Note sur les politiques STI

www.oecd.org/fr/sti/

Des politiques intelligentes pour les produits intelligents

Guide à l'usage des responsables de la formulation des politiques publiques pour le renforcement de la sécurité numérique des produits

La présente synthèse reprend les principales conclusions de deux rapports publiés par l'OCDE en 2021, intitulés « Understanding the digital security of products: an in-depth analysis » (OCDE, 2021a), et « Enhancing the digital security of products: a policy discussion » (OCDE, 2021b).

Des logiciels « traditionnels » aux services infonuagiques en passant par les appareils connectés à l'internet des objets (IdO), nos économies et nos sociétés font de plus en plus largement appel aux « produits intelligents », autrement dit à des produits comportant du code informatique et capables d'interconnexion, par exemple via internet. Ces dernières années, des cyberattaques comme Mirai, WannaCry, NotPetya et SolarWinds ont révélé que l'exploitation des vulnérabilités de ces produits pouvait avoir de graves conséquences économiques et sociales. Au-delà des pertes financières et des atteintes à la réputation, ces attaques ont aussi des répercussions toujours plus sérieuses sur la sécurité des utilisateurs et peuvent mettre des vies humaines en danger.

On a trop souvent tendance à considérer la conception de produits intelligents « suffisamment sûrs » comme une question purement technique qui appelle des solutions de même nature. Cependant, certains facteurs économiques jouent un rôle important dans la relative « insécurité » de ces produits, et les incitations émanant du marché ont peu de chance de suffire à combler le manque de sécurité numérique. La complexité et l'opacité des chaînes de valeur conduisent souvent à une attribution inadéquate des responsabilités de gestion du risque de sécurité numérique, tandis que d'importantes externalités et asymétries d'information ne permettent pas aux parties prenantes d'adopter un comportement optimal. Si le code est omniprésent, les produits intelligents sont néanmoins relativement nouveaux et ne rentrent pas nécessairement dans les catégories juridiques héritées du XX^{e} siècle. L'application aux produits intelligents du droit de la responsabilité civile, de même que leur certification, leur assurance et leur garantie ne vont pas sans difficultés, et réclameront probablement une révision des cadres juridiques en vigueur et leur adaptation aux dynamiques de l'économie numérique.

En bref

Les responsables de la formulation des politiques publiques ont un rôle clé à jouer pour réajuster les incitations du marché afin d'apporter aux produits intelligents un niveau de sécurité numérique optimal. La transparence et le partage d'informations, la coopération (notamment au niveau international) et le devoir de diligence des fournisseurs (en vertu, par exemple, des principes de sécurité dès la conception, de sécurité par défaut et de fin de vie responsable) sont des axes importants pour l'action des pouvoirs publics. Ceux-ci ont de nombreux outils à leur disposition pour atteindre ces objectifs, de la commande publique à la certification et aux partenariats multipartites en passant par les labels et les obligations juridiques *ex ante*. La présente note et les deux rapports qui lui sont associés (OCDE, 2021a et 2021b) offrent une revue détaillée de ces outils, une analyse de leurs avantages et de leurs limites ainsi que des éclairages sur l'usage qui en est fait dans les pays de l'OCDE.

À cet égard, la coopération internationale apparaît comme l'une des clés du succès. Les responsables de la formulation des politiques publiques ont intérêt à tirer les leçons des réussites et des échecs d'autres pays et à s'inspirer des mesures qui ont déjà donné ailleurs la preuve de leur efficacité. Certaines initiatives innovantes lancées au niveau national ont été le point de départ de nouvelles normes internationales. C'est ainsi qu'un code de bonnes pratiques édicté par le gouvernement du Royaume-Uni a ouvert la voie à la définition, par l'Institut européen des normes de télécommunication (ETSI), de spécifications techniques destinées à garantir la sécurité des utilisateurs de l'IdO. La coopération internationale est aussi essentielle pour permettre l'interopérabilité entre les stratégies nationales, éviter la prolifération des normes et limiter les incohérences entre juridictions, susceptibles d'être un frein majeur au développement de l'économie numérique.

Le code est omniprésent

Les administrations, les entreprises et les particuliers font aujourd'hui de plus en plus appel aux produits intelligents, une catégorie qui comprend notamment les logiciels, les produits informatiques « traditionnels », tels que les ordinateurs et les smartphones, et les produits liés aux technologies émergentes, comme les appareils connectés à l'internet des objets (IdO). En 2019, 60 % des grandes entreprises des pays de l'OCDE avaient recours à des services infonuagiques, et 68 % des particuliers aux services bancaires en ligne. D'après une enquête réalisée cette année-là par Consumers International, 69 % de la population possède au moins un appareil connecté.

La crise du COVID-19 a accéléré la transformation numérique, révélant ainsi notre dépendance croissante à l'égard de ces produits. Avec les mesures de confinement imposées par les autorités des pays de l'OCDE pour contenir la pandémie au printemps dernier, les employés de nombreux secteurs se sont mis massivement au télétravail, pour certains du jour au lendemain. Pour assurer la continuité de leur activité dans une situation sans précédent, les organisations publiques et privées ont rapidement mis en place des réseaux privés virtuels (VPN) et des outils de visioconférence ou, si elles étaient déjà équipées, fait un usage accru de ces moyens.

Il est difficile d'apprécier **le coût global des attaques de sécurité numériques** qui exploitent les vulnérabilités des produits intelligents. Beaucoup d'attaques en effet passent inaperçues, et beaucoup d'entreprises choisissent de protéger leur image de marque et ne révèlent pas que leurs actifs ont été compromis. Qui plus est, les attaques de sécurité numérique qui se traduisent par la violation de données personnelles et le vol d'éléments de propriété intellectuelle portent sur des actifs non financiers, ce qui rend leur coût difficile à quantifier. Cependant, selon des estimations courantes, le coût global de ces attaques serait compris entre 100 milliards et 6 000 milliards USD par an et tendrait à augmenter d'année en année.

Le code est vulnérable

Dans la mesure où ils reposent tous sur du code, les produits intelligents sont tous, dans une certaine mesure, vulnérables. En effet, le code contient pratiquement toujours des points faibles que des acteurs malveillants peuvent exploiter. Entre 2017 et 2020, 40 nouvelles vulnérabilités en moyenne, concernant des produits très courants, comme Android, iOS ou Windows, étaient signalées quotidiennement – et il est probable que bien plus encore aient été découvertes sans être révélées.

L'exploitation des vulnérabilités des produits intelligents peut avoir de graves conséquences économiques et sociales. En 2017, les attaques de sécurité numérique WannaCry et NotPetya ont touché des milliers de petites et grandes structures dans les pays de l'OCDE, dont Renault, Honda, Boeing, Merck, Maersk et le Service national de santé (*National Health Service*) du Royaume-Uni. Elles ont apporté la preuve que l'exploitation d'une vulnérabilité présente sur un seul produit pouvait paralyser des entreprises d'envergure mondiale et causer un préjudice évalué à plusieurs milliards de dollars.

Pourquoi les produits intelligents sont-ils vulnérables ?

Dans ce contexte, plusieurs questions se posent avec une acuité toute particulière. Pourquoi les produits intelligents sont-ils si vulnérables ? Est-ce seulement une question de normes et d'architectures techniques, ou est-ce que des facteurs économiques entrent aussi en jeu ? Quelles sont les responsabilités des pouvoirs publics, des acteurs de

l'offre et des utilisateurs finals ? Quels sont les principales dynamiques et les principaux enjeux ? Y a-t-il de ce point de vue des similitudes entre différents marchés ?

Pour répondre à ces questions, l'OCDE a élaboré **un cadre analytique fondé sur le cycle de vie et la chaîne de valeur des produits intelligents** (OCDE, 2021a). Ce cadre sert à révéler les lacunes dans la gestion du risque de sécurité numérique des produits intelligents, ainsi que les facteurs et les acteurs qui en portent la responsabilité. Il apparaît ainsi que diverses lacunes peuvent apparaître à différents stades du cycle de vie des produits.

- Si le processus de développement n'a pas été conforme aux meilleures pratiques du secteur, propres à garantir la « sécurité dès la conception », les produits intelligents peuvent comporter de nombreuses vulnérabilités. Les délais de commercialisation étant un facteur très important pour de nombreux acteurs de l'offre, il est fréquent que le mot d'ordre soit « produire d'abord, corriger plus tard ».
- Dans d'autres cas, le niveau de sécurité numérique d'un produit, jugé suffisant au moment de sa mise sur le marché, peut diminuer au fil du temps si les vulnérabilités nouvellement découvertes ne sont pas corrigées correctement, c'est-à-dire par le développement et la diffusion en temps utile de mises à jour de sécurité. En l'absence de mécanismes de mise à jour du produit, ou de traitement efficace des vulnérabilités par les acteurs de l'offre, par exemple par des politiques de divulgation des vulnérabilités et des mises à jour de sécurité automatiques, il est possible que des failles apparaissent.
- Les produits intelligents tendent à devenir moins sûrs avec le temps dans la mesure où leurs vendeurs cessent de proposer des mises à jour de sécurité au motif que les produits sont désormais en fin de vie. Or, l'attaque de sécurité numérique WannaCry nous l'a appris, de nombreux produits continuent d'être utilisés après avoir atteint leur fin de vie. Ces écarts entre fin de vie et fin d'utilisation montrent combien les facteurs économiques, et non pas les seuls facteurs techniques, contribuent au niveau de sécurité numérique insuffisant de nombreux produits intelligents.

À cela s'ajoute qu'il peut être difficile d'allouer la responsabilité du manque de sécurité numérique. Les chaînes de valeurs des produits intelligents sont mondiales, complexes et opaques. La découverte, en 2018, des vulnérabilités Spectre et Meltdown, qui touchaient les microprocesseurs, a révélé que les vulnérabilités de composants pouvaient affecter un large éventail de produits finis. Les vendeurs de ces produits finis ne sont pas nécessairement les mieux à même de fournir des mises à jour s'ils ne sont pas responsables de la couche de code défaillante. L'OCDE, dans son rapport (2021a), propose par conséquent l'utilisation de la notion de « responsables du code », plutôt que celle de vendeur, pour faciliter l'identification des parties responsables et amener davantage de clarté dans l'allocation des responsabilités.

Le rançongiciel WannaCry (2017)

Le logiciel malveillant WannaCry, qui a fait son apparition en mai 2017, visait les ordinateurs fonctionnant avec un système d'exploitation Microsoft Windows. Il s'appuyait sur EternalBlue et DoublePulsar, deux exploits dont on suppose qu'ils avaient été développés par la NSA (*United States' National Security Agency*) puis divulgués par le groupe de pirates « Shadow Brokers » en avril 2017. WannaCry était un rançongiciel : il chiffrait l'ensemble des données présentes sur les ordinateurs infectés, les rendant ainsi totalement inaccessibles jusqu'au versement d'une rançon en Bitcoin aux auteurs de l'attaque.

En avril 2017, soit plus d'un mois avant l'attaque, Microsoft avait publié une mise à jour de sécurité destinée à corriger les vulnérabilités qui allaient être exploitées plus tard par WannaCry. Cependant, cette mise à jour n'a été publiée que pour les versions de Windows pour lesquelles Microsoft assurait un suivi commercial à l'époque, c'est-à-dire Windows Vista et Windows 7, mais non, par exemple, pour Windows XP et Server 2003 qui avaient atteint leur fin de vie. Pour autant, ces versions obsolètes étaient encore utilisées par de nombreuses organisations relativement peu matures dans le domaine du numérique, des petites et moyennes entreprises (PME) et des établissements médicaux, par exemple. Le 13 mai, le lendemain du début de l'attaque, Microsoft a publié en urgence une mise à jour de sécurité pour ces versions de son système d'exploitation qu'elle ne prenait plus en charge. En l'espace de quelques jours seulement, le virus a infecté 200 000 ordinateurs dans plus de 150 pays, sans aucune interaction avec les utilisateurs. De nombreuses organisations et entreprises, dans les pays de l'OCDE, ont été victimes de WannaCry, dont Renault, Honda, Boeing et le NHS au Royaume-Uni. Elles ont été infectées parce qu'elles n'avaient pas installé les mises à jour de sécurité fournies par Microsoft, ou parce qu'elles continuaient d'utiliser des versions de Windows arrivées en fin de vie.

Le virus a gravement perturbé le fonctionnement d'hôpitaux, d'usines et de chaînes de production. Les estimations du préjudice total causé par cette attaque vont de plusieurs centaines de millions à plusieurs milliards d'euros. Ce préjudice résulte, pour partie, de l'impossibilité, pour les organisations visées, de retrouver un fonctionnement normal avant plusieurs semaines, du coût du nettoyage, de la mise à jour ou du remplacement des systèmes informatiques compromis, et de l'atteinte portée à leur image de marque. En 2018, le fabricant de semi-conducteurs TSMC a dû mettre à l'arrêt ses chaînes de production plusieurs jours durant en raison d'un virus qui présentait des similitudes avec WannaCry. Quelques-unes des organisations victimes de WannaCry pouvaient être considérées comme des « utilisateurs courants », c'est-à-dire qu'elles avaient par rapport à d'autres une moindre expérience du numérique, souvent en raison d'un manque de personnel compétent ou de ressources financières à consacrer à la sécurité numérique (par exemple dans le secteur médical). D'autres, en revanche, étaient des structures d'envergure mondiale, numéro un de leur secteur (par exemple, dans les transports ou l'automobile). C'est là la preuve que la gestion dynamique du risque de sécurité numérique, et notamment l'application des correctifs et le traitement du décalage entre fin de vie et fin d'utilisation, est un problème clé qui concerne toutes les parties prenantes au-delà des PME, des consommateurs et des autres utilisateurs courants.

Source : OCDE, 2021a.

Le manque de sécurité numérique tient souvent à des facteurs économiques

Afin de comprendre pourquoi le code est vulnérable, **l'OCDE, dans son rapport d'analyse en profondeur, s'attarde sur** trois études de cas : i) les smartphones et les ordinateurs de bureau ; ii) l'IdO grand public ; iii) les services infonuagiques (OCDE, 2012a).

Il ressort de ces études de cas que les mesures techniques, comme l'authentification multifactorielle ou les mises à jour automatiques, sont essentielles au renforcement de la sécurité numérique des produits. Or **l'adoption à grande échelle de mesures techniques efficaces, tant du côté de l'offre que de celui de la demande, est souvent contrariée par des facteurs économiques, les incitations qui émanent du marché ne suffisant généralement pas à l'adoption de comportements optimums**.

D'importantes asymétries d'information empêchent souvent les utilisateurs finals – et en premier lieu les utilisateurs courants que sont, par exemple, les PME et les consommateurs – de prendre des décisions éclairées quant aux produits dont ils font l'acquisition. Le recours en masse aux outils de télétravail durant la pandémie de COVID-19 est l'illustration à grande échelle de ce manque de transparence, dans la mesure où bien des consommateurs ont été dans l'impossibilité de comparer ces outils au regard du risque de sécurité numérique.

À cela s'ajoute que des **externalités négatives** conduisent souvent les producteurs et les utilisateurs de produits intelligents à négliger la gestion du risque de sécurité numérique, ce qui permet à des individus malveillants de créer des *botnets* et de lancer des attaques par déni de service distribué, dont beaucoup ont une dimension internationale. Le logiciel malveillant Mirai, qui a réussi à réunir des millions d'objets connectés au sein d'un *botnet* en 2016, illustre le rôle clé de ces externalités négatives et leur effet sur la sécurité numérique des produits.

De manière plus générale, **il y a une méconnaissance du risque de sécurité numérique et les incitations du marché sont en décalage.** Pour les acteurs de l'offre, le décalage entre fin de vie et fin d'utilisation peut être corrigé en incitant les utilisateurs finals à acheter de nouveaux produits (qui pourront être dotés de caractéristiques techniques ou d'une architecture plus performantes du point de vue de la sécurité), lesquels utilisateurs finals ne voient toutefois pas nécessairement l'intérêt de dépenser de l'argent pour acquérir des produits plus récents et ne mesurent souvent pas le danger. Sachant que des milliards d'appareils connectés arriveront en fin de vie au cours de la décennie à venir, la perspective de voir émerger un « internet des objets oubliés » a de quoi préoccuper les pouvoirs publics.

Principaux éclairages utiles aux décideurs publics

On trouvera ci-après les principales conclusions des études de cas (smartphones et ordinateurs ; IdO grand public ; services infonuagiques).

- Les produits connectés grand public présentent un manque important de sécurité numérique à chaque étape de leur cycle de vie.

- Les trois études de cas révèlent un manque très significatif de sécurité durant la vie commerciale des produits (mauvaises configurations ou déploiement incomplet des mises à jour de sécurité).
- Le décalage entre fin de vie et fin d'utilisation est considérable pour des produits comme les objets connectés et les smartphones, mais moindre pour les services, notamment infonuagiques.
- Le manque de sécurité numérique durant les phases de conception et de développement est particulièrement prononcé sur les marchés émergents et fragmentés comme celui de l'IdO, où les lignes directrices et normes techniques propres à garantir la « sécurité dès la conception » et la « sécurité par défaut » sont nombreuses, mais rarement utilisées. Un tel manque de sécurité numérique est moins fréquents sur des marchés plus matures et plus concentrés (ainsi ceux des smartphones et des ordinateurs).

Tout au long de l'analyse développée dans son rapport, l'OCDE met en lumière quelques enseignements clés à l'intention des responsables de la formulation des politiques publiques :

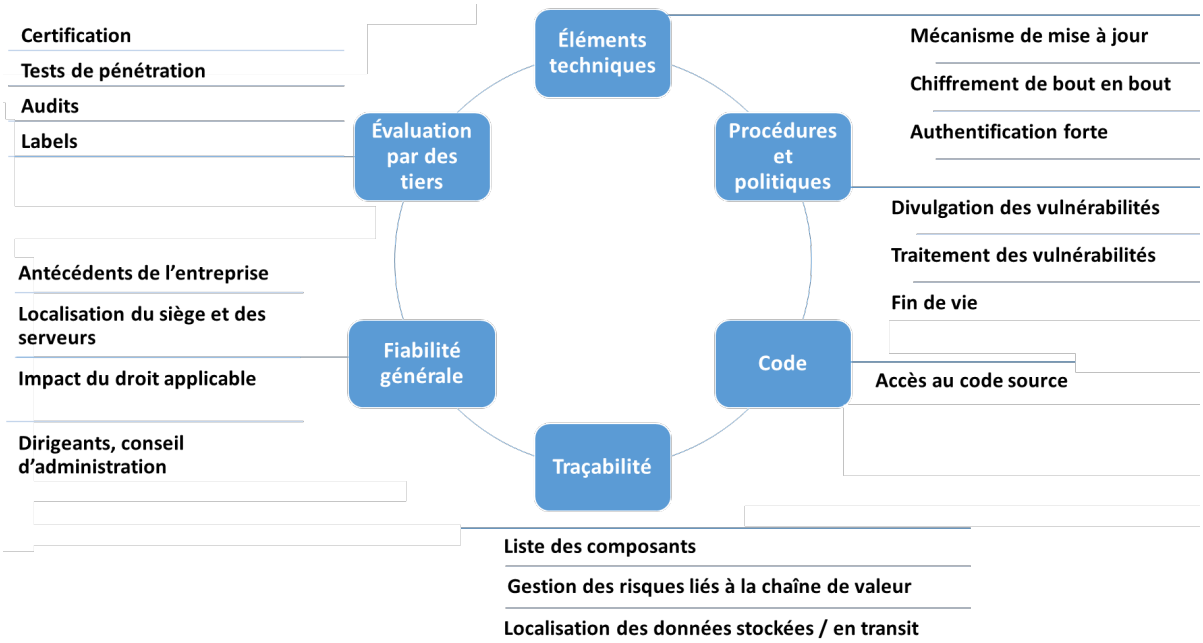
- La sécurité numérique des produits doit être considérée davantage comme un spectre que comme un concept binaire opposant le sûr au non sûr. Un produit peut être « suffisamment sûr » pour un contexte d'utilisation donné, mais offrir un niveau de sécurité numérique insatisfaisant dans d'autres situations.
- La gestion de la sécurité numérique des produits va au-delà des aspects techniques : de nombreux facteurs économiques entrent en jeu, et il y a peu de chances que les forces du marché corrigent d'elles-mêmes le manque de sécurité numérique.
- La sécurité numérique est un domaine dynamique. Au-delà du principe de sécurité dès la conception, les produits intelligents doivent faire l'objet de mises à jour tout au long de leur cycle de vie.
- Les acteurs de l'offre pourraient être encouragés à traiter les vulnérabilités de façon plus efficace, par exemple en adoptant des politiques de divulgation des vulnérabilités et en fournissant des mises à jour de sécurité automatiques (OCDE, 2021c).
- Il n'y a ni solution universelle ni panacée. La sécurité numérique des produits est une question complexe, qui recouvre de nombreux secteurs, marchés, catégories de produits et domaines d'action des pouvoirs publics.

Six principes de haut niveau pour renforcer la sécurité numérique des produits

Face à ces enjeux, l'OCDE, dans son rapport dédié à l'analyse des politiques publiques (2021b), énonce **six principes de haut niveau** à même de guider les décideurs et les parties prenantes dans leur action en faveur du renforcement de la sécurité numérique des produits. Ces principes sont les suivants :

- **Accroître la transparence et le partage de l'information**, pour lutter contre les asymétries d'information. On trouvera dans le Graphique 1 une vue d'ensemble des six principaux domaines dans lesquels une plus grande transparence permettrait aux consommateurs de prendre des décisions plus éclairées et d'évaluer les risques de manière plus effective. On y voit par ailleurs qu'outre les éléments techniques des produits (comme la possibilité d'effectuer des mises à jour), d'autres aspects gagneraient à une plus grande transparence, notamment les processus et politiques adoptés par les acteurs de l'offre (par exemple, au sujet de la fin de vie des produits), la traçabilité de leurs composants et l'évaluation par les tiers.
- **Sensibiliser les parties prenantes et les autonomiser**, à commencer par les utilisateurs finals et les chercheurs en sécurité, eu égard au rôle essentiel qui est le leur dans la gestion du risque de sécurité numérique.
- **Faire respecter les devoirs de responsabilité et de diligence** des acteurs de l'offre, pour corriger les externalités et réajuster les incitations émanant du marché. Le devoir de diligence peut se subdiviser en cinq principes subalternes : la sécurité dès la conception, la sécurité par défaut, la gestion dynamique de la sécurité numérique, la sécurité numérique de l'organisation et les politiques responsables relatives à la fin de vie, qui peuvent répondre aux problèmes tenant à la durée de prise en charge et à la réparabilité des produits.
- **Renforcer la coopération** entre les parties prenantes, les organisations publiques ainsi qu'au niveau international dans une optique d'amélioration de la sécurité numérique des produits.
- **Promouvoir l'innovation et la concurrence**, pour libérer le potentiel positif des acteurs du marché.
- **Traiter la sécurité numérique de manière proportionnée, selon une approche fondée sur la gestion du risque**, pour tenir compte de sa complexité. Les exigences de sécurité indiquées ou utiles sur un marché donné ou pour une catégorie de produits donnée ne conviendront pas nécessairement ailleurs.

Graphique 1 Domaines d'intervention à considérer pour renforcer la transparence et le partage d'information sur les produits



Source : OCDE, 2021b.

Guide pratique : « Des politiques intelligentes pour les produits intelligents »

À produits intelligents, politiques de sécurité numérique intelligentes. Les responsables publics pourraient aborder la politique de sécurité numérique tout comme les ingénieurs logiciels abordent le développement des produits : selon un processus itératif et centré sur l'utilisateur final. Des mécanismes légers, volontaires, pourraient être mis en place dans un premier temps. Si ces mécanismes se révèlent inopérants, ou si les industriels et les consommateurs – autrement dit les « utilisateurs finals » des politiques publiques – n'y sont pas réceptifs, alors les décideurs pourraient envisager de recourir à des instruments réglementaires plus contraignants, tels que des obligations *ex ante* et des mécanismes *ex post*. Les ingénieurs logiciels peuvent eux aussi s'inspirer des responsables de la formulation des politiques publiques. La prise en compte des intérêts des différents groupes de parties prenantes, des conséquences que leurs décisions entraînent pour autrui et des perspectives à long terme devrait faire partie intégrante du cycle de développement des produits intelligents.

L'opposition entre intervention des pouvoirs publics et laisser-faire est de plus en plus considérée comme trop simpliste pour rendre compte de toute la diversité des options qu'il est possible de prendre afin de renforcer la sécurité numérique des produits. On peut lire dans un rapport publié dernièrement aux États-Unis : « le statu quo ne nous permet pas d'avancer » (Cyberspace Solarium Commission, 2020). Les responsables de la formulation des politiques publiques ont de nombreux instruments à leur disposition, des campagnes de sensibilisation aux partenariats multipartites en passant par les dispositifs de labélisation et les exigences réglementaires. Il convient de noter que ces différents instruments ne s'excluent pas mutuellement, et qu'il n'existe ni panacée ni solution universelle. **Toute stratégie de renforcement de la sécurité numérique des produits supposera vraisemblablement la combinaison de différents instruments pour atteindre au maximum d'efficacité.**

La boîte à outils présentée dans le rapport (OCDE, 2021b) est destinée à donner aux pouvoirs publics les moyens de favoriser l'adoption des principes de haut niveau, l'accent étant ici mis davantage sur la manière d'agir plutôt que sur ce qu'il y a lieu de faire. Il y est question des nouvelles tendances de l'action des pouvoirs publics, illustrées d'exemples choisis parmi les pays de l'OCDE. La boîte à outils a été conçue de telle sorte que chaque administration puisse s'appuyer sur les instruments les plus indiqués au regard de la culture, de l'histoire et du type de gouvernement du pays. Les voies d'action considérées sont les suivantes :

- **Accroître la sensibilisation des utilisateurs courants et développer les compétences dans le domaine de la sécurité numérique**, afin d'augmenter le nombre d'utilisateurs avancés, dotés d'une réelle expertise, est la première des mesures à prendre pour renforcer la sécurité numérique des produits. Si importantes soient-

elles, les campagnes de sensibilisation ne sauraient toutefois suffire face aux enjeux économiques dont il a été question plus haut.

- **Au-delà de leur rôle de régulateurs, les pouvoirs publics sont aussi des agents économiques. En tant que tels, ils peuvent tirer parti de leur pouvoir d'achat et, par leur exemple,** influencer le comportement d'autres parties prenantes. Ils peuvent se servir de la commande publique pour inciter les acteurs de l'offre à faire certifier la sécurité numérique des produits intelligents et devraient s'efforcer eux-mêmes de se conformer aux principes qu'ils demandent souvent aux autres d'observer – par exemple lorsqu'il s'agit de corriger en temps opportun les vulnérabilités.
- **Les normes techniques et les cadres volontaires sont d'une importance primordiale**. Définis par les pouvoirs publics ou par la communauté multipartite, ces normes et cadres donnent aux acteurs de l'offre des orientations claires qu'ils peuvent adapter aux spécificités des marchés ou des catégories de produits. Cependant, sur les marchés où les externalités et les asymétries d'information sont importantes, il est probable que les directives d'application facultative soient peu suivies.
- Les **labels** seraient susceptibles d'inciter les acteurs de l'offre à adhérer à ces normes et cadres, et contribueraient ainsi à réduire les asymétries d'information. En novembre 2020, l'Allemagne, la Finlande et le Japon avaient lancé, ou envisageaient de lancer, un programme de labels sur la sécurité numérique applicables à certaines catégories de produits, comme les produits connectés grand public ou les routeurs. Il faut toutefois prendre en compte la possibilité d'une certaine lassitude des consommateurs et d'une adoption insuffisante par les professionnels du secteur lorsque l'on envisage ce genre d'initiatives.
- **Les mécanismes *ex post* sont très prometteurs, néanmoins leur efficacité reste à apprécier de façon plus complète**. Quoique le code soit omniprésent, les produits intelligents sont relativement récents et n'entrent pas nécessairement dans les catégories juridiques du XXe siècle. L'application du droit de la responsabilité civile, de même que l'assurance et la prise sous garantie ne vont pas sans difficulté en ce qui concerne les produits intelligents et nécessiteront sans doute un réexamen des cadres en vigueur en vue de les adapter aux dynamiques et aux chaînes de valeurs complexes qui caractérisent l'économie numérique.
- **Enfin, certains pays de l'OCDE penchent vers l'élaboration de règlements plus stricts afin d'améliorer la sécurité numérique des produits.** Qu'il s'agisse de prescriptions techniques ou de principes de haut niveau, ces règlements *ex ante* pourraient contribuer très efficacement au réajustement des incitations émanant du marché et assurer l'observation de leur devoir de diligence par les acteurs de l'offre. Cela étant, le risque existe d'une utilisation disproportionnée de ce genre d'obligations, et une législation mal préparée pourrait devenir rapidement obsolète ou inapplicable. L'OCDE dans son rapport (2021b) s'intéresse aux atouts et inconvénients de ces obligations, et apporte des éclairages très utiles au sujet, par exemple, de la nécessaire neutralité technologique, de la proportionnalité et de la coopération internationale.

Il est essentiel de renforcer la coopération internationale

Il est indispensable que les responsables de la formulation des politiques publiques appréhendent **dans sa globalité** la sécurité numérique des produits. Les pouvoirs publics ont aujourd'hui l'occasion de concevoir des politiques intelligentes pour les produits intelligents, de prévenir au lieu de guérir, et de façonner pour la sécurité numérique des produits un cadre d'action à visée prospective.

À cet égard, **la coopération internationale apparaît comme l'une des clés du succès**. Les responsables de la formulation des politiques publiques auraient intérêt à **tirer des leçons des réussites et des difficultés rencontrées par les autres pays** et à s'inspirer des mesures qui ont d'ores et déjà fait leurs preuves ailleurs.

La coopération internationale est aussi irremplaçable pour garantir l'interopérabilité des stratégies nationales, éviter la prolifération des normes et limiter les incohérences entre les juridictions, susceptibles de freiner considérablement le développement de l'économie numérique.

Pour aller plus loin

OCDE (2021a), « Understanding the digital security of products: an in-depth analysis », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris, https://doi.org/10.1787/cd9f9ebc-en.

OCDE (2021b), « Enhancing the digital security of products: a policy discussion », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris, https://doi.org/10.1787/cd9f9ebc-en.

OCDE (2021c), « Encouraging vulnerability treatment: overview for policy makers », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris, https://doi.org/10.1787/0e2615ba-en.

OCDE (2020a), « Risques liés à la sécurité numérique pendant la crise du coronavirus (COVID-19) », *Les réponses de l'OCDE face au coronavirus (COVID-19)*, Éditions OCDE, Paris, https://doi.org/10.1787/ba8e6d3a-fr.

OCDE (2020b), « Seven lessons learned about digital security during the COVID-19 crisis », *Les réponses de l'OCDE face au coronavirus (COVID-19)*, Éditions OCDE, Paris, https://doi.org/10.1787/e55a6b9a-en.

Site web

https://oe.cd/security

Direction de la science, de la technologie et de l'innovation

Cette série de Notes sur les politiques a été conçue pour mettre à la disposition d'un public plus large certaines des études destinées à un usage interne à l'OCDE.

Les commentaires sur cette Note sur les politiques sont les bienvenus et peuvent être adressés à l'OCDE, 2 rue André Pascal, 75775 Paris Cedex 16, France, ou par courriel à l'adresse : digitalsecurity@oecd.org.

Merci de citer cette Note comme suit : « Des politiques intelligentes pour les produits intelligents », *Note sur les politiques de la Direction de la science, de la technologie et de l'innovation*, OCDE, Paris, www.oecd.org/fr/numerique/politiques-intelligentes-produits-intelligents.pdf.

Pour rester au fait de l'actualité STI, abonnez-vous à la lettre d'information : **OECD News on Innovation, Science, Technology and Industry**, http://www.oecd.org/fr/sti/news.htm.

@OECDInnovation

https://oe.cd/security

Contact : digitalsecurity@oecd.org