

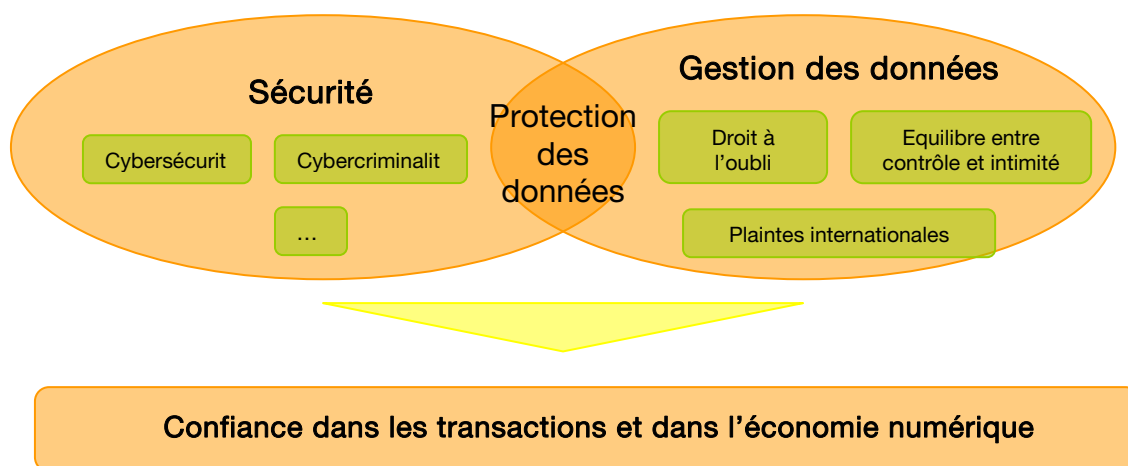
1.4.3 – Variable Sécurité/Confiance dans les Transactions/Gestion des données primées

Membres référents pour la Commission à l'Economie numérique : Philippe Lemoine et Frédéric Sutter

1 – Définition de la variable

Dans cette fiche, la **sécurité** (sécurité des systèmes d'information, cybercriminalité, droit à la vie privée...) est considérée comme un **pré requis « technique » à la gestion des données privées** (ou *privacy*, cf. lien avec la fiche usages 1.1.4). Cette fiche n'aborde pas les questions techniques (sécurité des réseaux et des systèmes informatiques...).

Des dispositifs numériques sécurisés, respectant la vie privée, établissent la confiance dans les transactions électroniques, une des conditions de l'essor de l'économie numérique.



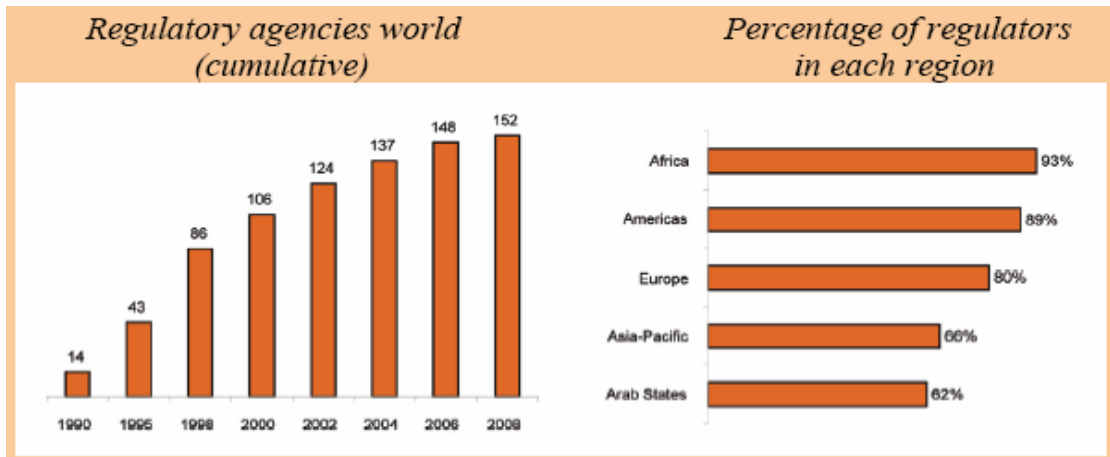
Dans cette fiche, les pas de temps sont de l'ordre de 10 ans (environ 7 ans pour la révision en profondeur des législations et la mise en œuvre des concertations internationales + 3 ans pour la mise en œuvre effective des recommandations).

Hypothèse fondamentale de la fiche

La régulation et la réglementation sont traitées à l'échelle internationale étant donné la montée en puissance d'Internet - système par nature décentralisé et sans frontières - comme support de l'économie numérique.

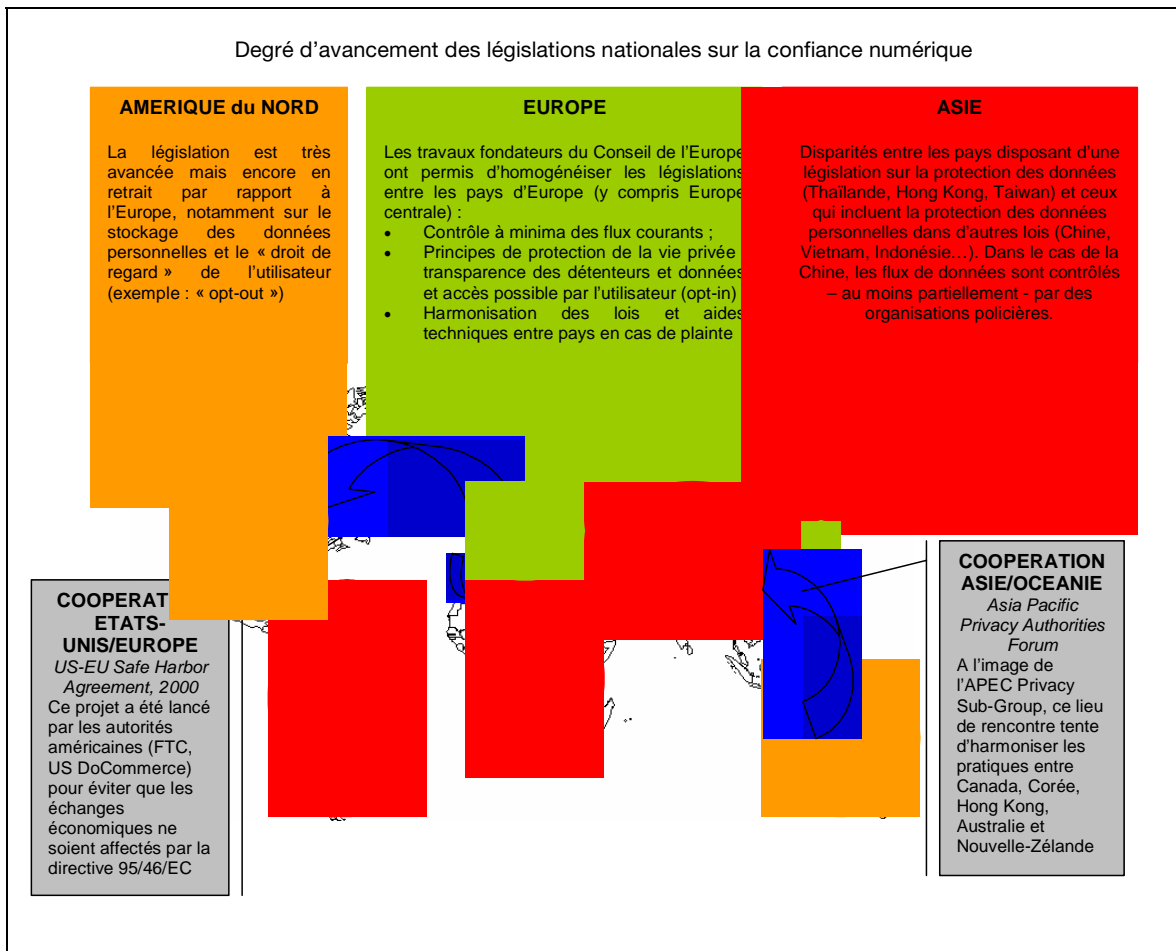
2 – Indicateurs pertinents (instruments de mesure pour évaluer la variable dans le temps)

- L'évolution du nombre d'agences régulatrices nationales, leur efficacité et leur taille



Source : Telecommunications trends 2009, ITU

- Indicateurs sur le niveau de sécurité et/ou de respect des données privées par pays et/ou zone géographique

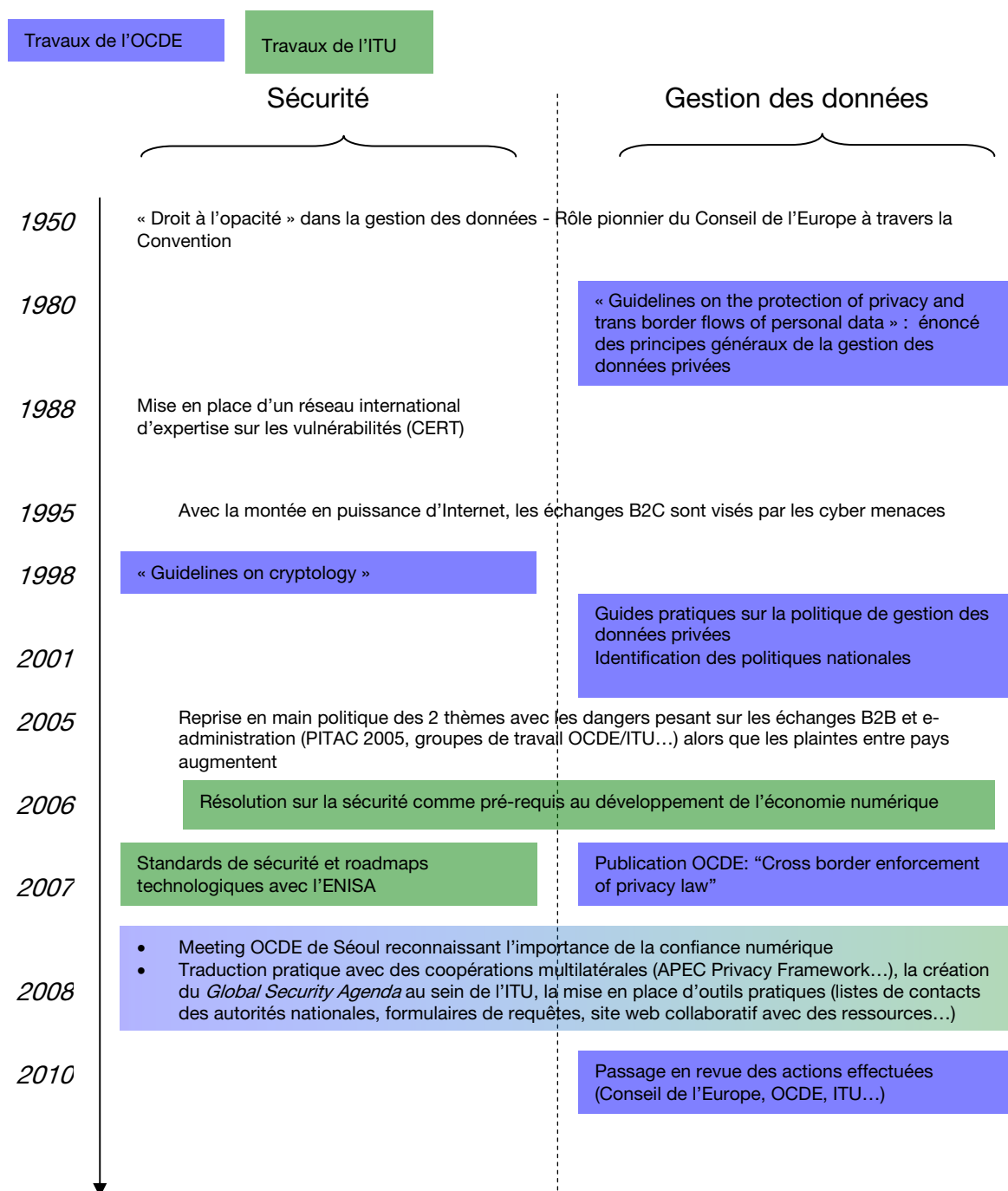


Source : CNIL

3 – Rétrospective (les 20 dernières années ; quoi, comment et par qui ?)

Evolution de la régulation depuis 50 ans

De l'approche négative « droit personnel à l'opacité » à l'approche positive « équilibre entre intimité et contrôle des données »



La régulation internationale dans les domaines de la sécurité et de la gestion des données est un sujet relativement récent. Entre 1950 et 1995 (téléphonie, échanges de données simples et structurées), les législations nationales étaient suffisantes pour réguler les télécommunications, qui avaient cours à l'intérieur du pays ou entre deux pays. Au début des années 1980 toutefois, deux institutions ont mené des travaux sur la gestion et la sécurité des données personnelles :

- en **1981, le Conseil de l'Europe** adopte la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel¹ », aboutissant à l'harmonisation des législations des pays européens ;
- l'**OCDE** avec sa publication « Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel » qui énoncent les **principes généraux**.

Puis, au milieu des années 1990, avec l'essor mal anticipé d'Internet (système par nature décentralisé et sans frontières), les autorités nationales de régulation ont été confrontées à l'augmentation des cas de litiges impliquant plusieurs pays.

Un changement de paradigme technique dans la gestion des données privées

En 15 ans, la gestion des données privées et de la sécurité est passée d'une approche centralisée et centrée sur les réseaux (faible niveau de cryptographie, incidents systémiques...) à une approche décentralisée, centrée sur l'utilisateur (données stockées sur le terminal en bout de chaîne, connexion basée sur des caractéristiques plus que sur l'identité de l'utilisateur, cryptographie avancée...). Cette tendance devrait encore se poursuivre avec l'essor de l'Internet participatif. Avec cette multiplication des terminaux et des connexions (ubiquité), les risques de sécurité sont importants, que ce soit pour l'individu (vol de numéro bancaire, usurpation d'identité...) ou les organisations (failles de sécurité dans les systèmes d'information, vols d'information dans les bases de données clients...), avec des conséquences économiques (spam, malware, espionnage...)

Les autorités nationales de régulation se sont donc concertées au sein d'instances internationales (OCDE, ITU, G X...) pour tenter de régler ces problèmes en adoptant un cadre cohérent (cf. historique *supra*). Avec un léger décalage, d'autres forums réunissant les acteurs économiques majeurs (APEC² Privacy Framework...) ont également traité des liens entre la sécurité des données et les échanges économiques.

4 – La situation actuelle (dynamique en cours et signaux faibles)

La **coopération sur ces thèmes a fortement progressé au cours des 20 dernières années**, concourant à harmoniser les législations nationales, en particulier en Europe. Toutefois, il existe toujours des **difficultés à traduire le dialogue constructif actuel en actions rapides** et efficaces entre les pays.

Une prise en compte et une concertation croissantes de la gouvernance et de la régulation...

On constate depuis environ **5 ans une accélération dans les concertations internationales** sur les thèmes de sécurité des dispositifs numériques et de protection de la vie privée. La plupart des pays ont donc pris conscience des problèmes de sécurité liés aux échanges numériques.

(1) Le résumé du texte de ladite Convention, consultable sur le site du Conseil de l'Europe, indique : *La Convention est le premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel, et qui régit les flux transfrontaliers des données.*

Outre des garanties prévues en ce qui concerne le traitement automatisé des données à caractère personnel, elle proscriit le traitement des données "sensibles" relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, etc., en l'absence de garanties offertes par le droit interne. La Convention garantit également le droit des personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications.

Seule restriction à ce droit : lorsque les intérêts majeurs de l'Etat (sécurité publique, défense, etc.) sont en jeu.

La Convention impose également des restrictions aux flux transfrontaliers de données dans les Etats où n'existe aucune protection équivalente.

(2) *Asia Pacific Economic Cooperation*. A la différence de l'Union européenne, les textes élaborés dans ce type de forum ne sont pas contraignants et leur application basée sur le volontariat.

En particulier, quelques **organismes de lutte contre les « infractions électroniques » les plus graves sont à la pointe de la coopération** dans l'application des lois : Eurojust en Europe, Interpol dans la lutte contre les abus sexuels, le projet IMPACT de l'ITU contre le cyber terrorisme... Cette plus grande **intégration répond souvent à des volontés politiques fortes** : pression de l'opinion publique dans le premier cas, enjeux de souveraineté nationale dans le second. Ces exemples de bonnes pratiques pourraient constituer des **modèles pour la protection du consommateur** (données des moteurs de recherche et des réseaux sociaux...).

... qui peinent encore à déboucher sur des mesures précises et opérationnelles

Cela tient à plusieurs raisons :

- Les **disparités régionales d'approche** de la sécurité et de la gestion des données privées (cf. encadré ci-dessous) mais aussi **de moyens**, avec en corollaire de fortes différences de législations. Les structures de coopération se mettent en place mais, à défaut d'une forte interopérabilité, le nombre grandissant de « couches » régionales et nationales ne facilitent pas la mise en place de systèmes opérationnels. Par ailleurs, avec le développement d'Internet, les **autorités nationales de régulation ont perdu une partie de leur contrôle sur les infrastructures et les terminaux**.
- Les **usages et les technologies - en évolution rapide - sont souvent en avance sur le régulateur ou le législateur**¹. Alors que la tendance de l'informatique ubiquitaire s'affirme, des innovations laissent augurer des difficultés futures pour les autorités nationales de régulation : intégration des moteurs de recherche et des réseaux sociaux, m-paiement, multiplication de terminaux multi usages, IPv6, RIFD, biométrie...

Différentes approches de la régulation à travers le Monde

On peut distinguer rapidement 3 types d'approches, qui correspondent à des zones géographiques et/ou économiques :

- **l'Europe est à la pointe** sur ces thèmes depuis les années 1950 avec la Convention du Conseil de l'Europe. Par la suite, en 1981, la Convention 108 dudit Conseil puis la Charte des Droits de l'Homme (2000) affirment le droit à la protection de la vie privée. Concernant plus spécifiquement la protection des données, la directive 95/46/EC, complétée par la directive 2002/58 pour le secteur des communications électroniques, impose la mise en place d'autorités nationales chargées d'identifier les entorses à la protection des données personnelles et de faire appliquer la législation. L'utilisateur dispose d'un droit de regard ;
- **l'Amérique du Nord adopte une approche similaire mais moins « coercitive »** sur les données des utilisateurs, liée à la recherche d'une meilleure fluidité des échanges et de liberté pour les agents économiques. Toutefois, depuis quelques années, les menaces informatiques croissantes ont amené à une prise de conscience des dangers (rapports de l'Académie des Sciences, du PITAC, de l'US Army...);
- les autorités centrales de **Chine** essaient de contrôler les échanges considérés comme inappropriés, grâce notamment à des milliers de « policiers d'Internet » (Le Monde, 31 juillet 2008).

Quelques signaux faibles

- La **révision de la Directive européenne 2002/58** et la dissolution du groupe d'experts chargé de réviser la directive 95/46 sur la protection des données personnelles. Par ailleurs, la Présidence tchèque soutient le programme pour un Internet plus sûr (« **Safer Internet plus** »

(1) Alors qu'un terminal téléphonique est renouvelé tous les 6 mois, un microprocesseur chaque année, les menaces informatiques protéiformes de plus en plus nombreuses (...), la régulation des télécommunications semble faire des avancées majeures tous les 10 ans.

sur la période 2009-2013, visant à défendre aussi bien les enfants que les contenus illégaux ou non sollicités par les utilisateurs).

- Depuis 2003, les autorités américaines se préoccupent fortement des menaces numériques, avec de nombreux rapports issus de l'Académie des Sciences, de l'Armée et de la Présidence (PITAC 2005). Dès ses débuts, l'administration Obama a ainsi lancé une réflexion d'ampleur sur la cyber sécurité (mission de 60 jours faisant suite au rapport du CSIS¹ de fin 2008 sur le sujet).

5 – Prospective (les 20 prochaines années)

(Les tendances lourdes et les incertitudes majeures, la différence entre les hypothèses étant construites sur les incertitudes)

Les tendances lourdes :

- La **coopération internationale** sur ces thèmes se renforce, incluant plus de pays, en réponse :
 - aux litiges trans-frontaliers en constante augmentation ;
 - aux usages et technologies en évolution rapide ;
 - aux menaces fortes pesant sur la souveraineté des Etats (cf. fiche 1.1.11 sur les infrastructures critiques).
- Le **changement de paradigme** depuis 15 ans : passage d'une sécurité/gestion des données centrée sur les réseaux à celle centrée sur l'utilisateur.

Les incertitudes :

- Les concertations internationales et l'harmonisation des législations seront-elles suivies d'actions ?
 - à cette fin, les **TIC** peuvent potentiellement devenir des outils très utiles : mise en place de plateformes collaboratives d'information, de signalement et de traitement des plaintes, etc. ;
 - au contraire, l'empilement de structures nationales faiblement inter-opérables ne va-t-elle pas freiner l'efficacité de la résolution des litiges ?
- Les **différences historiques, géopolitiques, culturelles** (...) des approches nationales concernant la sécurité et la protection de la vie privée ne sont-elles pas des **obstacles rédhibitoire** ?
- La capacité des régulations en place à répondre aux défis posés par les **nouveaux usages et les nouvelles technologies. Nouveau changement de paradigme** (retour en arrière) avec l'informatique dans les nuages ?

(1) Securing Cyberspace for the 44th Presidency.

Hypothèse 1 : Régulation à l'échelle régionale, en retard par rapport aux évolutions rapides des usages et des technologies

- ⇒ les **différences culturelles et géopolitiques empêchent une harmonisation forte de la législation** (à l'instar du processus européen), malgré l'élaboration au niveau international de codes de bonne conduite (ONU-ITU, OCDE, G X...). Cette harmonisation s'effectue essentiellement au sein de **zones économiques et/ou culturelles et/ou géographiques proches ou homogènes** ;
- ⇒ dans de nombreux pays, il existe parfois **plusieurs autorités de régulation avec des prérogatives floues, fonctionnant en silos**, mal intégrées aux décisions et disposant au final de moyens ou de pouvoirs insuffisants ;
- ⇒ les **technologies numériques ne sont pas intégrées pour régler les litiges entre pays** (plateformes collaboratives pour la diffusion d'informations mais pas de système d'information inter opérable fonctionnel entre la plupart des pays).

Hypothèse 2 : Une coopération volontariste à l'échelle mondiale et opérationnelle grâce à des outils numériques intégrés

- ⇒ les **codes de bonne conduite sont établis unanimement au niveau international et servent de base aux législations nationales**. Quelques disparités mineures demeurent ;
- ⇒ les **autorités nationales de protection** des données personnelles et de gestion de la sécurité numérique sont **placées au plus haut niveau de l'Etat et disposent de moyens/pouvoirs étendus**. Elles sont en contact permanent avec leurs homologues étrangers ;
- ⇒ les **TIC sont les outils naturels pour faciliter la résolution rapide des litiges**: plateformes collaboratives d'information et de recensement des menaces, systèmes d'information (unique, intégré, inter opérable, multilingue...) de saisie et de règlement des plaintes internationales ;
- ⇒ grâce notamment à ces outils, le **régulateur peut adapter son action à l'évolution rapide des technologies**.

Hypothèse 3 : Retard incessant de la régulation sur les usages ; suspicions internationales

- ⇒ devant les disparités régionales et nationales (accès aux technologies et structuration insuffisante des pays en développement...), les **efforts d'harmonisation législatives au niveau international sont ralentis (voire stoppés) pour de nombreuses années** ;
- ⇒ de plus, les **différences d'approche** (notamment militaire ?) entre les pays (protection des infrastructures critiques de télécommunications, cyber attaques...) aboutissent à des **replis nationaux** ;
- ⇒ les **contacts entre autorités nationales de régulation sont limités, les TIC sont peu utilisés** pour résoudre les plaintes internationales.

ANNEXES

Les autorités nationales dans l'OCDE chargées de la protection des données personnelles

Australia	Privacy Commissioner	www.privacy.gov.au
Austria	Datenschutzkommission	www.dsk.gv.at
Belgium	Commission de la Vie Privée	www.privacycommission.be
Canada	Privacy Commissioner of Canada	www.privcom.gc.ca
Czech Republic	Office for Personal Data Protection	www.uoou.cz
Denmark	Datatilsynet	www.datatilsynet.dk
Finland	Office of the Data Protection Ombudsman	www.tietosuojafi
France	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr
Germany	Federal Commissioner for Data Protection and Freedom of Information	www.bfdi.bund.de
Greece	Hellenic Data Protection Authority	www.dpa.gr
Hungary	Adatvédelmi Biztos	www.obh.hu
Iceland	Persónuvernd	www.personuvernd.is
Italy	Garante per la protezione dei dati personali	www.garanteprivacy.it
Japan	Cabinet Office	www5.cao.go.jp/seikatsu/kojin/index.html
	Competent Ministers (for the private sector)	
Korea	Ministry of Information and Communication	www.mic.go.kr
	Korea Information Security Agency	www.kisa.or.kr
Luxembourg	Commission nationale pour la protection des données	www.cnpd.lu
Netherlands	College Bescherming Persoonsgegevens	www.cbppweb.nl
	OPTA – Independent Post and Telecommunication Authority	www.opta.nl
New Zealand	Privacy Commissioner	www.privacy.org.nz
Norway	Datatilsynet	www.datatilsynet.no/
Poland	Inspektor Generalny dla ochrony danych osobowych	www.uodo.gov.pl
Portugal	Comissão Nacional de Protecção de Dados	www.cnpd.pt
Slovak Republic	Office for Personal Data Protection	www.dataprotection.gov.sk
Spain	Spanish Data Protection Authority	www.aqpd.es
Sweden	Datainspektionen	www.datainspektionen.se
Switzerland	Préposé fédéral à la protection des données	www.edsb.ch
United Kingdom	Information Commissioner	www.ico.gov.uk
United States	Federal Trade Commission	www.ftc.gov
	Department of Health and Human Services	www.hhs.gov
	Federal banking agencies	www.ffiec.gov
	Department of Justice	www.usdoj.gov

L'application du droit français pour la cybercriminalité (source : CGTI, 2005)

1. Les infractions spécifiques aux technologies de l'information et de la communication

Catégorie	Libellés des infractions	Texte de loi	Codification	Peines	Observations
Atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.)	Suppression/Modification de données	Loi Godfrain 05 I 1998	Code Pénal Art. 323 al. 1	1 an d'emprisonnement 15 000 € d'amende	
	Altération de fonctionnement		Art. 323-1 al.2	2 ans d'emprisonnement 30 000 € d'amende	
	Entrave au fonctionnement		Art. 323-2	3 ans d'emprisonnement 45 000 € d'amende	
	Introduction, suppression, modification de données		Art. 323-3	3 ans d'emprisonnement 45 000 € d'amende	
	Groupement de pirates		Art. 323-4	Idem à la plus sévère des infractions	
	Tentative d'infraction sur un STAD		Art. 323-7	Même peine que l'infraction visée	
	- Importation - Détention - Offre - Cession - Mise à disposition d'équipement, instrument ou programme informatique conçus ou adaptés pour commettre des infractions aux STAD	LCEN au 9 IV 2004 art. 34	Code Pénal Art. 323-3-1	Même peine que l'infraction au STAD visée	
Traitements automatisés de données personnelles	Traitement sans formalités CNIL	Loi Informatique et Libertés 06 I 1978	Code Pénal Art. 226-16	3 ans d'emprisonnement 45 000 € d'amende	
	Base de données non sécurisée		Art. 226-17	5 ans d'emprisonnement 300 000 € d'amende	
	Collecte déloyale ou malgré opposition		Art. 226-18	5 ans d'emprisonnement 300 000 € d'amende	
	Conservation des données "sensibles"		Art. 226-19	5 ans d'emprisonnement 300 000 € d'amende	
	Conservation supérieure à la déclaration préalable – (sauf à fins historiques, scientifiques, statistiques)		Art. 226-20	3 ans d'emprisonnement 45 000 € d'amende	
	Détournement des fins		Art. 226-21	5 ans d'emprisonnement 300 000 € d'amende	
	Cession des informations personnelles		Art. 226-22	1 an d'emprisonnement 15 000 € d'amende	
	- Non anonymisation des données dans certains cas - Non conservation des données techniques - Fabrication	LSQ 15 XI 2001 - art. 29	Code des P&T Art. L. 39-3 1	1 an d'emprisonnement 75 000 € d'amende	
Les infractions aux cartes bancaires		LSQ 15 XI 2001 Art. 35-39 et 40	Code monétaire et Financier	7 ans d'emprisonnement	
Les chiffrements non autorisés ou non déclarés	Utilisation non-autorisée de clé de chiffrement	L. Télécom 29 XII 1990 +	Code Pénal Art. 434-15-2 al. 1er	3 ans d'emprisonnement 45 000 € d'amende	
	Refus de répondre à réquisition pour remise de clé de chiffrement	art. 11 L. 10 VII 1991 mod.		2 ans d'emprisonnement	

	Refus de fournir une clé qui aurait pu éviter/limiter un crime ou un délit	par L.S.Q. – art. 31	Art. 434-15-2 al. 2	30 000 € d'amende 5 ans d'emprisonnement 75 000 € d'amende	
Interceptions	Régime des interceptions des correspondances émises par voie de télécommunication	Loi Perben II	Code de Procédure Pénale Art. 706-95	Autorisées par le juge des libertés, à la requête du Procureur, pour une durée de 15 jours renouvelables une fois	Interceptions en enquête préliminaire possible
	Violation de correspondance (interception illégale)	Ordonnance n° 2000-916 du 19/9/2000	Code Pénal Art. 226-15 et 432-9	1 an d'emprisonnement et 15 000 € d'amende (3 ans et 45 000 € si auteur dépositaire autorité publique ou exploitant de réseau de télécom)	Circonstance aggravante si auteur dépositaire de l'autorité publique

2. Les infractions liées aux technologies de l'information et de la communication

Catégorie	Libelles des infractions	Texte de loi	Codification	Peines	Observations
Pédo-pornographie	Fixation en vue de diffusion		Code Pénal	3 ans d'emprisonnement 45.000€ d'amende	La loi Perben II (art.47) incrimine la fixation et l'enregistrement en vue de sa diffusion ainsi que la transmission d'images pédophiles en bande organisée
	Enregistrement en vue de diffusion		Art.227-23		
	Diffusion sur un réseau d'images pédo-pornographiques		Art.227-23 al.3	Diffusion en ligne 5 ans d'emprisonnement 75.000€ d'amende	
	Détention d'image pédo-pornographique	L.04 III 2002	Art.227-23 al.4	En bande organisée 10 ans d'emprisonnement 500.000€ d'amende	
	Diffusion d'images pornographiques susceptibles d'être vues par un mineur		Code Pénal Art.227-24	3 ans d'emprisonnement 75.000€ d'amende	
Terrorisme, haine raciale...	Provocation aux crimes et aux délits	L.29 VII 1881	Art.23 et 24	5 ans et 45.000€ d'amende	
	Apologie de crime de guerre Provocation au terrorisme		Art.24, al.3&4	5 ans et 45.000€ d'amende	
	Provocation à la haine raciale		Art.24 al.6	1 an et 45.000€ d'amende	
	Contestation de crimes contre l'humanité		Art.24 bis	1 an et 45.000€ d'amende	
	Diffamation (raciale)		Art.29 à 32	12.000€ d'amende (1 an de prison et 45.000€ d'amende)	
	Injure (raciale)		art.29 à 33	12.000€ d'amende (6 mois de prison et 22.500€ d'amende)	
Atteintes aux personnes	Usurpation d'identité		Code Pénal Art.434-23	5 ans d'emprisonnement 75.000€ d'amende	Usurpation d'identité ou d'identifiant (adresse mail par ex.)
	Menaces et menaces de mort		Art.222-17	6 mois à 3 ans d'emprisonnement 45.000€ à 75.000€ d'amende	
	Atteintes à la vie privée		Art.226 al.1&2	1 an et 45.000€ d'amende	
	Atteintes à la représentation de la personne		Art.226-8	1 an et 45.000€ d'amende	
	Dénonciations calomnieuses		Art.226-10	5 ans et 45.000€ d'amende	

	Atteintes au secret professionnel		Art.226-13	1 an et 45.000€ d'amende	
Atteintes aux biens	Menaces de commettre une destruction, une dégradation ou une détérioration		Code Pénal Art.322-12	6 mois d'emprisonnement 7.500€ d'amende	

3. les infractions facilitées par les technologies de l'information et de la communication

Catégorie	Libellés des infractions	Texte de loi	Codification	Peines	Observations
Escroquerie en ligne	L'escroquerie par utilisation frauduleuse de numéro de carte de paiement sur internet et les escroqueries en général.		Code Pénal Art.313-1	5 ans d'emprisonnement 375.000€ d'amende	
Propriété intellectuelle	Toute contrefaçon d'une oeuvre de l'esprit y compris logiciels, marques, dessins ou modèles. Récidive ou si le délinquant est lié à la victime.	Loi Perben II 09 III 2004	Code de la Propriété intellectuelle Art. L.335-1 et 335-3	3 ans d'emprisonnement 300.000€ d'amende	La loi Perben II a modifié le quantum des peines applicables en matière de contrefaçon
			Art.L.335-9 Art. L.521-4 Art. L.716-9 et suivants	<i>En bande organisée</i> 5 ans d'emprisonnement 375.000€ d'amende En cas de récidive, les peines sont portées au double (art.335-9)	
Jeux de hasard	Participation à la tenue d'une maison de jeux de hasard.	Art.1 ^{er} – L 12VII 1983 mod.l. Perben II		3ans d'emprisonnement 45.000€ d'amende	Modification de la loi PerbenII
	Publicité en faveur d'une telle loterie	L. Perben II art.23		<i>En bande organisée</i> 7 ans d'emprisonnement 100.000€ d'amende 4.500€ d'amende	