Colloque de l'Institut des Amériques 2017

Philippe GIRARD-FOLEY
LL.M. University of Pennsylvania
Avocat à la Cour
Member Chartered Institute of Arbitrators

19 octobre 2017

LA SÉCURITÉ DES DONNÉES

“Sécurité”: un mot, plusieurs réalités

La Sécurité peut concerner:

➢ la protection des personnes ou celle des biens

➢ parmi celle des biens:

  ➢ les biens physiques: matériel, équipement, installations…

  ➢ les biens immatériels: propriété intellectuelle, réputation, mais aussi les “données” dont l’entreprise est détentrice ou dépositaire

À nouveau, les données peuvent se décomposer en deux catégories:

- les données que l’entreprise détient pour son propre compte: le “secret des affaires”
- les données que l’entreprise détient pour son avantage mais pour compte d’autrui: les données à caractère personnel relatives à des tiers

La sécurité des données: “le” sujet du moment

- **Secret des affaires**: la Directive (UE) 2016/943 du 8 juin 2016 sur “la protection des savoir-faire et des informations commerciales non divulguées contre l’obtention, l’utilisation et la divulgation illicite”
- **Protection des données**: Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 “relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données"

DEUX TEXTES FONDAMENTAUX POUR L’EUROPE

- ➢ bouleversent l’état du droit en la matière
- ➢ complémentaire avec les règles US pour le secret
- ➢ parfois en conflit pour la sécurité des données

SECRET DES AFFAIRES

LA DIRECTIVE EUROPÉENNE

• doit être transposée en droit interne au plus tard le 9 juin 2018

• définit les secrets d'affaires: informations secrètes ayant valeur commerciale parce que secrètes et ayant fait l'objet de dispositions raisonnables pour en conserver le secret

• champ très large de la "valeur commerciale": acquise dès lors qu'une atteinte est susceptible de nuire aux intérêts scientifiques et techniques, aux positions stratégiques, à la capacité concurrentielle même sous leur forme seulement "potentielle"

• condition de dispositions raisonnables destinées à garder secrètes les informations: recenser, matérialiser et consigner (inventaire préventif); accords de non divulgation / ingénierie inverse avec employés et partenaires commerciaux, contrôle physique de l'accès aux informations (contrôles, habilitation, cryptage), procédures, formation, suivi…etc. A FAIRE AUSSI EN ASIE !

REMÈDES

• mesures provisoires ou conservatoires par injonction: cessation, destruction des supports, interdiction de la production et mise ou maintien sur le marché

• contrepartie: action au fond dans 20/31 jours, limitation dans le temps, garantie, possibilité de contre offre de compensation financière.

• dommages intérêts sur manque à gagner ou redevance théorique.

LES ÉTATS-UNIS COMME PRÉCURSEURS ET COMME MODÈLE

LE DTSA (DEFEND TRADE SECRET ACT)

- signe le 11 mai 2016 par le President Obama
- considéré comme l'avancée legislative en ce domaine la plus considerable depuis le Lanham Act de 1946
- conçu pour répondre aux nouveaux risques générés par les progrès technologiques facilitant l'espionnage industriel et commercial
- jusqu'alors protection seulement par les lois d'Etat dans 47 Etats et DC (sur le modele du Uniform Trade Secrets Act) et sur la base de la common law dans les Etats de New York et Massachusetts
- la violation constituait un délit federal ("federal crime") par le Economic Espionage Act de 1996
- consequence: l'action civile en reparation devant les juridictions fédérales ne pouvait être engagée que par le U.S. Attorney General

L'AVANCÉE ESSENTIELLE DU DTSA

Le DTSA ouvre l'action civile devant les juridictions fédérales aux parties privées

- ne se substitue pas aux legislations d'Etat, le plaignant peut choisir
- limite aux violations de secret concernant un produit ou service commercialise ou offert a la commercialisation entre Etats ou a l'international ("interstate or foreign commerce")
- la definition du trade secret est très large et couvre tout type d'information ("all forms and types of information")
- l'information peut être de nature financière, scientifique, technique, économique, ou d'ingénierie ("financial, business, scientific, technical, economic or engineering information")
- toute information est concernée si le propriétaire a pris des mesures "raisonnables" pour en garantir le secret ("taken reasonable measures to keep such information secret") et si elle a une valeur économique distincte ("independent economic value") pour celui-ci
- les données numérisées quelle que soit leur nature sont clairement dans le champ du DTSA

LES DONNÉES À CARACTÈRE PERSONNEL

LE RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

- Entrera en vigueur sans le besoin d'un texte interne dans les États Membres de l'Union en mai 2018
- S'inscrit dans une tendance générale récente: "droit à l'oubli" en 2014, *EU-US Privacy Shield* adopté par la Commission le 12 juillet 2016, abandon de la doctrine de "*Safe Harbour*" avec l'arrêt de la Cour Européenne de Justice du 6 octobre 2015
- Sanctions dissuasives: jusqu'à 4% du chiffre d'affaires mondial !

LE RÈGLEMENT (Suite)

DES EFFETS AU DELÀ DE L'EUROPE

- S'applique aux entreprises non-européennes offrant leurs services dans l'EU, ce qui fera du Règlement une référence mondiale
- S'applique "aux personnes physiques indépendamment de leur nationalité ou de leur lieu de résidence" (article 14)
- Que le traitement de données à caractère personnel ait lieu ou non dans l'Union

DES PRINCIPES RIGOUREUX

- "Le traitement des données à caractère personnel devrait être licite et loyal" (article 39)
- "Pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la loi" (article 40)
- rappel du "droit à l'oubli", droit au déplacement vers un autre système de traitement, interdiction de décisions fondées sur le "profilage"…etc.

LE RÈGLEMENT (Suite)

DES CRITERES DE LICEITE DU TRAITEMENT RESTANT A CLARIFIER

- le consentement
- mais aussi la finalité du traitement

LES DEUX PRINCIPES OPERENT CONJOINTEMENT

- **le principe general dans tous les cas (meme avec consentement !): le principe de minimisation**
- peuvent être collectées uniquement les données nécessaires au traitement
- dans le cas de collecte avec consentement, peut permettre de contester
- dans le cas sans consentement, illégalité automatique si le principe de minimisation n'est pas respecte

DES CLARIFICATIONS INDISPENSABLES MAIS ABSENTES

- pas de definition de la finalise
- pas d'indication sur la durée de conservation

LE DATA PROTECTION OFFICER

RENDU OBLIGATOIRE PAR LE REGLEMENT

- obligatoire pour traitement par une autorité publique ou suivi régulier et systématique a grande échelle
- doit avoir accès a toutes les données et traitements et être “associe” aux decisions relatives au traitement
- mais sans être décisionnaire (il est organe de contrôle)
- il peut être extérieur a l’entreprise ou interne
- mais il doit être indépendant et ne pas recevoir d’instructions
- double competence juridique et technique
- attention aux conflits d’intérêt (autres taches ou responsabilités)

TRANSMISSION DES DONNÉES HORS UE

DES CONDITIONS IMPERATIVES DANS LE REGLEMENT

- s'applique aux transmissions vers les US
- niveau de protection adéquat dans le pays de reception : "decision d'adéquation" par pays tiers a l'UE
- règles internes contraignantes d'entreprise
- preuve de garanties appropriées par dispositions contractuelles
- decision administrative ou judiciaire reposant sur un accord international
- derogation pour "situation particuliere"
- derogation pour "intérêt légitime et impérieux"

UNE PROBLÉMATIQUE NOUVELLE ET SANS PRÉCÉDENT POUR LE CLOUD

- données peuvent être conservées dans et/ou accessibles depuis plusieurs endroits en constant changement
- question vis-a-vis des contraintes (comme dans le Règlement) concernant le niveau de protection dans les pays de reception
- question des audits des fournisseurs en cas de chaine de delegation
- question de l'accès des tribunaux aux données conservées dans un pays ayant une legislation de blocage ("blocking statutes")
- question accrue de compatibility entre legislations: par exemple EU/France v US data privacy laws, Gramm-Leach-Bliley Act pour les institutions financières, Health Insurance Portability and Accountability Act pour les informations de nature medical, ou encore les regles du Payment Card Industry Data Security Standards Council pour les cartes de credit

CHINA IPR SME HELPDESK

AU DELÀ DE l'EUROPE ET DES US: LA CHINE

Il existe une réglementation protectrice des données personnelles en Chine (République Populaire)

- Règles Générales de Droit Civil (entree en vigueur le 1er octobre 2017):
- "Les personnes physiques ont le droit au respect de leur vie privée"(article 110);
- "Toute organisation ou individu qui doit obtenir des informations personnelles sur un tiers doivent obtenir le consentement de celui-ci en conformity avec la Loi et s'assurer de la security de l'information. Il n'est pas permis de collecter, utiliser, traiter ou transférer illégalement les informations personnelles d'un tiers. Il est illegal d'acheter et de vendre, de fournir ou de publier les informations personnelles d'un tiers"

South-East Asia IPR SME HELPDESK

CHINA IPR SME HELPDESK

ET RÉGLEMENTATION SPÉCIFIQUE

- Loi sur la Cybersécurité [article 41](entree en vigueur le 1er juin 2017): "Les operators observeront les principes de 'legal, justifie et nécessaire' pour la determination de leurs regales concernant la collecte et l'usage de l'information personnelle, en précisant l'objet, les méthodes et l'étendue et en obtenant le consentement de la personne concernée"

MAIS DES CONTRAINTES DE BLOCAGE

- Neuvième Amendement du Code Penal [nouvel article 286(a)]: "C'est un crime pour les fournisseurs de service de réseau de ne pas se conformer a leurs devoirs concernant la sécurité de l'information personnelle"
- Loi sur la Cybersécurité [article 37]: "L'opérateur d'une infrastructure majeure d'information stockera l'information personnelle et les informations importantes collectées en Chine sur le territoire de la République Populaire de Chine"

AILLEURS EN ASIE DU SUD EST

- **Hong Kong**: Personal Data (Privacy) Ordinance (Cap. 486), Personal Data (Privacy) (Amendment) Bill of July 2012
- **Philippines**: Data Privacy Act of 2012 et Implementing Rules and Regulations of Republic Act N°10173, known as the “Data Privacy Act of 2012”
- **Singapour**: Personal Data Protection Act 2012
- et APEC

MALAISIE

ACT 709

PERSONAL DATA PROTECTION ACT 2010

Obligations (applicables notamment a toute personne qui a le contrôle sur ou autorise le traitement de données personnelles en rapport avec des transactions commerciales) relatives au consentement, a l'usage, l'information, la confidentialité, la sécurité, la durée de retention, l'enregistrement du traiteur de données, le droit a la correction, la divulgation, les données "sensibles", le refus du marketing direct, le tribunal d'appel, les inspections, les saisies, les transferts hors de Malaisie, les amendes forfaitaires (compounding), la responsabilité conjointe des dirigeants avec la société, la protection des lanceurs d'alerte.

LAWS OF MALAYSIA
ACT 709

PERSONAL DATA PROTECTION ACT 2010

- **Autres textes: Personal Data Protection Standards 2015 et Personal Data Protection (Compounding of Offences) Regulations 2016**

RÉCAPITULATION

Une premiere évidence: ne rien faire n'est pas une option

SECRET DES AFFAIRES:

- ➢ inventorier, classer, materialiser avec l'aide d'un expert
- ➢ mettre en oeuvre tous moyens de protection contractuelle
- ➢ mettre en oeuvre tous moyens de protection technique
- ➢ mettre en oeuvre tous moyens de protection physique (y compris avec procédures, manuels, règlement intérieur…etc.)
- ➢ verifier l'application effective et constante de ce qui précède

RÉCAPITULATION (Suite)

DONNÉES PERSONNELLES:

- ➢ s'informer très précisément sur la réglementation applicable (Europe, France, Etats-Unis, chaque autre pays où l'entreprise fait des affaires) et connaitre ses obligations
- ➢ modifier ses pratiques si nécessaire
- ➢ adapter les contrats avec les clients et les prestataires de service concernés
- ➢ ajuster ou mettre en place des procédures
- ➢ adopter un "guide" accessible aux tiers (ex. *Personal Date Protection and Privacy Policy*)
- ➢ nommer un DPO (Data Protection Officer) chargé de veiller à la *compliance* - qui peut être extérieur et pas à plein temps