Analyse d'impact, analyse de risque en matière de vie privée

Daniel Le Métayer

Gergely Acs, Claude Castelluccia, Sourya Joyee De

Règlement européen: prévalence des notions de risque et de responsabilité

- Obligation de conduire une analyse d'impact dans certaines situations
- Incidence sur de nombreux dispositions: plus de 100 occurrences des expressions « risque » and « analyse d'impact » (contre seulement 8 occurrences de « risque » et aucune d' « analyse d'impact » dans la Directive 95/46 CE)
- Evolution d'une vision administrative vers une démarche de responsabilisation (« accountability ») des acteurs

Quand l’analyse d’impact est-elle obligatoire ?

Article 35 – Analyse d’impact relative à la protection des données

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Quand l'analyse d'impact est-elle obligatoire ?

L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

Quand l'analyse d'impact est-elle obligatoire ?

L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

Prévalence de la notion de risque

Article 24 - Responsabilité du responsable du traitement

1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.

Prévalence de la notion de risque

Article 25 – Protection des données dès la conception et protection des données par défaut

Compte tenu de l'état des connaissances, des coûts de mise en œuvre … ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, …, des mesures techniques et organisationnelles appropriées, …, par exemple la minimisation des données,....

Prévalence de la notion de risque

- Article 32 – Sécurité du traitement
- Article 33 – Notification à l'autorité de contrôle d'une violation de données à caractère personnel
- Article 34 – Notification à la personne concernée d'une violation de données à caractère personnel
- Article 36 – Consultation préalable

Débats autour de la vision “analyse de risque”

- Régulation par la règle de droit (« right-based regulation »):
  - Prescriptive: mesure obligatoires
  - Déterministe: conformité facile à vérifier
- Régulation par la gestion de risques (« risk-based regulation ») :
  - Non prescriptive: des objectifs plus que des mesures (niveau de risque toléré, etc.)
  - Probabiliste: objectif de réduction plus que d’élimination des risques

Arguments en faveur de la régulation par la gestion de risques

- Grande variété de situations ⇒ besoin de flexibilité : la régulation par la règle est souvent trop rigide et ne conduit pas forcément à la meilleure protection
- Les risques ne peuvent pas être complètement éliminés ⇒ besoin d'une démarche rationnelle pour les analyser et prendre les décisions appropriées : priorités d'actions, calibration des mesures, allocation optimale des ressources en fonction des risques identifiés

Critiques de la régulation par la gestion de risques

- Risque de réduire un droit fondamental en un simple paramètre dans un processus d'optimisation des coûts ⇒ démarche pouvant se réduire à un outil de gestion dépourvu de toute substance (généralisation de techniques managériales issues du secteur privé)
- Démarche pouvant conduire à un exercice d'auto-justification

Position du Groupe 29 (mai 2014)

- L'analyse de risque ne doit jamais conduire à un affaiblissement du droit des personnes: les droits du sujet doivent être respectés quel que soit le niveau de risque (information, consentement, droit d'accès, de rectification, d'effacement, etc.)
- On doit considérer non seulement les risques pour les individus mais aussi les impacts sur la société

Etudes d'Impact sur la Vie Privée
Privacy Impact Assessments (PIA)

- Précurseurs: organismes d'évaluation des technologies (technology assessment, OTA) et études d'impact environnemental (EIS) dans les années 70
- Dans le domaine de la protection de la vie privée: Canada (1999), Nouvelle Zélande (2002), Australie (2006), Royaume-Uni (2007), Union Européenne (2011: RFID, 2014: smart grids)
- Guides: ICO (2011), BSI (2011), NIST (2015), CNIL (2015)

Retours d'expérience (Projet PIAF)

- Initier le PIA le plus tôt possible
- Ne pas réduire l'objectif à la production d'un rapport : le PIA doit faire partie d'un processus global de gestion des risques
- Impliquer toutes les parties prenantes
- Eviter les conflits d'intérêt ou les soupçons de green washing : un PIA doit être réalisé et/ou audité par un tiers indépendant, publié et approuvé par un responsable de haut niveau

Exemple: les guides de la CNIL

Trois documents:

- EIVP/PIA, la méthode – Comment mener une EIVP/un PIA
- EIVP/PIA, l'outillage – Modèles et bases de connaissance
- Mesures pour traiter les risques sur les libertés et la vie privée

CNIL : la méthode

1. Définition du contexte : traitement, périmètre, finalités, données personnelles, durée de conservation, supports, etc.
2. Définition des mesures : juridiques, organisationnelles, sécurité logique, sécurité physique
3. Définition des risques : sources de risques, événements redoutés, menaces, risques (gravité et vraisemblance)
4. Décision: PIA acceptable → plan d'action et validation formelle, PIA non acceptable → objectifs et itération

Situation actuelle

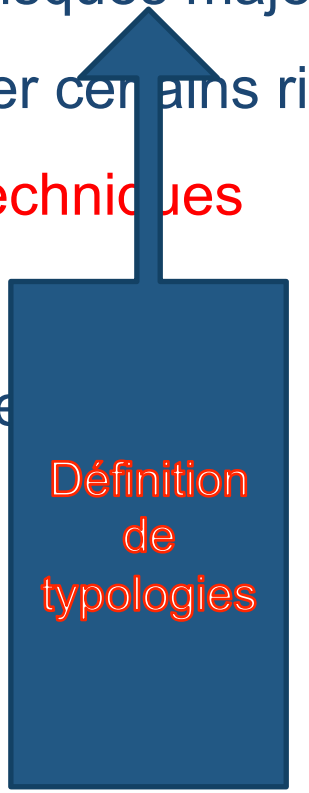
- Beaucoup de points communs entre les cadres existants
- Questions clef:
  - Types de risques considérés (risques pour les personnes / risques pour les responsables de traitement)
  - Prise en compte des parties prenantes
- Aspects organisationnels bien documentés mais peu de détails sur les aspects techniques (analyse de risques)
- Besoin d'une démarche systématique et rigoureuse

Analyse de risques: principaux défis

- Complétude: ne pas oublier de facteurs de risques majeurs
- Validité des hypothèses: ne pas sous-estimer certains risques
- Combinaison d'aspects techniques et non techniques (juridiques, sociaux)
- Evolution du contexte (techniques, usages, etc.)

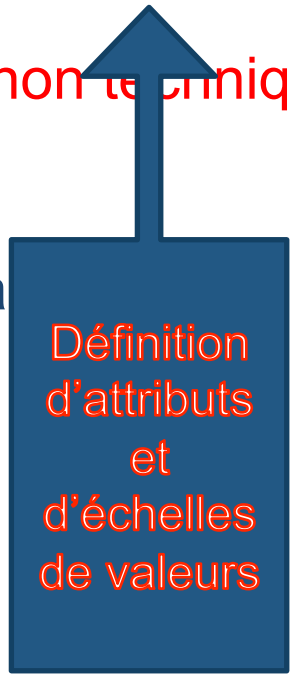
Analyse de risques: principaux défis

- Complétude: ne pas oublier de facteurs de risques majeurs
- Validité des hypothèses: ne pas sous-estimer certains risques
- Combinaison d'aspects techniques et non techniques (juridiques, sociaux)
- Evolution du contexte (techniques, usages, e



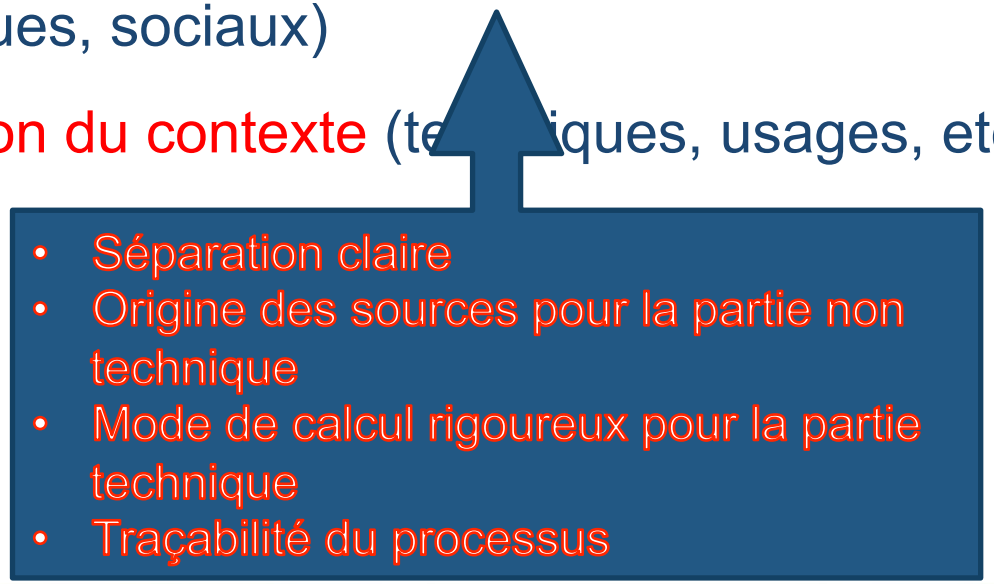
Analyse de risques: principaux défis

- Complétude: ne pas oublier de facteurs de risques majeurs
- Validité des hypothèses: ne pas sous-estimer certains risques
- Combinaison d'aspects techniques et non techniques (juridiques, sociaux)
- Evolution du contexte (techniques, usa



Analyse de risques: principaux défis

- Complétude: ne pas oublier de facteurs de risques majeurs
- Validité des hypothèses: ne pas sous-estimer certains risques
- Combinaison d'aspects techniques et non techniques (juridiques, sociaux)
- Evolution du contexte (te iques, usages, etc.)



Principaux composants d'une analyse de risques en matière de vie privée

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée

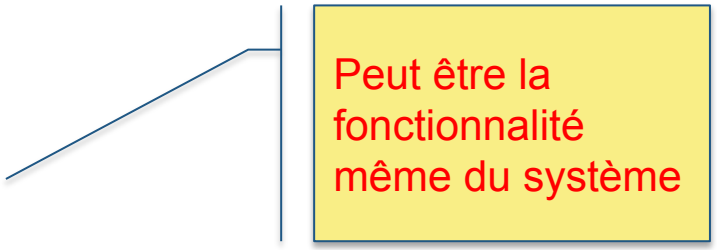
Principaux composants d'une analyse de risques en matière de vie privée

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée

Peut être le responsable de traitement lui-même

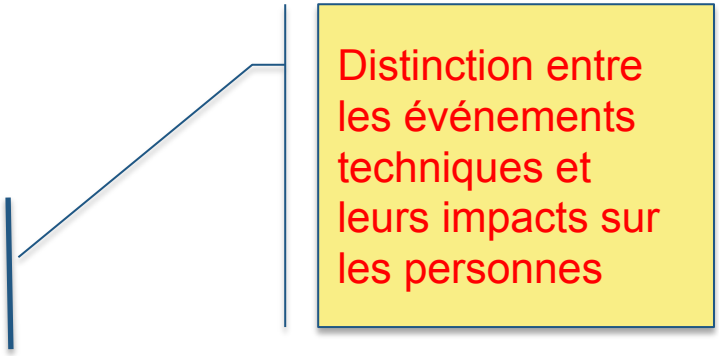
Principaux composants d'une analyse de risques en matière de vie privée

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée



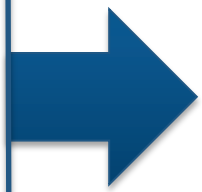
Principaux composants d'une analyse de risques en matière de vie privée

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée



Principaux composants d'une analyse de risques en matière de vie privée

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée



Analyse:

- Vraisemblance des impacts
- Gravité des impacts

Attributs des données personnelles

- Sensibilité (statut juridique)
- Niveau de précision (granularité)
- Volume (nombre de données)
- Format (chiffrement, bruitage, etc.)
- Finalité
- Durée de conservation
- Contrôle (qui peut accéder aux données)

Catégories de sources de risques

- Sources de risques liées au responsable de traitement : responsable de traitement, sous-traitants, employés, clients, etc.
- Sources de risques liées au sujet : famille, amis, collègues, fournisseurs de service, etc.
- Sources de risques liées aux états : police, justice, agences de renseignement, etc.
- Sources de risques génériques : hackers, escrocs, publicitaires, etc.

Attributs des sources de risque

Capacités:

- Droits d'accès
- Informations auxiliaires
- Ressources techniques (matériel, outils, expertise, etc.)

Déterminants (par événement redouté):

- Positifs: motivation, facteurs d'incitation (atteintes délibérées), manque de sensibilisation (atteintes accidentelles)
- Négatifs: facteurs de dissuasion, sensibilisation aux exigences de protection de la vie privée

Catégories d'événements redoutés

1. Collecte excessive de données (violation de principe de minimisation)
2. Usage excessif de données (violation de principe de finalité)
3. Divulgation de données à un tiers (violation des engagements affichés ou de la finalité)
4. Non-respect des obligations du responsable de traitement (effacement, droits d'accès, droit de correction, etc.)
5. Modification ou destruction intempestive de données (atteinte à l'intégrité ou à la disponibilité des données)

Attributs des événements redoutés

Ensemble des scenarios conduisant à l'événement redouté avec leurs:

- Faisabilité : dérivée des capacités des sources de risques et des faiblesses du système
- Vraisemblance : dérivée de la faisabilité de l'événement redouté et des déterminants des sources de risques
- Impacts sur la vie privée

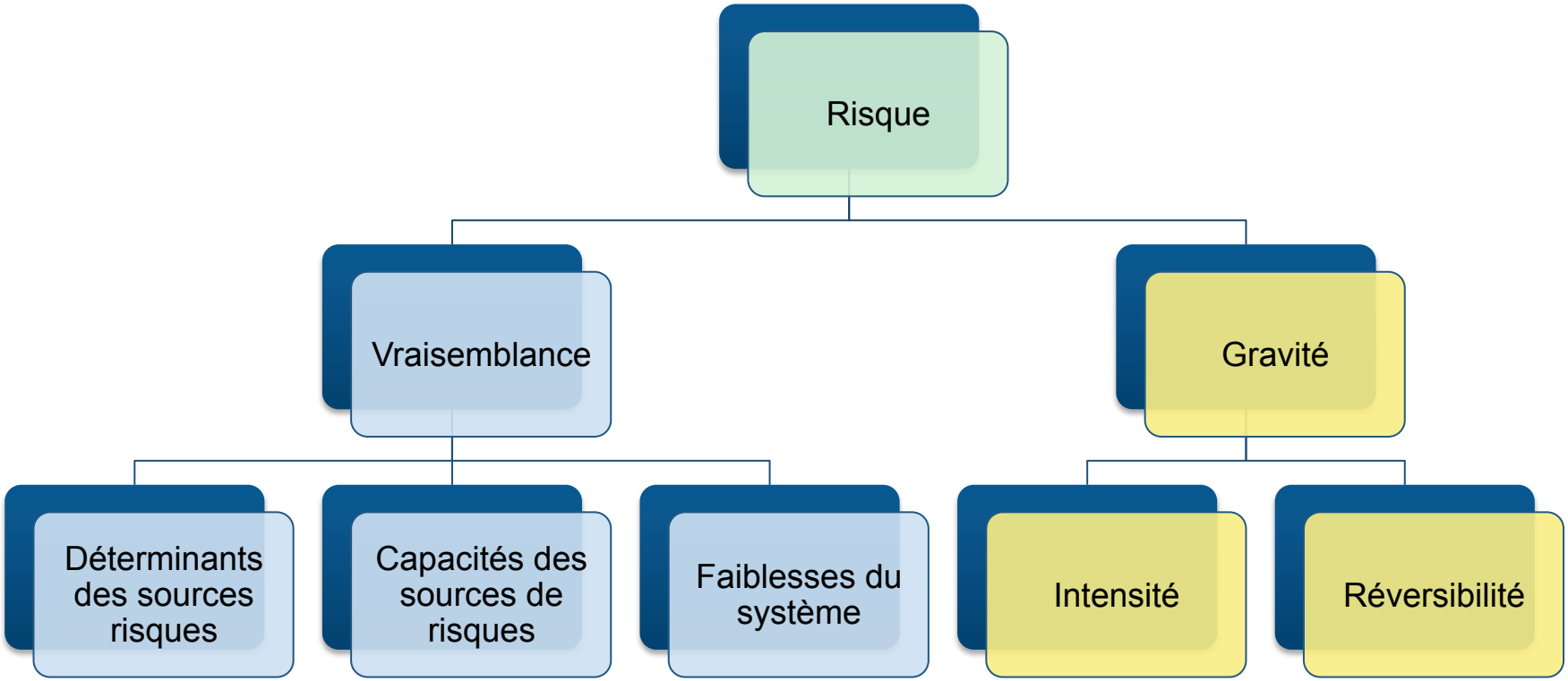
Catégories d'impacts sur la vie privée

1. Impacts physiques : des désagréments mineurs jusqu'aux maladies ou la mort
2. Impacts psychologiques : impression d'intrusion, de perte d'intimité, difficultés relationnelles, dépression, maladie de long terme, etc.
3. Impacts matériels : perte de temps, d'argent, d'opportunités, de travail, de logement, etc.

Attributs des impacts sur la vie privée

1. Vraisemblance : fonction de la vraisemblance des événements redoutés produisant l'impact
2. Gravité : fonction de l'intensité des conséquences et de la capacité des personnes à les surmonter

Risques d'impact sur la vie privée



Evaluation des attributs

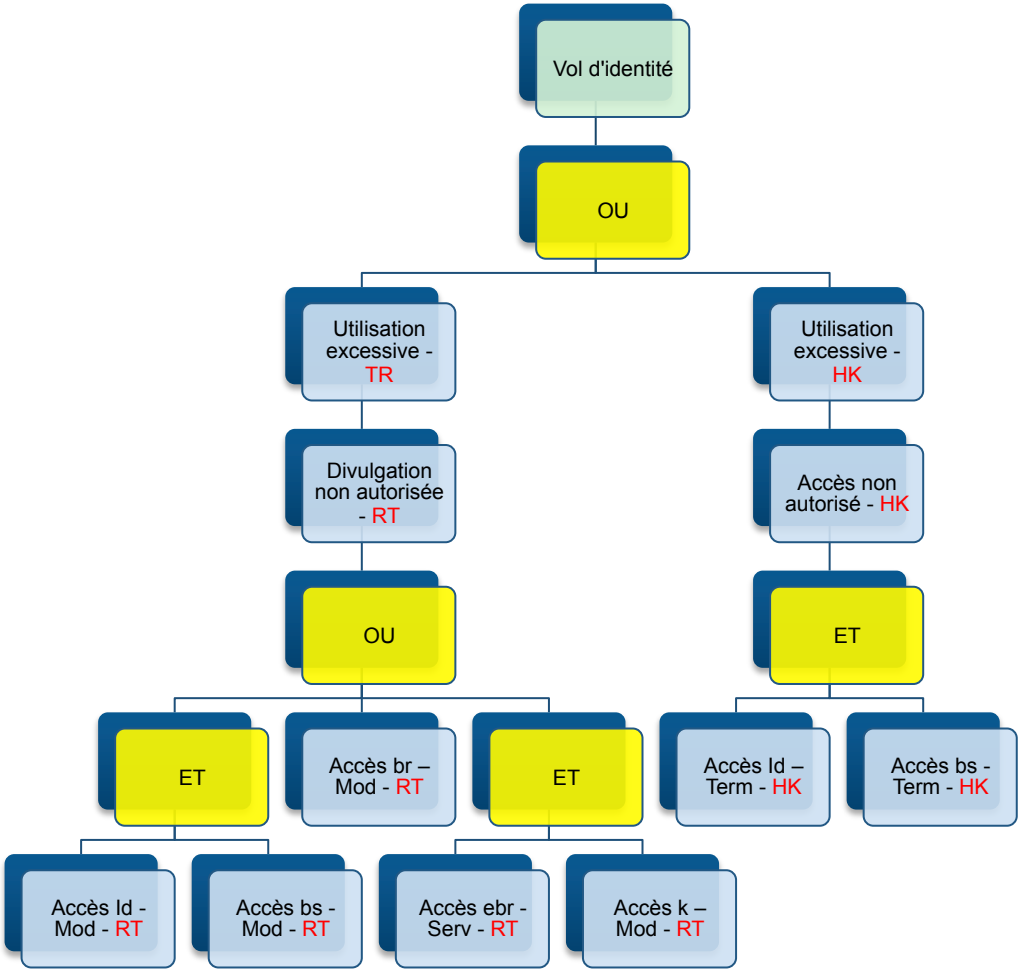
Gravité :

- En première approximation : utilisation de modèles existants (par exemple échelle de gravités proposée par la CNIL)
- Idéalement: après consultation des parties prenantes

Vraisemblance:

- Evaluation quantitative (rigueur) et/ou qualitative (compréhension): tables de correspondance
- Arbres d'impact (privacy harm trees)

Exemple d'arbre d'impact



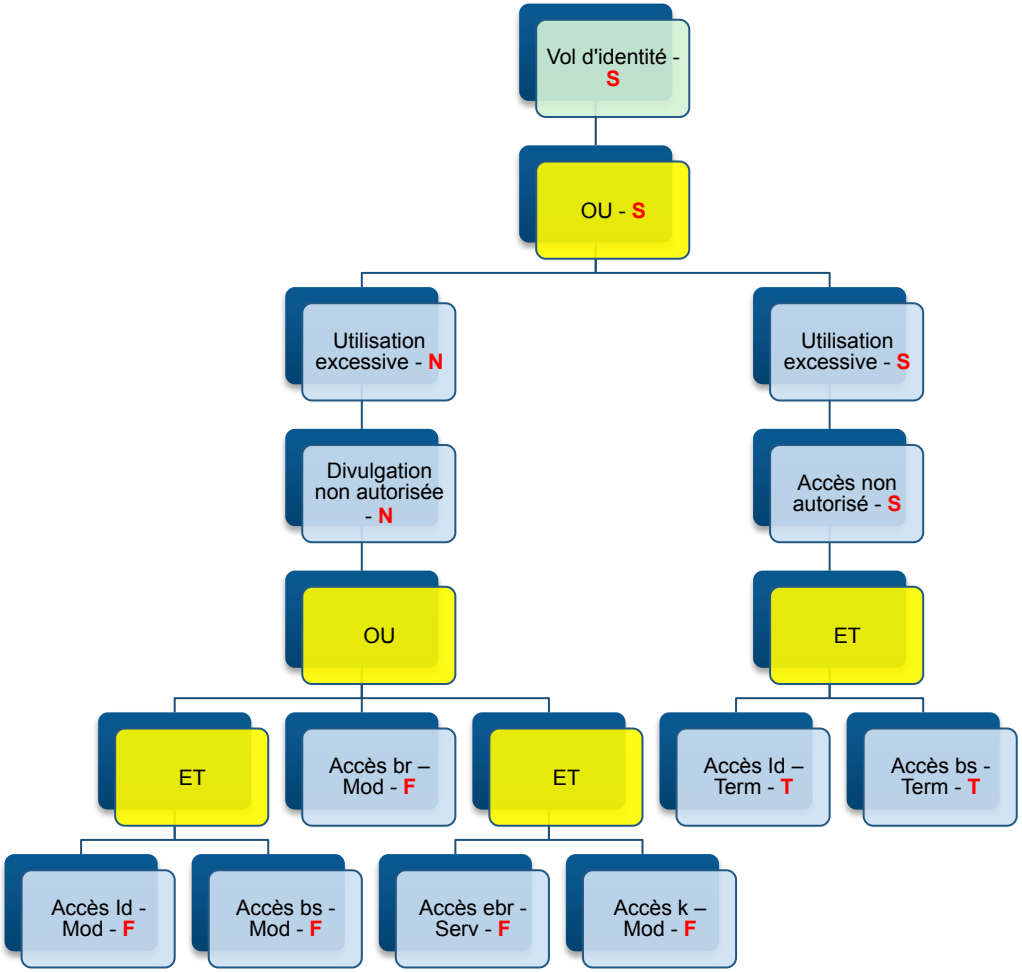
Exemple de table de correspondance

Vraisemblance	Quantitatif
Négligeable	$P < 0{,}01\%$
Faible	$0{,}01\% \leq P < 0{,}1\%$
Moyenne	$0{,}1\% \leq P < 1\%$
Significative	$1\% \leq P < 10\ \%$
Très élevée	$P > 10\ \%$

Exemples de règles de calcul

- Noeud ET, événements indépendants : $P_1 \times P_2$
- Noeud ET, événements potentiellement dépendants : $\text{Min}(P_1,P_2)$
- Noeud OU, événements indépendants : $P_1 + P_2 - P_1P_2$
- Noeud OU, événements mutuellement exclusifs : $P_1 + P_2$
- Noeud OU, événements dépendants : $\text{Max}(P_1,P_2)$

Exemple de calcul de vraisemblance



Perspectives

- Analyse de risques et protection de la vie privée par conception (privacy by design) : justification de choix de conception
- Analyse de risques et mécanismes d'anonymisation: justification de modèles et de métriques d'anonymat
- Outils: aide à la décision, traçabilité, accountability
- Intérêt de la démarche d'analyse de risques au-delà de la conformité: bonne pratique de gestion des risques pour les organisations

Conclusion

- Importance fondamentale de l'obligation de rendre des comptes et de la validation par un tiers indépendant (par exemple accrédité par l'autorité de protection).
- Sinon, loin de représenter un progrès, le nouveau règlement risque de se traduire par une régression des droits des personnes
- L'accountability joue un rôle central dans le règlement: si elle n'est pas mise en oeuvre de manière rigoureuse, c'est tout l'édifice des protections qui est menacé