Protocole cryptographique pour la protection des droits d'auteur·e et de la vie privée des acquéreur·e·s d'un contenu multimédia

Caroline Fontaine (DR CNRS, LSV), Ilham Dami (doctorante ENS Paris-Saclay, LSV)

11 septembre 2020

Afin de promouvoir la création intellectuelle, la loi protège les auteur·e·s d'une œuvre originale afin qu'iels puissent obtenir une rétribution (généralement financière) de l'exploitation de leur œuvre.

Dans le monde numérique, le respect des droits d'auteur·e est particulièrement mis à mal. En effet, sans outil technologique développé spécifiquement pour protéger les œuvres numériques contre une exploitation ne respectant pas les droits d'auteur·e, n'importe quelle personne disposant d'un ordinateur standard peut non seulement réaliser aisément des copies d'une œuvre numérique, mais aussi les distribuer à grande échelle sans que l'on puisse facilement remonter jusqu'à elle. Hormis quelques exceptions [1], dès lors que ces copies n'ont pas été autorisées par les ayants droit, il s'agit de copies illégales.

Quelques chiffres. Selon le rapport d'activité 2019 de l'Hadopi, **13** % des internautes de 15 ans et plus déclarent consommer des biens culturels dématérialisés illicites régulièrement [2]. Selon une étude menée par le cabinet d'audit financier et de conseil EY, le manque à gagner en 2017 pour la filière cinématographique et audiovisuelle française serait de **1,18 Md€** (soit 14 % du chiffre d'affaires total de la filière), et de **408 M€** pour l'État français, malgré une baisse par rapport à l'année 2016.

Outils technologiques de lutte contre la consommation illégale de contenus multimédia. Afin de lutter contre la diffusion de copies illégales, plusieurs moyens technologiques ont été développés. Ces moyens sont communément désignés sous le nom de *DRM* [3]. Ils peuvent se diviser en deux catégories aux stratégies différentes mais peuvent être utilisés conjointement. La première consiste en la prévention de la production de copies illégales, alors que la deuxième consiste en le traçage des copies illégales.

La première catégorie comporte ainsi les moyens technologiques visant à restreindre l'utilisation même d'une copie légitime. Ces mesures, bien que compliquant la production de copies illégales exploitables, ont l'inconvénient majeur de restreindre grandement la liberté d'usage des copies légitimes. Cela a pour effet contraire d'encourager les comportements illégaux ; certaines personnes cherchent effectivement à contourner ces restrictions jugées souvent abusives. Ces personnes vont ainsi préférer se procurer des copies illégales car, au-delà de la gratuité, celles-ci ont souvent l'avantage d'être débridées.

La deuxième catégorie comporte quant à elle les moyens technologiques visant à remonter jusqu'à la personne responsable de la production de copies illégales. Cela est rendu possible par des

1. Copie privée, information immédiate par voie de presse et catalogues de ventes judiciaires.
2. Cela inclut 3 % des internautes qui déclarent consommer des biens culturels dématérialisés uniquement de manière illégale, 3 % généralement de manière illégale mais parfois de manière légale, et 7 % autant de manière légale qu'illégale.
3. Digital Rights Management

techniques de tatouage numérique : on intègre dans le contenu multimédia même de l'information invisible/inaudible et difficilement altérable. Cette information est une empreinte numérique unique, ce qui permet d'identifier chaque copie légale. Ainsi, si au moment de l'achat l'identité de l'acquéreur·e a été devoilée, on pourra *a priori* remonter jusqu'à iel en cas de distribution *constatée* de copies illégales. L'inconvénient de cette technique est la perte de vie privée de l'acquéreur·e.

Le respect des droits d'auteur·e·s dans le monde numérique est ainsi un défi non trivial qui, encore aujourd'hui, n'admet pas de solution parfaite, c'est-à-dire une solution garantissant à la fois le respect des droits d'auteur·e·s, mais aussi le respect des libertés d'un·e acquéreur·e légitime d'un contenu multimédia (vie privée et absence de contraintes lors d'un usage privé).

Protocole de distribution de contenus multimédia. Nous travaillons sur un protocole permettant aux ayants droit de fournir du contenu multimédia (contre rémunération) à des acquéreur·e·s, tout en garantissant la traçabilité des copies ainsi distribuées et la vie privée des acquéreur·e·s.

Nous partons du protocole Pimento [4] qui a été conçu avec cela pour objectif. Lors d'une transaction du protocole Pimento, l'ayant droit sait quel contenu iel est en train de fournir mais ne sait pas à qui, et un tiers de confiance (autorité compétente) connaît l'identité de l'acquéreur·e impliqué·e dans chaque transaction sans savoir quel contenu multimédia est fourni durant celle-ci. Chaque copie distribuée est tatouée d'une empreinte unique, qui est partiellement révélée à l'ayant droit. Cela lui permettra d'associer une copie illégale à une transaction précise avec une certaine confiance. Si la suspicion est raisonnable, le tiers de confiance accepte de lever l'anonymat de l'acquéreur·e et exige de l'acquéreur·e qu'iel lui fournisse la copie en sa possession afin de la comparer avec la copie illégale. Il existe une probabilité non nulle qu'une copie légale soit considérée à tort comme génératrice de la copie illégale concernée, cette probabilité restant toutefois très faible.

Questions soulevées. Plusieurs questions se posent lorsqu'il s'agit de déterminer la responsabilité d'un·e prévenu·e. Tout d'abord, bien que nous puissions déterminer avec précision la probabilité qu'une copie donnée soit considérée comme génératrice d'une copie illégale donnée, nous souhaiterions savoir quelle valeur est acceptable pour que cette preuve soit considérée comme viable. Par ailleurs, il est possible que l'acquéreur·e légitime n'ait pas contribué à la production et diffusion de copies illégales même si sa copie (légale) s'avère bien être génératrice de copies illégales. En effet, il est possible que l'appareil sur lequel est stocké ce contenu multimédia légitime se soit fait piraté (par exemple). Or, il n'existe pas de méthodes sûres permettant de prouver l'absence d'intrusion malveillante dans un appareil. De plus, une personne ne peut être raisonnablement considérée comme responsable de la sécurité de son appareil quand ces derniers sont souvent sujets à des failles de sécurité non corrigées par les fabriquant·e·s. Qu'en est-il des contenus multimédia perdus par l'acquéreur·e légitime que ce·tte dernière ne peut donc remettre au tiers de confiance en cas de suspicion ? Peut-on raisonnablement punir une personne ayant perdu un bien ?

Finalement, il s'agit de savoir s'il peut exister un cadre légal juste rendant l'utilisation d'un tel protocole pertinente et efficace dans la lutte contre la distribution illégale de contenus multimédia.

4. Caroline Fontaine, Sébastien Gambs, Julien Lolive et Cristina Onete. Private Asymmetric Fingerprinting : A Protocol with Optimal Traitor Tracing Using Tardos Codes. LATINCRYPT 2014.