Sécurité informatique
Aspects juridiques
ENSEEIHT 3A SN-L/B

Pierre-Yves Bonnetain-Nesterenko
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

Année 2024-2025

B&A CONSULTANTS SECURITE INFORMATIQUE

La loi française

Un certain nombre de textes prennent en compte :

- Les atteintes au fonctionnement des systèmes informatiques (au sens large).
- Les atteintes à la vie privée, potentielles ou avérées.
- La protection de la correspondance privée.
- Et plein d'autres choses sympathiques.

Cela va sans dire

La loi française s'applique en France uniquement.

Internet n'est pas une zone de non droit

Un délit/crime informatique matérialisé en France peut être poursuivi en France, même si les serveurs sont à l'étranger.

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Lois pénales directement applicables

Deux grands textes, transcrits dans le Code Pénal, sont directement applicables à l'informatique :

Article 226-16 et suivants Ex-loi Informatique et Libertés. Concerne les traitement automatisés de données nominatives.

Article 323-1 et suivants Ex-loi Godfrain. Concerne toutes les atteintes au fonctionnement des systèmes de traitement de données.

Règlement Général pour la Protection des Données

RGPD applicable depuis 28 mai 2018. Change énormément de choses sur les données personnelles.

B&A CONSULTANTS SECURITE INFORMATIQUE

Usage de ces deux textes

- Art. 226-16 et suivants : vos données nominatives sont « mal protégées » par un tiers, une collecte paraît illégitime, ...
- Art. 323-1 et suivants : vous êtes victime d'une attaque (intrusion, déni de service, vol de données, ...)

Note à l'usage des gens normaux

Il est parfois « quelque peu difficile » de faire enregistrer sa plainte par les forces de police ⇒ pour une entreprise, cela doit se préparer en amont (qui contacter ?).

Attention

L'entreprise qui se fait voler ses données ~~peut être accusée (au sens du 226-16) par ses clients (protections inadéquates)~~ va sérieusement en baver.

Concernant les données à caractère personnel

Il est nécessaire de bien comprendre que :

- Le responsable du traitement a une obligation de moyens ;
- Les moyens mis en œuvre doivent correspondre à la criticité des données ;
- Le responsable du traitement est considéré comme connaissant la sensibilité des données qu'il gère ou fait gérer ;
- Le responsable du traitement reste responsable même en cas de sous-traitance des traitements ;
- RGPD : les sous-traitants sont co-responsables même si rien dans le contrat.

Conclusion évidente

Si vous pouvez, évitez de traiter des données nominatives, ou minimisez celles que vous traitez... C'est plus facile qu'on ne le croit.

Qu'est-ce qu'une DCP

Donnée à caractère personnel

Toute donnée ou information dont le contenu permet, de façon directe ou indirecte, d'identifier son porteur ou propriétaire

Donc, potentiellement, beaucoup de choses. Y compris si forme non numérique. ~~**Conclusion** Il est conseillé de toujours déclarer ses traitements à la CNIL.~~ Déclaration supprimée avec RGPD.

Conclusion

Da Scritch, Capitole du Libre 2017 : Une DCP, c'est comme de la matière fissile. Si tu ne sais pas la collecter, la stocker et la détruire, surtout tu n'y touches pas.

B&A CONSULTANTS SECURITE INFORMATIQUE

Pour faire simple

Une donnée à caractère personnel, c'est

Toute bribe d'information permettant d'identifier une personne.

Exemples :

- photos ou vidéos,
- adresses électroniques, numéros de téléphone,
- e-mails, messages vocaux. . .

Attention

Ne confondez pas données personnelles avec données privées. Les secondes sont **incluses** dans les premières, mais n'y sont pas égales.

B&A CONSULTANTS SECURITE INFORMATIQUE

Et autour des données ?

Méta-données peuvent aussi être (très) identifiantes :

- listes d'appels téléphoniques ou SMS envoyés (qui communique avec qui, quand, à quelle fréquence, quelle durée...)
- méta-informations ajoutées dans des fichiers (images, vidéos, bureautique...)
- recherches réalisées sur un moteur de recherche, traces de navigation sur le web, résolutions DNS
- traces GPS, traces de migration d'antennes mobiles.

B&A CONSULTANTS SECURITE INFORMATIQUE

Vie privée, vie personnelle et données

Chacun devrait toujours se poser quelques questions :

- Où sont mes données nominatives et mes données privées ?
- Qui en est responsable ?
- Qui y a accès ?
- Quelles sont les règles d'engagement de ces données ?
- Qu'arrivera-t-il, que m'arrivera-t-il si ces données deviennent publiques, volontairement ou à mon insu ?

Garder à l'esprit

Ces questions, et les réponses inappropriées qui peuvent y être apportées par les entreprises, sont autant de risques personnels (propriétaire légitime) et opérationnels et juridiques (entreprise responsable).

Du point de vue de l'entreprise

Inverser les questions précédentes.

Dès lors qu'il y a collecte d'informations nominatives...

1. Comment y donner accès pour leur propriétaire (droit d'accès et de rectification, obligation CNIL) ?
2. Pour quelle utilisation les propriétaires ont-ils confié ces données ? Ne fait-on bien que ces traitements et aucun autre ?
3. Où et comment sont-elles stockées, archivées, sauvegardées ?
4. Qui en a la responsabilité technique ? opérationnelle ?
5. Qui peut y avoir accès au sens opérationnel et au sens technique ?

Liste poursuivie sur transparent suivant

B&A CONSULTANTS SECURITE INFORMATIQUE

Du point de vue de l'entreprise – suite

Dès lors qu'il y a collecte d'informations nominatives...

6. Dans quelles situations ces données peuvent-elles être utilisées ? Transmises à des tiers ? Vendues ? Est-ce bien dans les règles de collecte initiales ?
7. Quelles sont les règles de conservation et d'effacement de ces données ? Comment sont-elles appliquées ?
8. Quelles sont les conséquences pour nous/nos clients en cas de perte/fuite de ces données ?

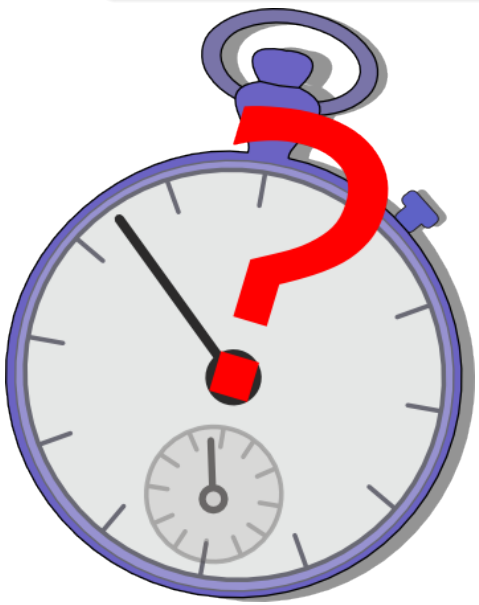
Bien trop souvent

Aucune de ces questions ne reçoit de réponse vraiment pertinente la première fois qu'on les pose. RGPD : registre des traitements et EIVP obligent à se poser ces questions.

Petit exercice

Ce n'est pas si difficile qu'on le pense...

Entreprise, comment (espérer) détecter vol de données (particulièrement données nominatives) ?
Particulier, comment (espérer) détecter fuite données nominatives et attribuer la fuite ?



Ca peut facilement arriver :

- Collaborateur parti à la concurrence avec des fichiers de l'entreprise
- Incident de sécurité et vol de données
- Matériel « jeté » sans avoir été nettoyé auparavant
- etc.

B&A CONSULTANTS SECURITE INFORMATIQUE

CNIL, RGPD, données personnelles et entreprises

N'oubliez pas l'imbrication :

1. La loi « Informatique et libertés » et le RGPD donnent des **droits** aux propriétaires des données nominatives, c'est-à-dire aux particuliers.
2. Ces droits imposent des **devoirs** aux entreprises responsables de traitements de données nominatives.
3. Ces devoirs sont maintenant des contraintes **très** fortes.

Le sens de l'histoire

Le respect de ces devoirs est de plus en plus contrôlé (cf RGPD)

Ça commence à taper – 1

2018, pré-RGPD

- Darty 100 000 € ;
- PhoneWarehouse UK 500 000 € ;
- Optical Center, 250 000 € ;
- Association pour le Développement des Foyers, 75 000 € ;
- OPH Rennes, 30 000 € ;
- DailyMotion, 50 000 €

Mouais...

Petits joueurs.

Ça commence à taper – 2

Post-RGPD...

- Septembre 2018, Alliance Francaise IDF 30 000 €
- 2019, Google, 50 millions €; Liga Espagnole, 250 000 €; Sergic, 400 000 €; Mariott, 20 millions € (init. 110); British Airways 22 millions € (init. 210);
- 2020, Carrefour, 2,25 millions €; Carrefour Banque 800 000 €; Google Irlande 100 millions €
- 2021, donneur d'ordres 150 000 €, sous-traitant 75 000 € (*credential stuffing*); AG2R La Mondiale, 1,75 millions €; BricoPrivé 500 000 €;
- 2022, Google, 250 millions €; Instagram, 405 millions €

Sans oublier...

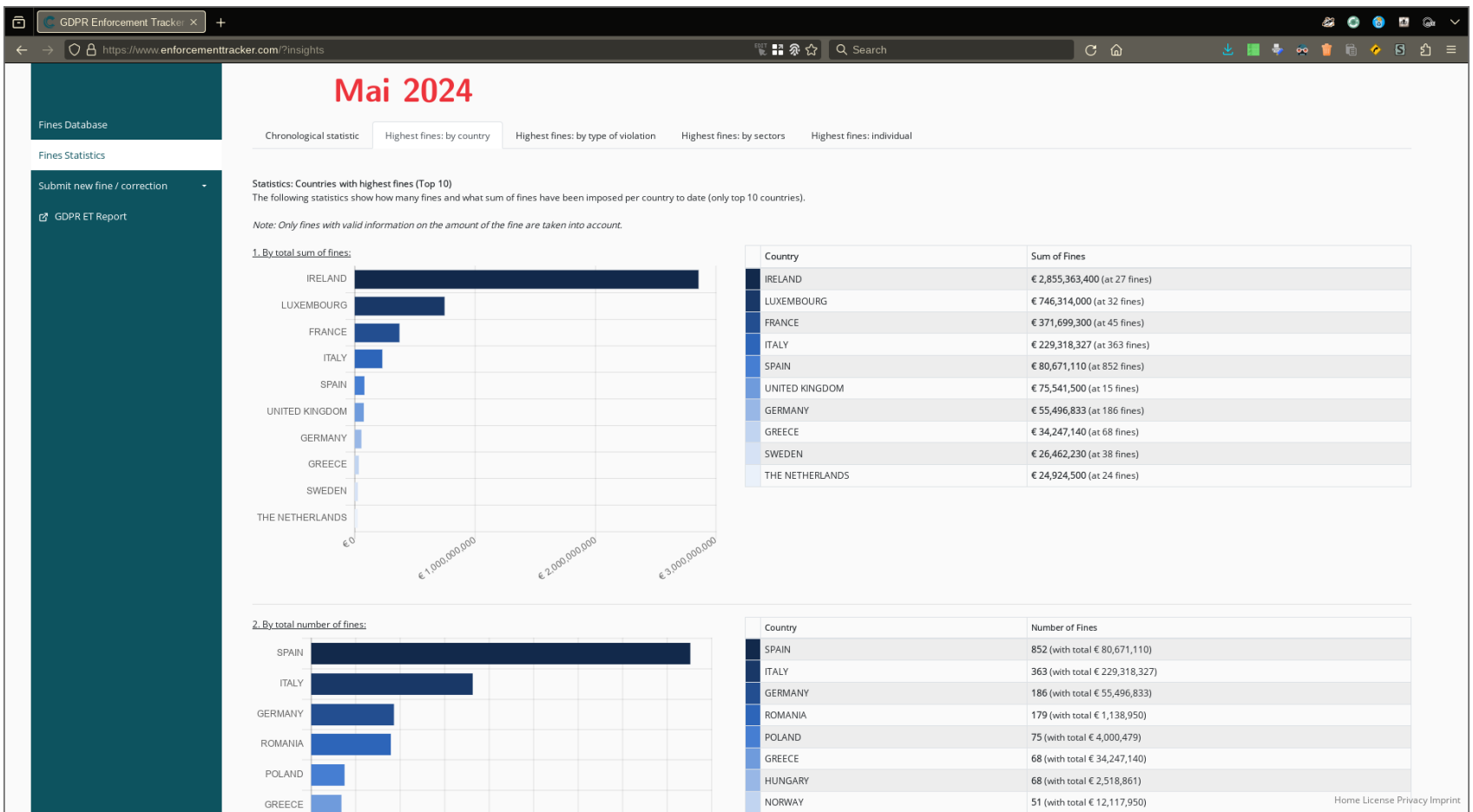
Amendes pénales. Reste dédommagement préjudices (actions de groupe), non plafonné (nécessaire prouver lien causalité).

Suivi des condamnations

Suivi des amendes et décisions

Suivi des condamnations

Suivi des amendes et décisions



Une évidence à rappeler

Une information que vous n'avez pas/ne collectez pas/ne transmettez pas ne fait courir aucun risque à personne.

- RGPD **impose** minimisation des données (nature, volume et durée)
- Nécessité analyse fine processus consommation des données
- Anonymisation ou pseudonymisation
- Études d'impacts sur la vie privée
- RGPD **impose** signalement toute atteinte aux DCP, aux moins aux autorités (CNIL en France)

B&A CONSULTANTS SECURITE INFORMATIQUE

Attention à l'exportation de données

Y compris si faite indirectement ou implicitement.

- *Safe harbor* : invalidé en 2019 ;

Attention à l'exportation de données

Y compris si faite indirectement ou implicitement.

- *Safe harbor* : invalidé en 2019 ;
- *Privacy Shield* : invalidé en 2020 ;

Attention à l'exportation de données

Y compris si faite indirectement ou implicitement.

- *Safe harbor* : invalidé en 2019 ;
- *Privacy Shield* : invalidé en 2020 ;
- Et en février 2022...

Attention à l'exportation de données

Y compris si faite indirectement ou implicitement.

- *Safe harbor* : invalidé en 2019 ;
- *Privacy Shield* : invalidé en 2020 ;
- Et en février 2022...
- l'utilisation de Google Analytics n'est pas conforme au RGPD ;

Réflexion à tous les niveaux

- L'intégration d'un outil tiers peut provoquer une non-conformité RGPD ;
- Avec ses conséquences désagréables voire douloureuses ;
- Nous ne sommes qu'au début des ≪ découvertes juridiques ≫ dans ce domaine.

Conséquences

Développeurs, architectes, exploitants...

Partir sur bases saines de conception (obligatoire // RGPD)

- orientée confidentialité (privacy by design)
- et orientée sécurité (security by design)

Commerciaux, responsables clients, marketing...

Intégrer dans vos réflexions et projets

- l'opportunité de collecter certaines informations
- les contraintes liées aux données qui sont collectées
- les procédures d'effacement des données
- les risques et conséquences (tech, comm, légales) incidents.

Tout cela AVANT la mise en production.

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

Nous revenons de loin

Entre 2007 et 2011...

- Changements réguliers politique de vie privée de Facebook, fiasco dénoncé « the next Facebook privacy scandal »
- Eric Schmidt (PDG Google, 2009) : « Only miscreants worry about privacy » et « If you don't want it known, don't do it »
- Maximilien Schrems, 2011, relève 22 infractions majeures de Facebook à la législation irlandaise sur la protection des données personnelles
- Directive européenne et 28 pays → 28 lois avec variations

Conséquences

Nécessité de changement significatif de la législation en place pour apparition « véritables sanctions » et « une même règle pour tous »

Ceux qui vont souffrir

- Pas forcément les GAFAM
  - bien meilleure gestion des risques juridiques
  - nette avance protection données personnelles
- plutôt les entreprises européennes
  - faible culture gestion risques juridiques
  - ne comprennent pas besoin protection données personnelles
  - peu de compétences en la matière

Toutefois...

... en Europe, la situation (sensibilisation, compétences...) s'améliore très vite sous l'impulsion des organismes de contrôle.

B&A CONSULTANTS SECURITE INFORMATIQUE

Principales évolutions

- réglement et non directive européenne
- homogénéisation probable (décisions, sanctions) niveau européen
- sanctions dissuasives (2 à 4% CA mondial, 10/20 M€ pour administrations, arrêt traitement)
- conservation majorité obligations antérieures
- suppression déclaration CNIL au profit responsabilisation et autocontrôle
- nouvelles obligations de sécurité
- étude d'impact obligatoire, avant mise en œuvre, pour certains traitements (données sensibles, profilage)
- renforcement droits personnes notamment sur preuve consentement

Et aussi. . .

- co-responsabilité **automatique** sous-traitants (y compris GAFAM. . .) → contractualisation impérative
- obligations « sécurité et confidentialité par conception » (pour les données nominatives)
- portabilité données personnelles
- obligation notification violations

Plan

Registre des traitements – 1

- Tracer tous traitements de données personnelles
- Théoriquement selon taille entreprise ($\geq$ 250 personnes)
- Obligatoire prouver conformité tous traitements
- Difficile sans liste exhaustive
- Registre doit être tenu à jour

Informatique interne
- Accès salles informatiques
- Traçabilité actions
- Gestion sauvegardes
- Outils prise contrôle à distance
- Gestion activité administrateurs
- Suivi outils bureautique
- Suivi photocopies/impressions
- Paie, congés, gestion RH
- Applications installées sur postes

Intranet
- Annuaire (LDAP/AD)
- Organigramme
- Site intranet
- Enquêtes satisfaction internes
- Système surveillance/sécurité
- Journaux activité
- Vidéosurveillance
- Messagerie

Internet
- Site web
- Lettre d'information
- Espace emploi
- Réseaux sociaux
- Fora discussion

Évolution poste

Désigner un délégué à la protection des données (*data privacy officer*). Obligatoire dans secteur public, ou si traitements à grande échelle

Registre traitements – 2

Registre doit indiquer, pour chaque traitement

- nom et coordonnées responsable(s) traitement et délégué à la protection des données
- finalités traitement
- catégories personnes concernées et catégories données personnelles
- catégories destinataires données, y compris tiers, hors pays collecte ou entité internationale
- existence transferts hors pays collecte ou vers entité internationale
- délais effacement selon catégories des données (quand donnée devient-elle inutile ?)
- description générales mesures de sécurité techniques et organisationnelles

Registre sous-traitance traitements – 3

Conseillé d'avoir deux registres de traitements (si applicable) :

- traitements dont vous êtes responsable ;
- traitements réalisés pour le compte de vos clients.

Registre sous-traitance :

- contenu similaire au registre « normal » ;
- indique coordonnées client (responsable de traitement) pour lequel traitement est réalisé ;
- indique coordonnées sous-traitants éventuels.

Registre traitements – 4

Quelques liens de référence

- Registre des traitements de la CNIL 2023
- Le registre des traitements (CNIL)
- Registre simplifié (tableur)

Registre des incidents

- Gérer des DCP $\Rightarrow$ gérer des incidents
- Pas crédible de n'avoir **aucun** incident
- Possible connaître incidents sans conséquences pour propriétaires DCP
- Chaque incident **doit** être tracé, analysé, avec bilan (notification ou pas, pourquoi, mesures limitation, mesures non répétition, etc.)

Contrôle CNIL

Auditeurs demandent registre traitements **et** registre incidents.

Minimisation des données

- Uniquement données personnelles *strictement nécessaires* pour chaque traitement
- Purger/nettoyer données existantes (volume collecté et durée conservation)
- Réflexion de fond sur *tous* traitements existants
- Avec contraintes légales de conservation de certaines données

Exemple minimisation

Liste de diffusion : adresse électronique (et rien d'autre)
Départ collaborateur : garder informations légales (contrat, versements, etc.), éliminer l'inutile (dates congés pris, photo pour badges, etc.).

B&A CONSULTANTS SECURITE INFORMATIQUE

Licéité traitement et consentement

Traitement licite si au moins une condition remplie :

1. Consentement explicite, éclairé et univoque ;
2. Traitement nécessaire pour exécution contrat (ou mesures précontractuelles) auquel la personne est partie ;
3. Traitement nécessaire pour respect obligations règlementaires du responsable du traitement ;
4. Traitement nécessaire pour sauvegarde intérêts vitaux personne ou tiers ;
5. Traitement nécessaire pour exécution service intérêt public par responsable du traitement ;
6. Intérêt légitime entreprise.

B&A CONSULTANTS SECURITE INFORMATIQUE

Consentement

- Consentement explicite, éclairé et univoque
- Fournir toutes informations nécessaires pour prise décision
- Pouvoir apporter preuve consentement utilisateur

Exemples

- lettre information : consentement explicite
- paye : obligation légale (noter celle-ci)

Question en suspens

Que faire pour traitements anciens, non conformes (pas trace consentement explicite) ?

Question réglée

Fournisseur peut-il dire « faute d'acceptation de tous ces traitements, pas de service » ? Non.

Mentions légales – 1

- identité et coordonnées responsable du traitement
- coordonnées *délégué à la protection des données* s'il existe
- finalité et base juridique traitement
- destinataires données
- transfert éventuel vers pays tiers/organisation internationale

Mentions légales – 2

- durée ou critères conservation
- droit d'accès, de rectification, d'effacement
- droit de limitation ou d'opposition au traitement
- droit de retrait du consentement
- droit réclamation auprès autorité de contrôle
- indication si fourniture données est à caractère règlementaire, contractuel ou conditionne conclusion contrat
- informations sur données obligatoires ou non et conséquences non fourniture données

Portabilité données

- Pouvoir fournir à l'intéressé *toutes les données* le concernant
- Dans délais raisonnables
- Dans format structuré, couramment utilisé, lisible par une machine

Attention !

Impératif vérifier demandeur a pleine légitimité à faire la demande. Héritiers/partenaires (officiels ou non) ne sont pas légitimes sans accord explicite du propriétaire (si décédé. . . compliqué).

Sur un sujet connexe. . .

Réfléchissez (côté perso et pro) sur organisation récupération informations importantes après (votre) décès.

Obligation notification

- Dans les meilleurs délais, de préférence sous 72 heures après détection incident
- violation (accidentelle ou intentionnelle) sécurité avec perte, destruction, altération, divulgation ou accès non autorisé(s)
- notification CNIL (prioritaire) et personnes concernées (moins prioritaires, doivent être prévenues selon conséquences)
- notification doit indiquer
  - description nature violation, catégories et nombre victimes, volume données concernées
  - nom et coordonnées DPD
  - conséquences probables pour victimes
  - mesures remédiation ou atténuation mises en place
  - mesures pour prise en charge préjudice

B&A CONSULTANTS SECURITE INFORMATIQUE

Et en plus de ça

- CNIL édite des recommandations sur sujets divers ;
- Exemple : 17 octobre 2022, recommandation sur les mots de passe (y compris gestion technique, entropie, etc.)
- Pourraient être considérées comme « bonnes pratiques à suivre » même si officiellement juste informatives ;
- Genre « pourquoi n'avez-vous pas suivi la reco X ? »

Plan

Plan

Quelques autres textes applicables

- Code de la Propriété Intellectuelle (contrefaçons), qui prévoit le cas des logiciels ;
- DADVSI, Hadopi, Loppsi-1, Loppsi-2. . . ;

LPM 2023

Introduit obligation (pour éditeur) signalement ANSSI et utilisateurs lorsque vulnérabilités significatives trouvées dans logiciels.

eIDAS art. 45 et 45 bis (EU)

Impose aux navigateurs des certificats racine (AC) d'entités désignées par les États membres, même si elles ne respectent pas les règles, normes et pratiques d'AC racines.

Autres textes

Sont indirectement applicables :

- Loi de 1881 sur la presse (diffamation, incitation à la haine, apologie de crimes...) ;
- Lois et règlements sur le secret de la correspondance ;
- Lois concernant la mise en péril de mineurs (notamment exposition à des contenus pornographiques).

Les plus intéressants sont les textes et décisions touchant au secret de la correspondance et au respect de la vie privée.

Une jurisprudence mouvante

De nombreux points évoluent rapidement, dans des directions parfois contradictoires :

- En fonction du contexte
- En fonction des acteurs
- En fonction du libellé des plaintes

Exemple

Protection de la vie privée vis-à-vis du contrôle du poste de travail par l'employeur.

Bon à savoir

Ne jamais généraliser une décision de justice sans connaître le dossier.

Plan

La légitime défense

Définition générale de la légitime défense :

- Situation de défense, de réponse à une agression. Il faut donc être attaqué en premier.
- Notion de danger imminent : c'est au moment de l'attaque qu'il faut se défendre, pas après (vengeance, représailles).
- S'arrêter une fois l'attaquant neutralisé ou en fuite.
- Proportion entre les moyens de défense employés et la gravité du danger encouru.

Existe-t-il une légitime défense en informatique ?

Réponse courte : non.
Quelques raisons :

- Analyse de l'attaque : on n'est plus dans l'imminence, c'est de la vengeance ou des représailles.
- Aucune certitude que l'attaquant "visible" est le véritable attaquant (mascarade IP, prise de contrôle. . .).
- Aucun signal indiscutable permettant de décider que l'attaquant est en fuite.

En bref

Ces idées sont à éviter absolument !

Cela ne signifie pas qu'on laisse tout faire.

B&A CONSULTANTS SECURITE INFORMATIQUE

Les défenses automatiques

Des outils automatiques de détection/réaction peuvent apporter une aide significative mais ils doivent être (très) bien configurés et utilisés.

- Ils peuvent se retourner (ou être retournés) contre le défenseur.
- Leur pertinence et intérêt doivent être analysés de manière fine et intelligente.
- Il est indispensable de suivre et d'analyser leurs actions.

Plan

La vie privée et l'entreprise

- Attente logique d'un respect de la vie privée des collaborateurs ;
- Tolérance institutionnalisée (en France) d'un empiètement de la vie privée dans la vie professionnelle (appels privés, mails privés...) ;
- Tout est question de dosage et de contexte ;
- L'entreprise peut surveiller, mais doit informer les représentants du personnel et ses collaborateurs (mais voir transparent 58) ;
- Les collaborateurs doivent loyauté à leur employeur.

Une fois cela dit

Tout est possible selon les situations.

Tout est dans le contexte

Legalis.net propose sur son site l'intégralité de l'arrêt du 8 décembre 2009 **qui a cassé les jugements précédents. La Cour de cassation, considérant que la Cour d'Appel n'a pas recherché** *"... comme elle y était pourtant invitée, dans quelle mesure cette utilisation personnelle de l'ordinateur professionnel avait nui à la bonne qualité de la prestation de travail de Monsieur X...."* **a dit que** *"...la seule conservation sur son poste informatique de trois fichiers contenant des photos à caractère pornographique sans caractère délictueux ne constituait pas, en l'absence de constatation d'un usage abusif affectant son travail, un manquement du salarié aux obligations résultant de son contrat susceptible de justifier son licenciement ".*

Traduction : *"... un fait relevant de la vie privée peut être sanctionné si l'employeur prouve la répercussion sur l'exécution du contrat de travail. Le régime est donc extensif, mais il faut prouver ".* ***Actualités du droit***.

Les notes de service et chartes informatiques pèsent le même poids que le règlement intérieur : significatif pour des mesures disciplinaires, insuffisant pour des sanctions fortes.

B&A CONSULTANTS SECURITE INFORMATIQUE

Utilisation preuve « illicite »

Les lignes ont bougé fin 2021.

Arrêt 6 décembre 2021, chambre sociale Cour Cassation

L'illicéité d'un moyen de preuve n'entraîne pas nécessairement son rejet des débats. Le juge doit apprécier si l'utilisation de cette preuve a porté atteinte au caractère équitable de la procédure dans son ensemble, en mettant en balance le droit au respect de la vie personnelle du salarié et le droit à la preuve. Ce dernier peut justifier la production d'éléments portant atteinte à la vie personnelle d'un salarié à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit strictement proportionnée au but poursuivi.

En bref...

Le contenu de votre mur privé Facebook peut être retenu contre vous, selon ce que vous y racontez sur votre employeur.

Entreprise et vie privée

Situation générale

L'ordinateur mis à disposition par l'entreprise est à but professionnel. Tout ce qu'il contient est réputé professionnel, sauf mention explicite contraire.

Pour simplifier un peu :

- L'employeur peut, à volonté, examiner le disque dur d'un poste de travail (ou la messagerie, etc.)
- Les zones ou éléments marqués comme privés peuvent être lus, mais uniquement après information du collaborateur

Entreprise et vie privée

- En cas de suspicion, invoquer la protection de la vie privée ne permet pas d'empêcher l'accès aux données.
- Mais il faut absolument que ce soit encadré juridiquement pour l'employeur.

Détail intéressant

Une clé USB personnelle connectée à un ordinateur professionnel peut être examinée par l'employeur (sauf mention explicite sur la clé comme quoi elle est personnelle).

Et demain ?

Utilisation de plus en plus fréquente de matériel personnel (tablette, téléphone portable) pour travailler (BYOD)...

Zones personnelles sur poste de travail

Il existe donc un droit de regard volumétrique des espaces personnels sur le poste professionnel, mais pas de droit d'examen détaillé en dehors de l'information/présence/accord du salarié.

L'employeur peut

- Demander la suppression (tolérance zéro) de données classifiées comme personnelles,
- ou empêcher leur sauvegarde,
- voire les supprimer d'autorité.

Par contre, il ne peut pas...

... lire le contenu de ces zones (sauf nécessité technique impérieuse) sauf en présence du salarié, qui peut se faire assister (procédure formelle de contrôle).

Chiffrement sur poste de travail

Deux possibilités clairement disjointes :

1. Données personnelles chiffrées : contraintes liées aux données privées s'appliquent. Peut être demandé leur déchiffrement (dans le cadre des procédures appropriées), mais pas le mot de passe de déchiffrement.
2. Données professionnelles chiffrées : l'entreprise peut exiger de disposer du mot de passe de déchiffrement (pas toujours malin, mais...) ou mettre en place des méthodes d'accès supplémentaires.

Posez-vous la question

Le chiffrement de données professionnelles sur le poste de travail signifie que le collaborateur ne veut pas que ses collègues voient ces données...
Il ne s'agit pas d'une protection contre le vol de l'ordinateur.

La surveillance des activités

La surveillance est un élément légitime et nécessaire dans toute entreprise. Toutefois,

- Le contenu des informations collectées, le but de la surveillance, les modalités d'accès aux informations doivent être clairs.
- Surveiller n'est pas intercepter (art. 432-9 CP).
- La durée d'archivage et les procédures de destruction doivent être définies.

Et surtout...

La surveillance ne peut se faire à l'insu des collaborateurs (information, CE, syndicats ou représentants du personnel, etc.) ou envers une personne spécifique.

La surveillance des activités

La surveillance concerne aussi des applications (fonctionnement, requêtes émises ou reçues, journal d'activité...).

Attention CNIL

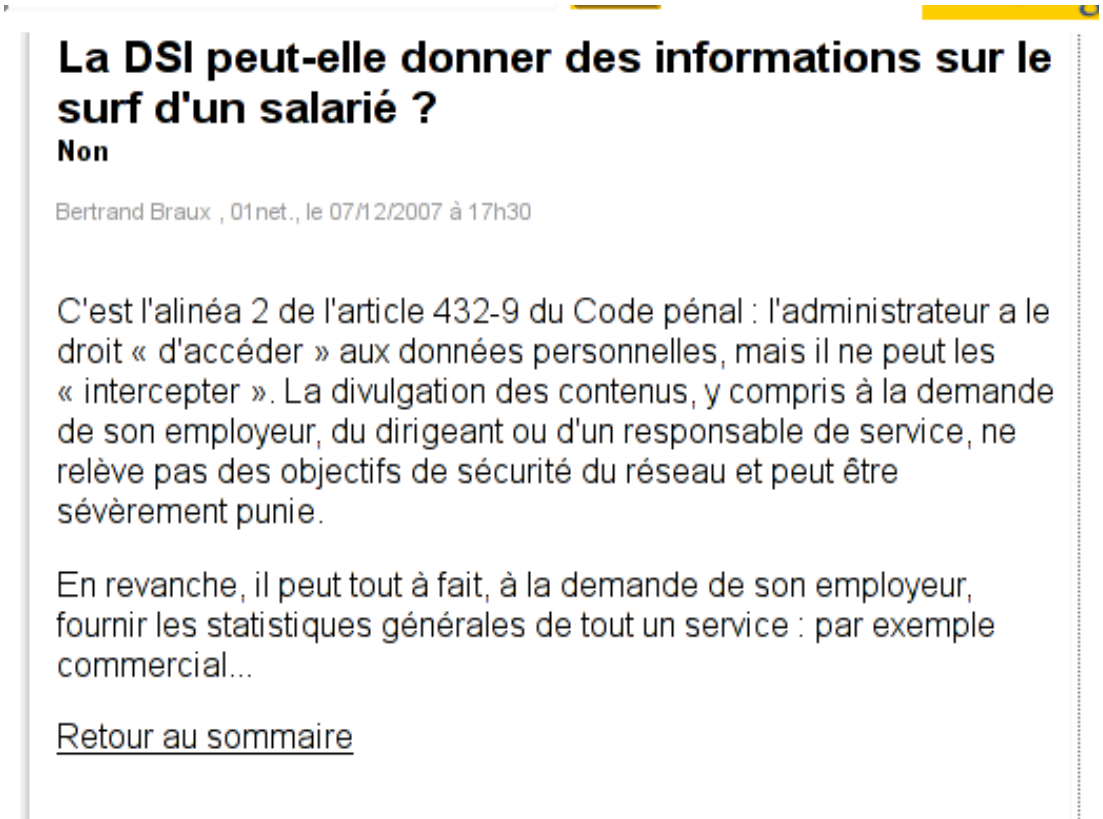
- S'il est possible de remonter à une personne à partir de ces données : cache de navigation avec authentification, journal des requêtes SQL avec id de la connexion...
- Aux traitements automatisés des traces d'activités.

Durée d'archivage préconisée : 1 an.

Attention

Les journaux ou bases de données stockant ces informations doivent être protégés de manière particulièrement soigneuse (accès ou modifications illégitimes).

Une question fréquente



La DSI peut-elle donner des informations sur le surf d'un salarié ?

Non

Bertrand Braux , 01net., le 07/12/2007 à 17h30

C'est l'alinéa 2 de l'article 432-9 du Code pénal : l'administrateur a le droit « d'accéder » aux données personnelles, mais il ne peut les « intercepter ». La divulgation des contenus, y compris à la demande de son employeur, du dirigeant ou d'un responsable de service, ne relève pas des objectifs de sécurité du réseau et peut être sévèrement punie.

En revanche, il peut tout à fait, à la demande de son employeur, fournir les statistiques générales de tout un service : par exemple commercial...

Retour au sommaire

http ://www.01net.com/editorial/366219/la-dsi-peut-elle-donner-des-informations-sur-le-surf-d-un-salarie-./

B&A CONSULTANTS SECURITE INFORMATIQUE