Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Réponse à la consultation sur le Document de travail 104 sur les questions de protection des données liées aux droits de propriété intellectuelle, élaboré par le groupe de travail "article 29" sur la protection des données

Vereecken, Isabelle; Poullet, Yves

Publication date:
2004

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Vereecken, I & Poullet, Y 2004, *Réponse à la consultation sur le Document de travail 104 sur les questions de protection des données liées aux droits de propriété intellectuelle, élaboré par le groupe de travail "article 29" sur la protection des données*. s.n., s.l.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026

Réponse à la consultation sur le Document de travail 104 sur les questions de protection des données liées aux droits de propriété intellectuelle, élaboré par le groupe de travail "article 29" sur la protection des données

Introduction

Le CRID (Centre de Recherches Informatique et Droit) fait partie des Facultés Universitaires Notre-Dame de la Paix (Namur-Belgique) et est un centre spécialisé dans le droit des technologies de l'information et de la communication. De nombreuses recherches ont été réalisées au sein du centre notamment dans le domaine de la propriété intellectuelle et du droit d'auteur ainsi que dans le domaine du respect de la vie privée et de la protection des données à caractère personnel (plus d'information sur http://www.crid.be).

Ce document a été élaboré par Isabelle Vereecken[1] avec la collaboration du Professeur Yves Poullet[2].

Pour de plus amples informations concernant cette réponse, veuillez contacter :

Isabelle Vereecken
CRID
Rempart de la Vierge, 5
B-5000 NAMUR
BELGIQUE
Tél : +32 81 72 52 05
Fax : +32 81 72 52 02
isabelle.vereecken@fundp.ac.be

Réponse

La réponse suit la structure du document de travail et se base autant sur des aspects relatifs à la propriété intellectuelle, qui nécessite des moyens de défense pour les détenteurs de droits, que sur les aspects de respect de la vie privée qui implique une mise en balance des droits des titulaires des droits d'auteurs avec les droits de tout individu au respect de sa vie privée et à la protection de ses données personnelles.

1. Introduction

Dans l'introduction du document de travail, le terme "information" peut être interprété d'un point de vue de propriété intellectuelle dans un sens inopportun.

En effet, la notion d' "information" doit être utilisée avec une certaine prudence lorsque l'on traite du droit d'auteur. Il semblerait plus judicieux de privilégier l'utilisation du terme "œuvre protégée par le droit d'auteur" plutôt que "information protégée par le droit d'auteur ". En effet, le terme "information" revêt une signification particulière en droit d'auteur, lequel

[1] Chercheuse au CRID.
[2] Doyen de la faculté de droit et professeur aux Facultés Universitaires Notre-Dame de la Paix à Namur.

l'oppose précisément à celui d' "œuvre". À ce titre, il est d'usage de considérer que le droit d'auteur protège les œuvres et non les informations[3].

II. Gestion des droits de propriété intellectuelle

Sous ce point, le document de travail effectue l'analyse des principes relatifs aux traitements des données ainsi que des obligations du responsable de traitement dans le cadre de traitements *a priori* au niveau de la gestion des droits numériques. Le commentaire souligne les différents points qui selon nous nécessiteraient une clarification.

Une finalité légitime

Le principe de la finalité légitime implique que le traitement se base sur une des finalités énumérées à l'article 7 de la Directive 95/46/CE[4] considérées comme *a priori* légitimes. On pourrait effectivement soutenir que défendre ses propres droits contre une utilisation interdite pourrait être justifiée sur base de l'article 7f (mise en balance des intérêts).

Il faut toutefois ajouter qu'une finalité légitime implique en outre que le traitement soit proportionné. Cela signifie ce notamment que, parmi les moyens disponibles permettant d'atteindre l'objectif visé, il convient d'opter pour celui le moins attentatoire à la vie privée.

Un tel principe n'apparaît pas suffisamment approfondi dans le document de travail[5]. Il conviendrait pourtant d'y accorder une attention particulière notamment afin d'évaluer clairement la proportionnalité du traitement consistant à identifier et tracer les données de l'ensemble des utilisateurs téléchargeant légalement des œuvres via un système DRM de manière systématique et *a priori* pour le cas où certains d'entre eux en feraient une utilisation illégitime.

En outre, il serait opportun de s'interroger sur l'existence et la mise en oeuvre de moyens alternatifs permettant d'empêcher l'utilisation illicite des œuvres sans qu'il soit recouru à un fichage systématique des utilisateurs. On notera à cet égard que dans le monde « hors ligne », les personnes achetant légalement un CD ou DVD ne sont pas systématiquement fichées, des systèmes de protection technique étant mis en place afin de limiter la copie[6].

Principes de nécessité et d'anonymat

Selon le principe de nécessité, il convient d'utiliser des données anonymes dans la mesure où un traitement de données à caractère personnel n'est pas nécessaire.

---

[3] Même si l'abaissement du niveau d'exigence des conditions de protection du droit d'auteur a fait naître une certaine controverse aujourd'hui à ce sujet.

[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.*

[5] Il y est fait cependant référence sous le point consacré à la durée limitée de stockage : "Conserver systématiquement des données d'utilisateurs uniquement dans l'éventualité d'une utilisation abusive présumée d'informations soumises à (un) droit d'auteur par un utilisateur spécifique ne serait pas conforme à ce principe", voy. page 7 du document de travail.

[6] Il convient, bien entendu, que ces mesures techniques ne soient utilisées que pour rendre impossible des actes qui sont normalement interdits et qu'elles ne limitent pas les droits légitimes des utilisateurs (par exemple la possibilité d'écoute sur différents supports).

Il conviendrait de faire à cet égard la distinction entre l'acte de transaction - qui permet à l'utilisateur d'obtenir gratuitement ou non l'œuvre -, et les moyens de protection ultérieurs de l'œuvre contre les contrefaçons.

Au sens de la Directive 95/46/CE, les données sont anonymes lorsqu'elles ne sont pas à caractère personnel (c'est-à-dire qu'elle ne permettent d'identifier directement ou indirectement une personne physique). L'anonymat sur l'Internet au stade de la transaction semble compromis dès lors qu'à tout le moins, l'adresse IP est nécessaire pour télécharger une information. Il conviendrait certainement de recommander la suppression des informations directement liées à une personne (son nom, adresse, etc.), lorsque cela n'est pas nécessaire, comme lors d'un téléchargement gratuit. En effet, si l'utilisateur achète une œuvre, le mode de paiement nécessitera généralement une identification de l'individu. Mais ces informations devront être supprimées une fois le paiement réalisé.

En ce qui concerne les mesures de protection postérieures à la transaction, le principe de l'anonymat retrouve alors tout son sens, comme le souligne à juste titre le document de travail: "lorsque les technologies DRM sont utilisées pour protéger des informations spécifiques, il convient d'utiliser des outils préservant l'anonymat de l'utilisateur".

Devoir d'information

Le principe de transparence, tel que découlant de la Directive 95/46/CE implique que le responsable de traitement informe clairement les personnes concernées notamment sur l'identité du responsable de traitement et sur les finalités du traitement. Un autre moyen d'assurer la transparence consiste pour le responsable de traitement de déclarer le traitement qu'il compte mettre en œuvre auprès d'une autorité de contrôle. En effet, les registres de ces autorités permettront aux personnes concernées de vérifier les finalités de traitement, les catégories de données traitées ainsi que les destinataires susceptibles de recevoir des données. Il pourrait s'avérer utile de rappeler le principe de l'obligation de notification à l'autorité de contrôle dans le document de travail.

Stockage limité des données à caractère personnel

Il nous semble que la conséquence de ce principe n'est pas de considérer non conforme une conservation *systématique* de toutes les données d'utilisateurs uniquement dans l'éventualité d'une utilisation abusive présumée d'informations soumises à droit d'auteur par un utilisateur spécifique[7], mais plutôt une conservation sans limitation de durée. Cela dit, le stockage systématique peut être remis en question au niveau de l'analyse de la proportionnalité des moyens mis en œuvre[8].

Autres obligations

Afin de mettre en œuvre un traitement respectueux de la vie privée, il faudrait également que le responsable de traitement mette en place des mesures de sécurité technique et organisationnelle afin de protéger les données. Par ailleurs les personnes concernées devraient pouvoir bénéficier d'un droit d'accès, de rectification et d'opposition (en cas de base de

[7] Ce qui est repris à la page 7 du document de travail.
[8] Voir sous le point ci-dessus intitulé « une finalité légitime ».

légitimité sur l'article 7 e, 7f ou en cas de traitement à des fins de commercialisation). Afin d'être exhaustif, le document pourrait également reprendre ces obligations.

III. Compétence d'enquête

Ici également, le document de travail effectue l'analyse des principes relatifs aux traitements des données ainsi que des obligations du responsable de traitement mais dans le cadre de traitements a posteriori consistant en le rassemblement de preuves disponibles en ligne par des personnes privées afin d'assurer la défense de leurs droits (ou des droits des personnes qu'elle représente). Le commentaire souligne les différents points qui, selon nous, nécessiterait une clarification.

Une finalité légitime

Que ce soit dans le monde réel ou virtuel, les sociétés de gestion collectives réalisent des enquêtes afin de protéger et défendre les droits de leurs membres. Les actions contre les individus soupçonnés de porter atteinte au droit d'auteur ne sont pas récentes. Le texte devrait peut-être préciser que les actions récentes visent les atteintes effectuées par le biais des réseaux.

En ce qui concerne la compétence d'enquête, l'examen de légitimité des finalités devrait comprendre un volet relatif au test de proportionnalité des moyens. Au regard de la proportionnalité, un traitement réalisé à des fins d'enquête *a posteriori* semble d'emblée moins contestable qu'un traitement global *a priori*[9].

Le principe de compatibilité

Selon ce principe, on ne peut normalement pas traiter ultérieurement des données pour de nouvelles fins si la finalité ultérieure du traitement est incompatible avec la finalité initiale. À ce titre, le document de travail suggère de ne pas réutiliser les bases de données Whois afin de compléter les informations obtenues sur les réseaux, par exemple de *peer-to-peer*.

Les informations communiquées sur les réseaux *peer-to-peer* ne sont pas, elles non plus, *a priori* destinées à être utilisées à de telles fins d'enquête. À suivre cette logique, on pourrait empêcher la réutilisation de l'ensemble des données disponibles sur l'Internet et ne permettre dès lors en pratique aucun moyen de collecte de données en ligne pour les détenteurs de droits intellectuels, désireux de faire respecter leurs droits.

Cela reviendrait à prétendre que si les détenteurs de droits intellectuels ont une finalité légitime, ils ne pourraient disposer de moyens pour traiter les données disponibles en ligne.

[9] On pourrait à cet égard s'inspirer des principes dégagés par le groupe de l'article 29 en ce qui concerne la surveillance des communications électroniques sur le lieu du travail (WP55), Document de travail du 29 mai 2002.

La définition de la compatibilité souffre certainement d'un manque de clarté au niveau européen. Cela implique en pratique une divergence d'interprétation au niveau national. Par ailleurs, les conséquences relatives à l'incompatibilité ne sont pas envisagées[10].

Face à ces incertitudes, plusieurs questions peuvent se poser :

- Peut-on prétendre que toute réutilisation pour une finalité différente est interdite?
- Ne serait-il pas possible de plutôt permettre une réutilisation dans les mêmes conditions que celle prévues pour la collecte initiale, c'est-à-dire par exemple en ayant une finalité légitime, en informant la personne concernée, etc.
- La réutilisation des données ne pourrait-elle être possible si une loi le permet ou si une autre base légitimant le traitement existe (selon les bases énumérées à l'article 7 de la directive) ? A cet égard, le test de proportionnalité semble déterminant. Ainsi, dans certaines hypothèses, il aboutirait à l'interdiction de la réutilisation des bases de données Whois, l'atteinte à la vie privée étant trop considérable compte tenu de la finalité envisagée (par exemple, lorsqu'il s'agit de finalité de commercialisation). Dans d'autres cas, par contre, le test autoriserait la réutilisation à des fins de préservation de droits intellectuels, si celle-ci est nécessaire et que d'autres moyens moins attentatoires ne sont pas disponibles.

Par ailleurs, le document de travail souligne, à juste titre selon nous, qu'il serait contraire au respect de la vie privée que les fournisseurs d'accès communiquent leurs données à des tiers, hormis dans certaines circonstances prévues par la loi, à des autorités publiques. À cet égard, il semblerait utile de citer l'article 8 de la Directive 2004/48/CE[11].

Rôle des fournisseurs d'accès à Internet.

Un stockage systématique *a priori* de toutes les données de trafic par les fournisseurs d'accès est parfois possible en dehors du cas de l'injonction des autorités judiciaires. En effet, certaines législations permettent également ce traitement, notamment à des fins de lutte contre la criminalité informatique[12].

---

[10] Il serait certainement utile de préciser les notions de compatibilité, d'incompatibilité et de conséquences dues à l'incompatibilité. Si ces interprétations seraient utiles pour tout type de traitement, il faut également souligner que pour les traitements réalisés à des fins historiques ou scientifiques, les problèmes d'interprétation sont encore accrus. En effet, si l'article 6.1.b Directive 95/46/CE établit qu' « un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées », les conséquences d'un traitement « non réputé incompatible » ainsi que les conditions d'un tel traitement ne sont pas claires en pratique, et cela spécialement lorsque les lois nationales des Etats membres transposent le principe sans déterminer de garanties appropriées ou de conditions de réutilisation (ce qui est la plupart du temps le cas), constatations réalisées lors du projet de recherche RESPECT, financé par la Communauté européenne, (DG IST) http://www.respectproject.org/

[11] Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, *Journal officiel* n° L 157 du 30/04/2004 p. 0045 – 0086.

[12] L'article 15 de la Directive 2002/58/CE permet à cet égard aux Etats membres d'adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques), *Journal officiel* n° L 201 du 31/07/2002 p. 0037 – 0047. Par exemple, l'article 14 de la loi belge du 28 novembre 2000 relative à la criminalité informatique oblige les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de

Traitement des données judiciaires

L'interprétation de la notion de « donnée judiciaire » est trop extensive même s'il est évident que la Directive 95/46/CE inclut dans cette catégorie de données sensibles des données qui n'étaient initialement pas prévues par la Convention 108 du Conseil de l'Europe. Cette convention ne visait que les données relatives aux «condamnations pénales», c'est-à-dire, selon le rapport explicatif de la convention, « les condamnations fondées sur une loi pénale et dans le cadre d'une procédure pénale ».

La Directive 95/46/CE vise les données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté[13]. Ces données ne peuvent normalement être traitées que sous le contrôle de l'autorité publique sauf si des garanties appropriées et spécifiques sont prévues par le droit national. Une lecture attentive de la directive ne permet pas, nous semble-t-il, d'inclure dans cette catégorie les données personnelles permettant à une personne privée de constituer un dossier sur une autre personne qui porte atteinte à ses droits. Si tel avait été le cas, la Directive 96/46/CE aurait certainement prévu une exception pour tout individu qui exploite des données personnelles dans le cadre d'un litige le concernant.

A cet égard, certaines lois nationales pourraient être interprétées différemment, comme par exemple la loi belge. Celle-ci semble inclure ce type de données, dès lors qu'elle vise les données relatives aux litiges, *aux suspicions*, aux poursuites, condamnations ou mesures de sécurité[14]. L'exception visant les personnes agissant dans le cadre de leur propre litige semble avoir été prévue à cet effet.

Dans ce contexte, il ne nous semble pas, en principe, que les données personnelles collectées sur l'Internet à des fins de défense des droits intellectuels puissent être assimilées à des données sensibles au regard de la Directive 95/46/CE et jouissent à ce titre du même régime de protection.

Par ailleurs, la Directive 2004/48/CE relative au respect des droits d'auteur vise effectivement à permettre aux autorités judiciaires d'ordonner la communication des informations sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle lorsque le requérant en fait une demande justifiée et

---

télécommunications, pendant un certain délai (qui ne peut être inférieur à 12 mois) en vue de l'investigation et de la poursuite d'infractions pénales, *M.B.*, 03.02.2001, pp. 2909 et s.

[13] Article 8.5 de la Directive 95/46.

[14] Article 8 de la loi relative à la protection des données à caractère personnel du 8 décembre 1992, *M.B.*, 18 mars 1993 telle que modifiée par les lois du 11 décembre 1998, *M.B.*, 3 fév. 1999 et du 26 février 2003, *M.B.*, 26 juin 2003. Version coordonnée disponible sur le site web http://www.privacy.fgov.be/ . Nous soulignons, car inclure les suspicions dans le champ des données judiciaires est la spécificité de la loi belge et pourrait être interprété comme les données relatives à la constitution d'un dossier par les personnes privées en vue de défense de leurs droits. Voir à cet égard l'avis d'initiative n° 44/2001 du 12 novembre 2001 de la Commission de Protection de la vie privée belge concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunication, également disponible sur http://www.privacy.fgov.be/ . On pourrait cependant plaider contre une telle interprétation en premier lieu du fait que le mot suspicion laisse clairement entendre qu'il s'agit de suspicion dans le cadre d'une procédure judiciaire mais également du fait qu'une telle interprétation impliquerait une divergence inopportune avec la directive.

proportionnée dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle.

Cette information peut être exigée auprès du contrevenant et également auprès d'une autre personne qui a été trouvée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités contrefaisantes.

Cette autre personne doit dès lors fournir des services à une échelle commerciale, services qui sont utilisés dans des activités contrefaisantes. Il ne s'agit donc pas de conditionner la communication d'informations aux seules « atteintes qui présentent une échelle commerciale »[15] ou lorsque un « avantage commercial [est] lié à l'infraction »[16].

Si cette personne tierce au contrevenant tire un avantage commercial de l'infraction, elle peut également être poursuivie ; sa responsabilité ne se limitant pas à la simple communication d'informations. En utilisant le critère de l'avantage commercial lié à l'infraction, le champ d'application de l'article 8 de la Directive 2004/48/CE est trop limité. Il nous semble que la condition d'avantage commercial est plutôt liée aux services utilisés dans les activités contrefaisantes[17]. Dès lors, si un fournisseur d'accès à l'Internet tire un profit de cet accès, il serait soumis à cette obligation, alors qu'une université n'y serait pas soumise.

IV. Conclusions

En guise de conclusions, nous préconisons que le groupe de travail de "l'article 29" :

- se positionne plus clairement sur la proportionnalité des moyens et des stratégies d'actions (*a priori* ou *a posteriori*) des détenteurs de droits intellectuels. A cet égard, il nous semble plus respectueux de la vie privée de privilégier des moyens d'action *a posteriori*, plutôt qu'un fichage systématique *a priori* des personnes[18], et ce d'autant plus que celles-ci souhaitent obtenir *légalement* des œuvres par le biais des réseaux. Outre la question de la proportionnalité des moyens mis en œuvre, le nombre de données traitées et donc susceptibles de réutilisation à des fins de profilage ou de marketing serait nettement moindre en ce qui concerne un traitement *a posteriori*.

- vérifie dans quelle mesure les législations relatives à la confidentialité des communications électroniques ne pourraient également constituer un obstacle pour les détenteurs de droits dans la collecte d'information sur les réseaux[19].

[15] Page 8 du document de travail.
[16] Page 8 du document de travail.
[17] On pourrait à cet égard tenter de faire un rapprochement entre la notion « d'échelle commerciale » et la notion de fournisseur service de communications électroniques accessibles au public, ce qui exclut les « closed user group », afin d'harmoniser l'interprétation de différentes directives, notamment de la Directive 2004/48/CE avec la Directive 2002/58/CE.
[18] On pourrait à cet égard s'inspirer des principes dégagés en ce qui concerne la surveillance des employés sur le lieu du travail, où l'on tend à exclure toute surveillance générale systématique, Document de travail du groupe de l'article 29, concernant la surveillance des communications électroniques sur le lieu de travail, du 29 mai 2002.
[19] L'article 5 de la Directive 2002/58/CE prévoit que « les Etats membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque

- définisse et de pose un cadre juridique clair en ce qui concerne les possibilités d'enquête des détenteurs de droits et cela pour limiter les divergences nationales qui risquent non seulement d'affecter le marché intérieur (1er pilier) mais également la coopération judiciaire (3ème pilier). Ce cadre devrait prendre en compte les aspects relatifs à la valeur probante des traces informatiques ainsi que de leur recevabilité en tant que preuve en justice :

  Valeur probante des traces informatiques

  - De manière générale, force est de constater que les traces informatiques sont certainement, d'un point de vue probatoire, des preuves imparfaites, comme en témoignent les adresses IP. En effet, même si elles sont considérées en principe comme des données à caractère personnel, celles-ci ne conduisent pas toujours directement ou indirectement à une personne déterminée. D'abord, elles ne renvoient qu'à une machine derrière laquelle s'est trouvé un individu déterminé à un moment donné et dont il va falloir prouver la présence. Ensuite, même si l'individu est identifié, il faut tenir compte du fait qu'il ne maîtrise pas nécessairement tout ce qu'il se passe sur son ordinateur (il arrive souvent qu'un virus envoie des mails à l'insu de l'utilisateur). Enfin, il faut également compter avec le développement de certaines technologies spécifiques (l'utilisation de NAT[20] ou de système WIFI par exemple), qui permettent maintenant à une multitude de personnes d'utiliser simultanément une seule adresse IP.
  - Par ailleurs, la valeur probante des données collectées à des fins d'enquête par des personnes privées doit, nous semble-t-il, être subordonnée à la prise en considération préalable des mesures relatives à leur intégrité. Par exemple, l'heure de connexion de telle adresse IP établie par le seul système informatique d'une personne privée ne peut avoir valeur probante parfaite, sans qu'un tiers de confiance n'intervienne avec un système d'horodatage. Par ailleurs, les traces informatiques sont vulnérables car elles peuvent être facilement modifiées…
  - En admettant un système d'enquête privées ou de traitement *a priori* (DRM), sans souligner la nécessité du maintien de l'intégrité des données, le document pourrait implicitement donner aval à l'admission de telles preuves au niveau probatoire. Les risques liés à la vulnérabilité de la force probante ne doivent pas être négligés et devraient être intégrés dans la réflexion même des moyens d'enquête disponibles considérés comme proportionnés.

  Recevabilité de la preuve

  Par ailleurs, il faut également souligner les risques inhérents au niveau de la recevabilité de la preuve des traces informatiques. Une preuve qui a été obtenue dans l'illégalité car ne respectant pas les droits et libertés des individus ne peut être acceptée en justice. Par conséquent, une position du groupe de

---

cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité », *op. cit.*

[20] ***N**etwork **A**ddress **T**ranslation.*

l'article 29 quant à la proportionnalité des moyens *a priori* et *a posteriori* pourrait clarifier certainement cette question.