NOTE STRATÉGIQUE N° 3

TOUS LES DROITS FONDAMENTAUX SONT PERTINENTS POUR LA CYBERSÉCURITÉ

Maintien d'une approche globale de la protection des droits fondamentaux dans le cadre de la cybersécurité dans l'UE

Lorsque la Commission européenne présente des propositions de politique et de réglementation en matière de cybersécurité, leur évaluation se concentre souvent sur la compatibilité des propositions avec le droit à la protection des données à caractère personnel et le droit au respect de la vie privée et familiale. En effet, dans l'environnement numérique, le droit à la protection des données et le droit à la vie privée figurent parmi les préoccupations les plus pertinentes. Cependant, tout en reconnaissant l'importance de ces deux droits inscrits respectivement dans les articles 8 et 7 de la Charte des droits fondamentaux de l'Union européenne (Charte de l'Union européenne), les responsables politiques devraient envisager un éventail plus large de droits fondamentaux qui sont ou pourraient être affectés par les politiques et les mesures réglementaires de l'UE en matière de cybersécurité.

Les responsables politiques devraient envisager un plus large éventail de droits fondamentaux qui sont ou pourraient être affectés par les politiques et les mesures réglementaires de l'UE en matière de cybersécurité.

Le droit primaire européen proclame la protection des valeurs de l'UE et des droits fondamentaux

Selon l'article 2 du traité sur l'Union européenne, « [l]'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités ». Ces valeurs communautaires sont déterminées par les principes de pluralisme, de non-discrimination, de tolérance, de justice et d'égalité de traitement entre hommes et femmes, et sont détaillées dans la Charte de l'UE. En outre, la Charte de l'UE prévoit un large éventail de droits fondamentaux dont jouissent les citoyens et les résidents de l'UE, notamment le droit à un procès équitable, la liberté de pensée, la liberté d'expression et d'information et le droit à la propriété, à l'éducation ainsi qu'à un recours effectif. Ces valeurs et droits doivent être pris en compte dans les mesures réglementaires de l'UE.

Étape 1 : Reconnaître les défis liés à la protection des droits fondamentaux dans l'environnement numérique au niveau de l'UE

Les documents stratégiques et la législation de l'UE dans le domaine de la cybersécurité reconnaissent que toute mesure prise en matière de protection des citoyens de l'UE, de la société ainsi que

des systèmes et infrastructures informatiques devrait être élaborée conformément à l'engagement de respect des droits fondamentaux de la personne. Dans son considérant 75, par exemple, la directive SRI indique que la directive « respecte les droits fondamentaux et observe les principes reconnus par la Charte de l'Union européenne, en particulier le droit au respect de la vie privée et des communications, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif devant un tribunal et le droit d'être entendu ». Ainsi, la directive devrait être mise en œuvre conformément à ces droits et principes.

La cybersécurité ne peut être solide et efficace que si elle est fondée sur les droits fondamentaux ainsi que sur les libertés et les valeurs fondamentales inscrits dans la Charte des droits fondamentaux de l'Union européenne.

Malgré la reconnaissance du rôle crucial que jouent les droits fondamentaux, leur mise en œuvre reste difficile en pratique. La complexité inhérente de ce sujet est exacerbée par les dispositifs de gouvernance de l'UE : de nombreux organes et institutions travaillant sur les questions de cybersécurité possèdent des compétences bien délimitées. Par exemple, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. L'Agence européenne de défense (AED) joue un rôle dans la politique de coordination militaire, de sécurité et de défense de l'Europe, tandis qu'Europol aide les États membres à mener des enquêtes sur la cybercriminalité. En outre, l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) s'occupe de la sécurisation de l'infrastructure informatique de l'UE.

Bien que tous ces organes disposent de moyens de coopération et d'échange d'informations, rien n'indique clairement si des mécanismes de protection des droits fondamentaux sont prévus et, le cas échéant, s'ils sont suffisants.

Étape 2 : Incitation au contrôle juridictionnel des mesures législatives de l'UE

La Cour de justice de l'Union européenne (CJUE) a interprété le droit de l'Union, y compris les mesures relatives à la cybersécurité. Dans sa jurisprudence, la CJUE a souligné que « l'applicabilité du droit de l'Union européenne implique l'applicabilité des droits fondamentaux garantis par la Charte ».

La décision concernant la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux de communication publics (directive sur la conservation des données) illustre parfaitement comment le pouvoir judiciaire de la CJUE peut déclarer le non-respect des droits fondamentaux européens. Cette directive a été annulée par la Grande Chambre de la Cour au motif que la collecte générale de données de communication, notamment les données de trafic et de localisation, par les fournisseurs de services de communication n'était pas proportionnée (c'est-à-dire excessive). Par conséquent, cette législation constituait une violation des droits des individus à la vie privée et à la protection des données à caractère personnel. Si la décision de justice n'a pas automatiquement annulé les lois d'application de la directive sur la conservation des données des États membres, elle offre un parfait exemple d'une mesure législative pouvant être rejetée pour des raisons d'incompatibilité avec les droits énoncés dans la Charte de l'UE.

L'avis 1/15 de la CJUE concernant le projet d'accord entre l'Union européenne et le Canada sur le transfert des dossiers passagers constitue également une parfaite illustration soulignant l'importance du respect des droits fondamentaux reconnus par l'UE. Dans cet avis, la CJUE a jugé que l'accord envisagé ne devrait pas être conclu sous sa forme actuelle, car les règles régissant le transfert des dossiers passagers de l'UE vers le Canada impliquent une entrave à l'exercice des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

Ces exemples démontrent que certaines mesures législatives de l'UE vont à l'encontre des valeurs découlant de la Charte de l'UE. Néanmoins, il existe une possibilité de vérifier que les mesures législatives ne sont pas mises en œuvre par défaut, mais reposent sur des institutions proactives de l'UE ou des juges de tribunaux nationaux. Le contrôle juridictionnel constituant l'un des principaux moyens de préserver les valeurs de l'UE, il convient de l'encourager.

Étape 3 : maintenir une approche européenne de la cybersécurité axée sur les valeurs

Il est nécessaire d'accorder une forte priorité à la protection des droits fondamentaux pour contribuer à une approche européenne de la cybersécurité axée sur le respect des valeurs fondamentales. La stratégie de cybersécurité 2013 affirme que : « La cybersécurité ne peut être solide et efficace que si elle est fondée sur les libertés et droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'Union européenne et sur ses valeurs fondamentales. » Néanmoins, cette approche est souvent contestée par les institutions européennes elles-mêmes (comme nous l'avons vu dans la section précédente).

Pour maintenir cette approche et adhérer à la Charte de l'UE, l'UE doit intégrer ses valeurs dans le cadre réglementaire applicable. Toutefois, il n'est pas facile de mettre cela en pratique lorsqu'il s'agit d'élaborer et de mettre en œuvre efficacement la législation ou les politiques de l'UE. Le processus d'intégration implique une prise en compte globale des « valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit et des droits de l'homme, y compris les droits des personnes appartenant à des minorités ». Par ailleurs, une compréhension approfondie du domaine de la réglementation est nécessaire, alors que l'expertise globale nécessaire ne peut être réalisée que par une implication, une action et une collaboration proactives des différentes parties prenantes. L'intégration des valeurs de l'UE inscrites dans la Charte de l'UE peut avoir lieu à la fois ex ante et ex post (via le contrôle juridictionnel, par exemple).

Intégration sur une base ex ante : Analyses d'impact et consultation des parties prenantes

Les institutions de l'UE exerçant un pouvoir législatif – à savoir la Commission européenne, le Conseil de l'UE et le Parlement européen – ainsi que les agences de l'UE, l'ENISA notamment, peuvent jouer un rôle important à cet égard sur une base ex ante.[1] Par exemple, la Commission européenne a élaboré une liste des bonnes pratiques en matière de contrôle de compatibilité et d'analyse d'impact des propositions législatives. On estime que ces pratiques atténuent le risque que les mesures législatives proposées violent les droits fondamentaux. Les connaissances générées au cours de ce processus peuvent alors faciliter la prise de décision, afin de garantir l'adoption de l'approche qui soutiendra au mieux la réalisation des droits fondamentaux. Pourtant, l'importance de ces outils est souvent remise en question au cours du processus législatif. Ce problème survient notamment par le biais d'amendements entraînant des modifications considérables du texte proposé qui portait à l'origine sur la protection des droits fondamentaux.

Dans le domaine de la cybersécurité, les consultations et les contributions des organes spécialisés de l'UE, tels que le CEPD, l'ENISA et le comité européen de la protection des données, se sont avérées utiles et ont permis de surmonter les limites des contrôles de compatibilité et des analyses d'impact initiaux. Par ailleurs, la réalisation d'une analyse d'impact du texte final au sujet d'une mesure législative constituerait une évolution positive. De plus, la dimension participative peut également faciliter l'intégration des valeurs de l'UE dans les cadres et les politiques réglementaires. Par exemple, au cours de la phase de rédaction des propositions législatives, la Commission européenne lance généralement un processus de consultation publique afin de dévoiler les principaux problèmes rencontrés par les parties prenantes concernées. En fait, la Commission européenne est tenue de mener « de larges consultations auprès des parties concernées afin de garantir la cohérence et la transparence des actions de l'Union ».[2] Sur la base des contributions reçues au cours du processus de consultation publique, la Commission européenne doit proposer des mesures permettant de concilier les différents intérêts des parties concernées. Cependant, ces propositions de mesures doivent également être compatibles avec les valeurs inscrites dans la Charte de l'UE. Les parties prenantes concernées peuvent rester actives après la fin des consultations en commentant les propositions législatives au cours des différentes étapes du processus législatif. Certaines organisations, notamment celles qui représentent des groupes de la société civile, fournissent souvent des analyses détaillées sur la manière dont une future mesure législative pourrait permettre de mieux mettre en œuvre les dispositions de la Charte de l'UE. Cependant, pour que ces analyses soient prises en compte par les législateurs, les parties prenantes concernées doivent mener des campagnes de lobbying onéreuses. Par conséquent, les groupes de défense des intérêts des entreprises continuent d'être mieux représentés.

1 De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016.

2 Version consolidée du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne (2010/C 83/01) ; le traité sur l'Union européenne (TUE), article 11(3).

Autres moyens d'assurer une approche européenne en matière de réglementation de cybersécurité

Outre les contrôles de compatibilité, les analyses d'impact des propositions législatives et la participation des parties prenantes, les législateurs peuvent choisir de mettre l'accent sur certaines valeurs dans le texte législatif, telles que le principe de protection des données, dès la conception prévu par l'article 25(1) du RGPD. Cet article impose explicitement aux responsables du traitement des données à caractère personnel de mettre en œuvre des mesures techniques et organisationnelles propres à atténuer les risques susceptibles de découler des activités de traitement, en particulier les droits et les libertés des personnes dont les données sont en cours de traitement. Ces mesures devraient garantir que les obligations et principes du RGPD sont intégrés dans l'activité de traitement dès sa mise en place et qu'ils sont continuellement réexaminés tout au long de l'activité de traitement des données. Dans les faits, ce principe renforce les obligations visées à l'article 5 du RGPD précisant les principes relatifs au traitement des données à caractère personnel. Des techniques législatives semblables pourraient être envisagées pour assurer une approche européenne de la cybersécurité fondée sur les valeurs, en reconnaissant l'importance de tous les droits fondamentaux dans l'environnement numérique.

Pour de plus amples informations

Cette note stratégique est basée sur les travaux de recherche réalisés dans le cadre du projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs). Des rapports détaillés sur ces travaux ont été publiés dans quatre livres blancs principaux :

1. Cybersécurité et éthique
2. Cybersécurité et droit
3. Attitudes et opinions concernant la cybersécurité
4. Défis technologiques de la cybersécurité

Tous les livres blancs sont consultables sur notre site Internet, avec toutes nos notes stratégiques (téléchargeables et imprimables), de brèves explications en ligne sur les principaux problèmes en matière de cybersécurité, ainsi que des listes de publications commentées afin d'approfondir le sujet :

canvas-project.eu

Vous trouverez d'autres documents liés au projet CANVAS sur notre site Internet :

Programme de référence du projet CANVAS
(intégration de l'approche prenant en compte les valeurs fondamentales dans la formation et l'éducation en cybersécurité)

CANVAS MOOC
(Cours en ligne ouvert à tous)

Livre en libre accès
« L'éthique de la cybersécurité »

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 du gouvernement suisse.

Objectif de CANVAS :
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.

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

Version et date de publication :
Version 2.0, octobre 2019

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 formaation, à la recherche et à l'innovation.

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

Durée du projet :
septembre 2016 – octobre 2019