Type de site web, moment et durée de consultation, téléchargement

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : champ d'application

- La CCT régleme le contrôle des données des **communications privées** du travailleur, à l'exclusion des échanges strictement professionnels (qui sont librement « contrôlables »)  
  
=> Cmt distinguer communication « privée » de « professionnelle » ?  
La CCT est muette ! Rapport : il incombe au travailleur de déterminer si la communication est ou non privée, en apportant une mention spécifique en ce sens dans l'objet du message !!!  
=> la communication est présumée professionnelle ? Attention : contrôle du juge reste possible sur base de 314bis, 124, art. 8 CEDH
- Applicable au **secteur privé** (et non au secteur public)

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : contrôle et modalités

- Distinction à faire entre :
  - modalités de contrôle des données **en général** (art. 4 à 10)
    - Pas de liens entre données contrôlées et travailleur déterminé
    - Contrôle possible moyennant une information préalable et le respect de certaines conditions (poursuites de certaines finalités déterminées et respect du principe de proportionnalité)
  - modalités **d'individualisation** des données en vue des les attribuer à un travailleur déterminé (art. 11 à 17)
    - Attribution des données contrôlées à un travailleur déterminé
    - Conditions à respecter pour pouvoir procéder à l'individualisation des données

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : contrôle général

- Le contrôle général des données n'est autorisé que si respect du (art. 4) :
  - Principe de **finalité** (art. 5)
    - => liste exhaustive des raisons pour lesquelles le contrôle général des données de communication est permis par l'employeur
  - Principe de **proportionnalité** (art. 6)
    - => le contrôle des données doit entraîner l'ingérence la plus réduite dans la sphère privée du travailleur
  - Principe de **transparence** (art. 7 à 10)
    - => information préalable (collective et individuelle) de la nature du contrôle et de la finalité de la mesure envisagée

Copyright Didier Gobert 2000-2019



## Cybersurveillance des travailleurs

### CCT n° 81 : contrôle général

- Principe de **finalité** (art. 5)
  - a) *la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;*
  - b) *la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;*
  - c) *la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;*
  - d) *le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.*

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : contrôle général

- Principe de **proportionnalité** (art. 5)
  - Implique la **collecte d'un minimum de données** en vue du contrôle afin d'entraîner l'ingérence la plus réduite dans la sphère privée du travailleur
  - Implique **l'interdiction d'individualisation systématique** et préalable des données de communication
  - La CCT tolère un **établissement de listes générales** portant notamment sur les données relatives aux sites Internet visités et à la durée de connexion ou sur le volume et le type de fichiers attachés à un courrier électronique, sans identification a priori des ordinateurs concernés ou des parties à l'e-mail => si abus constaté : individualisation des données
  - **Contrôle général peut-il être permanent ?** Oui pour CCT, non pour CPVP (uniquement sporadique)

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : contrôle général

- Principe de **transparence** (art. 7 à 10)
  - Information **collective** (art. 7)
  - Information **individuelle** (art. 8)
    - => information des travailleurs concernés sur tous les aspects du contrôle
    - => choix du support laissé à l'employeur (circulaire, règlement de travail, ctt de travail, affichage à l'écran, ...)
  - **Contenu** de l'information (art. 9)
    - => *exemple* : document Olivier Rijckaert
  - **Consultation**
    - => évaluation périodique du système en vue de réduire l'ingérence

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : individualisation des données

- Principe : contrôle **anonyme** des données
  - Individualisation systématique des données non permis
  - Permis uniquement si le contrôle général révèle un abus
    - + respect princ. finalité et proportionnalité (art. 13 et 14)
- **Individualisation** => attribuer les données à un travailleur identifié ou identifiable (art. 12, § 1)
- **Rappel** : principes de la CCT applicables uniquement si communication non professionnelle (privée) => distinction regrettable au regard de 314bis du Code pénal => prudence !

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### CCT n° 81 : individualisation des données

- Individualisation **directe** des données (art. 15)
  - Peut se faire **sans** en **avertir** préalablement le travailleur
  - Permis si contrôle poursuit l'une des 3 premières finalités de l'art. 5, § 1
- Individualisation **indirecte** des données (art. 16)
  - Hypothèse : art. 5, § 1, 4°
  - Nécessite une **information préalable** des travailleurs  
=> contrôle général a révélé une anomalie => prochaine anomalie constatée entraînera une individualisation !
  - Procédure d'information : art. 17

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### Géolocalisation des travailleurs

## Cybersurveillance des travailleurs

### Géolocalisation des travailleurs

- Les outils de géolocalisation permettent à un employeur de déterminer à tout moment la localisation de ses travailleurs et suivre les déplacements de ceux-ci
- Technologies **très utiles** dans certains cas (représentant, dépanneur, transporteur, etc.) mais **dérives possibles** (contrôles permanents et injustifiés, etc.)
- Application de la **loi du 8 décembre 1992** et CCT n° 81 => tout n'est pas permis !

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### Géolocalisation des travailleurs

- **Conditions** aux traitements des données de localisation : finalité déterminée et explicite, légitimité, transparence et déclaration à la CPVP
- **Légitimité suppose proportionnalité** :
  - Optimiser les déplacements de différents transporteurs : OK
  - Améliorer l'organisation des interventions urgentes : OK
  - Contrôle permanent pour mesurer la rapidité et la rentabilité d'un travailleur : OK ? Disproportionné ?

Copyright Didier Gobert 2000-2019

## Cybersurveillance des travailleurs

### Géolocalisation des travailleurs

- **Attention** : pas possible d'utiliser des données pour des finalités ultérieures (évaluation ou sanction) incompatibles avec les finalités annoncées (optimiser les déplacements)
- Légitimité implique **consentement indubitable, informé et individuel** du travailleur (on peut difficilement soutenir que données de localisation sont nécessaires à l'exécution du contrat de travail, même des travailleurs itinérants)
- **Déclaration** à la CPVP (exemption peu probable)

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Vidéosurveillance des travailleurs et des espaces (semi) publics (commerce, entreprise, etc.)

## Cybersurveillance

### Vidéosurveillance

- **CCT n° 68** : vie privée et surveillance par caméras sur le lieu de travail => application des principes de la loi du 8 décembre 1992
- Finalités **énumérées** dans la CCT n° 68
- Surveillance **permanente autorisée pour certaines finalités** (sécurité, protection des biens) mais pas pour les autres (contrôle de production et des travailleurs)
- **Information** des travailleurs et de leurs représentants  
=> si non respect : moyen de preuve irrecevable ! (+ S Pénale)  
=> clause dans contrat et/ou règlement de travail
- **Déclaration** à la CPVP

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Vidéosurveillance des espaces (semi) publics

- Loi du 21 mars 2007 sur caméras de surveillance
- Vise caméra, avec enregistrement ou non, utilisée pour « assurer la surveillance et le contrôle » (pas caméra factice ou vidéo-parlophone en principe)
- Conditions installation et utilisation varient suivant le lieu :
  - **lieu ouvert (au public)** : la voie publique, une place de marché, un grand parking, les rues, les rues commerçantes, les places, les jardins publics, les parcs...
  - **lieu fermé accessible au public** : les magasins, les centres commerciaux, les cinémas, les cafés, les gares, les campings, une place temporairement délimitée (Werchter, Tomorrowland)...
  - **lieu fermé non accessible au public** : une habitation privée, un immeuble à appartements, une usine, une école...

Copyright Didier Gobert 2000-2019

## Cybersurveillance


### Vidéosurveillance des espaces (semi) publics

- Respect **proportionnalité** :
  - Éviter image superflue ou viser autre lieu (ex. : porte entrée privée mais plus petite partie possible du trottoir OU place publique mais éviter portes et fenêtres privées ou, au moins, flouter)
  - Visionnage en temps réel et enregistrement permis uniquement que si justifiés par finalités visées par la loi
  - Conservation des images pendant max. 1 mois
  - Responsable *peut/doit* transmettre les images filmées uniquement aux services de police ou autorités judiciaires
  - Nombre et fonctionnalités (rotation, suivi automatique, zoom, ...) ne peuvent être excessifs en fonction des finalités poursuivies

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Vidéosurveillance des espaces (semi) publics

- **Information** :
    - Pictogramme à l'entrée du lieu (avant de pénétrer dans le lieu => porte entrée, panneau indiquant la commune)
- 
- The image shows a red pictogram of a surveillance camera mounted on a wall. Below the camera icon is a rectangular box containing the text 'Surveillance par caméra-Loi du 21-05-07'. Underneath this box are three horizontal lines for additional information, labeled 'Responsable', 'Adresse postale', and 'E-mail'.
- Affichage pictogramme vaut **autorisation préalable de la personne** qui entre dans le lieu
  - **Droit d'accès** sur demande motivée et détaillée

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Vidéosurveillance des espaces (semi) publics

- **Procédure pour installer :**
  - Pour tous les lieux :
    - notification, au + tard la veille de la mise en service, au service de police via : [www.declarationcamera.be](http://www.declarationcamera.be)
    - Nécessité d'avoir un RAT
  - Pas obligation de notification SI caméra **fixe** dans lieu **fermé non accessible au public** et utilisée à des **fins personnelles et domestiques** (intérieur d'une habitation privée)
  - Si lieu ouvert : en + => avis préalable, positif et motivé du conseil communal (qui consulte au préalable le chef de corps)

Copyright Didier Gobert 2000-2019

## Cybersurveillance

### Vidéosurveillance des espaces (semi) publics

- **Quelques remarques :**
  - Caméra à l'entrée d'un magasin où tout le monde peut visionner les images sur écran => en principe illégal car seul le responsable du traitement peut accéder aux images !
  - Citoyen place images filmées par caméras sur Internet (youtube, facebook), notamment pour rechercher coupable infraction => illégal car seul le responsable du traitement peut accéder aux images + traitement de données sensibles (judiciaires) sans consentement express ! (Exception pour instances judiciaires).
  - Droit d'accès => plus théorique que pratique car images conservées peu de temps (max 1 mois) => images souvent effacées au moment de la demande
  - Firme de surveillance qui gère les caméras n'est que le sous-traitant du responsable du traitement

Copyright Didier Gobert 2000-2019



## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- **Publicité/marketing et gestionnaire réseau**
- Questions relatives à la preuve
- Questions relatives à la propriété intellectuelle
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- Criminalité informatique et obligation de collaboration
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Publicité/marketing et gestionnaire réseau

### Pourquoi en parler ?

- L'entreprise dans laquelle vous allez travailler va utiliser divers techniques de communication pour faire de la publicité/marketing...
- Ces techniques sont soumises à des contraintes juridiques
- Vous allez parfois devoir gérer la mise en œuvre de ces techniques (courriel, gestion bases de données opt-in ou opt-out, cookies et paramétrage navigateur, paramétrage émetteur bluetooth, etc.)

Copyright Didier Gobert 2000-2019

# Les courriers électroniques publicitaires non sollicités (spamming)

## Courriers électroniques non sollicités Notions de publicité et courrier électronique

- Publicité : CDC, art. I.18, 6°
- Courrier électronique : CDC, art. I.18, 2°  
*« tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère »*

=> définition large ! Cela vise : e-mail classique  
mais aussi sms et messages sur boîte vocale  
(téléfax non visé mais règles comparables dans  
CDC, art. VI.110 !)

Copyright Didier Gobert 2000-2019

## Courriers électroniques non sollicités

### Principe du consentement préalable (opt-in)

- CDC, Art. XII.13, § 1 : « *L'utilisation du courrier électronique à des fins de publicité est interdite, sans le consentement préalable, libre, spécifique et informé du destinataire des messages* »
- Libre : le consentement ne peut être forcé, tacite ou contraint (attention à la case « oui » précochée)
- Spécifique : directement de la personne concernée
- Informé : du fait de recevoir de la publicité (info diluée dans Conditions Générales non suffisant)

Copyright Didier Gobert 2000-2019

## Courriers électroniques non sollicités

### Exceptions au principe de l'opt-in

- Pas nécessaire de demander le consentement préalable (AR 4/04/2003) si :
  - E-mail publicitaire envoyé aux **clients**
    - Suppose une relation contractuelle préalable avec le prestataire
    - Uniquement pour des produits ou services analogues offerts par lui
    - Possibilité offerte au client de refuser une telle exploitation de ses données au moment de la récolte
  - E-mail publicitaire envoyé à des **personnes morales** (info@company.be >< nom.prenom@company.be)  
>> à la position de la CNIL plus laxiste

Copyright Didier Gobert 2000-2019

## Courriers électroniques non sollicités

### Autres contraintes légales

- Principe d'identification (CDC, art. XII.12)  
=> mention « *Publicité* » si nécessaire
- Droit d'opposition (CDC, art. XII.13, § 2)  
=> Dans tous les cas, le prestataire est « *tenu, lors de l'envoi de toute publicité par courrier électronique, de :*  
*1° fournir une information claire et compréhensible concernant le droit de s'opposer, pour l'avenir, à recevoir les publicités ;*  
*2° indiquer et mettre à disposition un moyen approprié d'exercer efficacement ce droit par voie électronique* ».

Exemple : « *Si vous ne désirez plus recevoir de courriers électroniques de notre part, [cliquez ici](#)* »

Copyright Didier Gobert 2000-2019

## Courriers électroniques non sollicités

### Autres contraintes légales

- Pour assurer l'efficacité du droit d'opposition, art. 2 AR du 4/04/2003 précise :

« *Toute personne peut notifier directement à un prestataire déterminé, sans frais ni indication de motifs, sa volonté de ne plus recevoir, de sa part, des publicités par courrier électronique.*

*Le prestataire concerné est tenu de :*

*1° délivrer, dans un délai raisonnable, un accusé de réception par courrier électronique confirmant à cette personne l'enregistrement de sa demande ;*

*2° prendre, dans un délai raisonnable, les mesures nécessaires pour respecter la volonté de cette personne ;*

*3° tenir à jour des listes reprenant les personnes ayant notifié leur volonté de ne plus recevoir, de sa part, des publicités par courrier électronique ».*

Copyright Didier Gobert 2000-2019

## Courriers électroniques non sollicités

### Autres contraintes légales

- Méthodes interdites (CDC, art. XII.13, § 3) :

*« Lors de l'envoi de publicités par courrier électronique, il est interdit :*

*1° d'utiliser l'adresse électronique ou l'identité d'un tiers ;  
2° de falsifier ou de masquer toute information permettant d'identifier l'origine du message de courrier électronique ou son chemin de transmission ».*

Copyright Didier Gobert 2000-2019

Cas particulier du  
bluetooth marketing, RFID, NFC  
(Near Field Communication)

## Courriers électroniques et publicité

### Cas particulier du bluetooth marketing

- L'utilisation de la technologie bluetooth pour mener des campagnes publicitaires n'est pas interdite en tant que telle par la réglementation.
- Néanmoins, ce type de campagne doit être mené dans le respect strict des dispositions du CDC (particulièrement livres VI et XII).

Copyright Didier Gobert 2000-2019

## Courriers électroniques et publicité

### Cas particulier du bluetooth marketing

- La technique de transmission via bluetooth est-elle un courrier électronique ? **OUI**
- Le message transmis est-il publicitaire ? **A vérifier au cas par cas.** Si non, consentement préalable non requis.
- Quid du simple message de demande de connexion bluetooth (« Recevoir message via bluetooth de nom personne, entreprise ou marque ? ») ? **Selon SPF Economie, non !** Seulement une modalité pour recueillir le consentement.

Copyright Didier Gobert 2000-2019

## Courriers électroniques et publicité

### Cas particulier du bluetooth marketing

- ***Comment demander le consentement et à quelles conditions doit-il satisfaire ?***
  - Consentement du destinataire du message qui doit être *libre, spécifique et informé*.
  - La condition la plus délicate = consentement informé :
    - Demande de connexion = condition nécessaire mais pas suffisante
    - Délimitation d'une zone spatiale avec affiche d'informations AVANT d'entrer dans cette zone OU bouton à appuyer sur la fiche d'informations OU zone très réduite d'émission (+/- 20 cm) par rapport à l'affiche

Copyright Didier Gobert 2000-2019

## Cas particulier de l'utilisation des cookies

## Publicité

### Utilisation de cookies

- *Loi 13 juin 2005, art. 129 :*

- *Le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur est autorisée uniquement à condition que :*

*1° l'abonné ou l'utilisateur concerné reçoive (...) des **informations** claires et précises concernant les objectifs du traitement et ses droits (...);*

*=> nécessité de renvoyer vers une privacy policy complète propre à l'utilisation des cookies (voir partie vie privée), préalable au consentement*

*2° l'abonné ou l'utilisateur final ait donné **son consentement** après avoir été informé (...).*

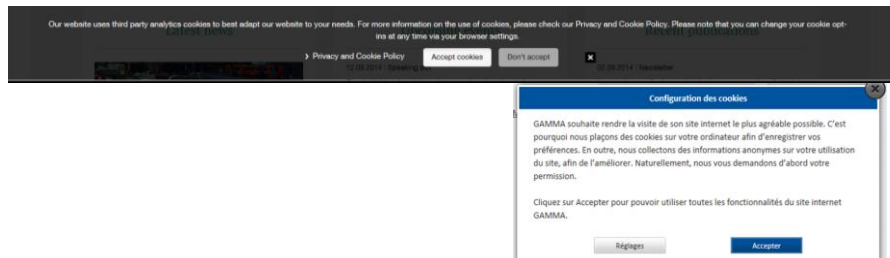
Copyright Didier Gobert 2000-2019

## Publicité

### Utilisation de cookies

- En pratique ? Controversé ! :

- Opt-in strict => consentement explicite (position CPVP, Groupe 29 et CE) :



=> Ce message reste affiché tant que choix non fait

=> Le site ne doit pas utiliser de cookies tant que le choix n'est pas fait (mais navigation tjrs possible) ou si refus.

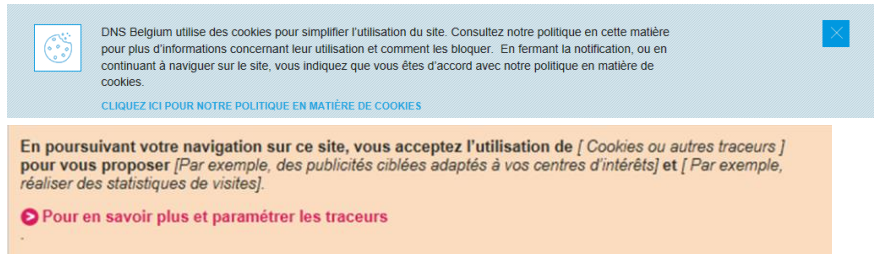
Copyright Didier Gobert 2000-2019



## Publicité

### Utilisation de cookies

- En pratique ? Controversé ! :
  - Soft Opt-in (cons. implicite) *voire* opt-out (position IBPT) :



- => Message disparaît et site utilise des cookies dès que navigation commence
- => consentement (opt-in) ou simple info avec possibilité de refus (opt-out) ?
- => problème : comment refuser en pratique => pas d'onglet « Refus » (voir la politique cookies) => on force *de facto* le consentement...

Copyright Didier Gobert 2000-2019

## Publicité

### Utilisation de cookies

- Informer uniquement que utilisation de cookies et dire que utilisateur peut **paramétrer son navigateur** pour les refuser ne suffit pas !
- Pour certains cookies, **consentement pas nécessaire** :
  - *L'alinéa 1er n'est pas d'application pour l'enregistrement technique des informations ou de l'accès aux informations stockées dans les équipements terminaux d'un abonné ou d'un utilisateur final ayant pour seul but de réaliser l'envoi d'une communication via un réseau de communications électroniques ou de fournir un service demandé expressément par l'abonné ou l'utilisateur final lorsque c'est strictement nécessaire à cet effet.*
  - Exemples : cookies liés à la sécurisation d'une connexion, cookies pour déterminer l'ordre d'échange des données ou détecter pertes de données, cookies de mémorisation de login/mot de passe, cookies de panier d'achat, cookies retenant le choix de langue...

Copyright Didier Gobert 2000-2019

## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- Publicité/marketing et gestionnaire réseau
- **Questions relatives à la preuve**
- Questions relatives à la propriété intellectuelle
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- Criminalité informatique et obligation de collaboration
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Les règles essentielles en matière de preuve

- En cas de contestations ou de litiges, important de pouvoir faire la preuve de son droit

=> réflexe à acquérir : se réserver et conserver un maximum de preuves !

(trop souvent négligé en pratique)

Exemple : votre patron vous demande « oralement » de contrôler le contenu des mails d'employés ! Prudence !!!

Question : sous quelles formes ?

Copyright Didier Gobert 2000-2019

## Les règles essentielles en matière de preuve

- Deux systèmes de preuve :
  - preuve libre : tout procédé susceptible de convaincre le juge peut être présenté  
  
exemples : un écrit signé, un témoignage, des documents non signés, le contenu d'un support numérique, fax, e-mail, etc  
**exemple : preuve d'un fait (>< preuve d'un droit)**
  - preuve réglementée : les moyens recevables sont énumérés de façon limitative par la loi  
  
Exemple : pour faire la preuve d'un acte juridique > 375 € à l'égard d'un particulier, seul un écrit papier signé manuscritement était accepté (sauf si on peut se prévaloir des exceptions)  
Exemples : assurance, cession droit auteur, etc.

Copyright Didier Gobert 2000-2019

## Les règles essentielles en matière de preuve

- Entre commerçants, la preuve est libre (sauf exception) :  
il est donc possible de faire preuve avec un fax ou un e-mail  
  
MAIS ces moyens de preuve ont leurs limites :
  - impossible de faire preuve avec un fax ou un e-mail si l'autre partie peut se prévaloir d'un écrit papier signé manuscritement (preuve parfaite)  
*exemple : contrat initial papier, puis en cours de projet, nouveaux engagements décidés par e-mail !*
  - Le fax ou l'e-mail sont recevables par le juge mais leur valeur probante est laissée à sa libre appréciation (preuve imparfaite) => incertitude !
- Conclusion : recevabilité n'implique pas force probante

Copyright Didier Gobert 2000-2019

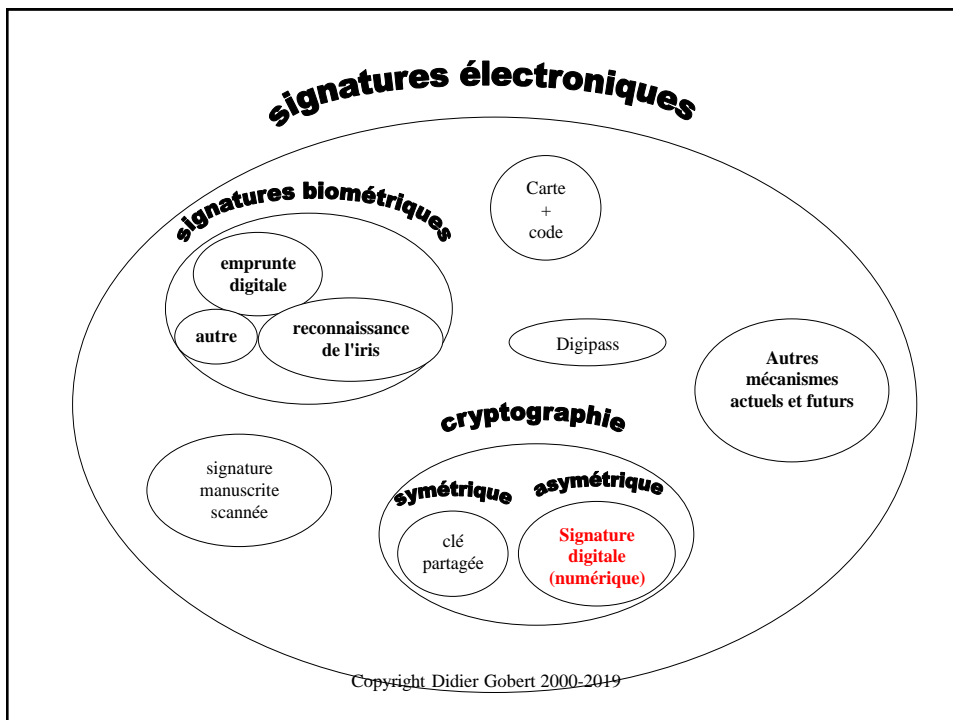
## Les développements législatifs

- Quid si un e-mail est signé électroniquement : cela vaut-il un écrit papier signé manuscritement ?

Notre droit prévoit depuis 2000 cette assimilation mais à certaines conditions !

- MAIS attention : pas tous types de signatures électroniques

Copyright Didier Gobert 2000-2019



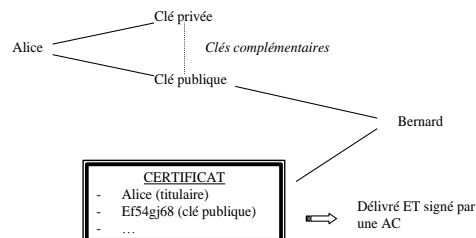
## La signature numérique

- Mécanisme prédominant : signature numérique
  - mécanisme qui s'impose *de facto* (certificat de signature sur notre carte d'identité électronique)
  - mécanisme qui répond sans aucun doute à la notion de *signature électronique avancée* (directive, lois de transposition)

Copyright Didier Gobert 2000-2019

## La signature numérique

- La technique de signature numérique permet:
  - de garantir la confidentialité
  - de signer (identité de l'émetteur et intégrité du message)
- L'utilisation de la signature numérique implique:



Copyright Didier Gobert 2000-2019

## Effets juridiques des SE

- **Non discrimination** : signature électronique
  - **Assimilation**  
=> signature électronique **avancée** = signature manuscrite **SI**
    - basée sur un certificat qualifié (Annexe 1)
    - ... délivré par un PSC conforme Annexe 2
    - créée par un dispositif sécurisé de création de signature (Annexe 3)
- => recevabilité - valeur probante?
- => recevabilité + force probante / même validité

Copyright Didier Gobert 2000-2019

## Vers un cadre juridique pour d'autres services de confiance

- Règlement européen du 23 juillet 2014 du Parlement européen et du Conseil sur **l'identification électronique et les services de confiance** pour les transactions électroniques au sein du marché intérieur, et abrogeant la directive 1999/93/CE
- Loi du 21 juillet 2016 portant insertion d'un titre 2, '**Certaines règles relatives au cadre juridique pour les services de confiance (signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification)**', dans le livre XII du Code de droit économique, et portant insertion des définitions propres au titre 2 précité et des dispositions d'application de la loi propres au même titre, dans les livres I et XV du Code de droit économique.

Copyright Didier Gobert 2000-2019

## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- Publicité/marketing et gestionnaire réseau
- Questions relatives à la preuve
- **Questions relatives à la propriété intellectuelle**
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- Criminalité informatique et obligation de collaboration
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Aspects de propriété intellectuelle

- Différents types de protection
  - droit d'auteur classique
  - droit d'auteur « aménagé » (programmes d'ordinateur)
  - droit sui generis (bases de données)
- Spécificités :
  - Exception pour copie privée ?
  - Cession des droits à l'employeur (présomption ?)

Copyright Didier Gobert 2000-2019

## Gestion réseau et propriété intellectuelle

- Programmes d'ordinateur sont protégés par le droit d'auteur =>
  - Veiller à disposer de toutes les licences nécessaires pour les logiciels installés
  - Interdire aux utilisateurs de télécharger et d'installer les logiciels protégés => installer un dispositif technique de protection ? limiter les droits sur le PC (pas administrateur) ?
- De nombreux éléments disponibles sur Internet sont protégés par le droit d'auteur... ou des contrefaçons !
  - Rappel des principes, droits et obligations dans la politique ICT
  - Attention à l'utilisation de logiciel peer-to-peer => interdire ?
  - Attention aux téléchargements réalisés par les utilisateurs => interdire ?

Copyright Didier Gobert 2000-2019

## Protection des bases de données

- Double système de protection et double objet :  
=> protections cumulatives
  - structure de la BD : protection par le droit d'auteur
  - contenu de la BD :
    - protection éventuelle par le droit d'auteur si le contenu satisfait aux conditions de protection du droit d'auteur => pas toujours le cas, ce qui pose un problème pour les bases de données non créatives (non originales)
    - protection par le droit *sui generis*
- Raison d'être du droit *sui generis* : protection de l'investissement et non de l'activité créative => éviter le « pillage d'informations »

Copyright Didier Gobert 2000-2019



## **Droit *sui generis* (bases de données non créatives)**

- Exemples de bases de données :
  - un annuaire téléphonique
  - un site web présentant les horaires des séances de cinéma
  - un guide d'adresses relatives à des organismes d'aide sociale
  - les sommaires des décisions de jurisprudence mis en ligne et accessible au moyen d'un outil de recherche
  - un site web d'annonces (emploi, immobilier, ticket, site de ventes aux enchères, marchés publics, etc.)
  - un site web d'informations financières
  - Banque carrefour des entreprises
  - une collection d'hyperliens classés par catégories

Copyright Didier Gobert 2000-2019

## **Droit *sui generis* (bases de données non créatives)**

- Condition de protection : investissement substantiel (humain, matériel ou financier) dans l'obtention, la vérification et/ou la présentation du contenu
  - **non** si création et/ou simple présentation des horaires des TEC (papier, page web)
  - **oui** si ces données sont organisées dans une BD sur internet, dotée d'un outil de recherche, d'un calcul d'itinéraire, etc.
- Etendue de la protection : droit d'interdire l'extraction (*sorte de droit de reproduction*) et/ou la réutilisation (*sorte de droit de communication au public ou distribution*) d'une partie substantielle, évaluée de manière quantitative ou qualitative, du contenu de la BD (problèmes d'interprétation)

Copyright Didier Gobert 2000-2019

## **Droit *sui generis* (bases de données non créatives)**

- Cela couvre les extractions répétée et systématique de parties non substantielles
- Exemple d'extraction et réutilisation non autorisée (Trib. Instance Bruxelles) :

*Un concurrent de Cinebel reprend chaque semaine les quelques horaires qui lui manquaient sur le site de Cinebel => partie non substantielle mais interdite car reprise répétée et systématique des données et atteinte à l'exploitation normale de la base de données*

*=> logique : on veut éviter le pillage d'informations, assurer une concurrence saine, éviter les pratiques déloyales*

Copyright Didier Gobert 2000-2019

## **Droit *sui generis* (bases de données non créatives)**

- Exemples d'application du droit *sui generis* :
  - Proposer à la vente un logiciel à intégrer dans les applications bureautiques visant à fournir diverses versions de traduction  
=> problème : le logiciel ne traduit pas lui même le texte proposé par l'utilisateur mais il permet de proposer la traduction d'un terme, d'une expression ou d'une phrase sans quitter l'environnement de travail **en allant consulter les moteurs de traduction et les bases de données terminologiques gratuites les plus réputés sur Internet et en reproduisant les résultats de la traduction réalisée par ces derniers**  
=> violation du droit *sui generis* ( + non respect des conditions générales d'utilisation des sites « pompés » + violation du droit d'auteur sur les traductions réalisées par le logiciel + concurrence déloyale / parasitaire)

Copyright Didier Gobert 2000-2019

## Logiciel libre

### Notion

- Logiciel libre =~ Free Software =~ Open source => en théorie, différent mais en pratique, ces notions se recoupent (GPL, LGPL, QPL, OSL, MPL, Apache, ...)
- Le modèle « libre » se distingue du modèle « propriétaire » essentiellement sur deux points :
  - stratégie économique : soit intervention non lucrative soit business orienté services (mais pas de revenus tirés du droit d'auteur) >< business assuré par licence payante (revenus du droit d'auteur) et services
  - stratégie juridique : distribution encadrée par une licence extrêmement étendue et souple (logique « d'autorisation ») + accès aux sources >< distribution **cadennassée** par une licence d'utilisation stricte et limitée (logique « d'interdiction ») + non divulgation des sources

Copyright Didier Gobert 2000-2019

## Logiciel libre

### Quelques malentendus à dissiper

- « Libre » ne veut pas dire :
  - *Contre* ou *anti* ou *non soumis* au droit d'auteur => applicable de la même manière au logiciel libre ! => les licences de logiciels libres sont une application du droit d'auteur !
  - *Que l'on est libre de faire ce que l'on veut avec le logiciel* => même si elle est (très) étendue, on est tenu de respecter les conditions de la licence (grandes variété de licences) => il s'agit d'un contrat que l'on doit respecter (convention-loi)
  - *Totalement gratuit ou non commercial* : a priori, licence gratuite mais services payants (installation, paramétrage, maintenance, support, formation, etc.)
- Distinguer : licences « open source » pour les logiciels des licences « Creative Commons » pour autres œuvres (musique, photo, clip, etc.) => légères différences (distinction commercial >< non commercial) !

Copyright Didier Gobert 2000-2019

## Logiciel libre

### Caractéristiques

- La licence de distribution du logiciel libre :
  - **gratuite**
  - très **étendue** : offre de nombreuses « libertés » à l'utilisateur (utiliser - même à des fins commerciales -, reproduire, modifier, adapter, évoluer, redistribuer tout ou partie, etc.)
  - donne libre **accès aux codes sources**
- Licence « copyleft » ou « non copyleft » ?
  - **Copyleft** = en contrepartie des droits étendus reconnus par la licence, le licencié qui souhaite distribuer le logiciel modifié est tenu de le faire sous la même licence que celle dont il a bénéficié  
=> **effet « viral » de la licence ! Attention aux effets nocifs !**
  - **Non Copyleft** (BSD) = le licencié peut distribuer le logiciel qu'il a modifié sous une autre licence (libre mais aussi propriétaire !)

Copyright Didier Gobert 2000-2019

## Logiciel libre

### Quelques questions problématiques

- **Distribué sans responsabilité ni garantie** (notamment d'éviction) de la part des auteurs => quid si un tiers invoque une contrefaçon et bloque l'utilisation de votre logiciel (utilisant du libre) ?
- **Effet « viral » du copyleft** => quid si vous incorporez du copyleft dans un autre logiciel libre voire dans votre logiciel propriétaire ?
  - Copyleft **faible** (Mozilla PL) : possible de déroger à certaines conditions (possible de refuser accès aux sources si peu de libre incorporé dans un logiciel original vaste)
  - Copyleft **fort** (GPL) : aucune restriction possible => si redistribution, nécessité de le faire sous la même licence => votre logiciel « propriétaire » qui intègre un peu de GPL devient un logiciel totalelement libre GPL si distribution ! => **prudence**
  - **Conflits possibles** entre différentes licences dans un même logiciel !

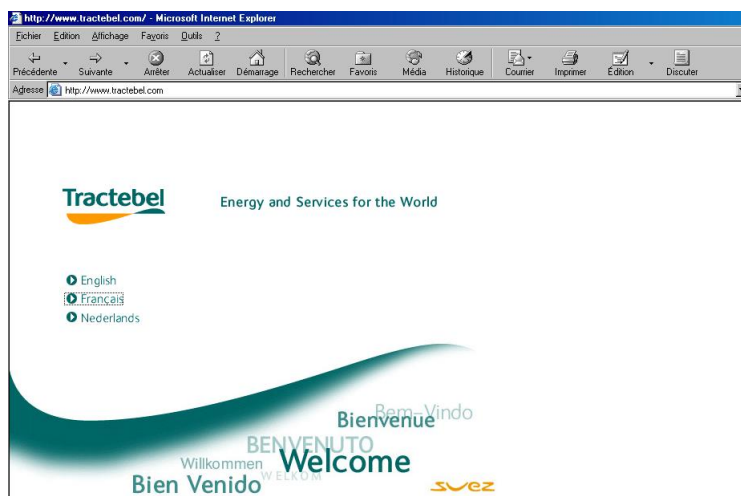
Copyright Didier Gobert 2000-2019

## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- Publicité/marketing et gestionnaire réseau
- Questions relatives à la preuve
- Questions relatives à la propriété intellectuelle
- **Problèmes liés à la réservation (récupération) d'un nom de domaine**
- Criminalité informatique et obligation de collaboration
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Affaire Tractebel



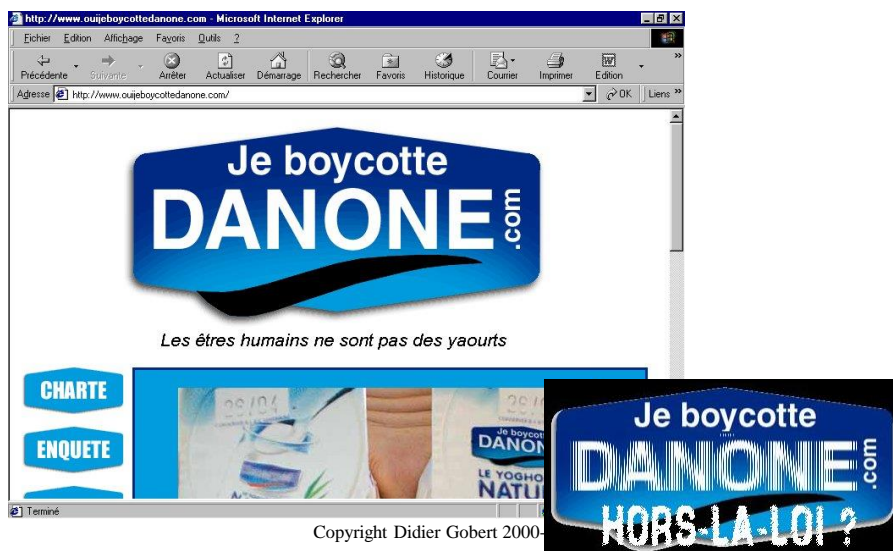
Copyright Didier Gobert 2000-2019

## Portail fédéral belge



Copyright Didier Gobert 2000-2019

## Affaire Danone



Copyright Didier Gobert 2000-

## Litiges en matière de noms de domaine

- **Problème** : dans de nombreux cas, les noms de domaine peuvent être librement enregistrés (aucun contrôle de l'organisme) par n'importe qui

=> quid si un tiers revendique un droit sur ce nom de domaine ? Peut-il récupérer le nom de domaine ?

- **Deux hypothèses** doivent être envisagées :
  - Le litige oppose des titulaires de droits concurrents
  - Le litige oppose des parties, dont l'une (celle qui a enregistré le nom de domaine !) n'est titulaire d'aucun droit légitime =>  
*Domain name grabbing* => +/- 90 % des cas

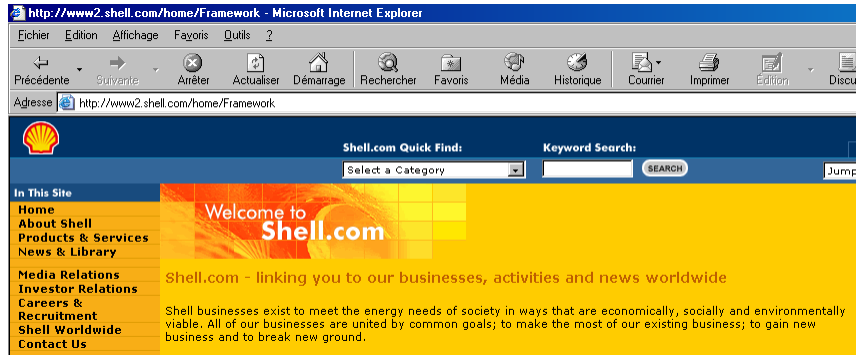
Copyright Didier Gobert 2000-2019

## Litiges en matière de noms de domaine 1ère hypothèse

- **Litige entre titulaires de droits concurrents** :
  - Deux **marques** (protection territoriale), qui coexistaient paisiblement sur des territoires distincts, entrent en conflit par le biais de l'Internet
  - Un **nom patronymique** déposé comme nom de domaine, au grand regret du titulaire d'une marque similaire
  - Deux **dénominations sociales** éloignées ou pour des activités distinctes que l'Internet rapproche subitement
  - Autres types de droits : ind. géogr., app. d'origine, nom commercial
- **Solution** :
  - Pas évident car chaque partie peut se prévaloir légitimement d'un droit.
  - Tendance : « premier arrivé, premier servi » => **difficile de récupérer le nom de domaine !**
  - mais certaines exceptions (abus de droit) et parfois décisions surprenantes !

Copyright Didier Gobert 2000-2019

## Affaire shell.de 1ère hypothèse



Copyright Didier Gobert 2000-2019

## Commune de Chimay 1ère hypothèse



Copyright Didier Gobert 2000-2019



## Litiges en matière de noms de domaine

### 2ième hypothèse

- **Domain name grabbing** (livres XII et XVII du CDE):  
usurpation du nom de domaine => consiste à enregistrer un nom de domaine sur lequel un tiers dispose d'un droit (marque, nom patronymique, nom commercial) pour diverses raisons :
  - Soit dans le but de faire du profit : le nom de domaine enregistré est revendu à un prix supérieur au coût de l'enregistrement
  - Soit dans le but d'empêcher le tiers (un concurrent par exemple) de disposer du nom de domaine
  - Soit dans le but de profiter de la réputation du tiers et du trafic sous-jacent (parasitisme) : enregistrer en « .com » le nom de la nouvelle vedette issue de « The Voice » et laisser libre en « .net » et « .fr » afin que le public arrive sur mon site en « .com »
- **Solution** : en principe, le titulaire du droit l'emporte (+ éventuelles conditions prévues par la loi)

Copyright Didier Gobert 2000-2019

## Litiges en matière de noms de domaine

### 2ième hypothèse

- **Domain name grabbing** => recours possibles :
  - si litige concernant un *.be* :
    - **devant le juge** (judiciaire) : action en cessation + ordre de transfert du nom de domaine consacrés par livres XII et XVII, CDE (procédure assez facile et rapide)
    - **devant le CEPANI** (arbitrage) : procédure rapide et peu coûteuse (1.620 euros pour 1 arbitre)
  - si litige concernant un domaine générique (*.com, .org, .biz, etc.*) :
    - **recours devant l'OMPI** (arbitrage) selon la procédure UDRP (Uniform domain name Dispute Resolution Policy) : tous les acteurs (ICANN, Titulaires, OMPI, Unités d'enregistrement) sont tenus contractuellement de se soumettre à cette procédure rapide et efficace => +/- 45 jours de procédure (1.500 USD pour 1 arbitre)
  - si litige concernant un *.eu* (Règl. 874/2004) : arbitrage possible devant la **Cour Arbitrale Tchèque** ! (1.300 euros pour 1 arbitre)

Copyright Didier Gobert 2000-2019

## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- Publicité/marketing et gestionnaire réseau
- Questions relatives à la preuve
- Questions relatives à la propriété intellectuelle
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- **Criminalité informatique et obligation de collaboration**
- Responsabilité pénale d'un gestionnaire de réseau

Copyright Didier Gobert 2000-2019

## Position du problème

- De plus en plus d'actes malveillants sont commis sur les réseaux informatiques (fermés ou ouverts)
- Or bon nombre de ces actes n'étaient pas punis car ils ne rentraient pas dans une catégorie connue d'infractions du code pénal ET interprétation par analogie non permise
- Nécessité d'introduire dans le code pénal des infractions spécifiques à l'informatique : loi du 28 novembre 2000 (*M.B.*, 3 février 2001)

Copyright Didier Gobert 2000-2019

## Nouvelles infractions

- La loi du 28 novembre 2000 introduit 4 nouvelles infractions dans le code pénal :
  - Le faux et usage de faux en informatique (art. 210*bis*)
  - La fraude informatique (art. 504*quater*)
  - L'accès et le maintien non autorisé dans un système informatique (art. 550*bis*) => *hacking*
  - Le sabotage de données et/ou système informatique (art. 550*ter*)

Copyright Didier Gobert 2000-2019

## Nouvelles infractions

- « Système informatique » défini de manière **très large** :  
ordinateur en soi, cartes à puce, réseaux et leurs composants, systèmes de télécommunications et leurs composants, appareils photos digitaux, caméras digitales, téléphones mobiles, systèmes de gestion automatique des distributeurs (boissons au autres)...

Copyright Didier Gobert 2000-2019

## Le faux et usage de faux en informatique

- « Art. 210bis : *Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement* ».

=> cela vise toute falsification, par le biais de manipulations, de données informatiques pertinentes.

Copyright Didier Gobert 2000-2019

## Le faux et usage de faux en informatique

- Exemples :
  - Falsification et/ou contrefaçon de cartes de crédit
  - Fausses signatures électroniques (sauf si pas de dol spécial !)
  - Modification du contenu d'un contrat électronique
  - Introduire un faux numéro de carte de crédit sur Internet
  - Introduire dans le logiciel comptable de fausses dépenses, etc.

Copyright Didier Gobert 2000-2019

## La fraude informatique

- « Art. 504quater : *Celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou en effaçant des données qui y sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement* ».

*Idem (mais peine moins lourde) si seulement tentative de commettre une telle infraction*

Copyright Didier Gobert 2000-2019

## La fraude informatique

- Exemples :
  - L'utilisation d'une carte de débit ou de crédit volée pour retirer de l'argent à un guichet automatique
  - Le détournement de fichiers ou programmes confiés dans un but précis dans l'objectif d'en tirer un profit
  - L'introduction d'instructions informatiques pour modifier le résultat de certaines informations et tirer un avantage financier (manipulations effectuées par un employé de banque sur les comptes des clients)
  - L'introduction dans un logiciel piraté d'une liste de numéros de licence trouvés sur Internet, etc.

Copyright Didier Gobert 2000-2019

## L'accès et le maintien non autorisé dans un système informatique (*hacking*)

- L'art. 550bis du CP vise plusieurs types d'infractions :
  - Atteintes portées à partir de l'extérieur du système (*hacking externe*)
  - Atteintes portées par des utilisateurs qui possèdent certains pouvoirs d'accès (*hacking interne*)
  - Les actes préparatoires
  - Le fait de commanditer un *hacking*
  - Le « recel » de données obtenues à la suite des infractions précédentes

Copyright Didier Gobert 2000-2019

## L'accès et le maintien non autorisé dans un système informatique (*hacking*)

- Les actes préparatoires :

« Art. 550bis, §5 : *Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1<sup>er</sup> à 4 peuvent être commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.* »

Copyright Didier Gobert 2000-2019

## L'accès et le maintien non autorisé dans un système informatique (*hacking*)

- Les actes préparatoires :
  - Exemples :
    - Conception et distribution de virus informatiques
    - Recherche (la simple recherche suffit), rassemblement et distribution de logiciels permettant notamment de violer la sécurité de systèmes informatiques (craquer des codes d'accès) ou de neutraliser les dispositifs de protection d'œuvres protégées par le droit d'auteur
    - Escroquerie aux codes d'accès
  - Il faut un **dol spécial** : intention frauduleuse ou dessein de nuire

Copyright Didier Gobert 2000-2019

## Le sabotage de données et/ou système informatique

- L'art. 550ter du CP vise plusieurs types d'infractions :
  - Toute manipulation de données effectuée dans le but de nuire
  - Le fait de causer des dommages aux données
  - Le fait d'empêcher le bon fonctionnement d'un système informatique
  - Les actes préparatoires tels la conception, mise à disposition ou diffusion de virus

Copyright Didier Gobert 2000-2019

## Le sabotage de données et/ou système informatique

- Manipulation de données effectuée dans le but de nuire :

*« Art. 550ter, §1 : Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement. »*

Copyright Didier Gobert 2000-2019

## Le sabotage de données et/ou système informatique

- Exemples :
  - Un employé licencié place une bombe logique sur le disque dur de son ordi ou envoie un virus en attach de son courrier électronique
  - Faire disparaître certains fichiers du disque dur ou les rendre définitivement indisponibles au moyen de techniques de cryptage
  - Introduire un programme ayant pour conséquence d'invertir certaines lettres du clavier de la victime
  - Blocage du système (total ou partiel) – ex : denial of service => flooding consistant à mettre un ordinateur hors d'usage en le surchargeant de données.

Copyright Didier Gobert 2000-2019



## Quelques questions de procédure : devoir de collaboration (« réquisition » !)

- **Art. 88quater CICr** : « §1. Le juge d'instruction ou un officier de police judiciaire auxiliaire du Procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible.

§2 Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou selon le cas de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite dans la mesure de leurs moyens ».

Copyright Didier Gobert 2000-2019

## Quelques questions de procédure : devoir de collaboration

- **Personnes visées** : formulation très large => responsable du système informatique, un utilisateur principal, gestionnaire du réseau, concepteur ou fournisseur des logiciels permettant de déchiffrer les données ou des techniques de cryptage ou d'accès à celles-ci, *trusted third parties* et autres détenteurs de clés de cryptage, experts en cryptographie, spécialistes de la sécurité  
**MAIS PAS** l'inculpé ni ses proches
- **Sanctions pénales en cas de refus** de coopération (sauf si secret professionnel)
- Personne qui collabore est tenue au **secret**
- **L'Etat est civilement responsable** des dommages causés de façon non intentionnelle par cette personne

Copyright Didier Gobert 2000-2019

## Plan de l'exposé

- Vie privée (RGPD et cybersurveillance)
- Publicité/marketing et gestionnaire réseau
- Questions relatives à la preuve
- Questions relatives à la propriété intellectuelle
- Problèmes liés à la réservation (récupération) d'un nom de domaine
- Criminalité informatique et obligation de collaboration
- **Responsabilité pénale d'un gestionnaire de réseau**

Copyright Didier Gobert 2000-2019

## Responsabilité pénale d'un GR

Quid si un utilisateur commet une infraction **pénale** à partir du réseau ?

- Exemple : actes terroristes, hacking, spamming, escroqueries, téléchargement de contenus pédophiles ou protégés par le droit d'auteur, utilisation frauduleuse de la carte de crédit d'un tiers, ventes illicites (drogue, médicaments, armes...)
- **Conseil si vous constatez ce type d'infraction** : informer la hiérarchie et proposer d'appeler la FCCU

Copyright Didier Gobert 2000-2019

## L'infraction **pénale**

Deux éléments doivent être réunis :

- Un élément **matériel** : le fait qualifié d'infraction
- +
- Un élément **moral** : l'imputabilité du fait à l'auteur (connaître le caractère illicite et vouloir)

⇒ *Le gestionnaire de réseau n'est pas coupable de l'infraction*

Copyright Didier Gobert 2000-2019

## La complicité en droit **pénal**

(art. 67 C. pénal)

- Le fait de fournir les instruments du crime ou du délit
- +
- L'intention de participer à la réalisation de l'infraction principale (savoir que l'instrument va servir à commettre un crime ou un délit)

⇒ *Le gestionnaire de réseau n'est pas complice*

Copyright Didier Gobert 2000-2019

## Pour approfondir

- Élaboration de brochures (gratuites) disponibles en 4 langues (FR, NL, EN, ALL) et distribuées grand public :
  - « Le spamming en 24 Questions & Réponses »
  - « Le spamming en question : exemples illustrés et conseils pratiques »



<https://economie.fgov.be/fr/themes/line/commerce-electronique/spamming>

Copyright Didier Gobert 2000-2019

## Pour approfondir

- Le site web des bonnes pratiques juridiques ! :

[www.infoshopping.be](http://www.infoshopping.be)



Copyright Didier Gobert 2000-2019

Merci pour votre attention