ÉCONOMIE DE LA CYBERSÉCURITÉ ET BÉNÉFICES DU RGPD

Analyse économique

Juin 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Introduction

En tant qu'instrument de régulation garantissant la protection des données personnelles, le RGPD soumet le traitement des données personnelles à des obligations de sécurité :

- **Il s'agit de l'obligation de mise en place de mesures garantissant un niveau de sécurité adapté** contenue dans l'article 32 ; et
- **de l'obligation de notifier l'autorité compétente s'il y a eu une violation de données personnelles** ou, en cas de risque élevé, **de communiquer la violation aux personnes concernées**, dans les articles 33 et 34.

L'économie de la cybersécurité permet notamment d'expliquer les décisions d'investissement en cybersécurité comme le fruit d'un arbitrage entre les coûts de l'investissement dans la cybersécurité et les bénéfices attendus de cet investissement. La littérature économique montre que ces décisions ne permettent pas toujours de mener au niveau de cybersécurité qui serait le plus bénéfique à la société. En effet, il y a de nombreuses défaillances de marché (Anderson et Moore, 2007 ; Cordes, 2011) liées au caractère profondément interdépendant des entreprises et des individus dans le cadre de la cybersécurité. Le cybercrime n'a pas seulement un impact sur l'entreprise touchée mais aussi sur ses clients et potentiellement sur les autres entreprises qui sont exposées à un risque de contagion.

En économie, ces impacts sont appelés des **externalités négatives** et elles sont particulièrement problématiques car une entreprise pourrait les mettre en balance avec ses propres enjeux financiers. Dans ce cadre, les entreprises ont tendance à ne pas optimiser leurs investissements dans la cybersécurité. La réglementation permet de palier à ses déséquilibres en faisant en sorte que les entreprises prennent mieux en compte les risques du cybercrime et ajustent leurs décisions d'investissement en cybersécurité en conséquence.

L'impact du RGPD dans la cybersécurité ne se limite pas à ce qui est appelé en économie une « internalisation de l'externalité », mais comprend aussi l'irrationalité et la mauvaise information (Lowenstein et al., 2013) des individus par rapport au risque cyber. Ainsi, la sensibilisation du public et des entreprises aux enjeux de la cybersécurité et le travail d'accompagnement de la CNIL en lien avec l'écosystème cyber (ANSSI, etc.) a aussi eu un impact bénéfique sur la société.

Ce travail fait suite à la précédente publication de la CNIL sur l'impact économique du RGPD[1], dans laquelle la CNIL appelait chercheurs et praticiens à explorer les bénéfices du RGPD. La CNIL entame ici un premier travail exploratoire pour mettre en lumière une partie des bénéfices du RGPD pour la société par son impact positif sur la prévention des crimes en ligne.

Ce qu'il faut retenir

Protection des données à caractère personnel et cybersécurité sont deux enjeux indissociables

La théorie économique montre que l'autorégulation des entreprises mène à un niveau insuffisant d'investissement dans la cybersécurité. Le RGPD permet de combler ces lacunes, donnant naissance à des bénéfices économiques du fait de l'obligation de sécurité.

Il est possible d'illustrer ces gains par une étude de cas sur l'usurpation d'identité, qui estime que le RGPD a permis des gains entre 90 et 219 millions d'euros en France, via le seul effet de la communication des violations de données aux personnes concernées. 82 % de ces gains sont perçus par les entreprises.

[1] « L'impact économique du RGPD, 5 ans après », CNIL : https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres

I. Un sous-investissement des entreprises dans la protection des données

1. Les violations de données personnelles : une asymétrie d'information entre l'entreprise et ses clients

Lorsqu'il y a une violation de données personnelles traitées par une entreprise, les clients ou salariés peuvent subir des conséquences négatives. Par exemple, les données obtenues par les criminels peuvent être utilisées afin d'usurper l'identité des individus. **En l'absence de réglementation, cette entreprise ne serait pas contrainte de révéler si une cyberattaque a eu lieu ou non.**

Certaines raisons économiques peuvent inciter les entreprises à être transparentes, car il y a un risque que la faille soit dévoilée par un lanceur d'alerte, ce qui serait catastrophique pour l'image de l'entreprise et sur son niveau d'investissement en cybersécurité. Cependant, ce raisonnement semble moins applicable lorsqu'il s'agit de failles de sécurité de grande ampleur, les inconvénients d'une transparence étant supérieurs aux avantages, au regard du nombre de personnes potentiellement exposées. Pour ces entreprises, la stratégie optimale serait alors de dévoiler une cyberattaque peu importante mais de ne pas révéler une fuite de données conséquente (Amir et al., 2018).

Dans ce cas, **les clients subissent les conséquences négatives de l'obtention de leurs données personnelles par des criminels sans pouvoir savoir quelle entreprise a été à l'origine de la fuite. L'entreprise responsable ne subira pas de conséquences négatives en termes de réputation. Cette situation entraîne un sous-investissement de la part des entreprises dans la cybersécurité** puisqu'une partie des dommages causés par les attaques n'affecte pas l'entreprise (il y a présence d'une asymétrie d'information) (Garcia, 2013).

En économie, l'asymétrie d'information est considérée comme une situation où deux personnes n'ont pas le même degré d'information sur un marché. Par exemple, sur le marché de l'occasion, il y a asymétrie d'information car le vendeur est mieux informé que l'acheteur sur la qualité réelle de ce qu'il vend. Ces situations sont des « défaillances de marché », soit des situations où la coordination des individus par les marchés mène à une situation sous-optimale du point de vue de l'efficacité économique.

S'il n'y avait pas d'asymétrie d'information, c'est-à-dire si les entreprises étaient contraintes à être transparentes, les individus pourraient savoir quelle est l'entreprise à l'origine de la fuite afin d'éviter de lui confier leurs données dans le futur (Nieuwesteeg et Faure, 2018). Ainsi, l'enjeu d'investir en cybersécurité deviendrait plus important pour les entreprises afin d'éviter une fuite de données personnelles.

Des travaux empiriques ont montré que suite à des communications de fuites de données personnelles, la valeur des entreprises en Bourse baisse (Acquisti et al., 2006 ; Bose et Leung, 2014). Ces conséquences négatives sont généralement faibles, mais peuvent être particulièrement fortes dans les rares cas où la cyberattaque est médiatisée (Martin et al., 2017). C'est un risque dissuasif pour les entreprises qui les responsabilise vis-à-vis des dommages occasionnés à leurs clients et salariés. Cette responsabilisation s'observe par une hausse des investissements en cybersécurité à la suite de la mise en œuvre de l'obligation de communication des violations de données (Murciano-Goroff, 2019 ; Miller et Tucker, 2011). Aussi, lorsqu'une entreprise est au cœur d'une affaire de cyberattaque, elle peut avoir tendance à engager des experts en cybersécurité pour rassurer les investisseurs et les consommateurs (Bana et al., 2022). Les investissements accrus en cybersécurité permettant de réduire la probabilité qu'une cyberattaque réussisse (Gandal et al., 2023), les communications de violations de données permettent donc de réduire le nombre de violations de données personnelles ayant des conséquences négatives sur les individus. Cette réduction a été estimée à deux reprises par son impact sur les usurpations d'identité : un premier article a estimé que les communications de violations de données causent une baisse de 6,1 % du nombre d'usurpations d'identité (Romanosky et al., 2011), alors que d'autres auteurs estiment plus récemment une baisse de 2,5 % (Bisogni et Asghari, 2020).

La communication de violation de données personnelles, rendue obligatoire sous peine de sanctions pécuniaires par l'article 34 du RGPD lorsqu'un risque élevé pèse sur les personnes concernées, est donc essentielle pour lutter contre l'asymétrie d'information affectant la cybersécurité.

Cependant, la simple communication de violation de données personnelles ne peut suffire à traiter la totalité du problème de sous-investissement en cybersécurité. Tout d'abord, s'il n'y a pas d'alternative équivalente au service proposé par l'entreprise, celle-ci ne considérera pas crédible la possibilité que des utilisateurs se

détournent de son service. C'est le cas pour certains acteurs dominants comme, par exemple, les réseaux sociaux réunissant de nombreux utilisateurs. En effet, pour un individu, quitter un réseau social est particulièrement coûteux puisqu'il y a une perte de contact avec les autres utilisateurs du réseau (Beknazar-Yuzbashev et al., 2024). Il est donc peu probable qu'un utilisateur change de réseau pour des raisons de cybersécurité (Qian et al., 2019 ; Chen, 2016), ce qui explique la nécessité d'ajouter également des standards de sécurité.

2. L'interdépendance des entreprises pour la cybersécurité comme source de défaut de coordination

Une autre justification à l'édiction de standards de sécurité est à trouver dans les interdépendances des entreprises dans leurs décisions d'investissement en cybersécurité. L'aspect le plus évident de cette interdépendance est le risque de contagion des cyberattaques. En 2017, le logiciel malveillant WannaCry s'est répandu d'ordinateur en ordinateur comme un virus jusqu'à prendre l'ampleur d'une pandémie informatique ayant coûté plusieurs milliards de dollars.

Un autre exemple illustratif sont les *botnets*, où des ordinateurs infectés par des pirates sont ensuite utilisés par d'autres pirates pour plusieurs usages malveillants tels que : envoyer des *spams*, faire de l'hameçonnage (*phishing*), des attaques par déni de service (DDoS), etc. Voir son ordinateur infecté a donc un impact négatif sur d'autres personnes.

Lorsqu'une entreprise décide d'investir en cybersécurité, elle vise à limiter les dégâts du cybercrime sur sa propre activité, mais elle n'investit pas en prenant en compte comment le risque de contagion pourrait affecter les autres entreprises (Fedele et Roner, 2022). Pour limiter l'impact du cybercrime sur l'ensemble de l'écosystème de l'entreprise, il faudrait alors prendre en compte ce risque de contagion lors des décisions d'investissement en cybersécurité, ce qui mènerait à un niveau d'investissement plus élevé (Böhme, 2012).

C'est une situation où il y a des externalités positives aux investissements en cybersécurité. Un exemple d'externalité positive est l'apiculture, puisque le producteur a un impact écologique positif du fait de son activité. Lorsqu'une entreprise investit dans la cybersécurité, cela ne bénéficie pas qu'à elle mais également aux autres entreprises.

Les entreprises sont aussi interdépendantes car une cyberattaque n'a pas uniquement un impact sur la valorisation boursière de l'entreprise mais également sur celle de ses concurrents. Il y a deux types d'impact possibles : un effet « débordement » et un effet « compétition ». L'effet compétition est intuitif : lorsqu'une entreprise subit une violation de données, ses utilisateurs risquent de vouloir se tourner vers ses concurrents. La fuite des données d'une entreprise a un impact positif sur ses concurrents. L'effet débordement est plus surprenant, puisqu'il représente la situation où la fuite des données d'une entreprise a un impact négatif sur ses concurrents. Cette situation tient au fait qu'une cyberattaque pousse les individus à reconsidérer à la baisse le niveau de sécurité de l'ensemble du secteur auquel appartient l'entreprise si elle a subi une cyberattaque (Kelton et Pennington, 2020).

Entre ces deux effets contraires, celui l'emportant sur l'autre est déterminé par l'ampleur de la violation de données. Lorsque les fuites sont de grande ampleur, les consommateurs ont tendance à considérer le risque suffisamment élevé pour aller vers la concurrence, l'effet compétition l'emporte. Lorsque la fuite de données est d'ampleur plus faible, il y a très peu de défections de clients, cependant le phénomène de « culpabilité par association » subsiste et l'effet débordement l'emporte (Martin et al., 2017). La majorité des fuites de données personnelles ne sont pas de grande ampleur et sont relativement peu médiatisées. Ainsi, dans la majorité des cas, les fuites de données ont principalement un effet débordement et affectent de manière négative toutes les entreprises du secteur concerné par la violation de données (Haislip et al., 2019). Cela décourage l'investissement en cybersécurité puisque même si une firme met en place les mesures de sécurité pour limiter l'impact des cyberattaques, elle risque quand même d'avoir mauvaise réputation par association avec les maillons faibles du secteur (Nagurney et Nagurney, 2015).

L'ajout de standards de sécurité dans le RGPD (article 32) bénéficie donc à l'ensemble des entreprises puisqu'il est optimal d'être coordonné à un niveau élevé de cybersécurité. Cette coordination n'est pas possible en l'absence de réglementation puisque des entreprises peuvent profiter du niveau de protection élevé du secteur sans en payer les coûts, par un effet de « passager clandestin », de la même manière qu'on peut profiter de la couverture vaccinale par exemple (Su et al., 2023).

L'économiste Hal Varian a notamment démontré dans son papier « *System Reliability and Free Riding* » (2001) que l'on peut modéliser ce cadre comme celui d'**un bien public**. Un bien public est un bien non rival et non excluable. Un bien non rival est un bien qui peut être consommé par plusieurs personnes à la fois sans que

cela affecte les autres (par exemple : une émission de télévision). Un bien non excluable est un bien qu'on ne peut pas empêcher les gens de consommer (par exemple : l'oxygène ou l'éclairage public).

Ici, le bien public n'est pas la solution de cybersécurité en tant que telle, mais l'environnement de résilience informatique créé par les investissements en cybersécurité. Ces biens publics font nécessairement l'objet d'un sous-investissement lorsqu'ils sont financés par des acteurs privés sans mesure coercitive pour punir la non-participation.

L'interdépendance des entreprises est aussi extrêmement forte dans le cadre des relations de sous-traitance. Lorsqu'une entreprise sous-traitante réalise un traitement pour le compte d'un responsable de traitement, la sécurité des données personnelles traitées par le responsable dépend également du niveau de sécurité du sous-traitant. Les dégâts d'une fuite de données vont principalement affecter le responsable de traitement. C'est le cas par exemple pour les cyberattaques de type « attaque de la chaîne logistique » où le cybercriminel essaye d'entrer par une entreprise d'une chaîne logistique ayant un niveau de cybersécurité plus faible pour pénétrer l'organisation cible. Dans le cadre de ces attaques, le maillon le plus faible de la chaîne détermine donc le niveau de sécurité de l'ensemble des acteurs de la chaîne logistique.

Or, du fait de l'asymétrie d'information, le sous-traitant connaît mieux le niveau de sécurité de ses systèmes d'information que le responsable de traitement. Dans ce scénario, le responsable de traitement ne peut pas être pleinement assuré que le sous-traitant maintient effectivement le niveau de sécurité déclaré, ce qui peut conduire le sous-traitant à négliger l'investissement en cybersécurité. L'article 27.3.c du RGPD établit la responsabilité juridique du sous-traitant en cas d'inadéquation du niveau de sécurité du traitement des données, ce qui pousse celui-ci à faire davantage attention à son niveau de cybersécurité.

3. Le rançongiciel comme un marché : la demande des entreprises affecte le coût des rançons

Le rançongiciel est un type de cyberattaque particulièrement connu. Le principe est qu'un virus informatique bloque l'accès aux données d'un individu ou d'une entreprise, à moins qu'une « rançon » soit payée.

Du point de vue du cybercriminel, comment déterminer le montant de la rançon ? Le montant de la rançon optimal est celui qui maximise les gains. Si la rançon est trop élevée, personne ne la paiera. *A contrario*, si la rançon est trop faible, les gains ne seront pas élevés. Choisir le montant optimal de la rançon implique donc pour le cybercriminel de prendre en compte la disposition à payer des individus.

La disposition à payer des individus forme une courbe de demande : plus le prix augmente, plus le nombre de personnes prêtes à payer diminue, c'est un mécanisme de marché.

Une conséquence nécessaire du mécanisme de marché est que plus le prix de la rançon est élevé, plus les individus sont lésés. En effet, si le prix est faible, alors un grand nombre d'individus récupéreront leurs données à bas prix. Si le prix est élevé, les individus payent moins souvent et donc perdent plus souvent leurs données, et ceux qui payent perdent davantage d'argent. En économie, les gains du consommateur (ici, les individus subissant un cybercrime) diminuent lorsque le prix augmente.

Or le prix à tendance à être élevé car la disposition à payer est très hétérogène. En se basant sur des données d'entretien, il est possible de distinguer les individus ayant une très forte disposition à payer et ceux ayant une disposition à payer faible. Économiquement, il est optimal pour les cybercriminels d'exploiter ceux qui ont une disposition à payer élevée et donc de fixer un prix élevé.

C'est en cela qu'il y a une nouvelle fois une externalité. Les individus et les entreprises qui ne prennent pas les mesures de cybersécurité appropriées se risquent à subir un rançongiciel, ce qui augmente la demande du point de vue du cybercriminel ainsi que le montant de la rançon, ce qui in fine impacte négativement la société (Hernandez-Castro et al., 2020). Cette externalité est source de sous-investissement dans des mesures telles que la sauvegarde informatique.

4. Quelle est l'ampleur du sous-investissement ?

En raison des très grandes difficultés d'obtenir des bases de données permettant d'étudier les investissements en cybersécurité, la fréquence et les impacts des cybercrimes, il est extrêmement difficile d'estimer la différence entre le niveau d'investissement en cybersécurité actuel et celui qui serait optimal.

Le modèle de Gordon et Loeb qui permet de déterminer le niveau d'investissement optimal pour les entreprises a été ajusté par ses auteurs pour montrer comment l'écart entre le niveau optimal d'investissement et le niveau

d'investissement des entreprises évoluait selon le niveau d'externalité (la part de dégât causé par le cybercrime non pris en compte par l'entreprise).

Tableau 1
Relation entre externalités et sous-investissement en cybersécurité dans le modèle Gordon-Loeb (2015)

Pourcentage d'externalité	Coût privé d'une cyberattaque	Niveau d'investissement optimal pour l'entreprise	Niveau d'investissement optimal pour la société	Pourcentage de sous-investissement
0 %	400 000 €	60 000 €	60 000 €	0 %
20 %	400 000 €	60 000 €	75 271 €	20,29 %
40 %	400 000 €	60 000 €	89 315 €	32,82 %
60 %	400 000 €	60 000 €	102 386 €	41,40 %
80 %	400 000 €	60 000 €	114 663 €	47,67 %
100 %	400 000 €	60 000 €	126 274 €	52,48 %
120 %	400 000 €	60 000 €	137 318 €	56,31 %
140 %	400 000 €	60 000 €	147 871 €	59,42 %
160 %	400 000 €	60 000 €	157 992 €	62,02 %
180 %	400 000 €	60 000 €	167 731 €	64,23 %
200 %	400 000 €	60 000 €	177 128 €	66,13 %

Gordon et Loeb montrent qu'à partir de leur modèle, une entreprise dont le coût privé d'une faille de cybersécurité est de 400 000 euros, devrait investir 60 000 euros dans la cybersécurité. Cependant, si 20 % des dégâts sont des externalités, alors le montant optimal à investir pour la communauté est de 75 000 euros. Si les externalités représentent deux fois le coût privé de l'entreprise, alors le montant optimal à investir pour la communauté est de 177 000 euros.

Il semble assez improbable, au vu des nombreuses externalités discutées précédemment, que la part d'externalité soit inférieure à 20 %. **Le niveau de sous-investissement des entreprises est donc probablement dans un intervalle situé entre 20 % et 66 %.**

À partir des données d'Eurostat, il est possible de constater que l'entrée en vigueur du RGPD a influencé la mise à jour des protocoles de cybersécurité par les entreprises françaises. L'enquête annuelle sur l'usage de l'IT dans les entreprises de l'UE d'Eurostat contient un volet sur la cybersécurité[2]. En 2015, 14,2 % des entreprises françaises comptant au moins 10 employés avaient actualisé leur protocole de cybersécurité au cours de l'année. Ce chiffre est monté à 18,3 % en 2019, avant de redescendre à 12,1 % en 2022. Ces données montrent donc que le RGPD a permis de lutter contre le sous-investissement dans la cybersécurité.

[2] « *Security policy, measures, risks and staff awareness by NACE Rev.2 activity* » [en anglais], 2024, Eurostat. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ran2/default/table?lang=en

II. Étude de cas : la communication de violation de données et l'usurpation d'identité

Pour donner une illustration du type de gains permis par le RGPD, il est possible d'estimer dans cette partie l'impact qu'a eu la communication de violation de données (art. 34) sur les usurpations d'identité. Seule une part relativement faible des gains est étudiée ici puisque ne sont évoqués que les cybercrimes les plus connus (Malware, DDoS) ; de plus, l'impact de la présence des DPO (art. 37) ou bien celui de l'instauration de standards de cybersécurité (art. 32) n'est pas évoqué.

1. Impact direct

Les études empiriques en cybersécurité font face à de nombreuses difficultés liées au manque de données disponibles pour étudier le phénomène (Moore et al., 2019). Par exemple, l'évaluation du coût du cybercrime est sujet à une variété d'estimations. Ainsi, en France, Statista estime le coût du cybercrime à 119 milliards d'euros [3] alors que le cabinet Astères estime ce coût à 2 milliards en 2022[4]. Ces difficultés ont poussé la Commission européenne à développer le projet E-crime, qui a notamment pour objectif d'estimer avec rigueur scientifique le coût du cybercrime. La CNIL s'appuie sur ces travaux afin d'illustrer les gains économiques liés aux investissements en cybersécurité favorisés par le RGPD.

La présente étude limite son analyse à l'impact sur les usurpations d'identité car il s'agit du délit en cybercriminalité dont le coût est le mieux documenté. Cependant, il faut garder en tête que ce n'est qu'une seule forme de cybercrime. Les gains reflétés par le RGPD dans cette partie ne sont vraisemblablement qu'une faible partie des gains totaux en matière de prévention du cybercrime puisqu'il est difficile de documenter, en raison du manque de données, ceux liés aux autres formes de cybercrime (comme les rançongiciels par exemple). À noter également qu'il semble plus simple de se concentrer sur les impacts sur les particuliers, mais les cyberattaques ont également des conséquences sur la productivité ou la réputation des entreprises qui ne sont pas prises en compte ici. À titre d'exemple, Derichebourg a annoncé le 16 avril 2024 avoir subi une cyberattaque qui a eu pour effet de rendre indisponible son logiciel d'exploitation. Cette attaque a causé un ralentissement de son activité, ce qui a occasionné des pertes estimées entre 15 et 20 millions d'euros[5].

Le présent document se concentre également sur l'impact des communications de violations de données. En effet, l'impact des autres dispositions du RGPD sur la cybersécurité n'a, sembe-t-il à ce stade, pas été traité par la littérature économique. En effet, le RGPD contient aussi dans son article 32 des obligations de sécurité du traitement des données personnelles (pseudonymisation, analyse d'impact, etc.).

Dès lors qu'il ne s'agit que d'étudier une partie de l'impact du RGPD sur la cybersécurité, les estimations ici présentées peuvent constituer un minorant des gains totaux du RGPD en matière de cybersécurité. La communication de violations de données aux personnes est une règle plus ancienne, qui a notamment été mise en place aux États-Unis au début des années 2000, ce qui explique que son impact ait été plus fortement étudié par les économistes.

Les usurpations d'identité ont lieu lorsqu'un cybercriminel se sert d'informations à caractère personnel obtenues sur une personne afin de se faire passer pour celle-ci. Quatre types peuvent être distingués en suivant la typologie de Riek et Böhme (2018), dont les travaux ont été financés par le projet E-crime de la Commission européenne. Les quatre types d'usurpations d'identité étudiées par l'auteur sont : les usurpations d'identité où le criminel obtient l'accès au compte en banque (IDT_OB), celles où le criminel obtient l'accès aux informations de la carte bancaire (IDT_BC), l'accès au compte Paypal (IDT_PP) et enfin l'accès à un compte d'achat en ligne (IDT_OS). Cela ne représente qu'une partie des usurpations d'identité ayant un impact sur les personnes concernées.. Ces usurpations d'identité ont un coût moyen en perte monétaire et en perte de temps pour l'individu (pour obtenir un remboursement, remplacer ses identifiants, changer de carte, etc.).

---

[3] « Le coût de la cybercriminalité explose en France », 2024, Statista. Disponible sur : https://fr.statista.com/infographie/31783/cout-annuel-cybercriminalite-cyberattaques-en-france/

[4] « Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 », Asterès. Disponible sur : https://asteres.fr/etude/les-cyberattaques-reussies-en-france-un-cout-de-2-mdse-en-2022/

[5] « Suite à une cyberattaque, Derichebourg perd 15 à 20 millions d'euros », 2024, Usine Digitale. Disponible sur : https://www.usine-digitale.fr/article/suite-a-une-cyberattaque-derichebourg-perd-15-a-20-millions-d-euros.N2211635

Les données de Riek et Böhme sur le coût du cybercrime ont été obtenues via des questionnaires auprès de de 6 394 individus de divers pays européens (Italie, Allemagne, Estonie, Pologne, Pays-Bas, Royaume-Uni) ce qui permet de prendre en compte les cybercrimes non déclarés aux autorités. Le tableau ci-dessous présente les coûts monétaires et temporels moyens des usurpations d'identité rapportés par les individus en 2018, présentés sous forme d'intervalle de confiance statistique à 90 %[6]. Il peut être noté que l'écart fort des intervalles de confiance reflète le caractère assez variable du coût du cybercrime, qui est très faible voire nul la plupart du temps mais qui peut avoir un coût très élevé de façon moins fréquente, si bien que la perte médiane est plus faible que la perte moyenne.

Tableau 2
Coût des usurpations d'identité

	Coût Monétaire (en euros)	Temps Perdu (en heures)	Part Usurpation Identité
Usurpation d'identité	$(\bar{C})$	$(\bar{T})$	
IDT_OB	[203 – 1396]	[6,2 – 10,1]	20%
IDT_BC	[250 – 534]	[6,9 – 11,2]	34%
IDT_PP	[170 – 1034]	[7,3 – 9,6]	15%
IDT_OS	[23 – 133]	[5,6 – 8,5]	29%

À partir de ces coûts, il est possible d'estimer la perte moyenne pour chaque individu d'un pays à cause du cybercrime par la formule suivante avec α un indicateur qui relie le temps perdu à un coût monétaire :

$$\mathcal{L}_{IDT} = \sum_{i \in \{IDT\}} \bar{p}_i(\bar{C}_i + \alpha \bar{T}_i)$$

À partir de l'eurobaromètre 2015, une approximation de la probabilité d'être victime d'une usurpation d'identité peut être estimée à 8 % dans l'UE[7] (ce qui est un chiffre cohérent avec l'approche de Riek) et de 9% en France. Pour l'estimation de α, il est possible de se baser sur le salaire médian en France et dans l'UE en 2018[8]. Enfin, l'impact du RGPD sur lequel la présente étude se focalise est l'impact des communications de violations de données. L'impact de ce type de politique sur l'usurpation d'identité a été étudié à deux reprises par la littérature économique. Romanosky (2011) trouve une baisse de 6,1% du nombre d'usurpations d'identité et Bisogni (2020) trouve une baisse de 2,5% suite à la mise en œuvre d'une politique de communication de violation de données. Il est possible d'utiliser ces deux chiffres afin d'estimer l'impact du RGPD sur le coût moyen par individu des usurpations d'identité :

$$Gains\ RGPD = Nb\_Internautes(\mathcal{L}_{Pre\_RGPD} - \mathcal{L}_{Post\_RGPD})$$

[6] C'est-à-dire qu'il y a 90% de chances que le coût moyen des usurpations d'identité en Europe soit contenu dans l'intervalle.
[7] « *Europeans' attitudes towards cyber security* » [en anglais], Union européenne. Disponible sur : https://europa.eu/eurobarometer/surveys/detail/2171
[8] « *Low-wage earners as a proportion of all employees (excluding apprentices) by sex* » [en anglais], 2021, Eurostat : https://doi.org/10.2908/EARN_SES_PUB1S

Pour trouver le nombre d'internautes de plus de 18 ans dans l'UE et en France, il suffit de se servir du pourcentage d'individus utilisant internet en 2018[9],[10] et des données de l'Insee sur la pyramide des âges en France[11] et d'Eurostat dans l'UE[12]. À partir de ces données, il est possible d'estimer que le coût des usurpations d'identité en France se situe entre 1 et 3,4 milliards d'euros sur 4 ans. Dans l'UE, ce chiffre est entre 6 et 15 milliards d'euros.

Tableau 3
Coûts directs des usurpations d'identité évitées par la notification de violation de données (en millions d'euros)

	Baisse de 2,5 %	Baisse de 6,1 %
Union européenne	**405** [189,7 – 620]	**988** [463 – 1512]
France	**54** [25,4– 83]	**132** [62 – 205,5]

Il est possible dès lors de conclure que le RGPD a permis d'éviter entre 54 et 132 millions d'euros de pertes liées aux coûts directs des usurpations d'identité en France et entre 405 et 988 millions d'euros de pertes à l'échelle de l'UE.

Le questionnaire de Riek contenait également des informations sur les montants d'indemnisation des individus par les entreprises ou les compagnies d'assurance, ce qui permet de déterminer combien de pertes les individus et les entreprises ont pu respectivement éviter.

En moyenne, 70 % des pertes occasionnées par les usurpations d'identité sont indemnisées par des entreprises. En France, les individus ont évité entre 16 et 40 millions d'euros de pertes et les entreprises entre 39,5 et 96 millions. À l'échelle de l'UE, les individus ont évité entre 105 et 257 millions d'euros de pertes et les entreprises entre 164 et 402 millions d'euros.

2. Impact indirect

Jusqu'à présent, cette étude a ignoré les coûts indirects, qui sont pourtant une part importante des coûts causés par le cybercrime. Les coûts indirects du cybercrime se répercutent sur la société dans son ensemble et peuvent être attribués à l'impact qu'a le cybercrime sur le niveau de confiance des individus dans la sécurité des activités en ligne où ils doivent transmettre des données sensibles (ex. : informations de carte bancaire), ce qui se traduit par une réduction du chiffre d'affaires des entreprises. Riek, Böhme et Moore (2015) montrent que le niveau de confiance des individus quant à la sécurité de leurs données personnelles lorsqu'ils utilisent internet est fortement affecté par leurs expériences passées avec le cybercrime. L'impact du cybercrime se répercute également sur le reste de la société en cela qu'il modifie les comportements en ligne des individus. Par exemple, une étude belge (Paoli et Visschers, 2017) estime que 5,9 % et 10,4 % de la population ont respectivement limité leurs usages des banques en ligne et de e-commerce en raison des risques de cybersécurité. Dans le baromètre du numérique 2018 de l'ARCEP, 29 % des sondés déclarent hésiter à faire des achats en ligne en raison de craintes sur la sécurité des paiements. Anderson et al., (2019) estiment les coûts indirects des fraudes aux moyens de paiement à 1,6 milliards de dollars au Royaume-Uni.

Comme il semble possible de l'imaginer, si le coût direct d'un cybercrime est complexe à estimer, ses coûts indirects le sont d'autant plus. Pour tenter d'estimer les coûts indirects, Riek et Böhme (2018) ont collaboré avec un prestataire de carte bancaire allemand afin d'observer comment les comportements de transaction des

[9] *Baromètre du numérique 2018* (PDF, 5,6 Mo), Arcep. Disponible sur : https://www.arcep.fr/uploads/tx_gspublication/barometre-du-numerique-2018_031218.pdf
[10] « *World Bank Indicators* » [en anglais], World Bank. Disponible sur : https://databank.worldbank.org/source/world-development-indicators
[11] « Pyramide des âges – projections de population 2021 – 2070 – Scénarios », Insee. Disponible sur : https://www.insee.fr/fr/outil-interactif/5896897/pyramide.htm#!y=2018&a=60,70&v=2&g&t=1&c=0
[12] « *Population on 1 January by age and sex* » [en anglais], Eurostat https://doi.org/10.2908/DEMO_PJAN

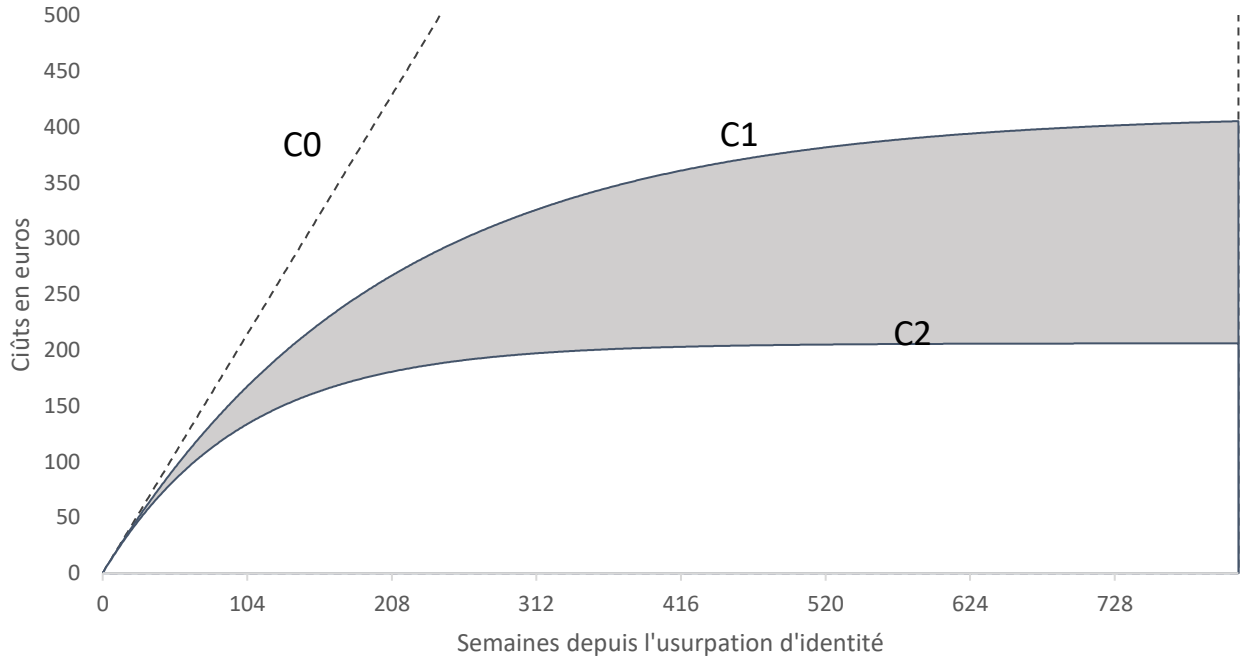
individus étaient modifiés lorsqu'ils subissaient une usurpation d'identité de carte bancaire (IDT_BC). L'auteur a ensuite interrogé une partie de la population pour comprendre comment leurs comportements (habitudes d'achats etc.) avaient changé. Les résultats montrent qu'une part importante des individus devient méfiante et réduit fortement le nombre de transactions effectuées en ligne sans que cela ne soit entièrement compensé par une hausse des comportements d'achats hors ligne. Il trouve notamment que le nombre moyen de transactions en ligne par semaine passe de 1,32 à 1,02 suite à l'usurpation d'identité. En comparant les comportements d'achats avant et après l'accident, il estime le coût indirect moyen pour le secteur de 2,06 euros par semaine à cette forme de cybercrime.

Cependant, l'étude a une limite : les individus n'ont été suivis que 18 semaines après avoir subi l'usurpation d'identité. Or, durant la période d'observation, l'auteur n'a pas observé de tendance vers un retour à la normale. Il paraît relativement irréaliste d'imaginer que les comportements des individus soient changés à jamais, mais il n'est pas possible de savoir à partir de quel moment les habitudes d'achat retournent à la normale à la suite d'un cybercrime. Pour compenser cette lacune, la présente étude suppose un effet de détérioration de l'impact du cybercrime sur le comportement de l'individu au fil du temps. Cette atténuation de l'impact est visualisée par une série géométrique avec un taux de dépréciation de l'impact de l'usurpation d'identité noté λ.

$$Perte\ Indirecte = \sum_{i=1}^{\infty} \lambda^{i-1} 2{,}06$$

Il n'y a, ne semble-t-il, aucune estimation de ce taux de dépréciation dans la littérature économique. Cependant, étant donné l'impact psychologique significatif du cybercrime sur les individus, pouvant entraîner des troubles comme le syndrome de stress post-traumatique (Bada et Nurse, 2020 ; Kirwan et Power, 2012) et la longue durée de vie de l'usurpation d'identité, où les données personnelles ayant fuité peuvent être réutilisées à plusieurs reprises par les cybercriminels pour ouvrir des comptes bancaires ou contracter des crédits, il semble raisonnable de supposer que l'impact psychologique sur les victimes perdure durant plusieurs années. Cette analyse propose donc deux λ : dans le premier, l'impact du cybercrime sur l'individu baisse de 0,5 % par semaine (λ1), et dans le deuxième l'impact du cybercrime s'atténue deux fois plus rapidement et baisse d'1 % par semaine (λ2). Le graphique suivant illustre la forme fonctionnelle des coûts indirects selon le paramètre retenu.

Figure 1
Coût indirect de l'usurpation d'identité sur carte bancaire (IDT_BC)



Note : 104 semaines ≈ 2 ans.
C0 représente le coût non déprécié, c'est l'hypothèse non réaliste selon laquelle l'impact psychologique d'avoir été victime d'une usurpation d'identité ne s'atténue pas avec le temps.
C1 représente le coût indirect du cybercrime avec le taux de dépréciation λ1.
C2 représente le coût indirect du cybercrime avec le taux de dépréciation λ2.

À partir de ces modélisations du coût indirect et de l'estimation de Riek (2015), il est possible d'estimer un coût indirect pour l'usurpation d'identité par la carte bancaire (IDT_CB) entre 206 et 412 euros, soit entre 52 % et 105 % de l'impact monétaire direct du cybercrime. En raison de la proximité de l'usurpation d'identité par carte bancaire avec les autres formes d'usurpation d'identité précédemment discutées, il semble possible de faire l'hypothèse que les ordres de grandeur des coûts indirect sont similaires pour les autres cas d'usage.

En ajoutant les coûts indirects à la fonction L précédemment estimée, il est possible de réestimer les gains moyens liés au RGPD du tableau 2 en prenant en compte les coûts indirects.

Tableau 3
Coûts totaux des usurpations d'identité évitées par la notification de violation de données (en millions d'euros)

	Baisse de 2,5 %	Baisse de 6,1 %
Union européenne	**585** [509,8 – 660]	**1427** [1244 – 1610]
France	**90** [78,5– 101,2]	**219** [191 – 247]

Note : L'intervalle représente l'estimation avec λ1 et λ2 ($[est_{\lambda 1} - est_{\lambda 2}]$). Le chiffre retenu en gras est la moyenne de ces estimations.

Il semble dès lors possible de conclure que le RGPD aurait permis d'éviter entre 90 et 219 millions d'euros de pertes totales liées aux usurpations d'identités en France et entre 585 et 1427 millions d'euros de pertes totales à l'échelle de l'UE. Les coûts indirects étant uniquement perçus par les entreprises, il est possible de les additionner aux coûts directs compensés par les entreprises pour obtenir les pertes totales évitées par celles-ci. **Il est possible d'estimer que 82 % de ces pertes évitées concernent les entreprises.**

Conclusion

Il est possible de de démontrer comment la recherche en économie permet de considérer la cybersécurité comme un choix d'investissement des entreprises. En théorie économique, ce choix est fait par les entreprises avec la perspective de maximiser leur profit. Ces investissements ont des effets sur les individus et les autres entreprises, qui ne sont pas pris en compte par les entreprises dans leur décision d'investissement. Lorsqu'une entreprise investit dans la cybersécurité, cela a un effet positif sur ses partenaires, ses concurrents, ses clients et ses salariés. Le RGPD incite les entreprises à investir davantage dans la cybersécurité, afin de limiter l'impact du cybercrime à l'échelle de la société et présente donc un bénéfice pour l'ensemble des acteurs.

Il est possible d'estimer les bénéfices : le RGPD aurait permis d'éviter des pertes au moins entre 90 et 219 millions d'euros en France uniquement via l'impact de la communication de violations de données (article 34). Sur 4 types d'usurpations d'identité, à l'échelle de l'UE, cette disposition aurait permis d'éviter entre 585 millions et 1,4 milliard d'euros de pertes. C'est un premier chiffre qui vise principalement à illustrer les potentiels gains du RGPD plutôt qu'à en rendre compte dans leur intégralité. En effet, en raison des limites dans les données disponibles, il est difficile de fournir une estimation rigoureuse des autres gains liés à la cybersécurité permis par le RGPD. À titre d'exemple, certains gains ont été omis de l'analyse. Pour les communications de violations de données, un élément essentiel a été omis : l'impact du RGPD sur le coût moyen des usurpations d'identité. Un des principes même de la communication de violations de données personnelles est de permettre à l'individu de mettre en place les mesures préventives appropriées pour éviter de subir des dommages.

Également, l'article 32 du RGPD prévoit que les entreprises doivent mettre en place des mesures de sécurité appropriées pour les données à caractère personnel telles que le chiffrement. D'après le rapport « *Cost of a data*

breach 2023 » d'IBM[13], le chiffrement permet de réduire le coût moyen d'une faille de sécurité de 5 % et représente une mesure de sécurité basique peu coûteuse à mettre en place. Il convient également de prendre en considération l'impact des principes de minimisation des données (article 5.1.c du RGPD), qui contribuent à réduire les conséquences des violations de données pour les individus. En effet les entreprises ayant minimisé la collecte de données sont moins susceptibles de subir une violation de données ayant un impact grave sur les individus puisqu'elles ne détiennent pas d'informations sensibles, n'ayant pas de raison de les collecter en premier lieu. De même, le principe de limitation de la durée de conservation (article 5.1.e du RGPD) permet de diminuer dans le temps le nombre d'informations à caractère personnel détenues par les entreprises, ce qui réduit l'impact négatif des cyberattaques.

Tous ces impacts du RGPD pourraient avoir pour effet de diminuer le coût moyen des cyberattaques (soit les chiffres du tableau 1), ce qui n'a pas été pris en compte dans la présente étude de cas puisque les gains du RGPD ont été basés uniquement sur la réduction de la fréquence des cybercrimes. Il reste donc tout un ensemble de gains liés à la réduction du coût moyen des cyberattaques permis par le RGPD à investiguer.

Le RGPD et les travaux de la CNIL en lien avec l'écosystème de la cybersécurité permettent de sensibiliser le public et les entreprises, notamment les PME, aux enjeux de cybersécurité, ce qui est un autre aspect par lequel la réglementation peut permettre de réduire l'impact du cybercrime. La réduction de l'impact du cybercrime pourrait également, par son effet indirect sur le climat de confiance en ligne, avoir pour effet de permettre plus facilement l'émergence de services innovants qui reposent fortement sur la confiance des utilisateurs.

Il reste de nombreuses pistes à explorer pour comprendre l'impact positif du RGPD dans le domaine de la sécurité informatique. Des rapports tels que celui du CESIN[14] ou de Spicework[15] évoquent que le RGPD a entraîné une hausse des investissements en cybersécurité, mais l'ampleur de cette hausse reste indéterminée. Quel impact du RGPD sur l'adoption des mesures de chiffrement, d'anonymisation, de sensibilisation ? Comment ces impacts se sont-ils répercutés sur le coût et l'impact du cybercrime ? Ces questions restent en suspens et il importe que la communauté scientifique se saisisse de celles-ci afin de fournir à leur tour des éclairages précisément quantifiés.

Références

ACQUISTI, Alessandro, FRIEDMAN, Allan et TELANG, Rahul, 2006, « Is there a cost to privacy breaches? an event study. », *ICIS 2006 proceedings*, p. 94.

AMIR, Emir, LEVI, Shai, and LIVNE, Tsafrir, 2018, « Do firms underreport information on cyber-attacks? evidence from capital markets. » *Review of Accounting Studies*, 23, pp. 1177–1206.

ANDERSON, Ross, BARTON, Chris, BÖHME, Rainer, CLAYTON, Richard, GAÑÁN, Carlos, GRASSO, Tom, LEVI, Michael, MOORE, Tyler, et VASEK, Marie, 2019,« Measuring the changing cost of cybercrime », *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*.

ANDERSON, Ross and MOORE, Tyler, 2007, « The economics of information security: A survey and open questions. », *Fourth bi-annual Conference on the Economics of the Software and Internet Industries*, pp. 19–20.

Arcep. Baromètre du numétique, 2018. Disponible sur : https://www.arcep.fr/uploads/tx_gspublication/barometre-du-numerique-2018_031218.pdf

BADA, Maria, et NURSE, Jason R.C., 2020, *The social and psychological impact of cyberattacks*, pp. 73–92.

BANA, Sarah, BRYNJOLFSSON, Erik, JIN, Wang, STEFFEN, Sebastian, et WANG, Xiupeng, 2022, « Human capital acquisition in response to data breaches. », *SSRN*.

[13] « *Cost of a Data Breach Report* » [en anglais], IBM Security. Disponible sur : https://github.com/jacobdjwilson/awesome-annual-security-reports/blob/main/Annual%20Security%20Reports/2023/IBM-Cost-of-a-Data-Breach-Report-2023.pdf

[14] *Baromètre de la cyber-sécurité des entreprises*, janvier 2019, CESIN. Disponible sur : https://cesin.fr/document.php?d=64355ec80c7ab

[15] « *The 2018 State of It* » [en anglais], Spiceworks. Disponible sur : https://www.spiceworks.com/sw-marketing/state-of-it-2018/

BEKNAZAR-YUZBASHEV, George, JIMENEZ DURAN, Rafael, et STALINSKI, Mateusz, 2024, « A model of harmful yet engaging content on social media. » *SSRN*.

BISOGNI, Fabio et ASGHARI, Hadi, 2020, « More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Communication Laws. », *Journal of Information Policy*, Vol. 10, pp. 45–82.

BÖHME, Rainer, 2012, « Security audits revisited. », *International conference on financial cryptography and data security*, Springer, pp. 129–147.

BOSE, Indranil et LEUNG, Alvin Chung Man, 2014, « Do phishing alerts impact global corporations? a firm value analysis. » *Decision Support Systems*, Vol. 64, pp. 67–78.

CHEN, Jiawei, 2016, « How do switching costs affect market concentration and prices in network industries?" *The Journal of Industrial Economics*, 64(2), pp. 226–254.

CORDES, Joseph J., 2011, « An overview of the economics of cybersecurity and cybersecurity policy. » *CSPRI Report*, pp. 1–18.

Commission européenne et Direction générale de la migration et des affaires intérieures, 2017, *Europeans' attitudes towards cyber security*. European Commission. Disponible sur : https://europa.eu/eurobarometer/surveys/detail/2171

Eurostat, 2012, « Low-wage earners as a proportion of all employees (excluding apprentices) by sex. ». DOI : https://doi.org/10.2908/EARN_SES_PUB1S

Eurostat, 2023, « Population on 1 january by age and sex. ». DOI : https://doi.org/10.2908/DEMO_PJAN

FEDELE, Alessandro, et RONER, Cristian, 2022, « Dangerous games: A literature review on cybersecurity investments. », *Journal of Economic Surveys*, 36(1), pp. 157–187.

GANDAL, Neil, MOORE, Tyler, RIORDAN, Michael, et BARNIR, Noa, 2023, Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, Vol. 133, 103380.

GARCIA, Michael E., 2013, *The economics of data breach: Asymmetric information and policy interventions*. The Ohio State University.

HAISLIP, Jacob Z., KOLEV, Kalin, PINSKER, Robert, et STEFFEN, Thomas, 2019, « The economic cost of cybersecurity breaches: A broad-based analysis. », *Workshop on the economics of information security (WEIS)*, Vol. 9.

KELTON, Andrea S., et Pennington, Robin R., 2020, « Do voluntary disclosures mitigate the cybersecurity breach contagion effect? », *Journal of Information Systems*, 34(3), pp. 133–157.

KIRWAN, Grainne, et POWER, Andrew, 2012, *The Psychology of Cyber Crime: Concepts and Principles*.

LOEWENSTEIN, George, JOHN, Leslie et VOLPP, Kevin G., 2013, « Using decision errors to help people help themselves. », *The Behavioral Foundations of Public Policy*.

MARTIN, Kelly D., BORAH, Abhishek et PALMATIER, Robert W., 2017, « Data privacy: Effects on customer and firm performance. » *Journal of marketing*, 81(1), pp. 36–58.

MILLER, Amalia R. et TUCKER, Catherine E., 2011, « Encryption and the loss of patient data. », *Journal of Policy Analysis and Management*, 30(3), p.. 534–556.

MOORE, Tyler, KENNEALLY, Erin, COLLETT, Michael et THAPA, Prakash, 2019, « Valuing cybersecurity research datasets. », *18th Workshop on the Economics of Information Security (WEIS)*.

MURCIANO-GOROFF, Raviv, 2019, « Do data breach disclosure laws increase firms' investment in securing their digital infrastructure. », *Workshop on the Economics of Information Security*, pp. 1–39.

NAGURNEY, Anna et NAGURNEY, Ladimer S., 2015, « A game theory model of cybersecurity investments with information asymmetry. » *NETNOMICS: Economic Research and Electronic Networking*, 16, pp. 127– 148.

NIEUWESTEEG, Bernold et FAURE, Michael, 2018 « An analysis of the effectiveness of the eu data breach communication obligation. » *Computer Law & Security Review*, 34(6), pp. 1232–1246.

PAOLI, Letizia et VISSCHERS, Jonas, 2017, « The impact of cybercrime on belgian businesses », *KU Leuven Centre for IT & IP Law Series*.

QIAN, Xiaofei, PEI, Jun, LIU, Xinbao, ZHOU, Mi et P. M. Pardalos, 2019, « Information security decisions for two firms in a market with different types of customers. », *Journal of Combinatorial Optimization*, 38, pp. 1263–1285.

RIEK, Markus et BÖHME, Rainer. *Towards a Robust Quantification of the Societal Impacts of Consumerfacing Cybercrime*. Universitäts- und Landesbibliothek Münster, 2018.

RIEK, Markus, BOHME, Rainer et MOORE, Tyler, 2015, « Measuring the influence of perceived cybercrime risk on online service avoidance. », *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261– 273.

RIEK, Markus et BÖHME, Rainer, 2018, « The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates », *Journal of Cybersecurity*, Vol. 4, 1.

ROMANOSKY, Sasha, TELANG, Rahul et ACQUISTI, Alessandro, 2011, « Do data breach disclosure laws reduce identity theft? », *Journal of Policy Analysis and Management*, 30(2), pp. 256–286.

Su, Yiqing, Zhang, Xiaoting et Zhang Shifei, 2023, « The impact of collective action dilemma on vaccine hesitancy: Evidence from China ». *Human Vaccines & Immunotherapeutics*, 19(2):2256041.

The World Bank. World development indicators. 2024, Disponible sur : https://databank.worldbank.org/source/world-development-indicators