EUROPEAN PARLIAMENT

IMPA
Impact Assessment

Première évaluation d'une analyse d'impact de la Commission européenne

Proposition de directive concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union

Analyse d'impact (SWD(2013) 32, SWD(2013) 31 (résumé)) pour une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union (COM(2013)0048)

• Contexte

La présente note a pour objectif de fournir une première analyse des points forts et des faiblesses de l'analyse d'impact de la Commission européenne jointe à la proposition de directive concernant la sécurité des réseaux et de l'information.

On entend par "sécurité des réseaux et de l'information" "la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles" (rapport d'analyse d'impact, p. 6). Les services dont dépend le fonctionnement de notre société et de nos économies, comme par exemple l'administration publique, la finance et la banque, l'énergie, le transport, la santé, ainsi que, par définition, des services en ligne comme les plateformes de commerce électronique ou les réseaux sociaux, reposent sur l'internet et sur d'autres réseaux et systèmes d'information.

La résolution du Parlement européen du 12 juin 2012 sur la protection des infrastructures d'information critiques - Réalisations et prochaines étapes: vers une cybersécurité mondiale[1] invite la Commission à proposer, entre autres:

- au moyen du plan d'urgence européen en cas d'incident informatique, des mesures contraignantes pour une meilleure coordination, au niveau de l'Union, des fonctions techniques et de pilotage des équipes d'intervention d'urgence en matière de sécurité informatique (CERT) nationales et gouvernementales;
- des mesures contraignantes visant à imposer des normes minimales de sécurité et de résilience et à améliorer la coordination entre les équipes nationales d'intervention d'urgence en matière de sécurité informatique;
- un cadre européen pour la notification des violations de la sécurité dans les secteurs critiques, notamment les secteurs de l'énergie, des transports, de l'approvisionnement en eau et en nourriture mais aussi les secteurs des TIC et des services financiers, afin d'informer les autorités des États membres concernés et les utilisateurs des incidents, des attaques et des perturbations informatiques.

[1] P7_TA-PROV(2012)0237, paragraphes 19, 22 et 35.

La proposition actuellement à l'examen crée, au niveau européen, des mécanismes de coopération et de partage d'informations de confiance sur les risques et incidents touchant la sécurité des réseaux et de l'information (ci-après "risques et incidents de SRI") entre les États membres.

- **Définition du problème**

Le problème qui nécessite une intervention de l'Union "peut être décrit globalement comme un niveau insuffisant de protection contre les incidents, risques et menaces pour la sécurité des réseaux et de l'information dans l'Union et préjudiciable au bon fonctionnement du marché intérieur" (rapport d'analyse d'impact, p. 12).

Le rapport d'analyse d'impact comporte une description détaillée des problèmes rencontrés, illustrés par des exemples d'incidents de SRI survenus par le passé. Étant donné que les réseaux et systèmes informatiques sont interconnectés, nombre d'incidents de SRI dépassent les frontières nationales et peuvent nuire au fonctionnement du marché intérieur. Le nombre, la fréquence et la complexité de ces incidents semblent être en augmentation, mais l'absence d'informations sur ces incidents empêche toute réaction rapide fondée sur des mesures adéquates visant à en atténuer les conséquences. Le secteur des TIC est l'un des moteurs de croissance de l'Union et, de ce fait, exerce une influence sur bien d'autres secteurs de la société et de l'économie, y compris des secteurs où la sécurité des réseaux et de l'information est indispensable au bon fonctionnement du marché intérieur. Les répondants à la consultation publique menée par la Commission considèrent les secteurs suivants comme étant particulièrement dépendants d'une bonne sécurité des réseaux et des systèmes d'information: l'énergie, le transport, la banque et la finance, la santé, les services en ligne et l'administration publique.

Selon la Commission, les sources sous-jacentes du problème sont les suivantes: premièrement, tous les États membres ne disposent pas des mêmes moyens (en termes de niveau de préparation et de capacité de réaction aux incidents informatiques), ce qui nuit à la création d'un climat de confiance, lequel est une condition préalable à la coopération et au partage d'informations concernant les risques, menaces et incidents de SRI; deuxièmement, l'absence de cadre au sein duquel partager de telles informations. En l'absence de mesures supplémentaires prises au niveau de l'Union, l'on assisterait à une perte de confiance des consommateurs dans le marché intérieur, à une pénurie d'investissement dans la sécurité des réseaux et de l'information, et à une perte de crédibilité sur la scène internationale.

À la demande du comité d'analyse d'impact de la Commission, le rapport comprend une section portant sur les lacunes du cadre réglementaire actuel, et détaille par ailleurs les limites de l'approche volontaire, actuellement en vigueur, envers la préparation et le partage d'informations en matière de sécurité des réseaux et de l'information. À titre d'exemple, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) apporte soutien et conseils à la Commission et aux États membres, mais ne dispose d'aucun pouvoir d'action et n'est pas en mesure d'intervenir pour résoudre les problèmes de sécurité des réseaux et de l'information.

- **Objectifs de la proposition législative**

L'objectif *général* de la proposition est de "relever le niveau de protection contre les incidents, risques et menaces pour la sécurité des réseaux et de l'information dans l'UE" (rapport d'analyse d'impact, p. 34).

Les objectifs *spécifiques* de la proposition sont les suivants, fondés sur l'objectif général et les problèmes décrits:

- instaurer un niveau minimum commun de sécurité des réseaux et de l'information dans les États membres et donc relever le niveau global de préparation et d'intervention. Cet objectif se décline lui-même en deux objectifs *opérationnels*: a) veiller à ce que tous les États membres disposent de moyens suffisants, sur les plans technique et organisationnel, pour prévenir et détecter les risques, menaces et incidents de SRI, et prendre les mesures d'intervention et d'atténuation nécessaires; et b) veiller à ce que tous les États membres développent et actualisent leur stratégie en matière de sécurité informatique et leur plan d'urgence et de coopération en cas d'incident informatique national;

- améliorer la coopération en matière de sécurité des réseaux et de l'information au niveau de l'Union, en vue de faire face efficacement aux menaces et incidents transnationaux. Cet objectif se décline lui-même en deux objectifs *opérationnels*: a) veiller à ce que les autorités nationales compétentes partagent les informations et les bonnes pratiques en matière de sécurité des réseaux et de l'information; et b) s'assurer que ces organes puissent échanger des informations d'un État à l'autre de manière fiable et confidentielle;
- créer une culture de gestion des risques et améliorer le partage d'informations entre le secteur privé et le secteur public. Cet objectif se décline lui-même en deux objectifs *opérationnels*: a) s'assurer que les principaux acteurs du secteur privé et les administrations publiques conduisent des études de risque et observent des pratiques de gestion des risques; et b) veiller à ce que les incidents de SRI ayant des conséquences graves soient signalés aux autorités nationales compétentes.

L'analyse d'impact permet d'avoir une vue d'ensemble, fort utile, de ces objectifs spécifiques, qui fait apparaître clairement le lien entre les problèmes définis, leurs causes et les différents objectifs à atteindre.

• Éventail d'options envisagées

Le rapport d'analyse d'impact présente un éventail assez limité d'options stratégiques, dont l'une consiste à ne pas modifier la stratégie adoptée.

Option 0 – Scénario de référence – Cette option consiste à maintenir le *statu quo*. L'approche volontaire actuellement en vigueur continuerait de l'être, la Commission continuant d'envoyer des communications aux États membres pour les encourager à mettre en place des équipes d'intervention d'urgence en matière de sécurité informatique réellement efficaces, à adopter un plan d'urgence et de coopération en cas d'incident informatique national, et à élaborer une stratégie nationale en matière de sécurité informatique.

Option 1 – Approche réglementaire – La Commission exigerait de touts les États membres:

- qu'ils mettent en place une équipe nationale ou gouvernementale d'intervention d'urgence en matière de sécurité informatique réellement efficace;

- qu'ils désignent une autorité nationale compétente en matière de sécurité des réseaux et de l'information, qui pourrait jouer un rôle de coordinatrice et être le point de contact pour la coopération transfrontalière. Il s'agirait de mettre en réseau les autorités nationales dans le but d'échanger informations et bonnes pratiques;

- qu'ils adoptent un plan national d'urgence et de coopération, dans lequel seraient définis des protocoles gouvernant la communication et la coopération entre les acteurs concernés au niveau national en cas d'incidents de SRI d'une magnitude déterminée;

- qu'ils adoptent une stratégie nationale en matière de sécurité informatique.

Ce scénario prévoit en outre d'imposer aux administrations publiques et à certains acteurs-clés dans des domaines sensibles du secteur privé (tels que la banque, l'énergie ou la santé) une politique de gestion des risques de SRI, ainsi qu'une obligation de soumettre des rapports. Ces exigences portent sur l'analyse régulière des risques, la gestion de la gouvernance et des risques, la sécurité en matière de ressources humaines, la sécurité des systèmes et des installations, la gestion des opérations et des incidents, et la gestion de la continuité des activités. En outre, les acteurs concernés auraient l'obligation de signaler les incidents qui, parce qu'ils représentent un réel danger pour le fonctionnement des réseaux et des systèmes d'information, sont lourds de conséquences pour les services fournis. **Il s'agit de l'option préférée par la Commission.**

Option 2 – Approche mixte – Cette option conjugue les exigences *d'ordre réglementaire* imposées dans l'option 1 (identiques en ce qui concerne les acteurs auxquelles elles s'appliquent et la teneur des obligations) avec des initiatives *d'ordre volontaire* visant à doter les États membres de moyens en matière de sécurité des réseaux et de l'information, ou de renforcer les moyens existants, et à mettre en place un cadre de coopération au niveau européen.

La Commission signale avoir écarté l'option qui consisterait à cesser toute action de l'Union en matière de sécurité des réseaux et de l'information pour laisser aux États membres le soin de poursuivre les efforts consentis en la matière. En effet, ce scénario n'est pas compatible avec les objectifs de la stratégie "Europe 2020" que sont le marché unique numérique et la croissance intelligente et durable.

Une autre option écartée d'office de l'analyse est celle qui conjuguerait une approche *volontaire* en ce qui concerne la gestion des risques de SRI et la présentation de rapports exigées aux administrations publiques et aux acteurs clés avec une approche volontaire ou réglementaire vis-à-vis des États membres. La Commission considère en effet qu'une approche volontaire "ne fonctionnerait pas, pour les motifs indiqués lors de la définition du problème" (rapport d'analyse d'impact, p. 45).

- **Subsidiarité et proportionnalité**

La proposition est fondée sur l'article 114 du traité FUE.

La Commission justifie la nécessité d'une action de l'Union dans le domaine de la sécurité des réseaux et de l'information en invoquant la nature transfrontalière du problème ainsi que la nécessité de créer un environnement égalitaire et de combler des lacunes législatives. Au moment de la publication de la présente évaluation, seul le parlement suédois a émis un avis motivé, soulevant des problèmes relatifs à la subsidiarité.

La Commission estime que l'approche proposée se justifie également en termes de proportionnalité, et ce à divers égards. Tout d'abord, l'obligation pour les États membres de se doter des moyens nécessaires et d'assurer une coopération systématique entre eux "n'impliqueraient pas de coûts disproportionnés". Ensuite, en ce qui concerne le secteur privé, les exigences en matière de sécurité ne seraient applicables qu'à certains secteurs, et les mesures proposées, parce que proportionnées aux risques réels, seraient donc raisonnables et dans l'intérêt des acteurs concernés. Enfin, bon nombre de ces entités, en tant que responsables du traitement de données, "sont déjà soumises par la réglementation en vigueur en matière de protection des données à l'obligation d'assurer la protection des données à caractère personnel" qu'elles traitent (rapport d'analyse d'impact, p. 33).

Néanmoins, eu égard à l'obligation de prouver que l'approche proposée respecte le principe de proportionnalité, la Commission aurait pu, dans l'idéal, procéder à une analyse complète des coûts et des incidences sur le niveau de sécurité de l'approche volontaire en ce qui concerne la gestion des risques de SRI et la présentation de rapports exigées aux organismes publics et privés, dans le but de les comparer aux coûts et bénéfices entraînés par l'approche

réglementaire. Or, la Commission se borne, pour justifier son choix d'écarter dès le départ l'approche volontaire, à une description largement anecdotique des problèmes posés par le scénario de référence, alors même que le comité d'analyse d'impact avait insisté sur la nécessité de fournir de solides arguments pour justifier l'imposition de mesures "à un large éventail d'organismes publics et de secteurs industriels", ainsi qu'une explication de leur valeur ajoutée.

- **Portée de l'analyse d'impact – Qualité des données, de la recherche et de l'analyse**

L'analyse d'impact est principalement qualitative, purement descriptive, et somme toute assez concise en ce qui concerne les incidences à prévoir des options envisagées sur le niveau de sécurité, sur l'économie et sur la société. Ainsi, en ce qui concerne l'approche réglementaire (option 1, préférée par la Commission), l'analyse des incidences sociales à prévoir se limite à affirmer qu'il est "très probable que cette option favorise, dans l'Union, l'emploi dans le secteur de la sécurité des réseaux et de l'information, eu égard aux exigences d'évaluation des risques de SRI et d'adoption des mesures de sécurité qui s'imposent" (rapport d'analyse d'impact, p. 48).

Le rapport d'analyse d'impact comporte une estimation des coûts liés à cette approche, reprise ci-dessous.

- Les coûts, pour les États membres, liés à la mise en place de moyens en matière de sécurité des réseaux et de l'information et à la coopération au niveau européen: pour les trois États membres qui ne disposent pas encore d'équipe d'intervention en cas d'urgence informatique, la création de celle-ci est estimée à 2,5 millions d'euros par équipe. Le coût maximal théorique pour les autorités nationales compétentes en matière de sécurité des réseaux et de l'information serait quant à lui de 9,72 millions d'euros par an, tous États membres confondus. La réalisation d'un exercice paneuropéen coûterait 55 555 euros par État membre. Le coût du réseau lui-même se monterait à 6 000 euros par État membre et par an pour les frais de déplacement et de subsistance, de 2 400 euros par an pour l'Union pour la maintenance d'un site internet commun, et de coûts supplémentaires liés à la construction d'une infrastructure physique, estimés, selon que l'on utilise ou non les infrastructures existantes, entre un et dix millions d'euros.

- Les coûts de mise en conformité pour les administrations publiques et les acteurs clés du secteur privé seraient, au total, compris dans une fourchette de 1 à 2 milliards d'euros.

- Les coûts liés, pour les administrations publiques et les acteurs clés du secteur privé, à l'obligation de signaler les incidents de SRI ayant des conséquences graves, sont estimés, par incident signalé, à 125 euros, ce qui représente un total de 212 500 euros par an, tous États membres confondus. Le coût maximal par enquête éventuellement réalisée à la suite d'un incident serait de 25 000 euros, soit un total, tous États membres confondus, compris dans une fourchette de 4,25 à 8,5 millions d'euros par an.

À l'annexe 3 du rapport d'analyse d'impact, la Commission détaille la méthode employée pour déterminer les coûts de mise en conformité pour les administrations publiques et les acteurs clés du secteur privé. Elle consiste à déterminer en premier lieu les secteurs concernés et à calculer le coût lié aux dépenses en matière de sécurité informatique qui ne sont pas encore réalisées "intrinsèquement" par les acteurs. Il est alors possible d'évaluer les coûts supplémentaires de gestion des risques que pourraient entraîner les exigences en matière de gestion des risques de SRI. Cette dernière évaluation semble reposer principalement sur l'hypothèse que "près de 40 à 70 pour cent des dépenses supplémentaires qui s'avèreront nécessaires pour assurer la sécurité informatique ne seront pas le fait de la réglementation de la sécurité des réseaux et de l'information". La Commission prévoit, eu égard à ces considérations, une fourchette extrêmement large, de 1 à 2 millions d'euros, pour les coûts supplémentaires.

Plus de la moitié de cette somme est liée à des mesures imposées aux organismes publics (annexe 3, p. 89). Un tableau des estimations par secteur et par acteur est également fourni, qui s'appuie également sur la fourchette, très large, de 40 à 70 pour cent.

La Commission signale que "très peu de données statistiques concernant les actions des entreprises au niveau de la sécurité des réseaux et de l'information sont disponibles, car il est difficile d'évaluer les montants consacrés à ce domaine, étant donné que la sécurité informatique ne dispose pas, en règle générale, d'une rubrique budgétaire distincte, et qu'une partie des coûts pourraient même figurer ailleurs que dans le budget informatique" (rapport d'analyse d'impact, annexe 3, p. 86). En outre, des obligations similaires en matière de sécurité existent déjà, tant au niveau national qu'européen, au titre des plans d'urgence polyvalents pour les infrastructures critiques ainsi qu'en vertu du règlement général en matière de protection des données.

- **Effets sur les PME et sur la compétitivité**

Bien que les micro-entreprises (structures comptant moins de 10 employés) soient exclus du champ d'action de la proposition, les exigences prévues par celle-ci s'appliqueraient à un grand nombre de petites et moyennes entreprises qui exercent leur activité dans les secteurs déterminés comme étant cruciaux. Le calcul des coûts de mise en conformité comprend une section dédiée au coût pour les PME, qui est estimé entre 2 500 et 5 000 euros par entreprise et par an. Toutefois, cette estimation se fonde en réalité sur une extrapolation du montant calculé pour le coût total de mise en conformité du secteur privé, chiffre qui, comme expliqué précédemment, est lui-même le produit de conjectures et d'extrapolations. À l'annexe 5 du rapport d'analyse d'impact, l'on trouve la rubrique obligatoire "effets sur les PME", qui se distingue par sa brièveté et dont le contenu est purement qualitatif. Dans les conclusions de cette rubrique, la Commission estime qu'"aucun élément n'indique qu'il soit nécessaire d'adopter des mesures spécifiques aux PME afin d'assurer la conformité au principe de proportionnalité" (rapport d'analyse d'impact, p. 95), la seule mesure retenue étant d'exclure les micro-entreprises du champ d'action de la proposition.

Le rapport comporte également une évaluation des "effets sur la compétitivité". En ce qui concerne la compétitivité des coûts, la Commission estime que "les coûts additionnels demeurent, en règle général, restreints, étant donné que de nombreuses mesures ont déjà été prises, en conformité avec les dispositions règlementaires existantes". La Commission s'attend également à des incidences positives sur la capacité d'innovation et à des avantages compétitifs sur le marché extérieur. En outre, l'environnement égalitaire créé par les mesures proposées permettrait d'améliorer la concurrence au sein du marché intérieur. Enfin, la Commission s'attend à des incidences positives sur la compétitivité des fournisseurs de services et de produits liés à la sécurité informatique.

- **Incidences sur le budget ou les finances publiques**

La proposition aura des incidences sur le budget de l'Union seulement si les États membres choisissent d'adapter des infrastructures existantes (sTESTA par exemple) pour coopérer et échanger des informations et chargent la Commission de mettre cela en œuvre au titre du CFP 2014-2020. Ce coût unique est estimé à 1 250 000 euros.

Le coût pour les États membres et sa méthode de calcul ont été rappelés ci-dessus.

- **Consultation des parties prenantes**

Lors de l'élaboration de cette analyse d'impact, la Commission semble avoir consulté comme il se doit les États membres et les autres acteurs concernés. Une consultation publique en ligne

s'est déroulée de juillet à octobre 2012. À la suite d'une recommandation formulée par le comité d'analyse d'impact, les résultats de celle-ci sont systématiquement rappelés dans le rapport d'analyse d'impact.

- **Suivi et évaluation**

Le rapport d'analyse d'impact comporte un tableau d'indicateurs principaux destinés à un suivi et à une évaluation futurs, se rapportant aux objectifs spécifiques de la proposition et fixant les outils à employer.

La Commission procédera à un examen régulier du fonctionnement de la législation proposée, en se fondant en particulier sur l'évolution des technologies et du marché, et présentera tous les trois ans un rapport à cet effet.

- **Comité d'analyse d'impact de la Commission**

Le comité d'analyse d'impact de la Commission, ayant examiné le projet d'analyse d'impact, a émis, en juillet 2012, un premier avis très critique. Il a exigé du rédacteur, la DG CONNECT, qu'il améliore la définition du problème, qu'il fournisse des arguments clairs en faveur de la nécessité d'une action de l'Union et qu'il justifie tant le respect de la proportionnalité que les mesures proposées. En octobre 2012, le comité a examiné le projet modifié et a fourni par écrit de nouvelles recommandations. Il y soulignait de nouveau la nécessité de justifier les mesures imposées aux acteurs du secteur privé, en particulier aux PME, et à fournir des éléments de preuve de leur réelle valeur ajoutée. Le comité exigeait également du rédacteur qu'il étaye davantage son évaluation des incidences significatives, y compris dans le domaine social et en termes d'emploi et dans les domaines de la compétitivité, de la protection des données et des conséquences sur le plan international. Cette recommandation du comité d'analyse d'impact semble toutefois ne pas avoir été entièrement observée.

- **Cohérence entre la proposition législative et l'analyse d'impact de la Commission**

L'analyse d'impact et la proposition législative sont cohérentes, étant donné que la proposition se fonde manifestement sur l'option préférée par la Commission dans l'analyse d'impact, à savoir l'approche réglementaire.

Auteur: Elke Ballon

Unité Évaluation de l'impact
Direction de l'évaluation de l'impact et de la valeur ajoutée européenne (G)
Direction générale des politiques internes de l'Union (DG IPOL)
Parlement européen

La présente note, élaborée par l'unité "Évaluation de l'impact" à l'intention de la commission du marché intérieur et de la protection des consommateurs (IMCO) du Parlement européen, vise à déterminer si l'analyse d'impact respecte les principaux critères établis dans les lignes directrices de la Commission concernant l'analyse d'impact et les autres paramètres définis par le Parlement européen dans son guide pratique des analyses d'impact. Elle n'a pas vocation à examiner le contenu de la proposition. La présente note est élaborée à des fins d'information et de mise en contexte afin d'offrir une assistance plus large aux commissions parlementaires et aux députés dans leurs travaux. Ce document est également disponible sur l'internet à l'adresse suivante:
http://www.europarl.europa.eu/committees/fr/studies.html

Vous pouvez contacter l'unité "Évaluation de l'impact" en envoyant un courriel à l'adresse suivante: impa-secretariat@ep.europa.eu .

Manuscrit achevé en avril 2013.

ISBN : 978-92-823-4377-7
DOI : 10.2861/20721
CAT : BA-31-13-929-FR-N