université de BORDEAUX

La protection des données à caractère personnel et la sécurité des données

François Pellegrini
Professeur, Université de Bordeaux
francois.pellegrini@u-bordeaux.fr

La CNIL (1)

- « Commission nationale de l'informatique et des libertés »
  - Autorité administrative indépendante
  - Créée par la loi n° 78-17 « informatique & libertés » du 6 janvier 1978
  - Chargée de l’application de cette loi
    - Et du RGPD et de quelques autres...

La CNIL (2)

- Article 1er de la loi « I&L » :

  « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* [...] »

La CNIL (3)

- Missions de la CNIL :
  - Autoriser / rendre des avis
  - Contrôler
    - Possibilité de contrôles en ligne
  - Sanctionner
    - Tribunal administratif spécialisé interne : la « formation restreinte »
  - Conseiller

Art. 4.1 du RGPD

- « Données à caractère personnel » :

  « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; 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 ; »

Art. 32 du RGPD (1)

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [.../...]

Art. 32 du RGPD (2)

« a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. […/…]

Art. 32 du RGPD (3)

« 2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. […/…]

Art. 32 du RGPD (4)

« 4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre. »

Art. 32 du RGPD (5)

- Les manquements aux obligations de sécurité des données peuvent être lourdement sanctionnés
  - Jusqu'à 10 M€ d'amende administrative ou 2 % du CA mondial

La CNIL et la sécurité (1)

- Le RGPD responsabilise (et donc éventuellement sanctionne) le responsable de traitement
  - Y compris si l'origine du trouble est le sous-traitant
- D'autres textes de loi ont pour rôle de sanctionner les attaquants
  - Loi « Godfrain » du 5 janvier 1988

La CNIL et la sécurité (2)

- L’art. 32 RGPD n’impose pas une obligation de résultat
  - Obligation de moyens renforcée
- L’art. 32 RGPD ne sanctionne pas l’erreur en tant que telle
  - Sanction de la négligence
    - Dans la conception
    - Dans la mise en œuvre

La CNIL et l'ANSSI (1)

- La CNIL s'occupe exclusivement de données à caractère personnel
- L'ANSSI s'occupe exclusivement de sécurité des systèmes d'information
  - Notamment des OIV et OSE
  - Pas de pouvoir de sanction
    - Possibilité de sanctionner les opérateurs prévue par la directive (UE) 2022/2555 « NIS 2 »

La CNIL et l'ANSSI (2)

- Collaboration approfondie entre les deux entités sur les sujets de sécurité
  - Partage de réflexions et d'analyses
  - Publications croisées
    - Guide ANSSI d'hygiène informatique
    - Guide CNIL sur la sécurité des données à caractère personnel

L’état de l’art (1)

- Les rapporteurs et la formation restreinte évaluent les actions des responsables de traitement à l’aune de l’« état de l’art »
  - Informations répandues et facilement accessibles à la personne de l’art
  - Pratiques recommandées dans les secteurs concernés

L’état de l’art (2)

- Exemples de ressources témoignant de l’état de l’art :
  - OWASP « Top-10 » des failles de sécurité des services web
  - Recommandations de l’ANSSI, de la CNIL et sectorielles
    - Guides et informations publiques
  - Magazines et sites web « IT »

L’état de l’art (3)

- Exemples de pratiques techniques non conformes :
  - Stockage en clair des mots de passe
    - Réutilisation et bourrage d’identifiants (« *credential stuffing* »)
  - Absence de filtrage des champs de formulaires web
    - Injection SQL

L'état de l'art (4)

- Usage du HTTP et non du HTTPS
  - Interception des transactions et des identifiants de connexion
  - Mais le HTTPS ne protège pas en cas d'usage d'un réseau de distribution de contenu (CDN) !
    - L'opérateur du CDN voit le trafic en clair
    - Nécessité d'un chiffrement applicatif de bout en bout
- Absence d'authentification de session
  - Réutilisation d'URL par des tiers
- Identifiants et/ou numéros d'items séquentiels dans les URL
  - Accès aux données de tiers

L’état de l’art (5)

- Mots de passe par défaut non changés
  - Intrusion dans divers systèmes
- Codes d’accès aux serveurs de production « en dur » dans le code source
  - Exfiltration de données suite à l’attaque du dépôt de code source

L’état de l’art (6)

- Exemples de pratiques organisationnelles non conformes (absence de PSSI) :
  - Absence d’audits de sécurité réguliers
    - Persistance d’erreurs de configuration
  - Absence de mise à jour régulière des paquetages logiciels
    - Exposition à des vulnérabilités connues voire déjà exploitées

En pratique (1)

- Les éléments de sécurité sont examinés lors de chacun des contrôles effectués
  - Niveau d’investigation adapté à la spécificité du cas considéré

En pratique (2)

- En 2022 :
  - 8 / 21 sanctions comprenant un manquement relatif à la sécurité
    - Voir : https://www.cnil.fr/les-sanctions-prononcees-par-la-cnil
  - 72 mises en demeure comprenant un manquement relatif à la sécurité
    - + 240 % par rapport à 2021
      - Mise en place de tests automatisés

Conclusion

- La sécurité des données à caractère personnel doit être prise au sérieux
  - Dommages potentiellement irrémédiables pour les personnes concernées
  - Risque financier et réputationnel conséquent pour les organisations
- La PSSI est ton amie...