L'évolution du contexte juridique de la sécurité des systèmes d'information

Bertrand Warusfel

Maître de conférences
à la faculté de droit de l'Université Paris V,
Avocat au barreau de Paris
(cabinet FWPA)

http://www. droit.univ-paris5.fr/warusfel

- L'assouplissement progressif des contrôles sur le commerce des moyens de chiffrement
- L'encadrement des conditions et des effets de l'utilisation de la signature électronique
- Le renforcement des moyens de lutte contre l'utilisation illicite des moyens de cryptographie

(NB : on prendra des exemples dans le droit français, mais la problématique est plus largement européenne, voire internationale)

L'assouplissement progressif des contrôles sur le commerce des moyens de chiffrement

- Des contrôles assouplis sur l'exportation de produits de chiffrement américains
- La libéralisation irréversible des limitations françaises sur le commerce du chiffrement
- Vers une révision des critères de contrôle à l'exportation fixés dans le cadre de l'arrangement de Wassenaar ?

La libéralisation irréversible des limitations françaises sur le commerce du chiffrement

- Régime actuel :
  - Liberté d'utilisation et d'exportation des moyens de signature
  - Autorisation préalable d'exportation du chiffrement > 56 bits
  - Déclaration préalable du chiffrement <= 128 bits de clé
  - Autorisation préalable pour chiffrement > 128 bits
- Prochaine libéralisation définitive
  (projet de loi Économie numérique art 18.III):

  "La fourniture, le transfert depuis un État membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au *b* du présent III. Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés"

L'encadrement des conditions et des effets de l'utilisation de la signature électronique

- La reconnaissance juridique de la signature électronique
- Les conditions techniques nécessaires pour bénéficier des effets juridiques de la signature électronique
- L'admission de l'écrit électronique à titre de preuve

La reconnaissance juridique de la signature électronique

- fonctions d'une signature (art. 1316-4 CCiv) :
  - identifie celui qui l'appose
  - manifeste son consentement aux obligations découlant de l'acte signé
- possibilité d'une signature sous forme électronique

  "Lorsqu'elle est électronique, [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache." (1316-4CCiv – Loi 130300)

⇒ tout moyen d'authentification électronique dont l'utilisateur peut prouver la fiabilité sera reconnu comme une signature électronique

Les conditions nécessaires pour bénéficier des effets juridiques de la signature électronique

- "La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié." (art 2 D300301)

⇒ signature sécurisée + dispositif de création sécurisé
+ certificat qualifié = présomption de fiabilité
= inversion de la charge de la preuve

Signature électronique sécurisée

=

"une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable." (art 1er D300301)

Exigences pour un dispositif sécurisé de création de signature électronique :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :
   a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée;
   b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
   c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

+ doit être certifié conforme à ces exigences par DCSSI (1er Ministre) après évaluation (CESTI) ou par un autre organisme de l'Union européenne

L'admission de l'écrit électronique à titre de preuve

- définition large de la preuve par écrit :

  "La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission." (art 1316 CCiv)

- équivalence avec écrit électronique :

  "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" (art 1316-1 CCiv)

Le renforcement des moyens de lutte contre l'utilisation illicite des moyens de cryptographie

- Le cadre général de l'accroissement des moyens procéduraux pour lutter contre la "cybercriminalité"
- Des instruments légaux pour favoriser la "mise au clair" des données chiffrées saisies ou interceptées
- L'aggravation des peines réprimant des délits préparés ou commis avec l'aide de moyens de chiffrement

Les moyens et procédures prévus par la Convention sur la cybercriminalité (23 nov 2001)

- Conservation rapide des données
- Injonction de produire
- Perquisition et saisie des données
- Collecte en temps réel
- Coopération internationale
- Extradition
- Entraide

Moyens utilisables pour infractions informatiques + infractions classiques commises via l'informatique

Conservation rapide des données (données stockés, données de trafic)

- pouvoir d'enjoindre à toute personne
  "la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification"
  + la sauvegarde de ces données conservées pendant une durée maximale de 90 jours, éventuellement renouvelable (art. 16.1)
- obligation aux fournisseurs de services
  de conserver et de communiquer les données de trafic
  pour permettre, notamment, *"l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise"* (art. 17)

Injonction de produire

- pouvoir d'enjoindre
  - à tout utilisateur de communiquer des données informatiques en sa possession
  - et à tout fournisseur de service de communiquer les données relatives à ses abonnés

  (art. 18)

Perquisition et saisie des données

- pouvoir de perquisitionner et d'accéder à tout système informatique installé sur le territoire national, et de saisir ou de copier toute information numérique qui y est stockée

  y compris à distance sur un autre système situé sur le territoire national et accessible depuis un système initial (art. 19)

Collecte en temps réel (données de trafic, interceptions de contenus)

- pouvoir de collecter (ou de faire collecter par les fournisseurs de service) en temps réel les données de trafic (art. 20)

+*"relativement à un éventail d'infractions graves à définir en droit interne"*, le pouvoir d'intercepter (ou de faire intercepter) le contenu de certaines communications
(art. 21)

Coopération et entraide

- Extradition
  inclusion automatique des infractions informatiques dans le champ des conventions d'extradition
- Entraide
  demande d'entraide urgente par télécommunications
  + informations spontanées (et confidentielles)
  + demande de conservation rapide de données
  + demande de perquisition ou de saisie
  + entraide pour la collecte et l'interception
  + accès transfrontière libre aux données ouvertes
  + Réseau de points de contact nationaux 24h/7j

favoriser la "mise au clair" des données chiffrées saisies ou interceptées

- "lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire. (…)
- Si la peine encourue est égale ou supérieure à 2 ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'État soumis au secret de la défense nationale" (futur art. 230-1 Code procédure pénale)

"Est puni de trois ans d'emprisonnement et de 45000 e d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités. Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75000 e d'amende" (futur *434-15-2.* CP)

Les personnes qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions. Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30 000 e d'amende (futur art. *11-1* loi 10 juillet 91)

L'aggravation des peines réprimant des délits préparés ou commis avec l'aide de moyens de chiffrement

"Lorsqu'un moyen de cryptologie au sens de l'article 17 de la loi n° du pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :
1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de 30 ans;
2° Il est porté à 30 ans de réclusion criminelle lorsque l'infraction est punie de 20 ans,
3° Il est porté à 20 ans de réclusion criminelle lorsque l'infraction est punie de 15 ans
4° Il est porté à 15 ans de réclusion criminelle lorsque l'infraction est punie de 10 ans;
5° Il est porté à 10 ans d'emprisonnement lorsque l'infraction est punie de 7 ans;
6° Il est porté à 7 ans d'emprisonnement lorsque l'infraction est punie de 5 ans;
7° Il est porté au double lorsque l'infraction est punie de 3 ans d'emprisonnement au plus.
(futur *Art. 132-77 Code pénal)*

conclusion

- on passe progressivement d'une problématique de limitation de l'utilisation des moyens de sécurité à l'acceptation (voire à l'encouragement) de cette utilisation dans la société et sur le marché
- dès lors, il faut prendre en compte les conséquences juridiques de ces utilisations
  et s'efforcer d'en tirer le meilleur profit (par ex. pour la protection des droits intellectuels sur les réseaux, ou pour l'authentification des échanges numériques par la signature électronique) tout en limitant les effets potentiellement dangereux de l'utilisation illicite de ces moyens.