Si vis pacem, para bellum

Du code au crochetage

Changement d'échelle avec la démocratisation d'Internet

→Augmentation de la masse de données collectées

→ Analyse en continu

Si vis pacem, para bellum

Acceptabilité sociale des technologies

Internet comme infrastructure essentielle

→Données personnelles, protection des sources, liberté d'expression, ou de l'application effective des droits et libertés fondamentaux

→ Nouvelles fragilités, crise de confiance systémitque

CASTEX 08/2021

JCSA 10 JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Mundi innumerabiles

Une construction progressive d'un droit français du chiffrement

JCSA 10 JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Mundi innumerabiles

Code ←→ Langue ←→ Mystère

De la volonté de pénétrer les secrets et mystères

De la volonté de se préserver du regard d'autrui

Mundi innumerabiles

Tensions

- Dans la sphère privée
- Dans la sphère publique

→ Dans la fabrique de la loi

Codage, chiffrage, cryptage

Risque d'interception

Mundi innumerabiles

Si vis pacem, para bellum

- Une méfiance à l'égard du chiffrement

- Chiffrement appréhendé par le droit comme une arme et fait l'objet d'un contrôle drastique

Mundi innumerabiles

Si vis pacem, para bellum

- Une méfiance à l'égard du chiffrement

- Chiffrement appréhendé par le droit comme une arme et fait l'objet d'un contrôle drastique

En 1939, décret pris en application de l'article 1er du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions

Les « machines cryptographiques » sont classées aux côtés des dispositifs de visée, de conduite de tir ou de détection dans les matériels de guerre en 1re catégorie comptant également les « Fusils, mousquetons, carabines de tous calibres conçus pour l'usage militaire »

CASTEX 08/2021

Mundi innumerabiles

Si vis pacem, para bellum

- Une méfiance à l'égard du chiffrement

- Chiffrement appréhendé par le droit comme une arme et fait l'objet d'un contrôle drastique

Régime d'autorisation préalable

Une définition posée par le décret du 18 février 1986 des moyens de cryptologie considérés comme « matériels ou logiciels conçus soit pour transformer à l'aide de convention secrète des informations claires ou des signaux en information ou signaux inintelligibles, soit pour réaliser l'opération inverse ».

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Régime complexe et inadapté

Loi du 29 décembre 1990 sur la réglementation des télécommunications

→ Régime strict d'autorisation préalable

→Régime plus souple de déclaration préalable :

L'utilisation ou la fourniture de moyens ou de prestations de cryptologie quand ils ne peuvent « **avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis** ».

CASTEX 08/2021

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Libéralisation progressive

Régime complexe et inadapté

Internet commence à entrer dans les foyers et les entreprises

Régime libéral dans les pays voisins : concurrence

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Libéralisation progressive

De la limitation de la liberté au risque d'abus

Déjà : Loi 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications

Au niveau international : l'arrangement de Wassenaar

CASTEX 08/2021

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Libéralisation progressive

Internet commence à entrer dans les foyers et les entreprises

Conseil de l'Europe, 11 septembre 1995 : recommandation adoptée par le Comité des ministres relative aux problèmes de procédure pénale liés à la technologie de l'information

Il est loisible de limiter l'impact du chiffrement sur l'enquête en matière pénale « sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale »

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Libéralisation progressive

Internet commence à entrer dans les foyers et les entreprises

Assouplissement progressif : loi du 26 juillet 1996

- Utilisation libre d'un moyen ou d'une prestation de cryptologie « si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis »

CASTEX 08/2021

Mundi innumerabiles

Si vis pacem, para bellum

Développement progressif des nouvelles technologies de l'information et de la communication

Libéralisation progressive

Internet commence à entrer dans les foyers et les entreprises

Assouplissement progressif : loi du 26 juillet 1996

- Fonction de confidentialité : l'utilisation devient libre sous réserve d'utiliser « des conventions secrètes gérées selon les procédures et par un organisme agréés »

➔ Séquestre : remise des clefs de chiffrement au tiers de confiance

JCSA JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

L'Architecte aux pieds nus

JCSA JOURNÉE DU CONSEIL SCIENTIFIQUE Afnic

Mundi innumerabiles

Evolutions au niveau international

- Lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) en mars 1997

  Recommande « veiller à la levée, ou d'éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés au commerce international et au développement des réseaux d'information et de communication »

En France, Conseil d'Etat (1998) insiste sur la nécessité d'une confiance accrue dans la confidentialité des échanges

L'Architecte aux pieds nus

Le 19 janvier 1999, à l'issu du second comité interministériel pour la société de l'information, le Premier ministre annonce une libéralisation de l'utilisation de la cryptologie

« moyen essentiel pour protéger la confidentialité des échanges et la protection de la vie privée »

L'Architecte aux pieds nus

Succession de textes :

- Loi relative à la sécurité quotidienne du 15 novembre 2001
- Loi pour la confiance dans l'économie numérique du 21 juin 2004

Du 10 au 12 décembre 2003, se déroule la première phase du **Sommet mondial sur la société de l'information → Volonté d'une vision d'ensemble et de tirer parti des possibilités des TIC**

L'Architecte aux pieds nus

Du 10 au 12 décembre 2003, se déroule la première phase du **Sommet mondial sur la société de l'information → Volonté d'une vision d'ensemble et de tirer parti des possibilités des TIC**

Quel équilibre ?

- Recherche ardue d'équilibre entre ordre public et confidentialité

- Obligation de déchiffrement

CASTEX 08/2021

L'Architecte aux pieds nus

Loi pour la confiance dans l'économie numérique du 21 juin 2004 : refonte du régime juridique

- Principe : **l'utilisation des moyens de cryptologie est libre**
- réécriture des définitions

Moyen de cryptologie désigne « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète »

- Avec des réserves

L'Architecte aux pieds nus

Avec des réserves

- l'utilisation d'un moyen de cryptologie pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission est une **circonstance aggravante**

Surveillance licite mais étendue et garanties → respects des droits et libertés fondamentaux

V. Conseil d'État, Le numérique et les droits fondamentaux, étude annuelle 2014, avis de la CNCDH, etc

L'Architecte aux pieds nus

Au niveau européen : adoption après de longs débats du règlement général sur la protection des données (2016)

- Appréciation du risque et d'un niveau de sécurité adapté

- L'article 32 impose de mettre mettent en œuvre « les mesures techniques et organisationnelles appropriées » dont le chiffrement fait partie

L'Architecte aux pieds nus

En France → **levée de confidentialité**

Article 230-1 du code de procédure pénale permet à l'autorité judiciaire ou à l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, de demander la mise au clair de données chiffrées

Recours aux moyens de l'État soumis au secret de la défense nationale

Obligation de coopération de l'article L. 871-1 CSI

L'Architecte aux pieds nus

Article 434-15-2 du code pénal : refus de remise aux autorités judiciaires ou de mise en œuvre d'une convention de déchiffrement d'un moyen de cryptologie

Conseil constitutionnel, 30 mars 2018, n° 2018-696 QPC

Jurisprudence hésitante au fond

L'Architecte aux pieds nus

Prolifération de textes à l'aune d'un renforcement de la lutte contre le terrorisme et le crime organisé

Différentes techniques d'enquête, de l'interceptions, à la captation de données, à la surveillance ciblée, etc

Chiffrement de bout en bout parfois perçu comme rendant inopérant les techniques de déchiffrement

Porte dérobée, faille de sécurité

L'Architecte aux pieds nus

Proportionnalité & nécessité

- **Recherche d'équilibre**
- Un chiffrement robuste contribue à l'**exercice des libertés et droits fondamentaux**
- CNIL : le chiffrement contribue à « la résilience de nos sociétés numériques et de notre patrimoine informationnel »

La confiance des citoyens numériques est un vecteur essentiel de démocratie et d'innovation.

Des questions ?

Contact :

Courriel

Twitter : @LucienCastex

LinkedIn : https://www.linkedin.com/in/luciencastex/

De l'auteur :

Castex L., à paraître, « Le chiffrement des communications électroniques, du droit au code » dans Theviot A. (dir.), Gouverner par les données, Paris, Edition de l'ENS.

CASTEX 08/2021


JCSA
JOURNÉE
DU CONSEIL
SCIENTIFIQUE
Afnic
10
EDITION
Merci !
Des questions ?