De la lecture croisée à une réflexion commune juriste/informaticien

Illustration, autour des virus informatiques et de la notion d'intégrité

Isabelle de Lamberterie et Marion Videau
CNRS-CECOJI
{delamberterie, marion.videau}@ivry.cnrs.fr

31 mai 2006

SSTIC'06

@sphales

Les limites de la sécurité...

- Ce que la sécurité ne peut pas faire
- Ce qui délimite, encadre, définit la sécurité
- Ce que la sécurité partage avec d'autres domaines

$\rightsquigarrow$ La sécurité informatique ressort de l'usage de l'outil informatique

- La régulation juridique de la sécurité informatique
- La recherche commune sur la sécurité informatique et juridique

Plan

- Recherche en informatique et motif légitime
  - Contexte législatif
  - Étendue de la réalité informatique
- Intégrité de l'écrit électronique
  - Intégrité et sécurité juridique
  - Intégrité et sécurité informatique
  - L'éclairage des archivistes

Détention ou mise à disposition de virus informatiques

Le contexte législatif

- Renforcement de l'arsenal répressif en 2004 (loi sur la confiance dans l'économie numérique)
- Vise directement la détention et la mise à disposition d'équipements, d'instruments, de programmes informatiques ou de toutes données conçus pour commettre les faits d'intrusion dans un système ou d'entrave au fonctionnement de ce système
- Permet de sanctionner la détention d'un virus informatique avant que le virus n'ait été introduit frauduleusement dans un système informatique.

Article 323-3-1 du Code pénal

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- 323-1 : $\begin{cases} \text{2 ans d'emprisonnement et 30000 euros d'amende} \\ \text{3 ans d'emprisonnement et 45000 euros d'amende} \end{cases}$
- 323-2 et 323-3 : 5 ans d'emprisonnement et 75000 euros d'amende

Recherche et détention de virus ?

- Le projet initial : exception au délit quand détention pour les besoins de recherche
- Débats parlementaires : besoins de la recherche scientifique et technique ou protection de la sécurité des réseaux de communication qualifiées de particulièrement imprécises, susceptibles de recouvrir des organismes irréprochables et d'autres qui le seraient moins, certains pouvant être tentés de développer des virus informatiques en excipant de leur mission de sécurisation des réseaux.

. . . sans motifs légitimes. . .

- La recherche scientifique et la sécurisation des réseaux pourront entrer dans le champ des motifs légitimes
- Il faudra justifier ceux-ci.

D'où l'inquiétude de la communauté scientifique. . .

Et l'invitation à une (re-)lecture des autres textes du code pénal relatifs aux systèmes de traitement automatisés de données ?

Étendue de la réalité informatique

- Mais de quoi parle-t-on ?
- accéder, se maintenir dans, entraver, fausser, introduire
- Accéder à un système de traitement automatisé de données est-il équivalent à entrer dans une maison ?

Changement de paradigme : de la sécurité physique à la sécurité logique

- Le vocabulaire, les métaphores influencent la perception du problème
- Et si on changeait de modèle ?

Exemple : affaire dite Kitetoa

Accès à des bases de données client non-protégées à partir d'un navigateur

- 13 février 2002 : Tribunal correctionnel de Paris déclare coupable
- 30 octobre 2002 : Relaxe suite à appel du Parquet général

Et si le Tribunal avait considéré un autre modèle ?

- Modèle client-serveur
- Une requête et une réponse à une requête

Que se passe-t-il pénalement lorsqu'on obtient de quelqu'un des informations ? Et si celles-ci étaient confidentielles ?

Le modèle : l'espion rusé et le dépositaire d'un secret

Scénario type :

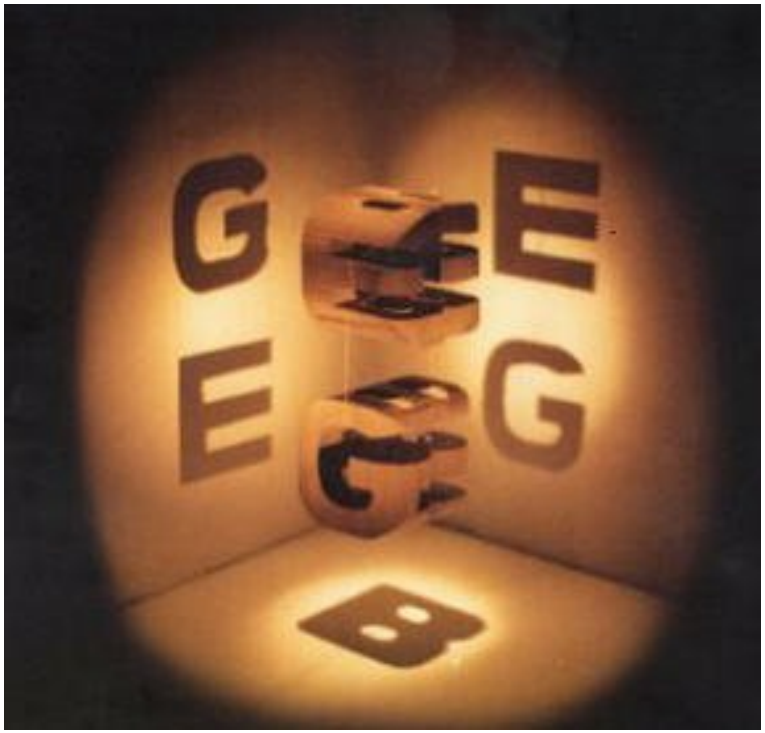
- Faire boire (de l'alcool) le dépositaire du secret
- Lui faire du charme (secrets d'alcôve ?)
- Lui soutirer les informations

Comment est-ce pris en compte par la loi ?

$\longrightarrow$ Le dépositaire du secret est responsable...

Les modèles et l'appréhension externe de l'informatique

- Réfléchir à des modèles liés à la logique plutôt qu'au monde physique



Métaphore de la triplettre de Gödel, Escher, Bach [Hofstadter 1979] : tant qu'on n'aura pas saisi l'essence de la notion, on ne travaillera que sur une de ses projections. . .

Cette étude est primordiale pour les activités des personnes dans cette salle !

Lorsque la potentialité du délit devient un délit

- Article 323-3-1 : tous les débitants d'alcool et les vendeurs d'alcôves devraient-ils prouver un motif légitime à leur activité ?

- Rôle de l'expert ?

[...] si l'expert est capable d'expliquer la logique interne des dispositifs, [...], il est aussi démuni que tout un chacun pour aborder les conséquences de la technique selon des points de vue externes. On sort du technique pour rentrer dans la politique, au sens où elle est l'affaire de chacun et non de quelques uns. [Bachimont 2004]

Pour aller un peu plus loin

- Que signifie système de traitement automatisé de données ?

Cela ne pourrait-il pas viser exclusivement les systèmes traitant de données personnelles ?

Dans ce cas l'article 226-17 du Code pénal dit que le responsable de traitement est tenu de prendre toutes précautions utiles [...] pour préserver la sécurité des données.

Quelle application ?

⟶ La quadrature du cercle [Sédallian 2003] ?

Intégrité de l'écrit électronique

La double caractérisation de l'intégrité

- Caractéristique de l'absence de modifications des données constituant un document
- En droit, qualités attendues d'un écrit signé traditionnel : durabilité, fidélité et fiabilité

Intégrité d'un écrit

- La valeur probatoire d'un écrit électronique dépend (entre autre) des conditions de son établissement et de sa conservation de nature à en garantir l'intégrité

Intégrité et signature

A. 1316-4 C.civ.

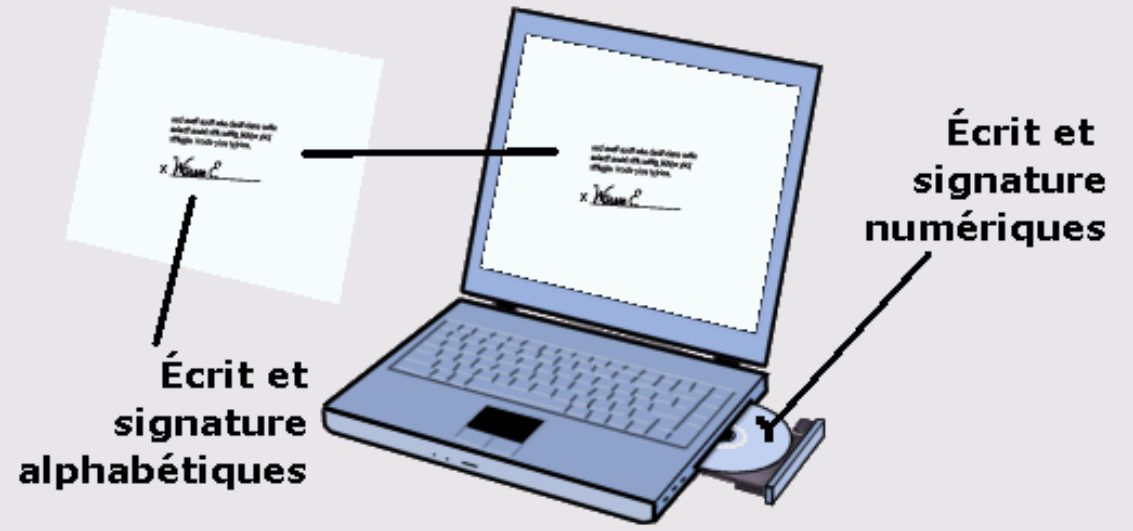
[...]
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État

Des questions techniques

- Que veut dire garantir l'intégrité ?
- L'une des finalités de la signature électronique n'est-elle pas d'apporter cette garantie ?
- Intégrité et migration?

Des questions d'informaticiens

- Mais de quoi parle-t-on ?

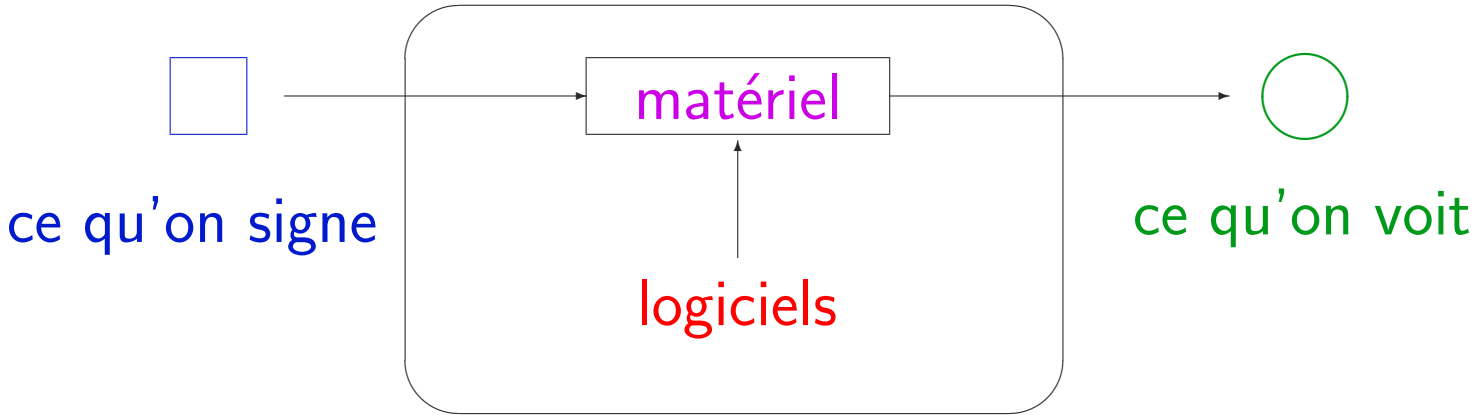


A. 1316-1 C.civ.

L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier,

sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Quel statut pour le matériel et le logiciel ?



Quel statut ?

Sur quel(s) élément(s) porte(nt) la nécessité de l'intégrité ?

- Pour l'informatique : sur ce qu'on signe
- Pour le droit : sur ce qu'on voit

Des réponses informatiques inadaptées ?

- Nécessité de conserver les données électroniques
- A-t-on des réponses cryptographiques, même informatiques qui prennent en compte l'aspect temporel du problème ?
- Les protocoles cryptographiques se révèlent adaptés à la transmission dans l'espace mais mal/pas dans le temps
- Comment prendre en compte cette nécessité pour les durées demandées par la loi ?
  - 5 ans, 10 ans, 30 ans
  - sans limite de durée pour les archives à valeur patrimoniale

L'éclairage des archivistes

- Remise en cause du lien entre intégrité physique et authenticité du document
- Il n'est pas possible de conserver un écrit électronique en tant qu'objet physique entreposé. Il est seulement possible de préserver un document manifeste.

À distinguer...

- Authenticité d'un document qu'il soit ou non électronique d'une part et l'authentification apportée par la signature électronique d'autre part.
- Vérification de la signature électronique entendue dans son sens technique se limitant aux moyens mis en œuvre pour atteindre l'identification et vérification au sens juridique de l'authentification d'un document (identification et adhésion au contenu d'un acte)

La chaîne de préservation

Ensemble des contrôles et des procédures qui assurent l'identité et l'intégrité d'un document au travers de la totalité de son cycle de vie.

Les recommandations du Forum des droits sur l'Internet

Les trois critères cumulatifs du processus de conservation :

- la lisibilité du document
- la stabilité du contenu informationnel
- la traçabilité des opérations sur le document.

La lisibilité du document

- Possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte
- Cette démarche est facilitée par les méta-données associées au document.

Stabilité du contenu informationnel

Désigne la nécessité de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine et qu'aucune n'est omise ou rajoutée au cours du processus de conservation.

La traçabilité

Désigne la faculté de présenter et de vérifier l'ensemble des traitements, opérés sur le document lors du processus de conservation.

Conclusion

- Les limites de la sécurité : deux exemples
- Régulation juridique de la sécurité informatique : la recherche pour maintenir possible la liberté de la recherche
- La recherche commune sur la sécurité informatique et juridique : cas de l'écrit et de la preuve électronique

$\Longrightarrow$ Nécessité de coopération inter-disciplinaire par la nature même du sujet qui porte sur les usages d'une technique.