



efrei

PARIS PANTHÉON-ASSAS UNIVERSITÉ

AUDIT ET GESTION DES RISQUES - NORMES ISO

Richard SANGARÉ

CISO

Expert Judiciaire auprès de la Cour d'Appel de Rouen

Réserviste Opérationnel à la Gendarmerie

PLAN DE COURS AUDIT S.I ET AUDIT CYBER

- Introduction à l’Audit de Système d’Information (SI)
- Normes et Référentiels d’Audit de SI
- Méthodologie de l’Audit de SI
- Introduction à l’Audit de Cybersécurité
- Normes et Référentiels pour la Cybersécurité
- Méthodologie de l’Audit de Cybersécurité
- Outils d’Audit de SI et Cybersécurité
- Exemples de Rapport d’Audit et Recommandations
- Bonnes Pratiques et Pièges à Éviter

PLAN DE COURS NORME ISO

- Introduction aux Normes ISO
- ISO 27001 : Système de Management de la Sécurité de l'Information (SMSI)
- ISO 27002 : Code de Bonnes Pratiques pour la Sécurité de l'Information
- ISO 27005 : Gestion des Risques en Cybersécurité
- Autres Normes ISO Pertinentes pour la Cybersécurité
- Implémentation des Normes ISO en Entreprise
- Étude de Cas et Retour d'Expérience
- Conclusion et Discussion

MODULE 1

Audit S.i et audit cyber

Audit S.I et audit cyber

Objectifs du Cours

- Comprendre les principes d'un audit de SI et de cybersécurité
- Identifier les étapes clés de l'audit
- Analyser les meilleures pratiques et les référentiels utilisés
- Appliquer les concepts de manière pratique

Audit S.i et audit cyber

Introduction à l'Audit de Système d'Information (SI)

- **Définition et importance de l'audit SI**

L'audit des systèmes d'information (SI) est un processus d'évaluation systématique des ressources informatiques, des processus, et des infrastructures d'une organisation pour vérifier leur conformité, leur efficacité, et leur sécurité. Il permet d'identifier les failles et les risques potentiels, d'évaluer la performance des systèmes, et de garantir qu'ils répondent aux objectifs et aux exigences réglementaires de l'organisation.

- **Objectifs principaux : conformité, sécurité, efficacité**
- **Différence entre audit interne et externe**

Audit S.i et audit cyber

Normes et Référentiels d'Audit de SI

- ISO 27001 : Système de gestion de la sécurité de l'information
- COBIT : Gouvernance et management des SI
- ITIL : Gestion des services informatiques
- Importance de la conformité réglementaire (ex. : RGPD, PCI-DSS)

Audit S.i et audit cyber

Méthodologie de l'Audit de SI

- Étapes : Planification, Collecte de données, Évaluation, Conclusion
- Identification des objectifs et périmètre de l'audit
- Techniques de collecte : entretiens, observation, revue documentaire

Audit S.i et audit cyber

Introduction à l'Audit de Cybersécurité

- Définition et rôle de l'audit de cybersécurité
- Objectifs : identifier les vulnérabilités, évaluer les contrôles de sécurité, conformité
- Différence entre audit de cybersécurité et tests de pénétration

Audit S.I et audit cyber

Normes et Référentiels pour la Cybersécurité

- ISO 27005 : Gestion des risques liés à la sécurité de l'information
- NIST Cybersecurity Framework : Identification, Protection, Détection, Réponse, Récupération
- Autres standards : CIS Controls, OWASP (sécurité des applications web)

Audit S.I et audit cyber

Méthodologie de l'Audit de Cybersécurité

- Évaluation des risques et menaces
- Analyse des vulnérabilités et des contrôles de sécurité existants
- Techniques de vérification : scan de vulnérabilités, revue des configurations, tests d'intrusion

Audit S.I et audit cyber

Outils d'Audit de SI et Cybersécurité

- Outils de scan de vulnérabilités : Nessus, Qualys
- Outils de gestion des risques : RiskWatch, MEGA
- Outils de monitoring et détection : SIEM (ex : Splunk, ArcSight)

Audit S.I et audit cyber

Exemples de Rapport d'Audit et Recommandations

- Structure d'un rapport : résumé exécutif, constatations, analyse des risques, recommandations
- Recommandations type : durcissement des configurations, gestion des accès, sensibilisation

Audit S.I et audit cyber

Bonnes Pratiques et Pièges à Éviter

- Éviter les biais dans l'évaluation des risques
- Documenter rigoureusement les constatations
- Prioriser les recommandations en fonction de l'impact et des risques

Audit S.I et audit cyber

Conclusion et Questions

- Synthèse des points clés abordés
- Importance de l'audit régulier pour la sécurité et la conformité
- Questions et échanges

MODULE 2

Norme iso

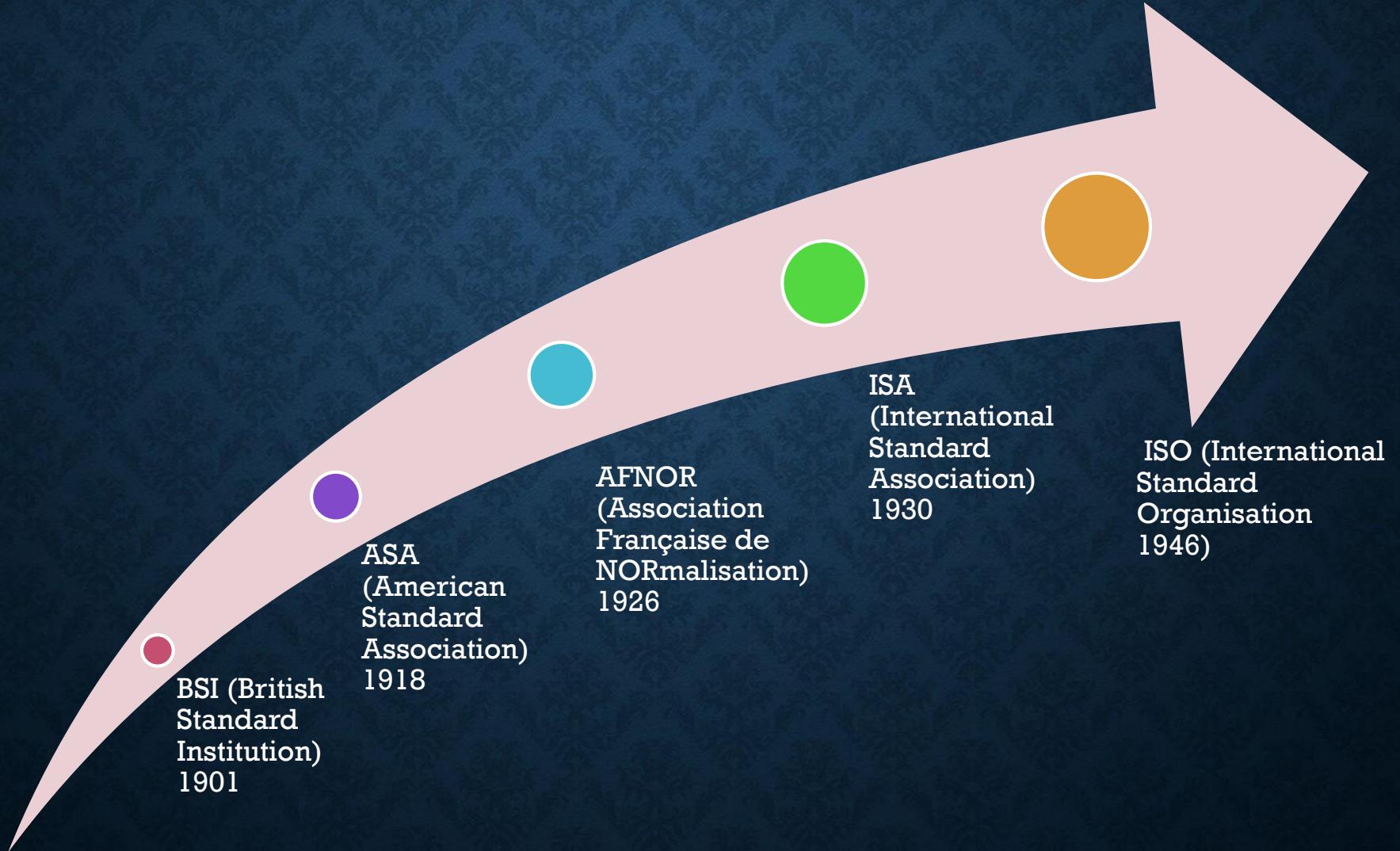
Norme ISO

Objectifs du Cours

- Comprendre le rôle des normes ISO dans la cybersécurité
- Présentation des normes clés : ISO 27001, ISO 27002, ISO 27005, etc.
- Apprendre à implémenter et auditer ces normes en entreprise

Norme ISO

Un peu d'histoire





International Standard Organisation

Les missions:

- Elaboration des normes applicables;
- Promotion du développement de la standardisation et activités annexes,
- Développement des coopération dans les sphères des différents activités

A ce jour, face à la mondialisation des échanges, à l'évolution des besoins métiers et à la diversification des menaces, l'ISO demeure un des organismes de normalisation les plus avancés dans le domaine de la sécurité de l'information.

Norme ISO



La famille ISO2700x pour la sécurité de l'information

Norme ISO

Quelques conventions:

La dénomination officielle des normes est du type « *ISO/IEC numéro de la norme : année de dernière version* »

ISO/IEC (*Commission Electrotechnique Internationale*)
Exemple: ISO/IEC 27001:2005

On adoptera une appellation plus commune: « ISO 27001 » et pour généraliser « ISO 2700x »

Norme ISO

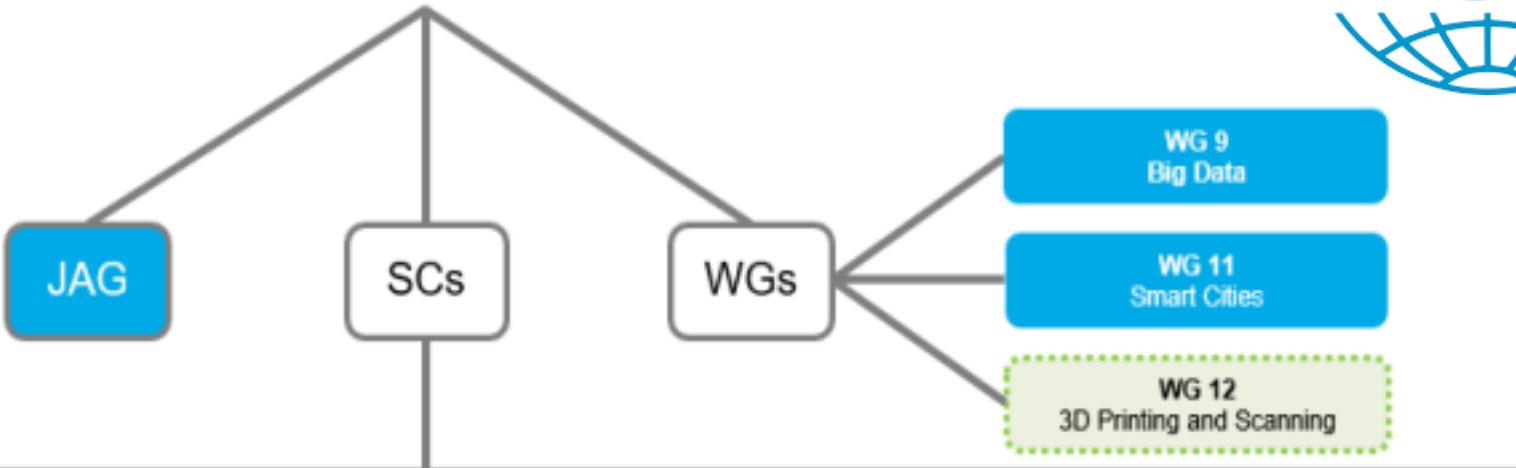
Où est la sécurité de l'information ?

JTC 1 (Joint Technical Committee): Instance traitant spécifiquement le domaine des TI (Technologie de l'Information).

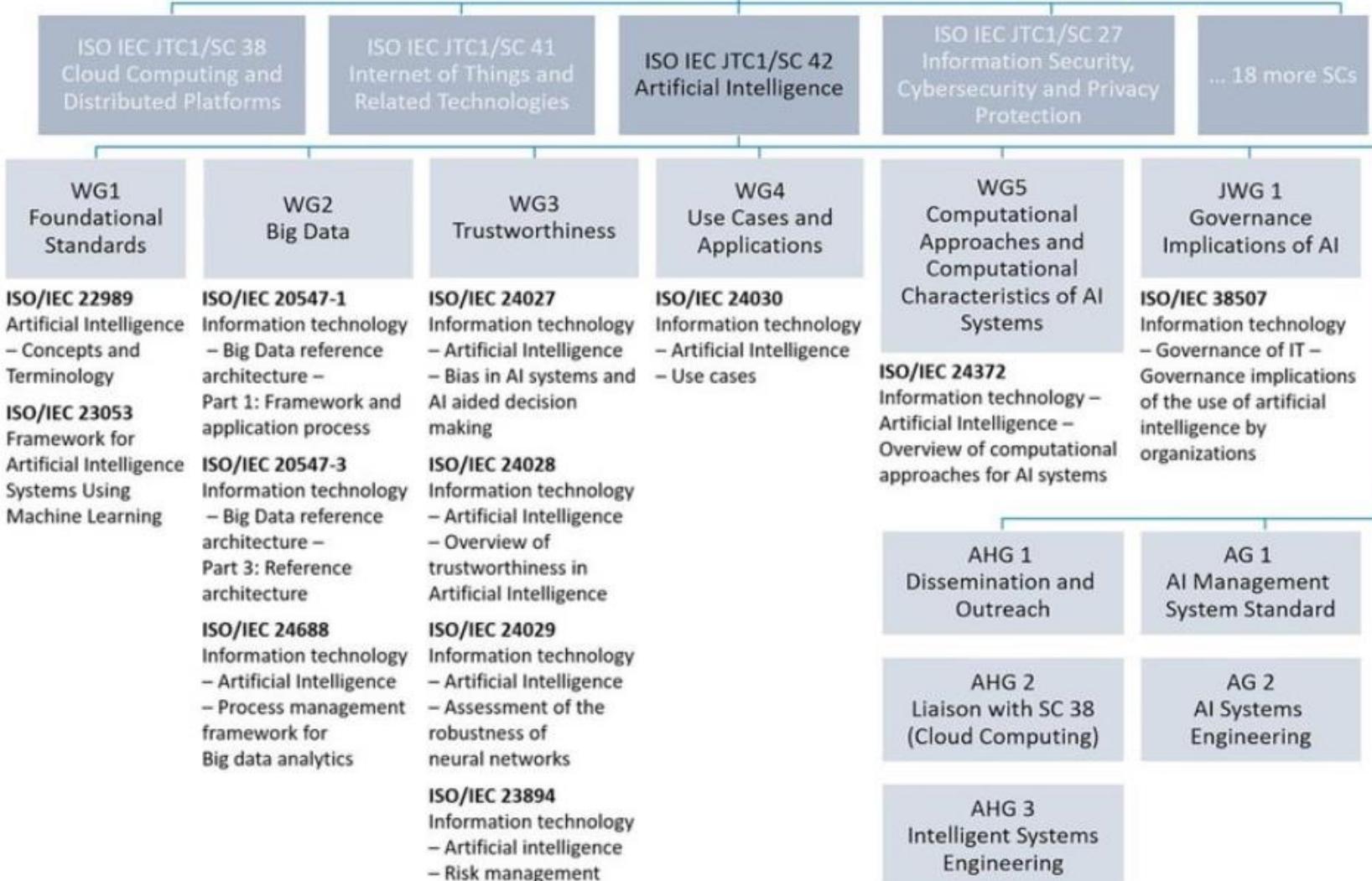
JTC 1 est, à ce jour, subdivisé en 22 Sous comités (SC2 à SC42) et 19 groupes de travail :
- Liste <https://www.iso.org/fr/committee/45020.html>

JTC1/SC27, traite « IT Security Techniques » et est composé de 10 groupes de travail :
- Liste <https://www.iso.org/fr/committee/45306.html>

- Newly created (JTC 1 plenary meeting – October 2017)
- Luxembourg's current involvement
- Not involved



SC 2 Coded Character Sets	SC 6 Telecommunications and information exchange between systems	SC 7 Software and Systems Engineering	SC17 Cards & Personal Identification	SC 22 Programming Languages	SC 23 Digitally recorded media for information interchange and storage	SC 24 Computer graphics, image processing, and environmental data representation	SC 25 Interconnection of information technology equipment	SC 27 IT security techniques	SC 28 Office equipment	SC 29 Coding of audio, picture, multimedia and hypermedia information	
SC 31 Automatic identification and data capture techniques	SC 32 Data management and interchange	SC 34 Document description and processing languages	SC 35 User interfaces	SC 36 Information technology for learning, education and training	SC 37 Biometrics	SC 38 Cloud Computing and Distributed Platforms	SC 39 Sustainability for and by information technology	SC 40 IT Service Management and IT Governance	SC 41 Internet of Things and related technologies	SC 42 Artificial Intelligence	



JTC	Joint Technical Committee
SCS	Subcommittee
WG	Working Group
JWG	Joint Working Group
AHG	Ad Hoc Group
AG	Advisory Group

Norme ISO ISO 27001 : Système de Management de la Sécurité de l'Information (SMSI)

- Objectif : établir, mettre en œuvre, entretenir et améliorer un SMSI
- Principes clés : approche basée sur le risque, amélioration continue
- Exigences pour la certification ISO 27001

Norme ISO

SMSI



ISO 27001 est:

Une norme correspond à la révision de la norme BS7799-2. Elle a été publiée en octobre 2005 puis révisée en 2013 (ISO/IEC 27001:2013) avec 2 rectificatifs techniques, 2014 et 2015.

Destinée à tout type de société.

Elle a pour but de décrire un objectif à atteindre et non la manière concrète d'y arriver, Est à la base de la certification d'un SMSI (System Management Security Of Information) à l'instar de ces homologues ISO 9001 pour la qualité et ISO 14001 pour l'environnement.

Une norme élaborée pour fournir un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SMSI.

<https://www.iso.org/fr/standard/54534.html>

Norme ISO

ISO27001



Norme ISO ISO 27002 : Code de Bonnes Pratiques pour la Sécurité de l'Information

- Lien avec ISO 27001 (support des contrôles de sécurité)
- Structure : 14 domaines de contrôle, y compris la gestion des actifs, le contrôle des accès, la sécurité physique
- Utilisation pratique pour établir des politiques de sécurité

Norme ISO ISO 27005 : Gestion des Risques en Cybersécurité

- Objectif : fournir une méthodologie pour évaluer et traiter les risques de sécurité
- Processus : identification des actifs, évaluation des menaces, des vulnérabilités et de l'impact
- Importance dans l'élaboration d'une stratégie de cybersécurité efficace

Norme ISO

ISO 27005



		Vraisemblance				
		Négligeable	Peu probable	Possible	Probable	Très probable
Conséquence	Critique		R2			
	Majeure		R6			
	Modérée	R8		R3		
	Mineure			R1		
	Insignifiante		R4 R5	R7		

		Gravité				
Probabilité		Mineure	Significative	Sévère	Critique	Catastrophique
	Fréquent	A				
	Probable	B				
	Peu probable	C				
	Rare	D				
	Extrêmement rare	E				

Risque inacceptable, mesures indispensables de réduction du risque

Risque à surveiller, mesures adaptées de réduction du risque

Risque acceptable

ISO 27005 :

- Utilisable de manière autonome,
- Pour entreprise soumise à de fréquents changements,
- Méthodologies d'analyse de risque conforme à l'ISO 27005 (MEHARI, EBIOS RM, ...)



ISO 27006 & ISO 27007 :

- ISO 27006 a pour but de fournir les prérequis pour les organismes d'audit et de certification afin de les guider sur les exigences nécessaires à atteindre pour être accrédités en tant qu'organisme de certification d'un SMSI.
- ISO 27007 propose les lignes directrices composant un guide spécifique pour les audits des SMSI, notamment en support à l'ISO 27006.

Norme ISO

Autres Normes ISO Pertinentes pour la Cybersécurité

- ISO 27701 : Protection des données personnelles (extension de la norme ISO 27001 pour le RGPD)
- ISO 22301 : Continuité d'activité, minimisation des impacts des incidents
- ISO 31000 : Gestion des risques (approche générique de la gestion des risques)

Norme ISO

Implémentation des Normes ISO en Entreprise

- Étapes : analyse de l'existant, définition des politiques, formation, documentation
- Exigences pour l'adhésion aux bonnes pratiques (documentation, contrôle, évaluation continue)
- Processus de certification : audit interne, audit externe

Norme ISO

Étude de Cas et Retour d'Expérience

- Exemples d'implémentation réussie de l'ISO 27001 dans les grandes entreprises
- Bénéfices constatés : réduction des incidents de sécurité, conformité accrue, protection de la réputation
- Challenges courants : gestion des coûts, complexité de la documentation, implication des équipes

Norme ISO

Conclusion et Discussion

- Résumé des normes ISO principales en cybersécurité et leurs apports
- Importance de la culture de sécurité et de la conformité
- Questions et échanges pour approfondir

MODULE 3

Cyber en France

Audit et Norme ISO



L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 2009.

Ce service à compétence nationale est rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information, créée par décret en juillet 2001 .

<https://www.ssi.gouv.fr/>

Audit et Norme ISO



Mission de l'ANSSI:

« L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information.

À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.

Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. »

L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des **opérateurs d'importance vitale (OIV)**.

<https://www.ssi.gouv.fr/agence/missions/ledito-du-dg/>

Audit et Norme ISO



La Loi de Programmation militaire (LPM):

Promulguée le 18 décembre 2013, la loi de programmation militaire fait suite aux orientations fixées par le Livre blanc sur la défense et la sécurité nationale 2013.

Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale et confère à l'ANSSI de nouvelles prérogatives :

l'agence, au nom du Premier Ministre pourra imposer aux OIV (opérateurs d'importance vitale) des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques.

De plus, l'article 22 rend obligatoire la déclaration des incidents constatés par les OIV sur leurs systèmes d'information.

La protection physique des points d'importance vitale (PIV) vis-à-vis des actes de sabotage

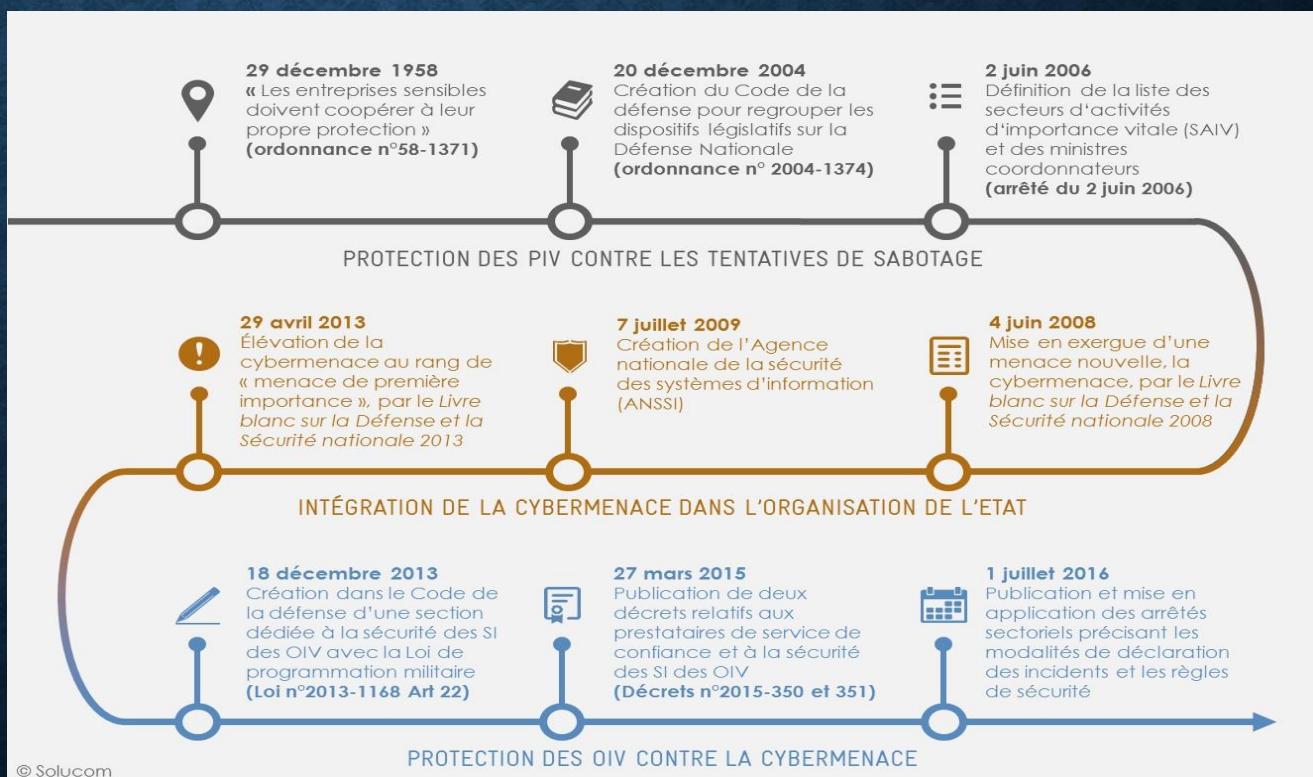
<https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/>

Audit et Norme ISO



Plusieurs exigences sont imposées :

respect de règles de sécurité spécifiques, recours à du matériel et des prestataires qualifiés pour la détection des événements de sécurité, notification obligatoire des incidents de sécurité, contrôles de sécurité réguliers commandités par l'ANSSI. Les sanctions pénales applicables aux OIV lorsqu'ils ne satisfont pas aux obligations prévues s'élèvent à 150 000 € pour le dirigeant de l'OIV et à 750 000 € pour la personne morale.





Audit et Norme ISO

La directive européenne Network and Information System Security (NIS v2):



Audit et Norme ISO – NIS2



Audit et Norme ISO – NIS1 vs NISv2

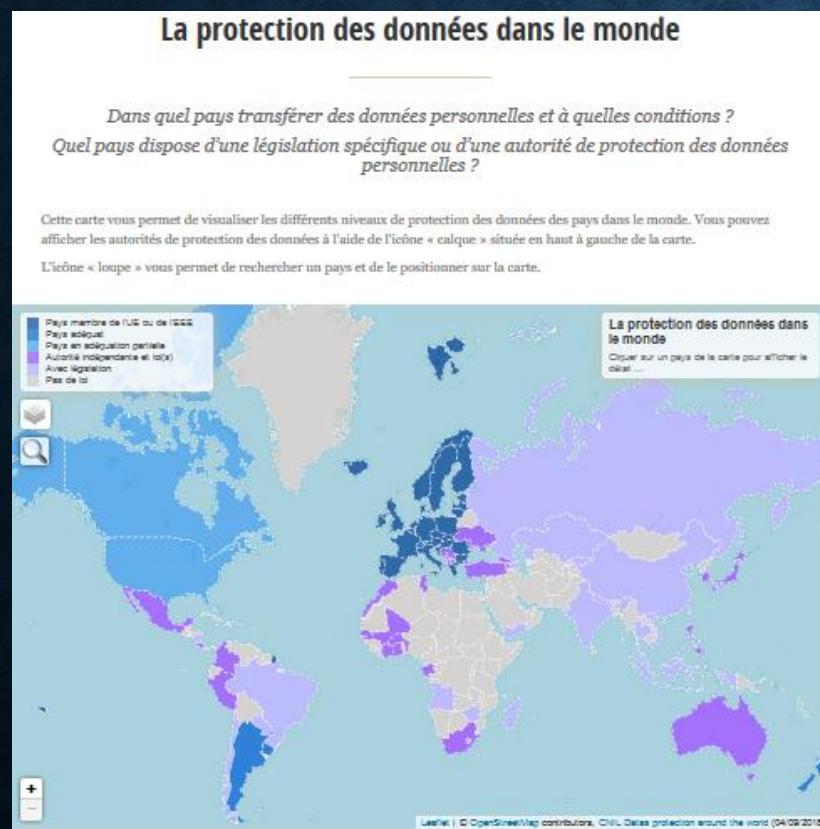
Secteurs hautement critiques		Autres secteurs critiques	
	Banque		Santé
	Infrastructure numériques et gestion des services TIC		Transports
	Eau potable		Gestion des eaux usées
	Énergie		Administration publique
	Infrastructures des marchés bancaires et financiers		Espace
Périmètre NIS1		Périmètre étendu NIS2	
	Fournisseurs numériques		Gestion des déchets
	Production, transformation et distribution des denrées alimentaires		Recherche
	Fabrication, production et distribution de produits chimiques		
	Fabrication		
	Services postaux et d'expédition		

Audit et Norme ISO

La Commission nationale de l'informatique et des libertés (CNIL) de France est une autorité administrative indépendante française.

La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Elle exerce ses missions conformément à la loi no 78-17 du 6 janvier 1978 modifiée le 6 août 2004.



Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Le GDPR pour « General Data Protection Regulation » ou règlement général sur la protection des données (personnelles) est le dernier règlement européen devant entrer en vigueur en mai 2018.

Le dispositif prévoit notamment des obligations renforcées de protection des données détenues , des dispositifs relatifs à l'expression du consentement de la collecte et le développement de la notion de portabilité.

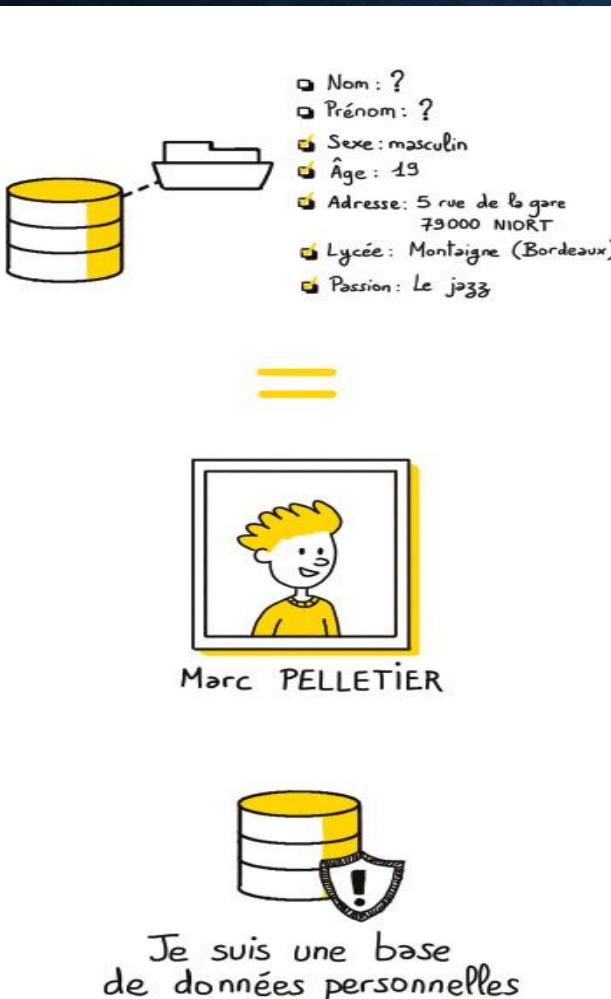
L'objectif est de responsabiliser les divers acteurs du marché afin qu'ils soient en mesure de démontrer à **la Commission Nationale de l'Informatique et des Libertés** qu'ils respectent leurs obligations en matière de protection des données à caractère personnel. Le RGPD renforce également les pouvoirs de sanction des autorités de contrôle.



Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Qu'est-ce qu'une donnée personnelle ?



La notion de « données personnelles » est à comprendre de façon très large

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

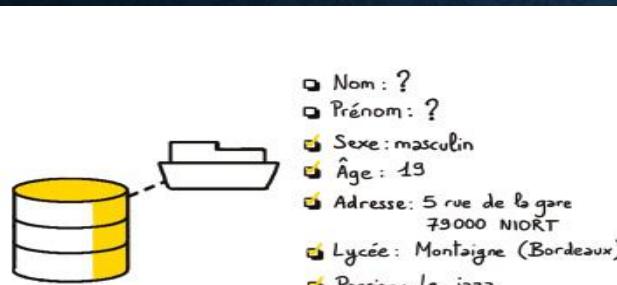
Une personne peut être identifiée :

- **directement** (exemple : nom, prénom)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Qu'est-ce qu'une donnée personnelle ?



=



L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : numéro de sécurité sociale, ADN)
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Qu'est-ce qu'un traitement de données personnelles ?

Cette notion est également très large.

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Exemple : tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.



Je m'assure que
les données collectées
servent bien l'objectif prévu

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

1 – Désigner un pilote: nomination d'un chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données.

2- Cartographier: commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3- Prioriser: Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4- Gérer les risques: Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD)

5- Organiser: Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

6- Documenter: Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminiés et actualisés régulièrement pour assurer une protection des données en continu.

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et règlementation

0.

Lancer un nouveau traitement

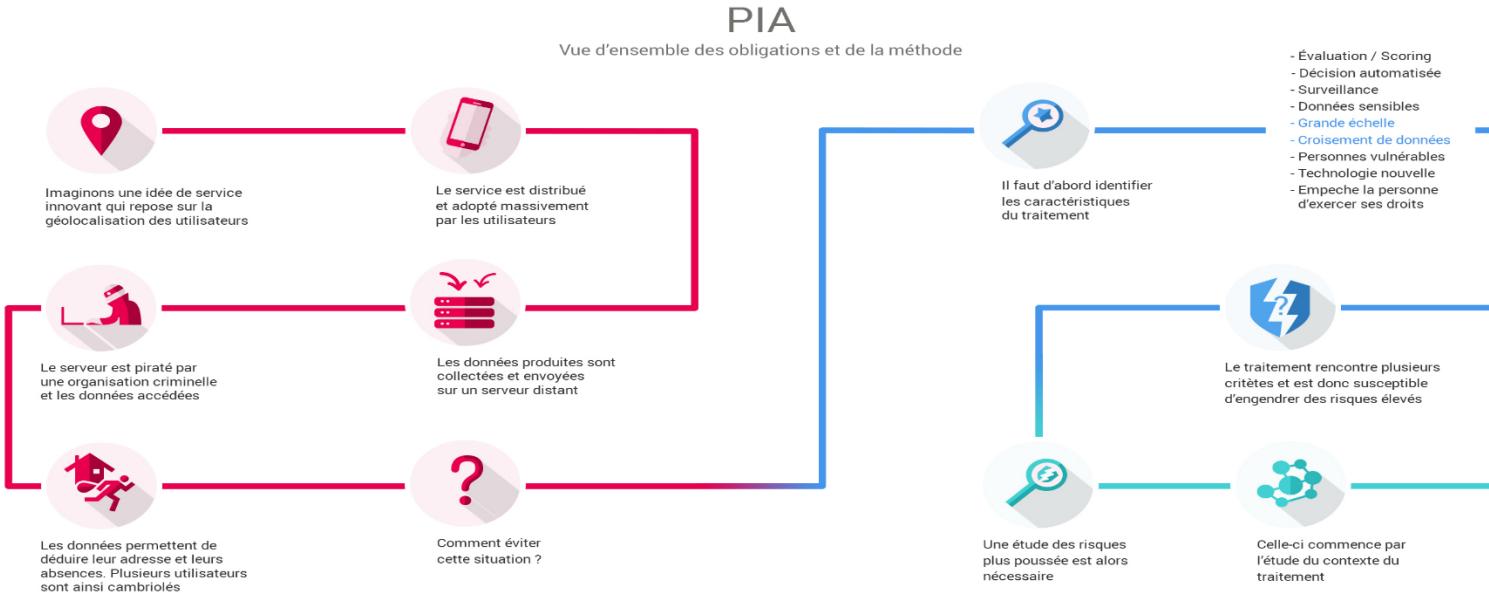
De nombreux services sont créés tous les jours dans le monde du numérique.

Qu'ils répondent aux besoins internes d'organismes ou à ceux de leurs clients, ces services reposent pour la grande majorité sur des traitements de données à caractère personnel.

Adressés à des groupes d'utilisateurs définis, ils collectent ces données à la volée lors de leur usage.

Stockées sur des serveurs, les données collectées sont vulnérables à différents risques : l'accès illégitime, la modification non désirée et la disparition.

Ces risques sont susceptibles d'avoir un impact important sur la vie privée des utilisateurs concernés.



1.

Qualifier le traitement

Ces risques sont indésirables, aussi bien pour le responsable de traitement que pour les utilisateurs du service.

Ainsi, avant de lancer un traitement, il est important d'en faire une première analyse afin d'en déterminer les risques qu'il est susceptible d'engendrer.

Plusieurs facteurs influencent la dangerosité d'un traitement comme par exemple le type de données traité.

En général, si deux des critères listés sont rencontrés, le traitement comporte probablement des risques importants sur la vie privée. Dans ce cas de figure, il est approprié de mener une « analyse d'impact relative à la protection des données ».

2.

Apprécier les risques vie privée

L'analyse établit tout d'abord le contexte dans lequel évolue le traitement, en posant, entre autre, les bases de son rôle et de son fonctionnement.

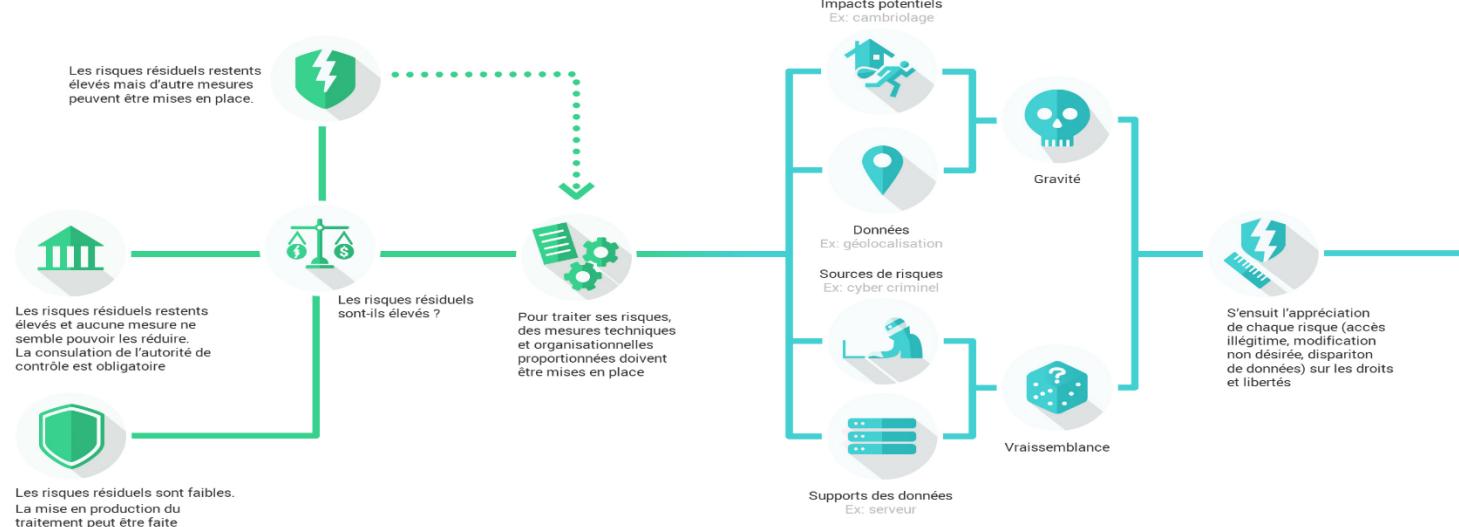
En complément de l'étude juridique consistant à évaluer la nécessité et la proportionnalité du traitement, il est nécessaire d'analyser chaque risque et d'estimer sa vraisemblance et sa gravité selon les impacts potentiels sur les droits et libertés, les données traitées, les sources de risques, et les vulnérabilités des supports de données.

Traiter les risques

Une fois les risques identifiés, des mesures techniques et organisationnelles doivent être déterminées jusqu'à ce que les risques soient réduits à un niveau acceptable.

Si ça ne semble pas possible avec les moyens envisagés, l'autorité de contrôle doit être consultée.

Dans tous les cas, les mesures devront être appliquées avant la mise en œuvre du traitement.



Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Avant les amendes, les avertissements.

La CNIL dispose de différents moyens pour contraindre les entreprises à se conformer au RGPD. Elle peut ainsi :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement de données ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

L'entreprise persiste ? Elle risque jusqu'à 20 millions d'euros...

Les amendes administratives que les agents de la CNIL pourront infliger aux entreprises contrevenantes sont particulièrement lourdes et dissuasives. En fonction de **la durée, la nature et la gravité de la violation**, elles pourront ainsi **s'élever jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros** (contre 3 millions d'euros précédemment). Des montants très importants de nature à affaiblir, voire à porter un coup fatal à l'activité d'une entreprise.

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Données personnelles : les plaintes à la Cnil ont augmenté de 34%

A LA UNE / EU OUEST ÉCO / RÉSEAUX SOCIAUX / Publié le 23/11/2018 à 10h04 par SudOuestFr avec AFP.

S'ABONNER À PARTIR DE 1€     2 COMMENTAIRES



▲ 9 700 plaintes ont été déposées depuis le début de l'année, soit 34% de plus que l'an dernier à la même époque. ©AFP

La Cnil a reçu 1 000 notifications de violations de données en 2018, "soit environ sept par jour depuis le 25 mai" et l'entrée en vigueur du règlement européen sur la protection des données (RGPD).



TOUTE L'ACTUALITÉ / SÉCURITÉ / DONNÉES PERSONNELLES

1e alerte d'amende RGPD pour Microsoft aux Pays-Bas

Maryse Gros, publié le 20 Novembre 2018

Sanction RGPD : premier dégât à 250 000€ pour Optical Center

Par Eléonore Lefaix

Le 16 juin 2018

0

À peine deux semaines après l'entrée en vigueur du Règlement Général sur la Protection des Données, un premier cas de sanction a été relevé en France. La CNIL a ainsi dressé une amende de 250 000€ à Optical Center, qui a laissé fuiter les données personnelles de ses clients.

C'est une faille de sécurité qui date de 2017. À cette époque, la CNIL a été informée d'une « fuite de données conséquentes », certains internautes ayant pu accéder à des centaines de factures d'autres clients, à leurs données de santé et à leurs numéros de sécurité sociale.



Au total, plus de 3 millions de documents confidentiels téléchargeables depuis le site d'Optical Center. L'entreprise avait réagi en expliquant « qu'effectivement le site web ne vérifiait pas que les clients étaient connectés à leur compte client avant d'afficher les factures. »

RGPD : le réseau social allemand Knuddels.de condamné à payer une amende de 20 000 €

Pour avoir stocké des mots de passe en clair

Le 23 novembre 2018, par Stéphane le calme, Chroniqueur Actualités



Le réseau social allemand Knuddels.de va devoir payer une amende de 20 000 euros, car il stockait des mots de passe non chiffrés. Ainsi, la société de Karlsruhe a violé l'obligation de garantir la sécurité des données à caractère personnel, a informé le commissaire à la protection des données du Bade-Wurtemberg, Stefan Brink, jeudi à Stuttgart.

Il a expliqué qu'après avoir été victime d'une attaque, la société s'était adressée à la DPA pour tenir informés immédiatement les autorités ainsi que les utilisateurs. Selon la société, environ 808 000 adresses de courrier électronique et 1 872 000 pseudonymes et mots de passe ont été volés par des inconnus et publiés sur Internet.

En plus des pseudonymes utilisés pour accéder à la plateforme, les pirates ont également rendu publics les mots de passe associés, les adresse mail ainsi que des informations sur le prénom ou le lieu de résidence. Les utilisateurs de la plateforme ont donc été invités à changer leur mot de passe, pour ceux qui sont concernés et ne l'avaient pas encore fait. Une nécessité pour ceux qui utilisent le même mot de passe ou une variante similaire sur d'autres sites Web.

Ces données ont été publiées en septembre 2018.



Le Sénat américain pense à un RGPD made in US dès 2019

Par Alexandre Boero 
Le 29 novembre 2018



Un projet de loi sur la régulation stricte de la vie privée, équivalent du RGPD européen, pourrait arriver au début de l'année 2019 aux États-Unis. Les discussions sont engagées.

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Article 32

EU RGPD

"Sécurité du traitement"

=> Raison: 83, 74, 75, 76, 77

=> administrative fine: Art. 83 (4) lit a

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 traiter les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le **chiffrement** des données à caractère personnel;

=> Article: 4

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés et;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assu

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 l'autorisation de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles

=> Raison: 75

3. L'application d'un code de conduite approuvé comme le prévoit l'[article 40](#) ou d'un mécanisme de certification approuvé comme le prévoit les dispositions prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorisation ou la direction du responsable du traitement, et qui a accès aux données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le c



La pseudonymisation et le **chiffrement** des données à caractère personnel

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Article 32 EU RGPD "Sécurité du traitement"

=> Raison: 83, 74, 75, 76, 77
=> administrative fine: Art. 83 (4) lit a

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 des droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles nécessaires, y compris entre autres, selon les besoins:

a) la pseudonymisation et le **chiffrement** des données à caractère personnel;

=> Article 4

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés et;

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.

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 données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles

Article 34 EU RGPD "Communication à la personne concernée d'une violation de données à caractère personnel"

=> Raison: 75, 86, 87, 88
=> administrative fine: Art. 83 (4) lit a

Une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique; le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

=> Article 75

La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

Le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation de données à caractère personnel, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le **chiffrement**.

Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus ou ne l'est plus ou ne l'est plus susceptible de se matérialiser, ce qui exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout au moins générale.

Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir déterminé si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 1 n'est pas remplie.



... en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès telles que le **chiffrement**

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation



Le National Institute of Standards and Technology, ou NIST (qu'on pourrait traduire par « Institut national des normes et de la technologie »), est une agence du département du Commerce des États-Unis qui publie des standards ouverts d'interopérabilité appelés FIPS.

(Federal Information Processing Standard) Standard de traitement de données fédéral.

Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.

Cette agence a pris la suite en 1988 du National Bureau of Standards fondé en 1901 avec substantiellement les mêmes missions.

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation



Le « Clarifying Lawful Overseas Use of Data » Act ou CLOUD Act (H.R. 4943) est une loi fédérale des États-Unis adoptée en 2018 sur la surveillance des données personnelles, notamment dans le Cloud.

Elle modifie principalement le Stored Communications Act (en) (SCA) de 1986 en permettant aux forces de l'ordre (fédérales ou locales, y compris municipales) de contraindre les fournisseurs de services américains, par mandat ou assignation, à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers.

Critiquée par certaines associations de défense de la vie privée, cette loi permet notamment aux forces de l'ordre américaines d'obtenir les données personnelles d'un individu sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit.

Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation



Le US PATRIOT Act (acronyme traduisible en français par : « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ») est une loi antiterroriste qui a été votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001.

L'un des axes centraux de ce long texte (132 pages) est d'effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur et les agences fédérales responsables des enquêtes criminelles (FBI) dès lors qu'elles impliquent des terroristes étrangers.

Elle crée aussi les statuts de combattant ennemi et combattant illégal, qui permettent au gouvernement des États-Unis de détenir sans limite et sans inculpation toute personne soupçonnée de projet terroriste.

Dans la pratique, cet Act of Congress autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable et sans en informer les utilisateurs.



Module 2, Management de la Cyber Sécurité

Normes, standards, directive et réglementation

Cloud Act vs Patriot Act:

La grande différence entre ces deux lois est leur champ d'application et les acteurs pouvant accéder aux données.

Le Patriot Act permet aux agences gouvernementales américaines (FBI, CIA, NSA, armée) d'obtenir des informations dans le cadre d'une enquête relative à des actes de terrorisme ou d'espionnage industriel.

Le Cloud Act, lui, permet aux autorités américaines qui bénéficient d'un mandat d'obtenir des informations dans le cadre d'une enquête judiciaire

Ainsi, « le Cloud Act est de l'ordre du judiciaire quand le Patriot Act est de l'ordre du renseignement dans un cadre limité.



FIN

