Mesures légales et harmonisation

1ère observation

- Les pays en voie de développement et les pays développés sont confrontés à des défis similaires
- La cybercriminalité est internationale → l'harmonisation des législations est impérative
- Mais les solutions dépendent des ressources de chaque pays
- On constate que les normes juridiques et techniques sont souvent convenues entre les pays industrialisés …
- … et n'incluent pas les pays en développement

2ème observation

- La lutte contre la cybercriminalité peut être liée à plusieurs ministères (selon les pays) :
  - ministère de la Justice
  - ministère de la Sécurité Nationale
  - ministère de l'Economie, de l'Industrie et du Numérique
  - et d'autres selon les pays…
- Le rôle de chaque institution impliquée doit être clairement défini
- Trop d'institutions impliquées → communication difficile

3ème observation

- Droit pénal « matériel » : on ne peut pas appliquer la même disposition et la même sanction au même fait commis physiquement ou par Internet
- Les auteurs peuvent agir de n'importe où dans le monde
- Ils peuvent prendre des mesures pour masquer leur identité
- Les outils nécessaires pour enquêter sur la cybercriminalité sont différents de ceux utilisés pour enquêter sur les crimes ordinaires

La législation doit admettre la preuve électronique

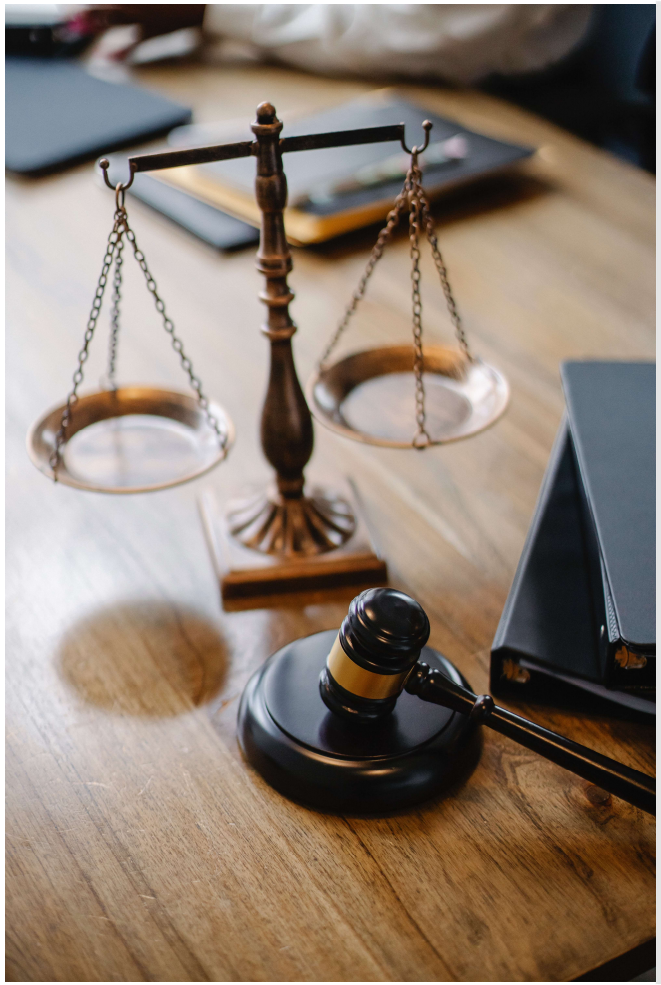
- Le succès de la procédure dépend de l'évaluation des preuves électroniques
- Nouvelles technologies → nouvelles possibilités d'investigations
- Experts judiciaires et experts en cybercriminalité : nouveaux métiers, nouvelles compétences, nouvelles formations

La preuve électronique

- 2 conditions sont nécessaires à la recevabilité de l'écrit électronique (exemple : un email) selon l'article 1366 du Code civil :
  - la personne dont elle émane doit pouvoir être dûment identifiée
  - il doit être établi et conservé dans des conditions de nature à en garantir l'intégrité
- *« l'écrit sur support électronique a la même force probante que l'écrit sur support papier »* : les preuves informatiques ne souffrent pas de leur caractère immatériel en termes de force probante
- La force probante peut être mise à mal par les doutes relatifs à l'intégrité de la preuve informatique

Coopération internationale

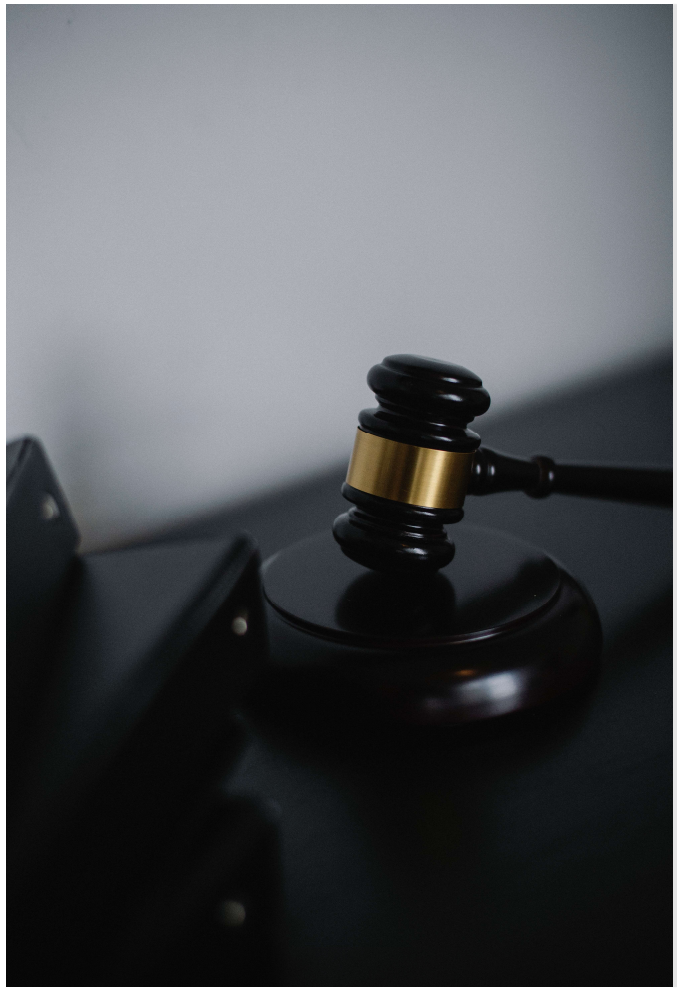
- Objectif : combattre la dimension internationale de la cybercriminalité
- Très grandes différences entre :
  - les législations
  - les ressources allouées
- Les pays doivent renforcer leur capacité à coopérer avec d'autres pays
- Il faut rendre la communication et la procédure plus efficaces



Coopération internationale

Le principe de souveraineté nationale

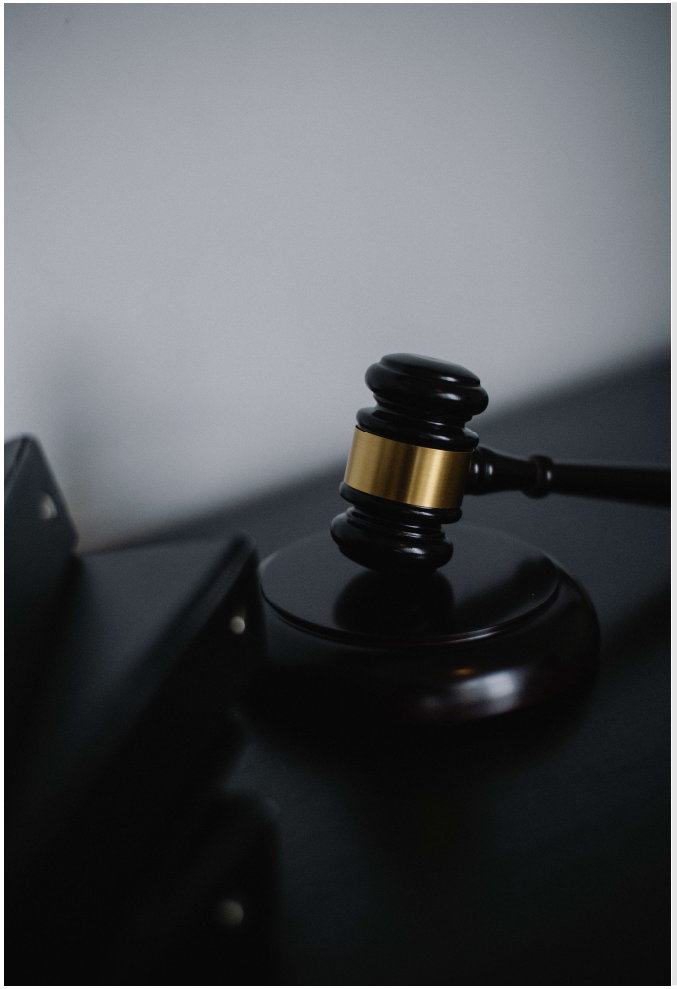
- Les enquêtes transnationales sans le consentement des autorités compétentes des pays concernés sont difficiles au regard du principe de souveraineté nationale
- Ce principe ne permet pas à un pays de mener des enquêtes sur le territoire d'un autre pays sans l'autorisation des autorités locales



Coopération internationale

Gagner en réactivité

- Il y a un court laps de temps pendant lequel des enquêtes peuvent réussir
- L'application des régimes classiques d'entraide judiciaire n'est pas suffisante lorsqu'il s'agit d'enquêtes sur la cybercriminalité
- L'amélioration de la coopération internationale est cruciale pour gagner en réactivité



Éduquer les utilisateurs

- Certains cybercrimes (phishing, spoofing, ...) ne reposent pas sur un manque de protection technique
- Ils dépendent d'un manque de sensibilisation de la part des victimes
- Si les utilisateurs savent que leurs institutions financières ne les contacteront jamais par e-mail pour leur demander des mots de passe ou des coordonnées bancaires, ils ne peuvent pas être victimes d'attaques de phishing ou d'usurpation d'identité
- L'éducation des utilisateurs réduit le nombre de cibles potentielles

Éduquer les utilisateurs

- Les utilisateurs peuvent être éduqués par le biais de campagnes publiques, de cours dans les écoles, les bibliothèques, les centres informatiques et les universités, et bien sûr dans leurs entreprises
- Certains états et/ou entreprises privées refusent de souligner que les citoyens et les clients sont touchés par les menaces de cybercriminalité afin d'éviter qu'ils ne perdent confiance dans les services de communication et d'achats en ligne
- Par exemple, le FBI a explicitement demandé aux entreprises de surmonter leur aversion pour la publicité négative et de signaler les cybercrimes

Alors …
que faire ?

Impliquer les parties prenantes

- La politique de sécurité doit impliquer toutes les parties prenantes :
  - entreprises
  - éditeurs de logiciels
  - fabricants de matériels
  - fournisseurs d'accès
  - toute personne utilisant le numérique

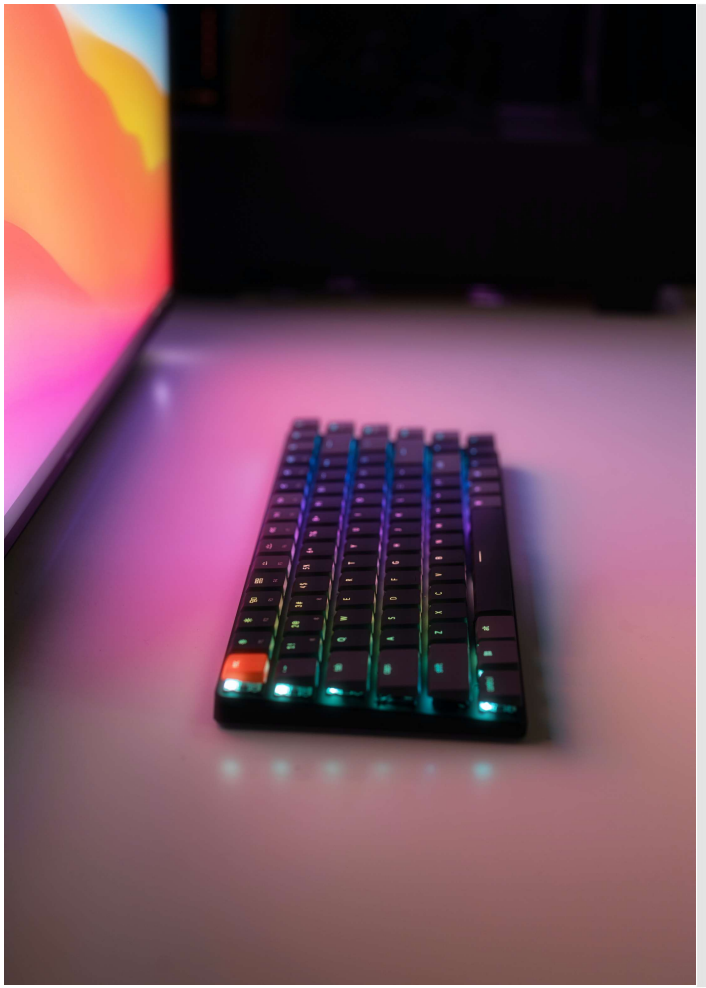
Sécuriser les logiciels

Choisir les bons prestataires

- Un logiciel sécurisé garantit la protection des utilisateurs
- Cela garantit la protection globale de l'organisation
- Le choix des fournisseurs d'accès Internet et des éditeurs de logiciels est essentiel
- Cela réduit mécaniquement la probabilité de subir des dommages numériques importants

Responsabilité des prestataires de service

- La cybercriminalité peut difficilement exister sans l'utilisation d'un fournisseur d'accès Internet (FAI : Fournisseur d'Accès Internet, ISP: Internet Service Provider)
- Les e-mails au contenu suspect sont envoyés en utilisant le service d'un fournisseur de messagerie



Responsabilité des prestataires de service

- Le contenu illégal téléchargé à partir d'un site Web implique également un fournisseur de services
- Les FAI sont souvent au centre des enquêtes criminelles
- Les FAI n'ont pas la capacité de prévenir ces crimes
- La responsabilité des fournisseurs d'accès Internet doit-elle être limitée ?