
# CYBERSECURITE : QUELS SONT LES BENEFICES ECONOMIQUES DU RGPD ?

La CNIL vient de publier une analyse sur l'impact économique du RGPD en matière de cybersécurité. En renforçant les obligations dans ce domaine, le règlement aurait permis d'éviter, par exemple sur l'enjeu d'usurpation d'identité, entre 90 et 219 millions d'euros de préjudices cyber en France.

Dans son bilan de l'impact économique du RGPD, 5 ans après son entrée en application, la CNIL relevait que les études économiques sur l'impact du RGPD se concentrent principalement sur les coûts et ne traitent que marginalement de ses bénéfices. La CNIL a donc entrepris d'étudier ces bénéfices et de proposer une analyse quantifiée. L'analyse utilise l'angle de la cybersécurité (articles 32, 33 et 34 du RGPD), pour mettre en évidence les bénéfices de ce dernier.

Dans l'économie de la cybersécurité, la sécurité informatique est considérée comme une décision d'investissement des entreprises. Cette décision d'investissement suit une logique de rentabilité : l'investissement dans la cybersécurité est mis en balance avec son coût et le risque de cyberattaque.

Cependant, ce calcul que fait l'entreprise ne prend pas en compte un élément crucial, l'impact de son investissement sur le reste de la société, ce qui s'appelle en économie une externalité. Du fait de ces externalités, le niveau d'investissement spontané des entreprises dans la sécurisation des systèmes d'information n'est pas optimal en l'absence de régulation. Les réglementations comme le RGPD permettent alors de remédier à cette défaillance du marché en exigeant la mise en place de règles de sécurité bénéficiant aux personnes concernées, mais aussi aux entreprises et à leurs partenaires.

La CNIL a donc entrepris d'étudier les bénéfices du RGPD via une analyse quantifiée sous l'angle de la cybersécurité dont voici une synthèse des principales conclusions.

La CNIL distingue tout d'abord trois grands types d'externalités selon l'acteur économique affecté : les autres entreprises, les cybercriminels et les clients/utilisateurs :

**- Les externalités affectant les autres entreprises**

Le niveau de cybersécurité d'une entreprise dépend également de l'investissement dans la cybersécurité des autres entreprises. Un virus informatique peut s'étendre de machine en machine de la même manière qu'un véritable virus se répand par contagion. Par conséquent, lorsqu'une entreprise investit dans la cybersécurité, cela permet de constituer un environnement global plus résilient au cybercrime, selon un mécanisme qui peut être rapproché de l'immunité collective :

- dans le cadre de la relation de sous-traitance, car la sécurité des données du responsable de traitement est dépendante du niveau de sécurité de son prestataire ;
- avec les entreprises partenaires, voire concurrentes, qui peuvent par exemple « profiter » du niveau élevé de sécurité des données d'un secteur, dans une logique de « cercle vertueux ».

Cependant, une entreprise n'a pas d'incitation à prendre en compte les bénéfices que ses investissements en cybersécurité apportent à ses concurrents, ce qui limite son investissement dans ce domaine.

**- Les externalités pour les cybercriminels**

Le sous-investissement dans la cybersécurité augmente la rentabilité du cybercrime, notamment via les rançongiciels (ces attaques visent à extorquer une rançon).

Lorsque les mesures de sécurité sont insuffisantes, les attaques réussissent plus facilement. Plus le nombre d'attaques réussies est élevé, plus les cybercriminels peuvent exiger des rançons importantes, tout en s'assurant qu'un certain nombre de victimes finiront par payer. Les cybercriminels ajustent le montant des rançons afin d'optimiser leurs gains en équilibrant deux paramètres. D'une part, une rançon trop élevée risque de dissuader les victimes de payer : de l'autre, une rançon trop basse ne permettrait pas de maximiser le profit.

Étant donné que seules quelques entreprises sont prêtes à verser des sommes très élevées, la stratégie optimale dépend du nombre d'attaques réussies. Si celles-ci sont rares, il est plus rentable d'exiger des rançons modérées que la majorité des victimes accepteront de payer. En revanche, si le nombre d'attaques réussies est élevé, la probabilité qu'une entreprise attaquée accepte de payer une somme très importante augmente. Il devient alors plus avantageux pour le cybercriminel de fixer des rançons élevées afin de maximiser son profit sur ces rares paiements.

Ainsi, le manque d'investissement en cybersécurité crée un cercle vicieux : il favorise la réussite des attaques, renforce la capacité des cybercriminels à exiger des sommes croissantes et, in fine, renforce la rentabilité et la gravité du cybercrime.

**- Les externalités affectant les clients**

Régulièrement, les fuites de données affectant les entreprises concernent les données personnelles de leurs clients/utilisateurs (personnes physiques). Celles-ci peuvent être utilisées pour effectuer de nouvelles attaques cyber à l'encontre de la personne concernée (hameçonnage, usurpation d'identité, bourrage d'identifiant). Les individus subissant les conséquences négatives d'une fuite de données ne peuvent pas toujours savoir quelle est l'entreprise à l'origine de la fuite de leurs données personnelles.

Lorsqu'une entreprise communique sur une fuite de données, elle s'expose à certaines conséquences : perte de réputation, baisse de la valorisation, perte de confiance des clients, etc. Pour éviter ces répercussions, leur comportement spontané en l'absence de réglementation est de ne pas révéler ces incidents.

Ce phénomène d'externalité négative n'est pas optimal en ce qu'il conduit à ce que les entreprises concernées échappent à leur responsabilité face aux conséquences négatives causées à leurs clients en raison de leur manque d'investissement dans la cybersécurité, réduisant ainsi leur incitation à renforcer leurs protections. Ce faisant, elles empêcheraient également la personne concernée d'être vigilante et de prendre les mesures nécessaires pour se protéger.

Le RGPD a rendu cette opacité illégale, les responsables de traitement sont désormais tenus d'informer l'autorité de protection des données de toute violation mais aussi les personnes concernées en cas de risque élevé lié à une violation de données à caractère personnel. En cas de non-respect de ces obligations, l'entreprise s'expose à des sanctions. En réduisant cette externalité, le RGPD permet donc des gains pour la société dans son ensemble.

Le plus souvent, ces différentes externalités ne sont pas prises en compte lorsque l'entreprise détermine les montants à investir dans la cybersécurité. La conséquence est donc un niveau d'investissement dans la sécurisation des systèmes d'information insuffisant en l'absence d'obligations réglementaires comme le RGPD.

**Les gains au RGPD sous l'angle de la cybersécurité**

La conformité au RGPD permet ainsi de lutter contre le sous-investissement en matière de cybersécurité.

Par exemple, en obligeant les acteurs à révéler aux personnes concernées les fuites de données graves (article 34), les individus peuvent décider d'arrêter de traiter avec des entreprises qui n'ont pas un niveau de cybersécurité suffisant. Cette disposition permet donc de réduire l'externalité affectant les clients de l'entreprise. L'entreprise doit faire face à ses responsabilités, ce qui la pousse à investir davantage dans la cybersécurité.

Ainsi, la recherche économique s'est penchée sur les conséquences liées aux usurpations d'identité :

En comparant le nombre d'usurpations de données avant et après l'instauration de cette politique, des économistes ont trouvé que les notifications de violation de données entraînent une diminution de 2,5 % à 6,1 % d'usurpations d'identité.

En rapprochant cette diminution avec le coût des usurpations d'identité en France, il est possible de calculer qu'entre 90 et 219 millions d'euros de pertes ont pu être évitées depuis 2018 en France et entre 585 millions et 1,4 milliards d'euros à l'échelle de l'UE ;

En tenant compte du niveau d'indemnisation de ces pertes et de l'impact des usurpations d'identité sur la confiance des victimes à acheter en ligne, il est possible d'estimer que 82 % de ces pertes évitées bénéficient aux entreprises.

Ces gains ne représentent qu'une faible partie des gains totaux dus au RGPD en matière de réduction du cybercrime. Il ne s'agit que de l'impact d'une de ses dispositions sur un type spécifique de cybercrime (l'usurpation d'identité). Il faudrait également y ajouter l'impact positif de la conformité RGPD sur les rançongiciels, les botnets (réseau de programmes connectés via Internet), les logiciels malveillants, etc. Il serait pertinent que les économistes approfondissent la dimension de la cybersécurité pour offrir une vision plus complète de ce sujet.

Pour les entreprises, se conformer au RGPD et aux nouvelles exigences de cybersécurité n'est plus une simple obligation réglementaire. C'est un levier stratégique pour renforcer la résilience, améliorer la gouvernance et garantir la confiance des clients, partenaires et investisseurs, estime Gaetan Fron, Directeur Commercial France et Luxembourg chez Diligent : « *En 2024, avec une augmentation de 20 % des violations de données, la cybersécurité est devenue un enjeu de premier plan pour les entreprises, en particulier face à des menaces de plus en plus sophistiquées. Toutefois, ce n'est pas seulement la gestion des cyber risques qui est cruciale, mais la manière dont les organisations gèrent leurs données et se conforment aux réglementations telles que le RGPD. L'étude récente de la CNIL révèle qu'une gestion plus efficace des risques a permis aux entreprises de faire l'économie de 219 millions d'euros, soit 82 % des pertes évitées. Cela démontre que l'intégration des bonnes pratiques en matière de gouvernance et de conformité peut offrir des avantages financiers substantiels.*

*À mesure que les entreprises font face à des régulations de plus en plus strictes et des risques cyber qui augmentent, il devient crucial d'adopter des outils et des processus qui assurent non seulement la conformité, mais aussi une gestion proactive des risques. L'adoption de solutions intelligentes, telles que l'automatisation des processus de gouvernance et de gestion des risques, vise à améliorer la sécurité des données et à prédire l'impact des menaces avant qu'elles ne surviennent. Alors que les entreprises ont de gros enjeux de digitalisation, accélérée par l'adoption de l'IA, le véritable défi réside dans la capacité des entreprises à se préparer, à évaluer et à gérer ces risques de manière stratégique, en alliant sécurité, innovation et rentabilité.* »

Source : IT Channel - Juin 2025