NOTE STRATÉGIQUE N° 3

TOUS LES DROITS FONDAMENTAUX SONT PERTINENTS POUR LA CYBERSÉCURITÉ

Réglementation de la cybersécurité dans l'Union européenne

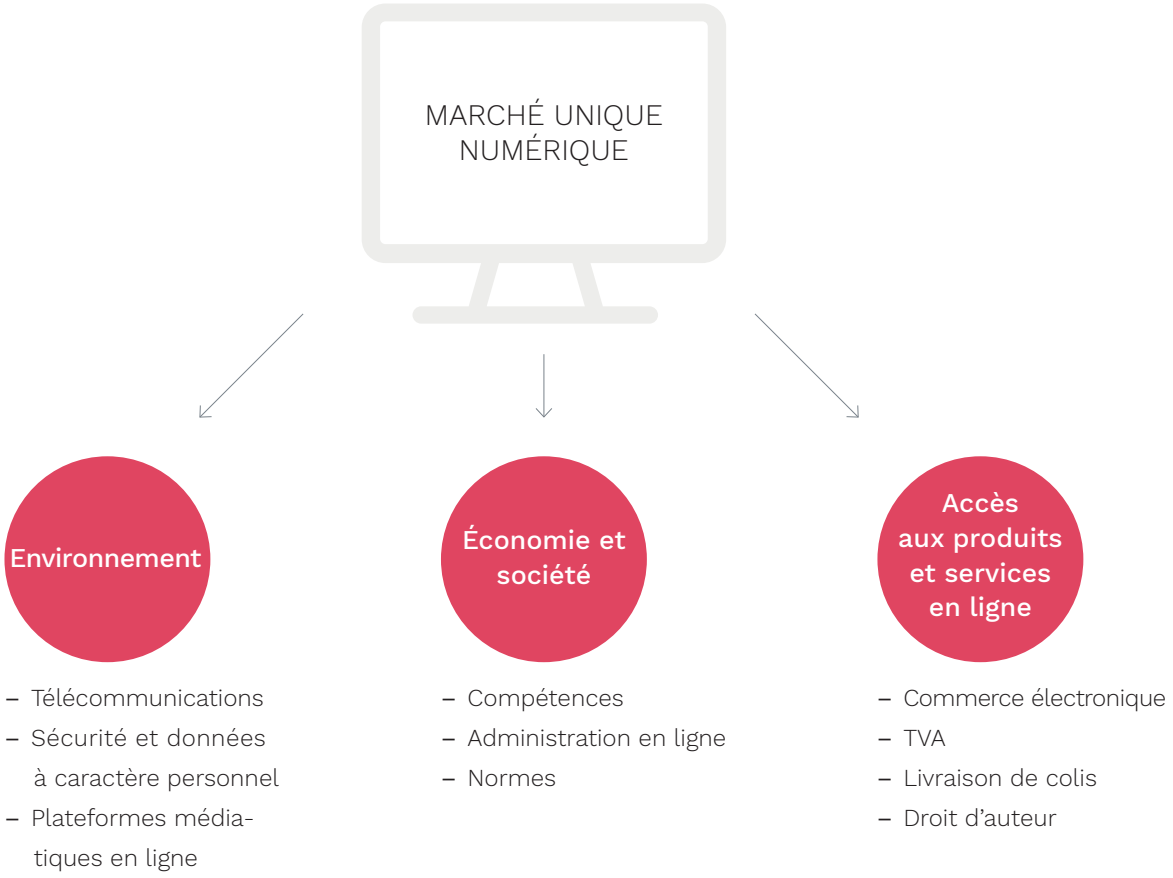
Pour saisir l'importance des droits fondamentaux dans le domaine de la cybersécurité de l'Union européenne (UE), les informations de référence suivantes doivent être considérées :

1. L'UE peut réglementer sur les questions de cybersécurité uniquement dans les **limites des compétences législatives de l'Union.**
2. Cependant, les compétences de réglementation de l'UE dans le domaine de la cybersécurité ne sont pas clairement définies.
3. Par ailleurs, les décideurs politiques européens ne peuvent pas éviter les débats sur la cybersécurité alors que la **vie quotidienne et économique des citoyens dépend de plus en plus des technologies numériques** et que ces derniers courent le **risque d'être exposés à de graves cyberincidents.**
4. Il s'agit d'un **domaine politique émergent et complexe** concerné par le fonctionnement harmonieux du marché unique numérique.

L’UE s’efforce de garantir un environnement numérique équitable, ouvert et sécurisé

Des documents politiques ainsi que des mesures législatives de l’UE pertinents pour la cybersécurité se retrouvent dans des cadres traitant :

1. de la sécurité des réseaux et de l’information
2. des communications électroniques (y compris les questions relatives à la confidentialité et à la protection des données)
3. de la cybercriminalité
4. de la cyberdéfense



Garantir la protection des droits fondamentaux

L'économie numérique de l'UE pourrait progresser jusqu'à représenter 4 % du PIB de l'Union, à condition de profiter de conditions-cadres adéquates, notamment de mesures législatives et politiques appropriées.

La législation communautaire en matière de cybersécurité influe sur un **large éventail de droits fondamentaux** conférés par la Charte des droits fondamentaux de l'Union européenne, tels que la liberté d'expression, l'égalité, les droits des personnes âgées et le droit d'exercer une activité.

Pourtant, les analyses d'impact et les débats autour des propositions législatives ont tendance à se **focaliser excessivement** et exclusivement sur le respect de la vie privée et familiale ainsi que sur le droit à la protection des données à caractère personnel. Une analyse plus profonde et holistique de l'impact sur le cadre des droits fondamentaux est nécessaire.

La Charte des droits fondamentaux de l'UE

Toutes les propositions législatives formulées par la Commission européenne, y compris celles relatives à la cyber-sécurité, doivent être compatibles avec les droits et les libertés conférés par la Charte des droits fondamentaux de l'UE.

Éléments importants :

- La Charte est fondée sur l'idée que la protection des droits fondamentaux est une « condition préalable indispensable à la légitimité de l'Union ».
- La Charte a initialement été proclamée au conseil de Nice en 2000 et est devenue juridiquement contraignante à l'entrée en vigueur du traité de Lisbonne en 2009.
- La Charte complète les documents nationaux relatifs aux droits de l'homme ainsi que la Convention européenne des droits de l'homme (CEDH).
- Elle fournit la codification la plus récente des droits fondamentaux en Europe.

Les valeurs de la Charte des droits fondamentaux de l’UE

Les décideurs politiques doivent prendre en compte un éventail plus large de valeurs et droits fondamentaux qui sont ou peuvent être affectés par les politiques et mesures législatives européennes en matière de cybersécurité, telles que

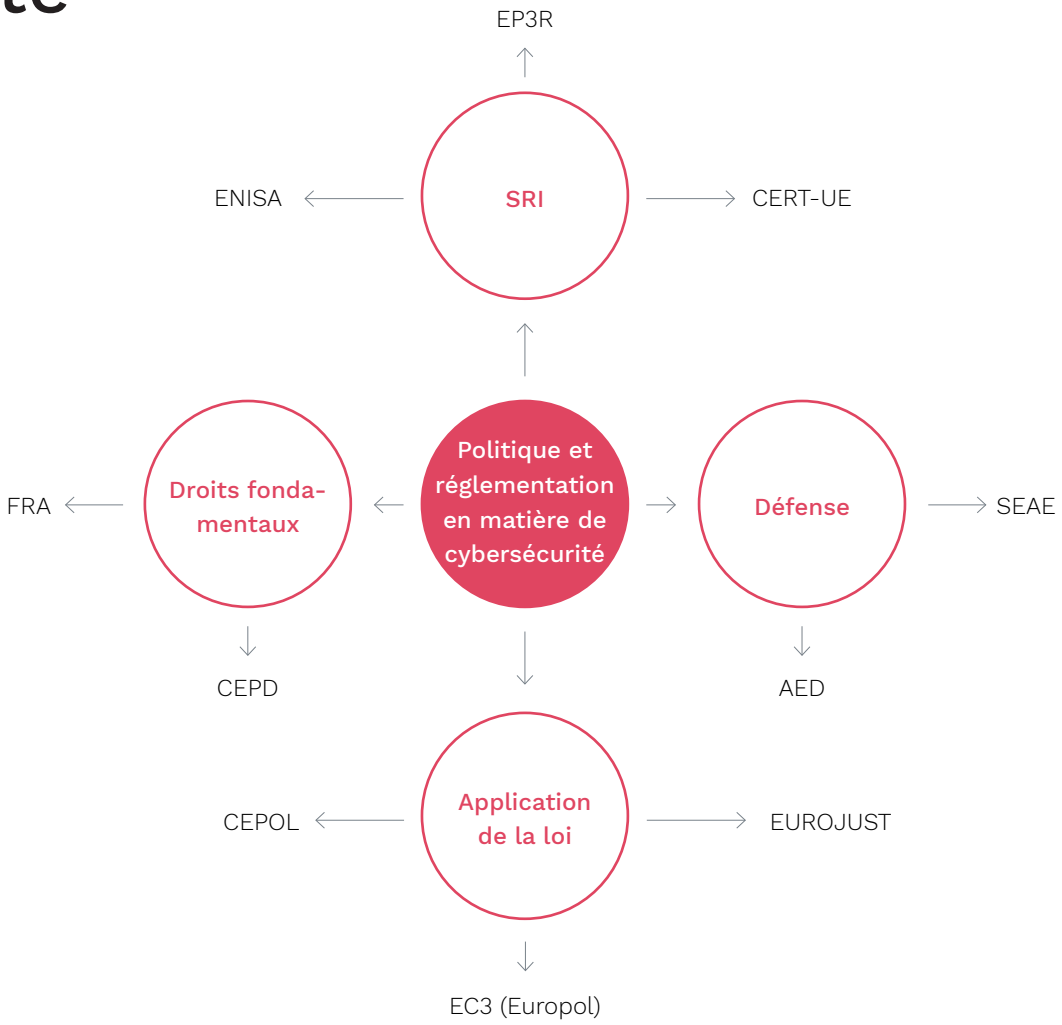
- la dignité humaine
- a liberté
- l’égalité
- la solidarité
- la démocratie
- l’État de droit
- le respect de la diversité des cultures et traditions des peuples européens (pluralisme)
- la subsidiarité (le respect de l’organisation des autorités publiques aux niveaux national, régional et local)
- le développement équilibré et durable
- la libre circulation des personnes, services, marchandises et capitaux, et la liberté d’établissement

Pays exemptés :
Royaume-Uni, Pologne et République tchèque.

Un aperçu des instances spécialisées de l'UE impliquées dans la réglementation et la politique en matière de cybersécurité

Les institutions (la Commission, le Parlement et le Conseil), les agences et les organismes de l'Union sont tous liés par la Charte des droits fondamentaux de l'UE.

L'arrangement institutionnel du cyberespace de l'UE est complexe et composé de plusieurs dimensions, à cheval sur différents domaines politiques internes. Cet arrangement reconnaît la nécessité d'une coopération de différentes parties prenantes dotées d'expertises diversifiées pour traiter des questions de cybersécurité.



En dépit de ces défis, plusieurs moyens permettent d'intégrer les valeurs de l'UE dans les politiques et cadres législatifs

Les défis de la réglementation en matière de cybersécurité

Il convient de reconnaître les défis posés par la protection des droits fondamentaux au sein de l'environnement numérique à l'échelle européenne. Ces défis sont les suivants :

1. Le domaine de la cybersécurité est en constante évolution et comporte des mesures législatives très fragmentées.
2. La cybersécurité constitue une problématique horizontale et un dénominateur commun à une variété de nouvelles technologies connectées à Internet.
3. Les accords de coopération entre les organismes et agences de l'UE pourraient intégrer des aspects relatifs à la protection des droits fondamentaux.

Première recommandation : promouvoir le contrôle juridictionnel des mesures législatives européennes par la CJUE

La jurisprudence de la Cour de justice de l'Union européenne ne cesse de s'étoffer en ce qui concerne la compatibilité de la Charte de l'Union européenne avec la directive UE sur la conservation des données. Cette directive oblige les FSI et les fournisseurs de services de télé-communications opérant dans l'Union à collecter et conserver les données des abonnés relatives à leur utilisation du service.

Une telle jurisprudence cherche à savoir si un équilibre approprié a été atteint entre les divers intérêts, tout en exhortant à prendre sérieusement en considération les droits fondamentaux dès le début du processus législatif.

Exemples :

Arrêt de la Cour du 8 avril 2014 dans l'affaire Digital Rights Ireland (affaires jointes C-293/12 et C-594/12)

Avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur les données des dossiers passagers

Deuxième recommandation : maintenir une approche de la cybersécurité européenne axée sur les valeurs

Encourager les actions suivantes

1. Réaliser une analyse d'impact du texte final d'une mesure législative. Cela contribuerait à la conformité des textes avec les valeurs inscrites dans la Charte de l'UE.
2. Impliquer diverses parties prenantes dans les délibérations législatives, tels que les instances spécialisées de l'UE (CEPD ou ENISA), des ONG et d'autres acteurs pertinents.
3. Élaborer de nouvelles techniques législatives – reposant, par exemple, sur le principe de la protection des données dès la conception – qui renforceront davantage les obligations découlant du Règlement général sur la protection des données.
4. Viser une utilisation accrue des mesures et principes existants (p. ex., la mise en œuvre de mesures de sécurité appropriées).
5. Les accords de coopération entre les organismes et agences de l'UE pourraient intégrer des aspects relatifs à la protection des droits fondamentaux.

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.