NOTE STRATÉGIQUE N° 2

LA CYBERSÉCURITÉ ET LE CADRE EUROPÉEN DE PROTECTION DES DONNÉES

Le défi : plusieurs sources de conflit entre protection des données et sécurité

Souvent, les incidents de cybersécurité entraînent la perte, la compromission ou la divulgation non autorisée de données à caractère personnel d'individus.

Les incidents peuvent couvrir un très large spectre, y compris, le piratage informatique, le chantage au cryptage de données et le vol de données ou d'identité.

Nombre d'acteurs différents peuvent causer des incidents de cybersécurité pour diverses raisons.

Ces événements ont des effets variables, souvent imprévisibles, qui peuvent sérieusement entraver la disponibilité, l'intégrité et la confidentialité des technologies numériques.

La cybersécurité et la protection des données créent de nombreux défis et conflits

- Les entreprises axées sur la récolte et l'utilisation des données ne veulent pas investir dans la sécurité et la protection des données
- Les citoyens ne veulent pas de compromis entre protection de la vie privée et sécurité
- Protection contre l'atteinte à la vie privée en tant que droit constitutionnel
- Risque d'utilisation abusive
- Caractère intrusif des outils de sécurité nuisant au respect de la vie privée
- Technologies qui évolue rapidement
- Dépendance croissante vis-à-vis de systèmes informatiques vulnérables
- De nombreuses mesures de cybersécurité reposent sur la surveillance
- Mesures offensives susceptibles d'affaiblir la sécurité de tous
- « Course aux armements » des stratégies offensives
- Les exploits informatiques « d'accès légal » peuvent représenter une faille exploitable pour des parties malveillantes

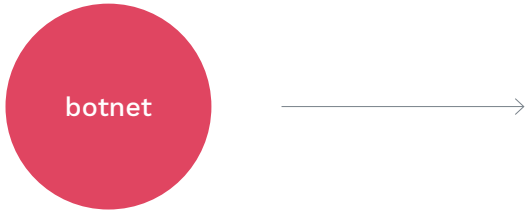
- Conditions de concurrence complexes pour les acteurs, manque de transparence
- Conditions d'encadrement juridique et factuel souvent obscures
- Identification difficile des intervenants pour les incidents de cybersécurité
- Impact variable et imprévisible des incidents
- La cybersécurité est un problème mondial très complexe
- Manque généralisé de sécurité de base, qui devient plus urgent avec la montée en puissance de l'IdO
- Manque de soutien aux PME, par exemple par des financements et des programmes de formation pour une meilleure sécurité informatique

- Manque généralisé de sécurité de base, qui devient plus urgent avec la montée en puissance de l'IdO
- Manque de soutien aux PME, par exemple par des financements et des programmes de formation pour une meilleure sécurité informatique

Le manque d’efficacité de la cybersécurité affecte presque tout le monde

Le fameux botnet « Mirai » est un exemple typique d’incident de cybersécurité touchant une large frange de la population mondiale.

À l’origine, de jeunes étudiants cherchaient simplement à tricher dans un jeu en ligne en concevant le botnet Mirai pour créer une panne sur le serveur du jeu. Cependant, le botnet a fini par échapper à leur contrôle. Les appareils infectés étaient alors intégrés au botnet, puis contrôlés à distance pour lancer des attaques de réseau à grande échelle. En octobre 2016, le logiciel malveillant avait presque complètement détruit le réseau Internet de tout l’est des États-Unis.



Les botnets sont des appareils infectés, tels qu’un ordinateur ou un appareil IdO (Internet des objets), contrôlés par une partie malveillante. IdO est le terme utilisé pour décrire les appareils électroniques connectés capables d’échanger des données, p. ex. par Internet. Il peut s’agir de routeurs Internet, de caméras, de télévisions ou d’enregistreurs vidéo numériques.

L’importance du nouveau cadre européen de protection des données

En Europe, la protection des données à caractère personnel des citoyens est réglementée par le **règlement général sur la protection des données (RGPD)** et la **directive 2016/680** (pour les secteurs de la police et de la justice).

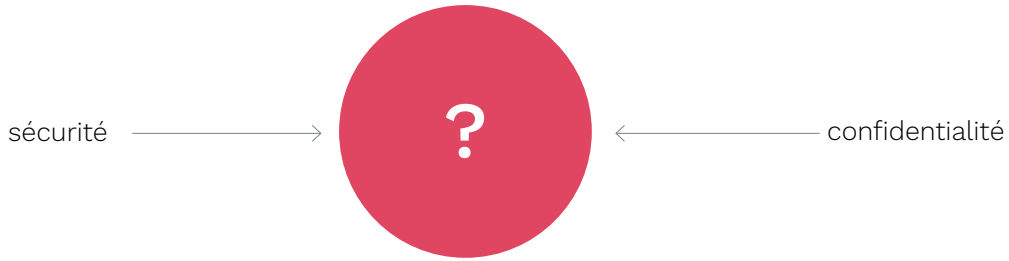
Le processus législatif qui permettrait l’application d’un règlement sur la confidentialité et la protection des données aux communications électroniques n’a toujours pas été mené à bien (**règlement « vie privée et communications électroniques »**).

Trouver un compromis entre sécurité et protection des données est difficile

Chacun sait que certaines mesures visant à améliorer la cybersécurité peuvent aller à l'encontre des droits fondamentaux des individus, notamment en ce qui concerne le droit au respect de la vie privée et à la protection des données à caractère personnel.

Exemple 1
Une entreprise privée souhaite protéger ses secrets commerciaux et déploie donc des mesures de sécurité internes, tel qu'un contrôle rigoureux de l'accès. Toutefois, ces mesures privent la personne concernée par ces données de ses droits, même valides, comme le droit à une information transparente et à l'accès aux informations.

Exemple 2
Les agences d'application de la loi et de renseignements s'appuient souvent dans leurs travaux sur des technologies de sécurité axées sur la surveillance, et demandent parfois plus de pouvoirs dans ce domaine. Cependant, nombre de ces technologies – telles que l'inspection approfondie des paquets, ou l'accumulation et l'utilisation de vulnérabilités de sécurité dans les logiciels – peuvent affaiblir la sécurité et la confidentialité de tout le monde.



Les technologies de sécurité axées sur la surveillance peuvent s’avérer dangereuses

La lutte contre la criminalité peut-elle justifier les moyens employés, c.-à-d. sacrifier la sécurité des appareils techniques en général et pour tout le monde ?

L’utilisation de la technologie pour infiltrer les appareils et les communications des citoyens en vue de retrouver des criminels a été maintes fois critiquée en raison du **risque important d’utilisation abusive, de partialité et de manque de transparence qu’elle présente.**

Les chercheurs en sécurité nous ont mis en garde contre les **effets secondaires indésirables** de telles mesures : p. ex. les outils de surveillance pourraient tomber entre les mains de criminels, ou des acteurs malveillants pourraient utiliser les mêmes vulnérabilités logicielles que les autorités d’application de la loi.

Affaiblir la sécurité est-il le meilleur moyen d'assurer la sécurité ?

En 2011, le Chaos Computer Club (CCC) allemand a découvert un programme malveillant (« Bundestrojaner », traduit par « Cheval de Troie fédéral » ou « Cheval de Troie d'État »), qui surveillait des appareils ciblés, permettant ainsi leur **contrôle clandestin à distance**.

La révélation de l'utilisation de ce logiciel malveillant a déclenché des critiques concernant l'affaiblissement de la sécurité des appareils ciblés. En effet, l'on craignait que **si les forces de l'ordre pouvaient utiliser de telles fonctionnalités, les criminels et les États autoritaires le pourraient aussi**. Cette révélation a suscité un vaste débat public sur la légalité de l'utilisation de telles technologies dans des sociétés démocratiques.

Les citoyens ne veulent pas être constamment surveillés

La technologie devrait-elle aider à ce que des individus soient la cible d'activités de la police en leur attribuant un **risque de criminalité plus élevé sur la base d'hypothèses** ?

Qu'advient-il de la transparence, des limites et des principes de freins et contrepoids efficaces lorsqu'une personne est **constamment surveillée en raison de facteurs circonstanciels, personnels ou comportementaux peu nombreux, incertains ou choisis de manière sélective**, tels que le fait d'être pauvre, de vivre dans le mauvais quartier ou d'avoir une couleur de peau différente ?

Équité, État de droit et respect de la légalité

L'intrusion à grande échelle de la surveillance de l'État peut nuire à la protection de la vie privée et aux autres droits fondamentaux et principes démocratiques.

Une telle intrusion met en péril les principes démocratiques tels que la présomption d'innocence et le dogme « pas de sanctions sans loi ».

Le principe de proportionnalité pose un problème de taille, outre la question générale de savoir si une surveillance étendue d'une grande partie des citoyens devrait être autorisée ou non dans une société démocratique.

Dans le secteur privé, l'économie l'emporte sur la sécurité et la protection des données

La sécurité et la protection des données peuvent représenter un obstacle aux intérêts économiques d'une entreprise, notamment lorsque son activité est axée sur les données.

Dans le monde des affaires, peu d'entreprises déploient suffisamment d'efforts en faveur de la cybersécurité et de la protection des données en raison des **coûts liés** à la mise en place et au maintien d'une sécurité informatique efficace ainsi que de procédures de gestion de la protection des données.

Afin de réaliser des économies, on confie souvent les questions de protection des données aux experts internes de la sécurité informatique. Toutefois, cette approche est **contreproductive**, car la sécurité informatique et la protection des données comportent généralement **des perspectives, des objectifs et des exigences d'expertise bien différents**.

Le manque d’investissement affecte également les infrastructures critiques

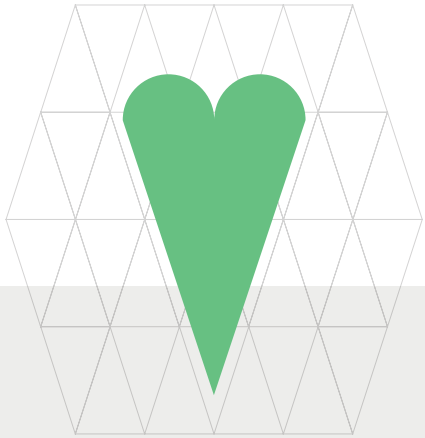
Les coûts liés au déploiement de mesures techniques et organisationnelles sont souvent jugés trop élevés, y compris dans les domaines où les responsables du traitement des données traitent des informations personnelles sensibles, telles que les données de santé.

Les établissements de santé publique sont classés parmi les infrastructures critiques d’un pays.

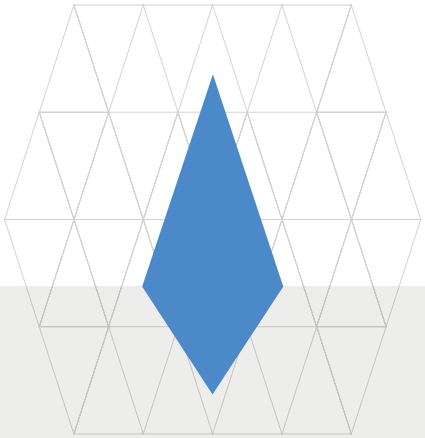
Pourtant, nombre de cabinets médicaux, hôpitaux et établissements de recherche médicale **ne disposent pas des financements et de l’expertise nécessaires pour appliquer de manière exhaustive les mesures adéquates** afin d’empêcher, par exemple, l’infection d’appareils médicaux par des virus ou la perte et la compromission de données de santé.

Les citoyens de l'UE veulent tout : sécurité, confidentialité et protection des données !

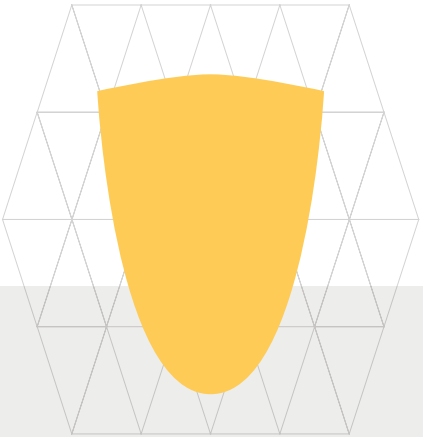
Diverses études et activités de recherche menées dans l'UE ont démontré que les citoyens européens souhaitaient une approche holistique de la sécurité et de la protection des données.



Dans le **domaine de la santé**, les citoyens semblent être particulièrement sensibles au traitement des données relatives à leur santé. Leur consentement et leur confiance dépendront de la personne avec qui ils partagent leurs données et du contexte de cet échange.



Dans le **domaine du commerce**, les citoyens s'inquiètent également des atteintes à la vie privée et de la sécurité informatique, notamment lors de l'utilisation de services sur Internet tels que les magasins en ligne. Ils ne sont pas convaincus que les sociétés privées traiteront leurs données à caractère personnel de manière responsable.



Dans le **secteur de la police et de la sécurité nationale**, les citoyens trouvent les mesures de sécurité nationale plus acceptables s'ils envisagent l'État comme un gardien plutôt que comme un intrus ; cette perception dépend souvent de leur expérience et de l'histoire de leur pays.

La responsabilité des personnes responsables du traitement des données est essentielle

En vertu du RGPD, les responsables et les sous-traitants du traitement des données à caractère personnel ont l'obligation légale de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de protéger ces données. Dans certains cas, une analyse d'impact relative à la protection des données doit d'abord être réalisée.

Les mesures à déployer dépendent du cas, de la situation et de l'état de l'art dans des domaines spécifiques. Des synergies entre les solutions de cybersécurité et de protection des données existent et doivent être mises à profit.

Exemples de mesures techniques et organisationnelles

- Contrôle de l’accès
- Chiffrement
- Séparation des données
- Anonymisation
- Pseudonymisation
- Historique des activités de traitement
- Procédures de sauvegarde et de restauration
- Entrée en communication avec le système
- Procédures de notification prédéfinies en cas de violation des données.

Le RGPD comme la directive 2016/680 prévoient des obligations spécifiques en matière de sécurité des systèmes et services informatiques en ce qui concerne leur

- confidentialité,
- intégrité,
- disponibilité,
- et résilience
- dans le contexte du traitement de données à caractère personnel.

Les procédures de gestion efficaces et la garantie du respect de la vie privée dès la conception peuvent aider

Les responsables et les sous-traitants du traitement des données doivent mettre en œuvre des mesures raisonnables pour démontrer la conformité avec le RGPD.

Il est conseillé aux responsables du traitement des données de **mettre en place un service efficace de gestion de la protection des données** au sein de leur propre organisation, qui doit être **distinct** du service de sécurité informatique, **mais travailler étroitement avec ce dernier**.

En outre, **les contrôles de sécurité annuels, les audits et la mise en œuvre des meilleures pratiques** dans le domaine de la sécurité contribuent tant à la cyber-sécurité qu'à la protection des données. Ces mesures peuvent s'agir de tests de pénétration ou de suivi des incidents de sécurité.

En résumé : application des approches axées sur les valeurs et interdisciplinaires

- Reconnaître **la transparence, la confiance, les freins et les contrepoids** comme étant des enjeux clés pour créer une cybersécurité axée sur les valeurs.
- Prendre en considération ces **valeurs** dans le processus législatif du **futur règlement « vie privée et communications électroniques »**.
- Les mesures, les technologieset les scénarios d'application en matière de sécurité, devraient faire l'objet d'une **analyse d'impact relative à la protection des données**.
- **Abandonner** l'optique selon laquelle il faut trouver un compromis entre sécurité et confidentialité.
- Chercher plutôt à trouver un **équilibre subtil** avec des compromis équitables et légitimes entre sécurité, confidentialité, protection des données et respect des droits fondamentaux.
- **Mettre à profit les synergies** entre les approches et mesures relatives à la cybersécurité et à la protection des données.
- **Renforcer** les obligations et la responsabilité des responsables et sous-traitants du traitement.
- **Soutenir** les recherches interdisciplinaires.

Où trouver de plus amples informations

Les diapositives sont fondées sur les travaux de recherche menés par le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs).

L'objectif du projet CANVAS est de réunir les parties prenantes des domaines clés de la stratégie numérique pour l'Europe afin de relever le défi consistant à définir les modalités d'alignement de la cybersécurité sur les valeurs européennes et les droits fondamentaux.

CANVAS fournit notamment les ressources suivantes :

- Documents d'information
- Programme de référence du projet CANVAS
- CANVAS MOOC
- Livre en libre accès
  « L'éthique de la cybersécurité »

La diapositive suivante présente nos livres blancs abordant les détails des défis de la cybersécurité.

Bibliographie : les défis de la cybersécurité (livres blancs de CANVAS)

Défis éthiques

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan et Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” Document universitaire SSRN No 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Défis juridiques

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle et Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” Document universitaire SSRN No 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Défis technologiques

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter et Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” Document universitaire SSRN No 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Informations sur le projet

Coordination du projet et contact :
PD Dr. sc. ETH Markus Christen
Université de Zurich (UZH),
Digital Society Initiative
Rämistrasse 66, 8001 Zurich

Version du document visuel :
Version 2.0 octobre 2019

Durée du projet :
sept. 2016 – oct. 2019

Partenaires :
Le consortium CANVAS comprend 11 partenaires (9 établissements universitaires et 2 partenaires extérieurs au monde universitaire) répartis dans 7 pays européens.

Financement :
1,57 million d'euros, dont 1 million financé par la Commission européenne, la partie restante provenant du Secrétariat d'État suisse à la formation, à la recherche et à l'innovation.

Avis de financement pour CANVAS

Cofinancé par le programme Horizon 2020
de l'Union européenne

Le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs) a bénéficié d'un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de la convention de subvention n° 700540. Ce travail a été financé (en partie) par le Secrétariat d'État suisse à la formation, à la recherche et à l'innovation (SEFRI) sous le numéro de contrat 16.0052-1. Les opinions exprimées et les arguments employés dans le présent document ne reflètent pas nécessairement les points de vue officiels de l'UE et du gouvernement suisse.