PROBLEMATIQUE DES FICHIERS ET PROTECTION DES JUSTICIABLES.

- Il nous faut en premier lieu procéder à un inventaire, survoler l'existant :

  - Évoquer ce que nous connaissons tout en ayant conscience que de nombreux fichiers existent en secret.

    Ce que nous connaissons résulte de lanceurs d'alerte, défenseurs courageux qui ont dénoncé certaines pratiques des états.

  - Cet inventaire ne concerne que les fichiers de police c'est-à-dire : **les fichiers qui intéressent la sûreté de l'état, la défense ou la sécurité publique** reprenant ainsi la définition de la loi française informatique, fichier et libertés de 1978.

    Le champ d'investigation est très large, car en effet les pouvoirs donnés aux services de sécurité et aux services de police dans de très nombreux états leurs permettent d'accéder aux fichiers sociaux, fiscaux, aux fichiers de sociétés privées, les collecter, conserver et exploiter les données recueillies à l'occasion des échanges des citoyens dans le monde entier.

Nous ne traiterons que les fichiers les plus importants au plan international.

Je ne pense pas qu'il soit util ici d'évoquer la centaine de fichiers de police qui existent légalement et illégalement en France. En 2011 et 2013 deux missions parlementaires avaient noté que sur les 86 fichiers existants, 1/3 n'avait aucune base légale.

Nous évoquerons ainsi les thèmes relatifs à :

Échelon

Carnivore,

Le Patriot act,

Le PNR,

Et le SIS Schengen.

Dans un deuxième temps nous évoquerons la difficile question de la protection des justiciables.

<u>Le système Échelon</u> ancêtre de la surveillance globale.

1947-1948 les États-Unis, le Royaume-Uni s'accordent pour avoir des informations sur l'Union Soviétique : c'est **l'accord UK-USA** .

se joignent :

-le Canada,

-l'Australie,

-la Nouvelle-Zélande.

Échelon est principalement géré par la <u>NSA</u> (National Security Agency**) et exploite <u>SIGINT</u> :** système d'interception des communications privées et publiques.

C'est une surveillance sur l'ensemble des moyens de communication sur la planète : **Fax – Téléphone – courriel.**

<u>On passe d'un usage militaire à un usage civil</u>.
On surveillait des armées et des mouvements de troupes, on surveille désormais des citoyens et des entreprises.

- **<u>Le Parlement Européen</u>** dans un rapport du 11 juillet 2001 sur Echelon dénonce les opérations des USA sur le territoire de l'Union :
  <u>(i)</u> ces opérations étant secrètes – constituent une violation de l'accès au droit.

  <u>(ii)</u> la violation du principe de prévisibilité,

  (iii) une violation de l'article 8 de la Convention, relative au respect de la vie privée.

<u>Échelon échappe à tout contrôle.</u>

Carnivore

On découvre par hasard l'existence de carnivore qui est un outil logiciel installé par le FBI sur le serveur des FAI américains – fournisseur d'accès à Internet.

Le système est capable de scanner plusieurs milliers de courriels par seconde.

Il apparaît par la suite que :

- l'Angleterre,
- la Norvège,
- la Nouvelle-Zélande,
- la Pologne,
- la Russie

ont des dispositifs de même nature que Carnivore.

« **Quand vous avez la capacité d'avoir des informations, il est très dur d'imposer des barrières arbitraires à leur acquisition.**
Devons-nous refuser de lire ? »

interroge Monsieur Brzezinski, conseiller à la sécurité nationale sous Jimmy Carter.

USA Patriot Act :

« Uniting and Strenthening America by Providing Appropriate Tools Required to Intercept and Osbruct Terrorism ».

« Unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ».

À la suite des attentats du 11 septembre 2001, le Président américain BUSH a fait voter le 25 octobre 2001 le US Patriot Act.

- **Texte de 132 pages,**
- **Pas lu par la plupart des membres du congrès,**
- **Concerne les américains et les étrangers,**
- **Voté pour 4 ans, ……reconduit en 2006,**
- **Prorogé jusqu'en juin 2015.**

Dispositions particulières :

la section 215 modifie le titre 5 du FISA Act : « Foreign Intelligence Surveillance Act » de 1978 dans les sections 501 à 503 .

La nouvelle disposition porte sur des perquisitions concernant les « Books Records, papers documents and other items » détenus par des entreprises.

(i) La perquisition est secrète. Elle est faite à l'insu du perquisitionné. La notification est faite plus tard selon les circonstances.

(ii) La personne qui est sollicité - détentrice des éléments - ne doit pas signaler l'existence de la perquisition (section 501).

(iii) La perquisition est autorisée par un juge qui statut secrètement : « FISA court » : Foreign Intelligence Suveillance Act Court.

Un mandat obligeant les opérateurs de téléphonie est émis afin de fournir l'intégralité des métadonnées téléphoniques de leurs clients.

En 2005 un Juge considère illégal la communication de la liste des livres demandés pour consultation dans les bibliothèques.

En 2015, un tribunal a jugé que la base de la section 205 était insuffisante.

Les sections 504 et 505 –

Les sections 504-504 permettent à toute autorité de sécurité et à la police d'accéder aux données hébergées sur une plateforme Cloud si l'entreprise hébergeant les données est de droit américain.

Dans un autre domaine, le patriot act permet d'arrêter, inculper, détenir sans durée des personnes soupçonnées de terrorisme.

Le Patriot Act a absorbé Carnivore.

Qu'est devenu le Patriot Act ??

- **promulgué en 2001, reconduit en 2006 jusqu'en juin 2015.**

En juin 2015 lui a succédé le USA Freedom Act le 2 juin 2015.

Désormais ce sont les compagnies téléphoniques qui conservent les données téléphoniques : et pour la section 215 il faut un lien « raisonnable de détaillé »

Cela ne concerne que les citoyens américains et non pas les citoyens étrangers.

……..

Observations sur l'impact du Patriot Act sur la concurrence commerciale.

Tous ces éléments sont recueillis, stockés exploités, sans contrôle.

Les entreprises européennes ont fait valoir en Europe l'intérêt qu'il y avait à éviter de travailler avec des sociétés américaines : plus aucun secret, plus aucune confidentialité.

Mais cet intérêt s'est estompé par le durcissement des législations européennes qui s'approchent de celles du Patriot Act.

LE PNR : PASSENGER NAME RECORD

Dès 2003 les compagnies aériennes et agences fournissant une prestation de vols à destination, via ou au départ des Etats-Unis, doivent collecter certaines données et les transmettre aux autorités américaines ; par exemple :

- nom,
- itinéraire,
- réservation d'hôtel,
- préférence alimentaire :
  - Muslim meal,
  - Hindou meal,
  - cacher meal,
  - vegetarian ….

En 2007 un accord est conclu entre les États-Unis et l'Union Européenne : conservation des données pendant 15 ans.

Le Contrôleur Européen à la Protection des Données (CEPD) émet un avis très critique :

- Absence de justification de la collecte de ces informations ;
- Absence de la sécurité juridique du dossier car : secret du destinataire du dossier. (Communication à des tiers ?)
- Absence de protection

L'Europe suit et créée le 14 avril 2016 le PNR européen :
461 voix pour au Parlement européen
175 voix contre
9 abstentions

La France suit et créée le PNR France. Cela concerne 100 millions de personnes par an et 230 compagnies.

L'affaire Swift :

- **Swift est une société belge de droit privé : Society for World wild Interbanque Financial Télécommunication.**

- **un accord occulte entre cette société,** la CIA et l'administration fiscale des États-Unis est dévoilé.

Cet accord contraignait la société SWIFT à remettre aux États-Unis la totalité de toutes les transactions financières.

Le Parlement européen s'est dit *vivement préoccupé* :

- **finalement le 1er août 2010** est conclu un accord TFTP (Terrorism Finance Tracking Program) qui permet aux citoyens européens d'accéder aux données les concernant via leur Commission de protection des données (CNIL nationale) (articles 15 et 16).

SIS SCHENGEN

Le système d'information Schengen

Le SIS centralise au niveau européen plus de 17 millions de signalements concernant :

- soit des **personnes recherchées** ou **placées sous surveillance**,
- soit des **véhicules** ou des **objets recherchés**.

L'autorité de contrôle commune Schengen exerce un contrôle technique du fichier central (C-SIS) installé à Strasbourg et vérifie le respect par les états participants au système, des droits accordés aux personnes.

La partie nationale du système en France est sous l'autorité du ministre de l'intérieur.

II- LA PROTECTION DES JUSTICIABLES

Le dictionnaire définie une personne justiciable comme une personne qui relève d'un juge, d'une juridiction.

C'est une position très confortable de relever d'un juge, d'une juridiction ,parce que doivent alors être appliqués les principes du contradictoire, d'égalité des armes, des droits de la défense, et de prévisibilité.

Or, en cette matière des fichiers, rien de tout cela n'existe.

1- Vous pouvez figurer dans un fichier à votre insu ; exemple Interpol.

2- Lorsque vous le découvrez, à l'occasion d'un blocage à une frontière par exemple, il est très difficile de connaître l'origine du signalement et de déterminer l'autorité vers laquelle se tourner pour en avoir communication et demander éventuellement son effacement.

3- Un fichier français, le TAJ illustre bien cette situation.

Le TAJ Traitement des Antécédents Judiciaires est le fichier qui rassemble le STIC et JUDEX,

Le STIC relevait du ministère de l'intérieur, et JUDEX du ministère de la défense (gendarmerie)

Le STIC a pu comporter jusqu'à 20 millions de personnes, s'agissant d'infractions constatées.

De très nombreuses « *infractions constatées* » n'ont jamais fait l'objet de poursuite judiciaire de telle manière que des personnes intégrées dans le fichier ne peuvent en sortir qu'après une procédure complexe et sous la discrétion du procureur de la république.

En Conclusion :

- **c'est un combat des citoyens face à des puissances publiques.**

- **Combat inégal.**

Ou sont les contrepouvoirs ??

- **Les associations de protection des droits de l'homme**, par exemple en France la ligue des droits de l'homme et certains syndicats d'avocats et de magistrats se battent pour la réduction de ces fichiers.

- **Les CNIL : les autorités CNIL dans les divers pays européens ont finalement très peu de pouvoir.** L'exemple de la CNIL française est édifiant, jusqu'en 2004 la CNIL française devait produire un avis conforme pour la création d'un fichier de police.

  Depuis 2004, cet avis qui devait être conforme est devenu un avis motivé de telle manière que le gouvernement n'est plus lié par l'avis de la CNIL qui a ainsi perdu un pouvoir de pression.

- **En Europe le G29** qui réunit les CNIL de l'Union Européenne (appelé Groupe 29 du fait de l'article 29 de la directive) n'a qu'un pouvoir consultatif.

- **Au plan des fichiers internationaux, il n'y a quasiment pas de recours utile. Ex : Interpol (situé à Lyon) : On ne peut pas même savoir d'où vient le signalement.**

  Au final, l'ultime recours pour la défense des libertés des personnes fichées est l'avocat.

  Mais il faut être préparé à ce que les démarches seront difficiles à mener, les recours hasardeux et les résultats très décevants.

Alain WEBER
Cabinet Henri Leclerc & Associés
Barreau de Paris