Observatoire de la Sécurité des Systèmes d'information et des Réseaux (OSSIR)

–

Journée de la Sécurité des Systèmes d'Information (JSSI)

–

Journée « Anonymat, vie privée et gestion d'identité… »

Anonymat et anonymisation dans la sphère Santé-Social

–

Des principes et concepts de base aux applications opérationnelles

Gilles Trouessin

Consultant Senior OPPIDA Sud

gilles.trouessin@oppida.fr
Tél. : 05.61.32.17.86
Gsm : 06.72.87.67.93

Docteur des Universités (1991)
Certifiés AFAI-CISM (2003)
Responsable d'Audit SMSI (2006)

Une sensibilité particulière dans le secteur de santé et du soin

- Décision relative au maintien des relations avec une entreprise, après avoir eu connaissance de ses pratiques abusives autour de la collecte et l'utilisation de données à caractère personnel :
  - ***83%*** ***arrêt total***
  - *16%* *forte réduction*
  - *1%* *continuation*

- Différents critères de décision avant de choisir de travailler avec une entreprise donnée (de *'important'* à *'très important'*) :
  - *91%* *expérience antérieure*
  - *78%* *réputation de l'entreprise*
  - ***68%*** ***transparence en matière de politique "privacy"***
  - *62%* *recommandation par un 'proche'*
  - ***57%*** ***rapport d'audit externe sur la politique "privacy"***
  - ***21%*** ***actions de communication en politique de "privacy"***

- Importance de la définition des politiques en *"privacy"* selon les secteurs d'activités (de *'important'* à *'très important'*) :
  - ***96%*** *services financiers*
  - ***93%*** *fournisseurs de soins*
  - ***90%*** *pharmacie*
  - ***87%*** *télécommunications*
  - ***77%*** *distribution*
  - ***68%*** *transports*
  - ***64%*** *services d'abonnement*
  - ***50%*** *publicité*

Fil conducteur de la présentation

PREAMBULES

- **Préambules sur** le respect de… la vie privé — *intimité*
- **Préambules sur** la sphère Santé/Social — *santé*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- **Sûreté de fonctionnement** d'un système — *sûreté*
- **Protection & Sécurité** de l'information — *sécurité*
- **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- **Anonymat** des informations — *anonymat*
- **Anonymisation** des données — *anonymisation*
- **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- **Besoins / Objectifs / Exigences** d'anonymisation — *démarche*
- **Irréversibilité / Inversibilité / Réversibilité** de l'anonymisation — *X-versibilité*
- **Chaînage / Robustesse / Inférence / Multiplicité** d'une anonymisation — *propriétés*

Illustrations en Santé & Social

- **Exemple de double anonymisation** dans la santé — *PMSI*
- **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

CONCLUSIONS

- …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

Vie privée (et respect de la…)

- ***Notions et périmètres variables de la « vie privée… » :***
  - *"privative" :* contexte personnel, familial, intimiste et privatif
  - *"publique" :* dans les lieux publics, lors d'activités publiques
  - *"citoyenne" :* contexte électoral, sur le lieu du bureau de vote
  - *"internaute" :* lors des connexions à un Intranet, Extranet, Internet
  - *"professionnelle" :* dans le cadre professionnel et sur le lieu travail

- ***Obligation commune de « respect… » de la vie privée :***
  - *"administratif" :* vis-à-vis de fichiers du fisc, de la police, etc.
  - *"statistique" :* fichiers INSEE, statistiques, enquêtes, sondages
  - *"médical" :* dossier médical, de soins, généraliste/spécialité
  - *"social" :* ANPE, URSSAF, DDASS/DRASS, CPAM/CRAM

Données personnelles (et notions/catégories de…)

- ***Diverses notions de « donnée personnelle… » :***
  - *"caractère personnel" :* associée à une personne physique
  - *"atomique (non agrégée)" :* significative d'un individu donné
  - *"agrégée (fusionnée)" :* relative à l'ensemble d'une population
  - *"pseudonymisée" :* ayant un lien direct avec l'individu physique
  - *"dépersonnalisée" :* sans lien direct avec l'individu physique

- ***Diverses catégories de « donnée personnelle… » :***
  - *"de nature comportementale" :* consommations, habitudes, profils
  - *"à caractère professionnel" :* rythmes, horaires, lieux de travail
  - *"à caractère génétique" :* génome humain, critère génétique
  - *"à caractère médical" :* pathologies, antécédents, symptômes
  - *"à caractère social" :* trajectoires sociales, allocations diverses

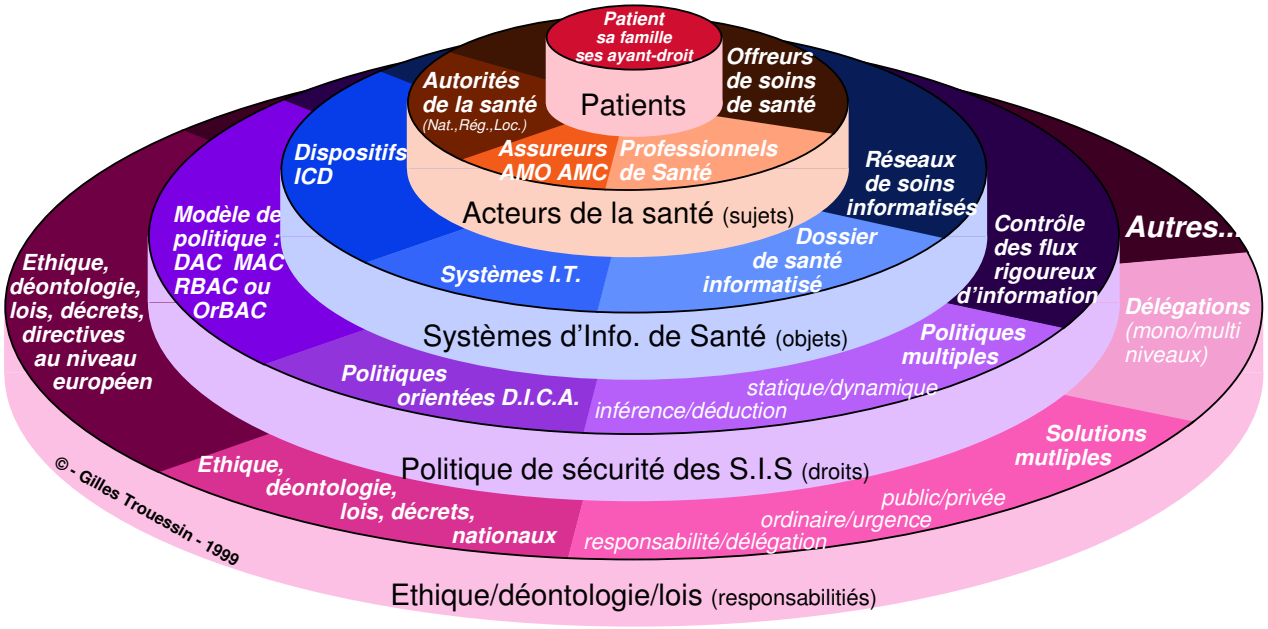
Données personnelles nominatives (et types/catégories de…)

- ***Divers types de « données personnelles nominatives » :***
  - *"directement nominative" :* une donnée au registre d'état civil
  - *"indirectement nominative" :* le NIR (RNIPP ou n° de "sécu.")
  - *"très indirectement nominative" :* séjour d'un patient en hôpital
  - *"très très indirectement nominative" :* avec l'exemple d'un avion :
    { numéro de siège + [rang du siège + (numéro de vol + 'date du vol')] }
  - *"anonymisée" :* un n° de séjour d'hospitalisation (patient inconnu)
  - *"anonyme" :* *"la connexion au serveur vocal a eu lieu entre 17h42 et 17h44"*

- ***Divers types et/ou catégories de « secret privatif » :***
  - *"ordinal" :* les professions à ordre (médecin, notaire, juge, avocat)
  - *"intime / intimiste" :* mœurs, sexe, religion, politique, syndicat
  - *"partageable" / "partagé" :* donnée médicale, élément de soin
  - *"échangeable" / "échangé" :* donnée sociale, élément salarial
  - *"communicable" / "communiqué" :* extrait de dossier médical

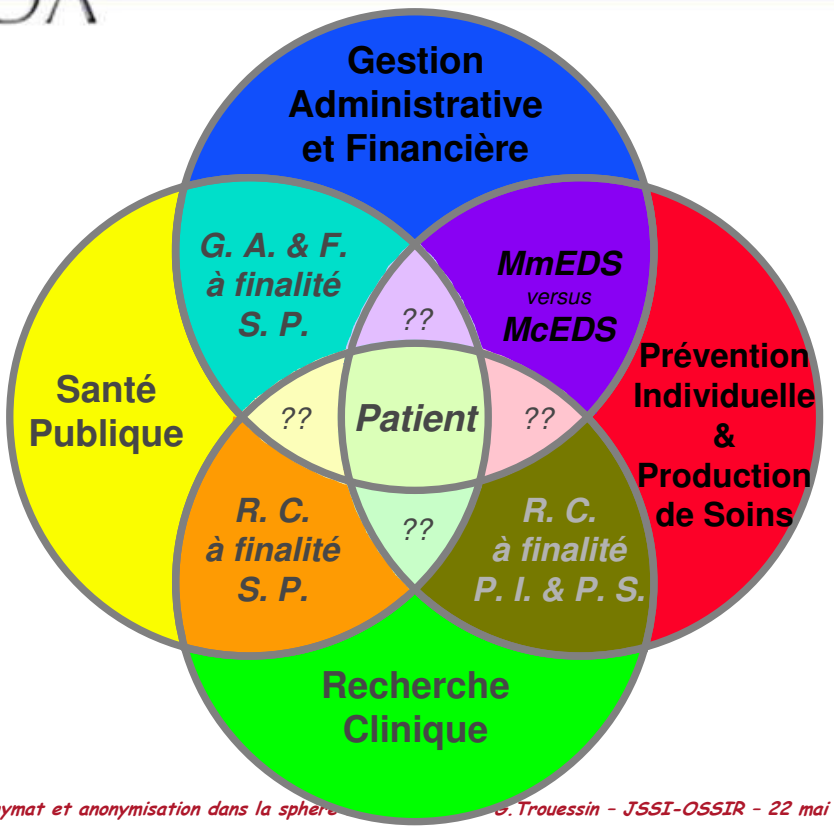
Patient + Sujet.Objet.Droit + Responsabilité

Exigences de flexibilité et de robustesse pour la SSI



Systèmes d'Information de Santé :

les domaines / missions / fonctions / métiers



Fil conducteur de la présentation

PREAMBULES

- ☑ **Préambules sur** le respect de… la vie privé — *intimité*
- ☑ **Préambules sur** la sphère Santé/Social — *sécurité*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- ❑ **Sûreté de fonctionnement** d'un système — *sûreté*
- ❑ **Protection & Sécurité** de l'information — *sécurité*
- ❑ **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- ❑ **Anonymat** des informations — *anonymat*
- ❑ **Anonymisation** des données — *anonymisation*
- ❑ **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- ❑ **Besoins** / **Objectifs** / **Exigences** d'anonymisation — *démarche*
- ❑ **Irréversibilité** / **Inversibilité** / **Réversibilité** de l'anonymisation — *X-versibilité*
- ❑ **Chaînage** / **Robustesse** / **Inférence** / **Multiplicité** d'une anonymisation — *propriétés*

Illustrations en Santé & Social

- ❑ **Exemple de double anonymisation** dans la santé — *PMSI*
- ❑ **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

CONCLUSIONS

- ❑ …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

Sûreté de Fonctionnement & Sphère Santé / Social

- ❑ *La "**Sûreté de Fonctionnement**" d'un système informatique est cette "propriété générique qui permet aux utilisateurs de ce système de placer une confiance justifiée dans le service qui leur est délivré par ce système [Laprie88 (LAAS)]"*

- ❑ La ***Sûreté de Fonctionnement*** est visible/perceptible selon différentes facettes (ou attributs perceptifs), telles que :
  - ➢ La ***"Sécurité de l'"Information"*** (dite ***"Sécurité-Immunité"*** au sens de ***"Security"***) vis-à-vis de ***"sa capacité à garantir que toute manipulation de l'information est autorisée/autorisable"***
  - ➢ La ***"Sûreté du système"*** (dite ***"Sécurité-Innocuité"*** au sens de ***"Safety"***) : vis-à-vis de ***"la non-occurrence de conséquences catastrophiques sur les individus et l'environnement"***
  - ➢ La ***"Fiabilité du système"*** (au sens de ***"Reliability"***) : vis-à-vis de ***"sa capacité à offrir une continuité de service"***
  - ➢ La ***"Maintenabilité du système"*** (au sens de ***"Maintainability"***) : vis-à-vis de ***"sa capacité de réparation ou d'évolution"***

Sécurité de l'information & exigences en Santé/Social

- La *"**sécurité de l'information**"* peut être vue comme *"la combinaison des 4=3+1 propriétés de base qui, si elles sont fournies, permettent de garantir que les informations sont manipulées de façon autorisée"*

- La ***Sécurité de l'Information*** est souvent composée de :
  - La *"**disponibilité**"* (au sens de *"availability"*) : _____vis-à-vis de *"son aptitude à être prêt à l'utilisation"*
  - L' *"**intégrité**"* (au sens de *"integrity"*) : _____vis-à-vis de la *"non-occurrence de modifications inadéquates"*
  - La *"**confidentialité**"* (au sens de *"confidentiality"*) : _____vis-à-vis de la *"non-occurrence de divulgations inappropriées"*
  - L' *"**auditabilité du système**"* (au sens de *"ability to audit"*) : _____vis-à-vis de la capacité du système à *"auditer le(s) sous-système(s) mis en œuvre et à auditer la(les) sécurité(s) mise(s) en place"*

Confidentialité(s) & "ex- Secret médical"

- *La **"confidentialité"** est la **"propriété qui permet de garantir que les informations sont divulguées de façon autorisée"** :*
  - Confidentialité_____accès à l'information en justifiant du *"besoin d'en connaître"*
  - Secret "médical"_____accès légitime mais dans le respect du *"colloque singulier"*
  - Secret professionnel_____accès autorisé à l'information mais *"obligation de réserve"*
  - Discrétion professionnelle__accès inévitable avec obligation de *"respect de l'individu"*
- **Mais aussi :**
  - Anonymat strict_____suppression (irréversible) des identités (directes ou indirectes)
  - Pseudo-anonymat_____remplacement (inversible) des identités par des numéros (muets)
  - Vrai-faux anonymat_____modification provisoire (réversible) des informations "ré-identifiantes"

La confidentialité classique : ou "confidentialité-discrétion© "

- *La "**confidentialité-discrétion©**" est la "**propriété garantissant que les informations sont divulguées en toute discrétion**" :*
  - Cryptographie_____techniques consistant à protéger l'information électroniquement
  - Chiffrement à Clés…____ *exemples :* chiffrement symétrique et chiffrement asymétrique
  - Techniques éprouvées_____techniques actuelles pouvant être testées mondialement
  - Techniques réversibles_____ *exemples :* protection des données durant leur transport
- **Et aussi :**
  - En respectant la loi__longtemps restreinte d'utilisation, la cryptographie s'est assouplie
  - Avec l'accord de l'individu_____prendre en compte les exigences émises par la CNIL
  - Dans le respect de l'état de l'art_____ces techniques pointues ne s'improvisent pas
- **Et donc ⇒ *obligation de protection et de discrétion :***
  - Les *risques* résident dans une mauvaise application des techniques de base
  - Les *parades* consistent à pratiquer, ou à faire faire, une veille cryptographique pointue et permanente et à intégrer les outils de chiffrement le plus en amont possible de la chaîne logique de la sécurité…

La confidentialité non-classique : ou "confidentialité-séclusion© "

- *La "**confidentialité-séclusion©**" est la "**volonté intime de garantir que les informations sont divulguées entièrement anonymisées**" de façon :*
  - Irréversible_____aucun retour possible depuis les anonymats vers les noms et/ou identités
  - Inversible_____seul retour possible aux noms et/ou identités : la voie légale et réglementaire
  - Chaînable_____possibilité de relier ensemble tous les épisodes de soins et/ou de remboursement
  - Robuste_____robustesse aux attaques par inférences (déductives, inductives, abductives, adductives)
- **Et aussi :**
  - Anonymisation vraie_____irréversibilité totale et prouvée (juridique, organisationnelle, technologique)
  - Fonction à sens unique_____fonction cryptographique proche du chiffrement irréversible
  - Dimension juridique/éthique_____organisation indispensable pour garantir un anonymat vrai
- **Et donc ⇒ pas d'atteinte à l'intimité de la vie privée :**
  - Les *risques* sont plus difficilement mesurables car une perte de confidentialité (i.e., là où il y avait volonté de préserver l'intimité de l'individu) est souvent irréparable
  - Les *conséquences* peuvent être définitives tant pour le fautif que pour la victime
  - Les *menaces* sont de 3 ordres : juridiques, organisationnels et technologiques
  - Les *solutions* passent par : analyse de risques et expression des besoins précis

Fil conducteur de la présentation

PREAMBULES

- ☑ **Préambules sur** le respect de… la vie privé — *intimité*
- ☑ **Préambules sur** la sphère Santé/Social — *sécurité*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- ☑ **Sûreté de fonctionnement** d'un système — *sûreté*
- ☑ **Protection & Sécurité** de l'information — *sécurité*
- ☑ **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- ❑ **Anonymat** des informations — *anonymat*
- ❑ **Anonymisation** des données — *anonymisation*
- ❑ **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- ❑ **Besoins / Objectifs / Exigences** d'anonymisation — *démarche*
- ❑ **Irréversibilité / Inversibilité / Réversibilité** de l'anonymisation — *X-versibilité*
- ❑ **Chaînage / Robustesse / Inférence / Multiplicité** d'une anonymisation — *propriétés*

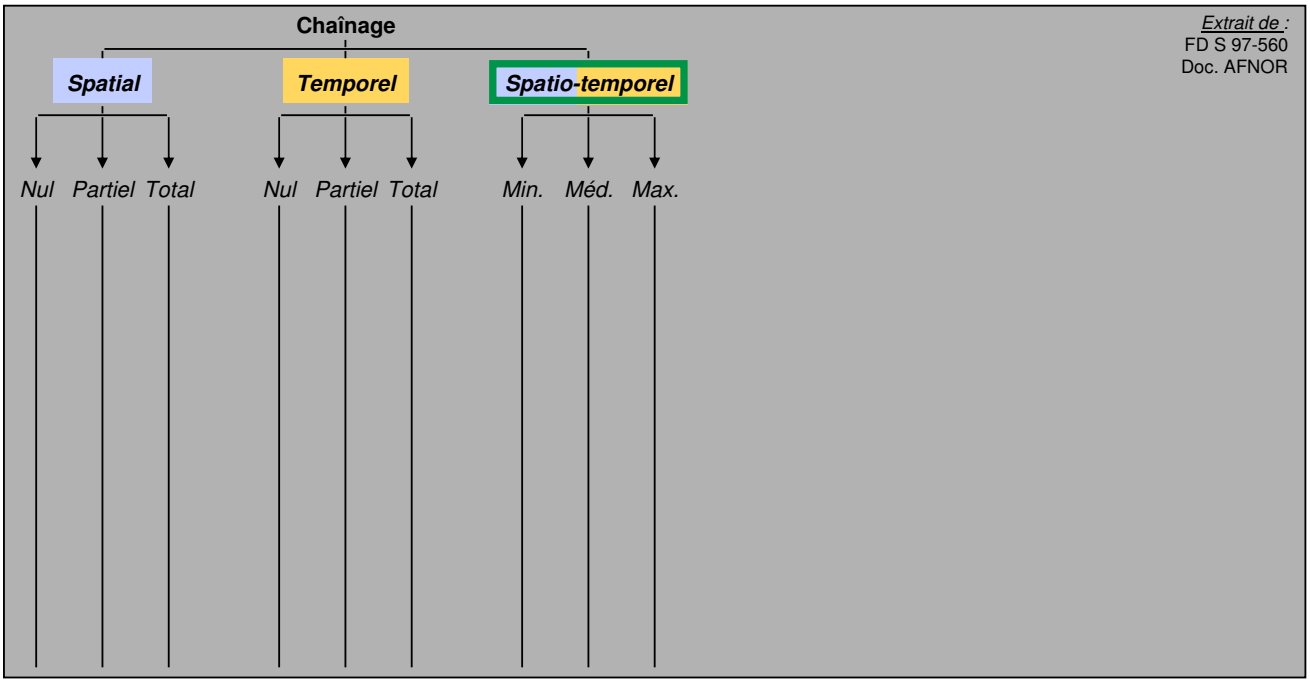
Illustrations en Santé & Social

- ❑ **Exemple de double anonymisation** dans la santé — *PMSI*
- ❑ **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

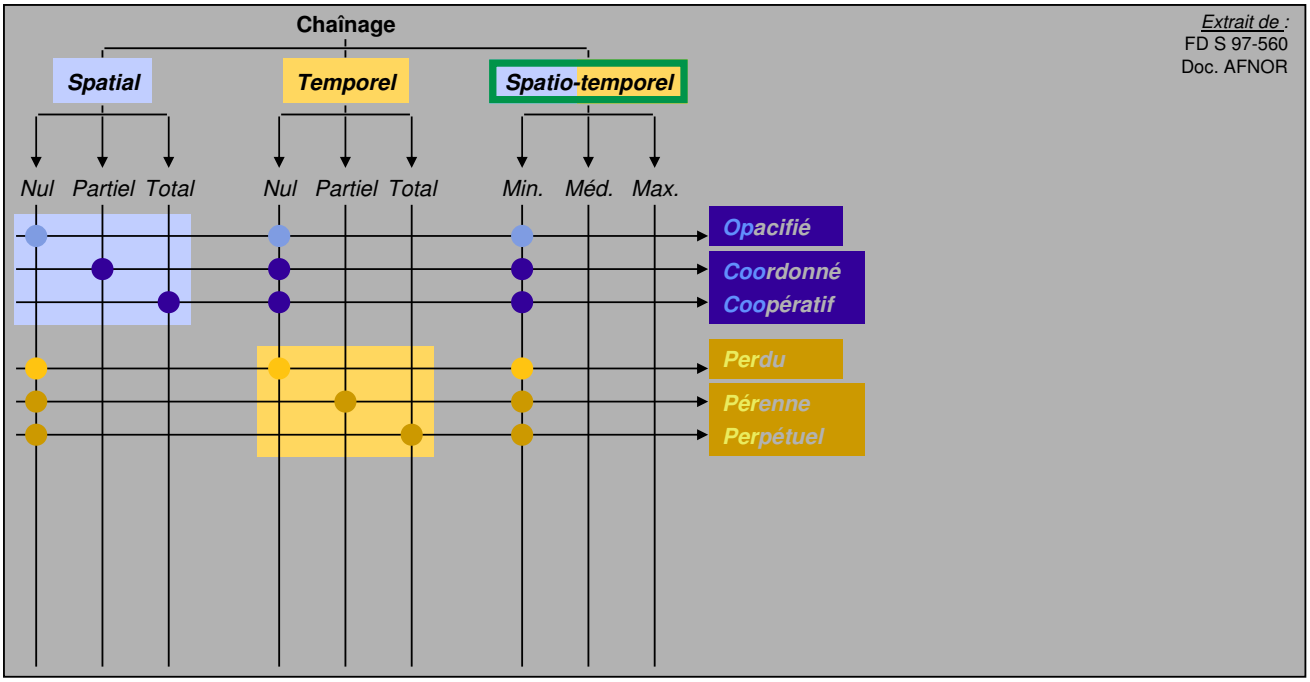
CONCLUSIONS

- ❑ …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

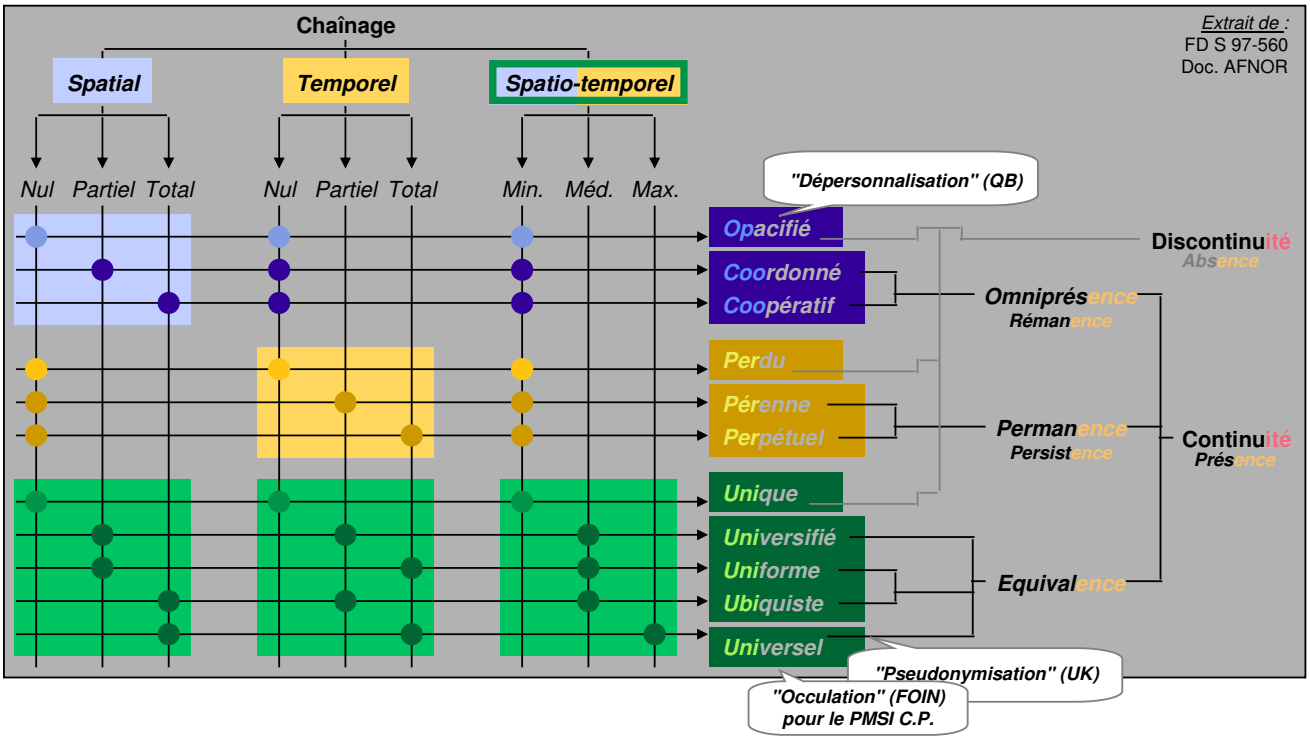
Classification des modes de chaînages des identifiants (nominatifs/anonymes)



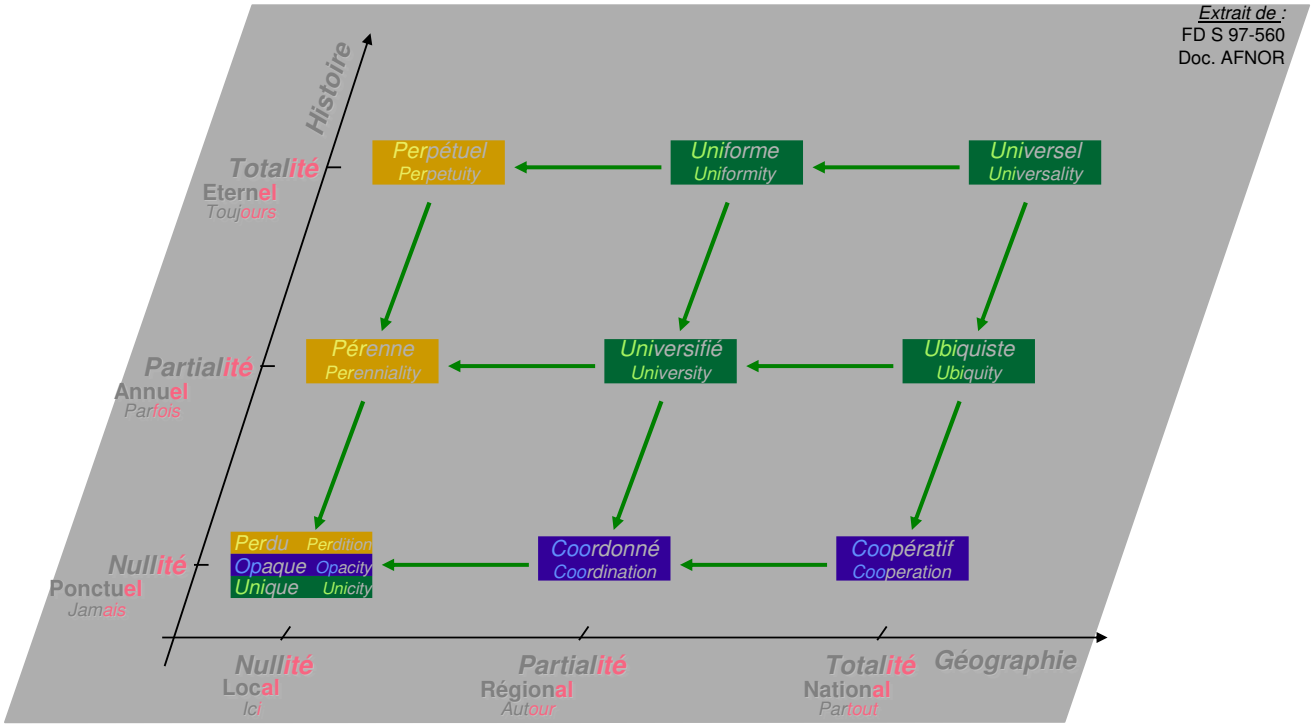
Classification des modes de chaînages des identifiants (nominatifs/anonymes)



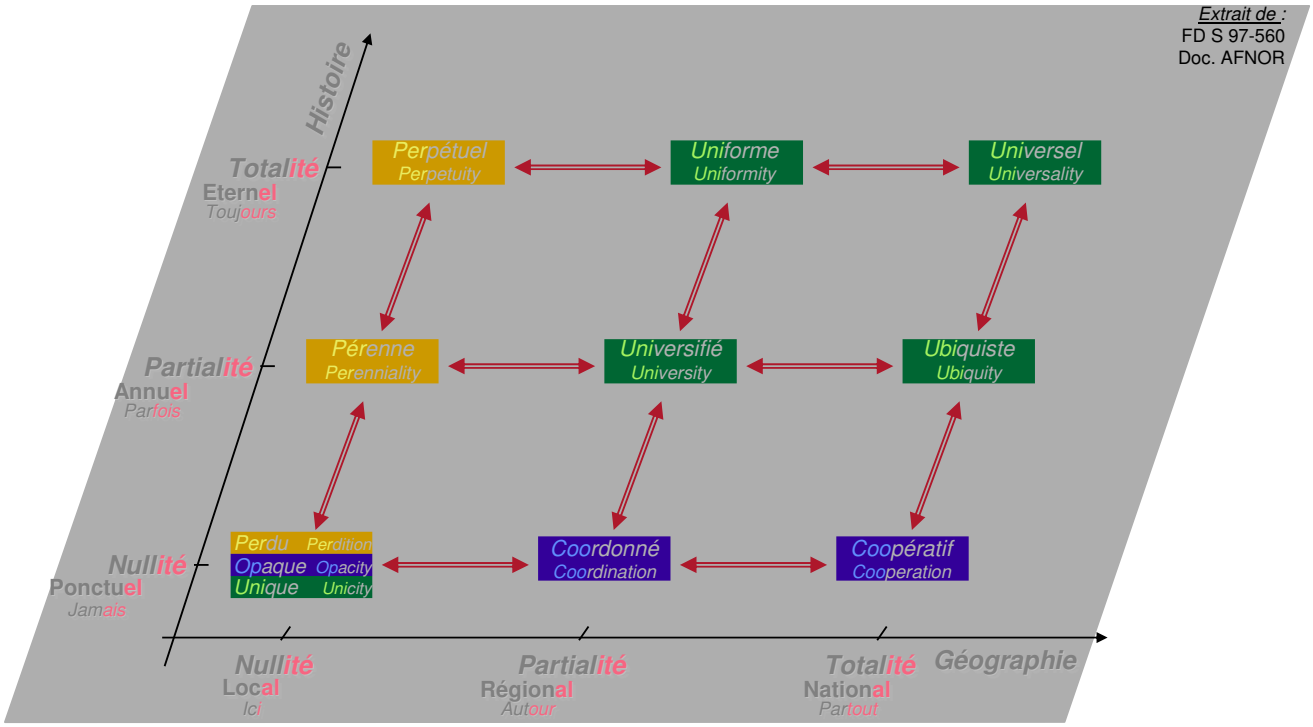
Classification des modes de chaînages des identifiants (nominatifs/anonymes)



Réseau des techniques de chaînages d'anonymisation (irréversible)



Réseau des techniques de chaînages de "pseudo-anonymisation" (réversibles)



Fil conducteur de la présentation

PREAMBULES

- ☑ **Préambules sur** le respect de… la vie privé — *intimité*
- ☑ **Préambules sur** la sphère Santé/Social — *sécurité*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- ☑ **Sûreté de fonctionnement** d'un système — *sûreté*
- ☑ **Protection & Sécurité** de l'information — *sécurité*
- ☑ **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- ☑ **Anonymat** des informations — *anonymat*
- ☑ **Anonymisation** des données — *anonymisation*
- ☑ **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- ❑ **Besoins** / **Objectifs** / **Exigences** d'anonymisation — *démarche*
- ❑ **Irréversibilité** / **Inversibilité** / **Réversibilité** de l'anonymisation — *X-versibilité*
- ❑ **Chaînage** / **Robustesse** / **Inférence** / **Multiplicité** d'une anonymisation — *propriétés*

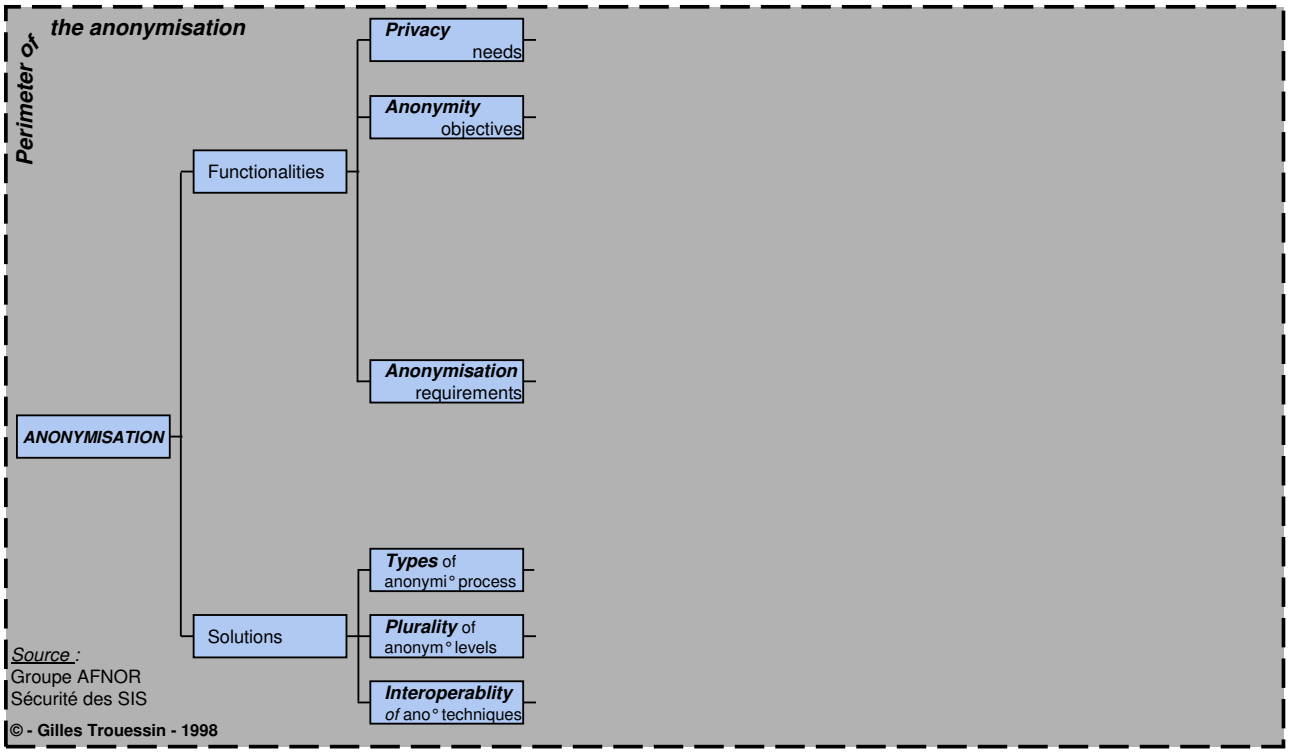
Illustrations en Santé & Social

- ❑ **Exemple de double anonymisation** dans la santé — *PMSI*
- ❑ **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

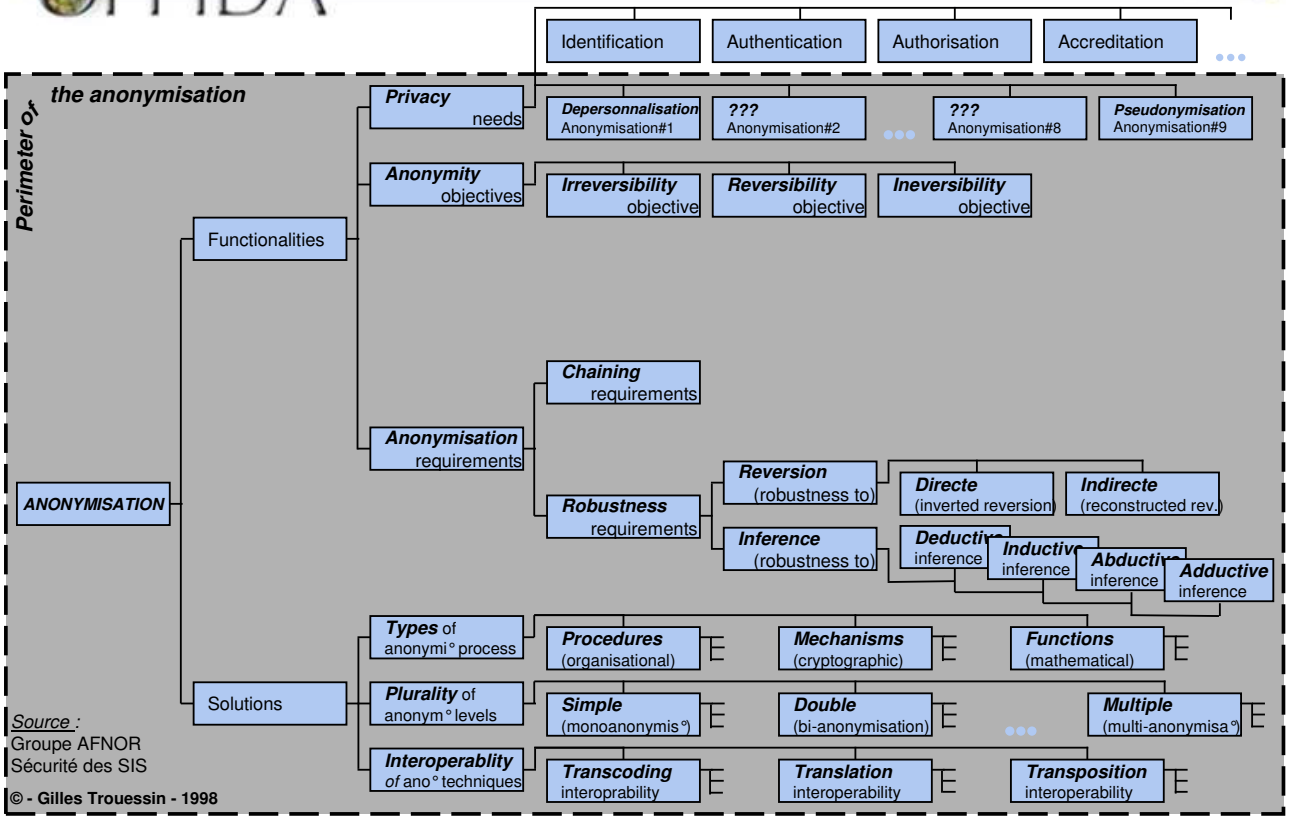
CONCLUSIONS

- ❑ …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

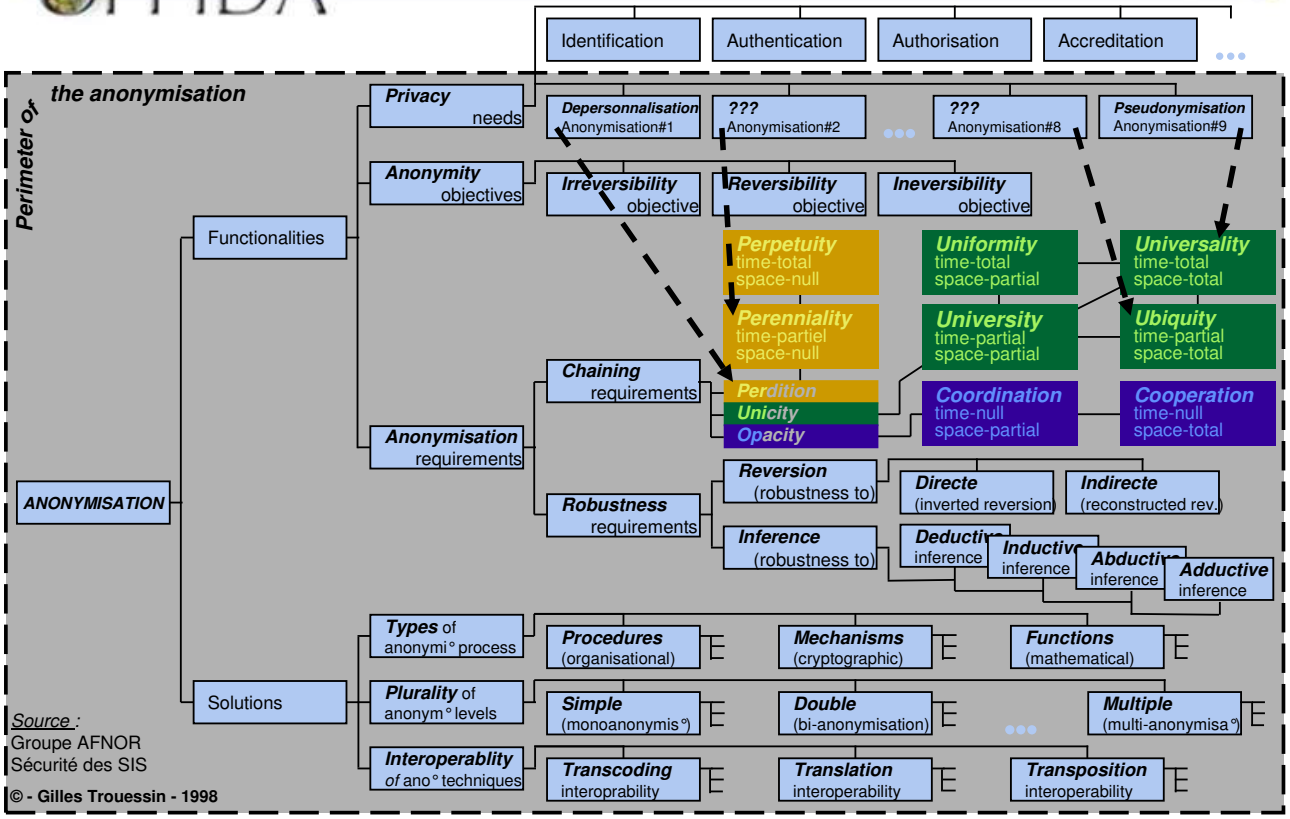
Taxinomie de l'anonymisation dédiée à la sphère Santé/Sociale



Taxinomie de l'anonymisation dédiée à la sphère Santé/Sociale



Taxinomie de l'anonymisation dédiée à la sphère Santé/Sociale



Fil conducteur de la présentation

PREAMBULES

- ☑ **Préambules sur** le respect de… la vie privé — *intimité*
- ☑ **Préambules sur** la sphère Santé/Social — *sécurité*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- ☑ **Sûreté de fonctionnement** d'un système — *sûreté*
- ☑ **Protection & Sécurité** de l'information — *sécurité*
- ☑ **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- ☑ **Anonymat** des informations — *anonymat*
- ☑ **Anonymisation** des données — *anonymisation*
- ☑ **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- ☑ **Besoins / Objectifs / Exigences** d'anonymisation — *démarche*
- ☑ **Irréversibilité / Inversibilité / Réversibilité** de l'anonymisation — *X-versibilité*
- ☑ **Chaînage / Robustesse / Inférence / Multiplicité** d'une anonymisation — *propriétés*

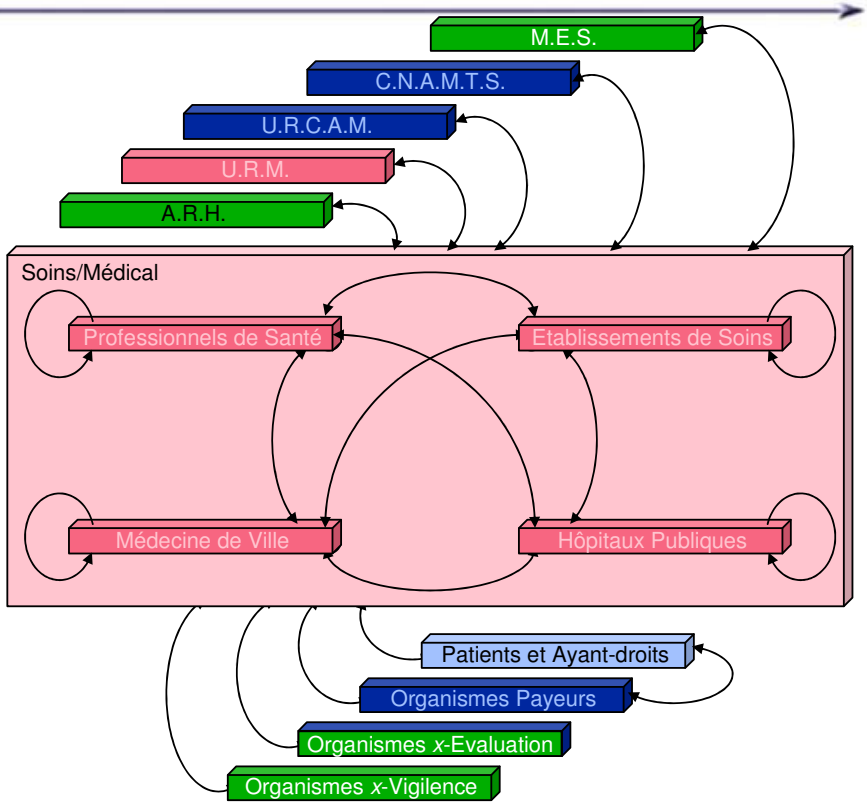
Illustrations en Santé & Social

- ❑ **Exemple de double anonymisation** dans la santé — *PMSI*
- ❑ **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

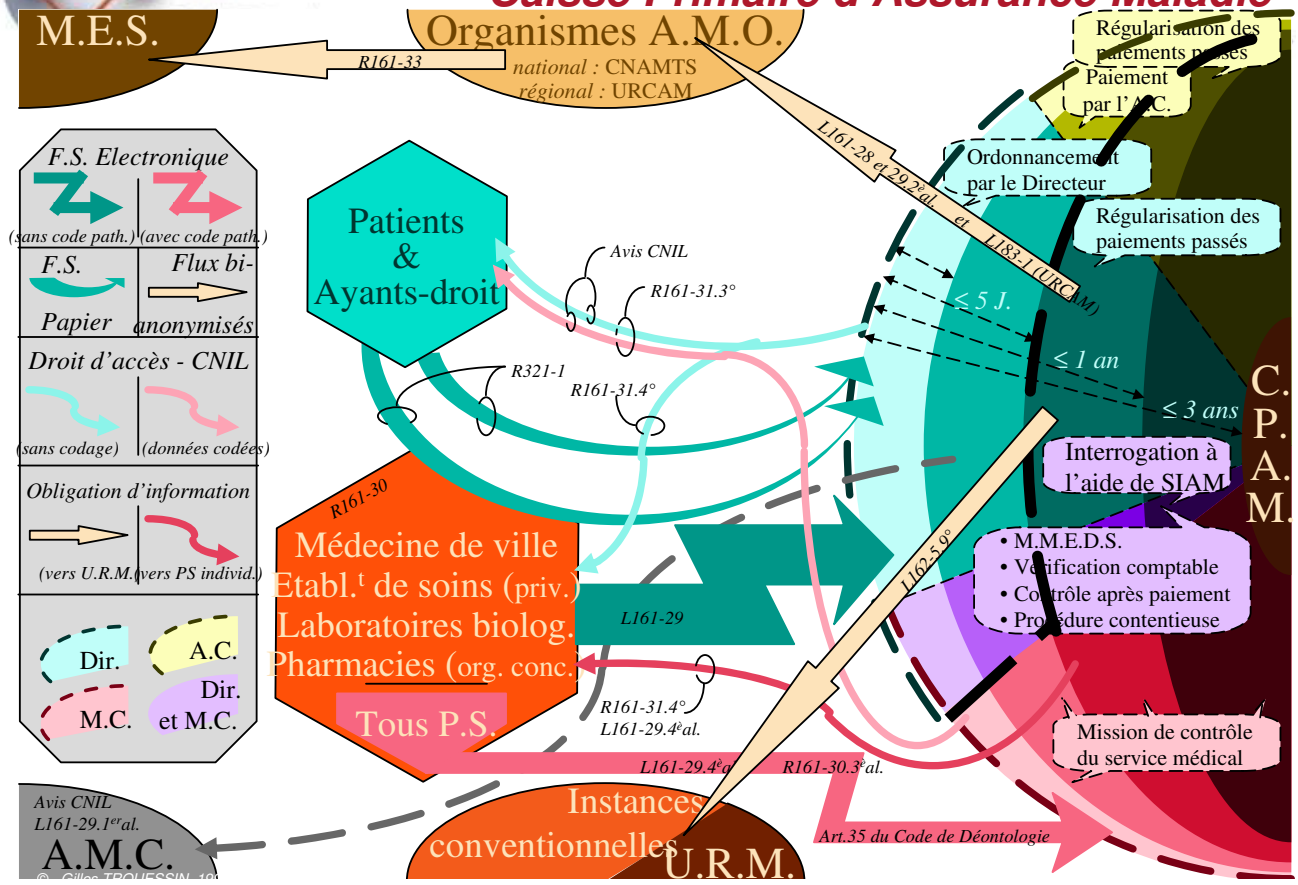
CONCLUSIONS

- ❑ …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

Familles de flux d'information à sécuriser dans la sphère Santé/Social



Exemple-1 : flux entrants/sortants d'une Caisse Primaire d'Assurance Maladie



Exemples-2 & -3 : sécurisation des données / flux pour les Systèmes d'Informations de Santé/Social

OPPIDA

Anonymisation (irréversible) des trajectoires de soins des assurés et bénéficiaires en hospitalier (privé, ...)

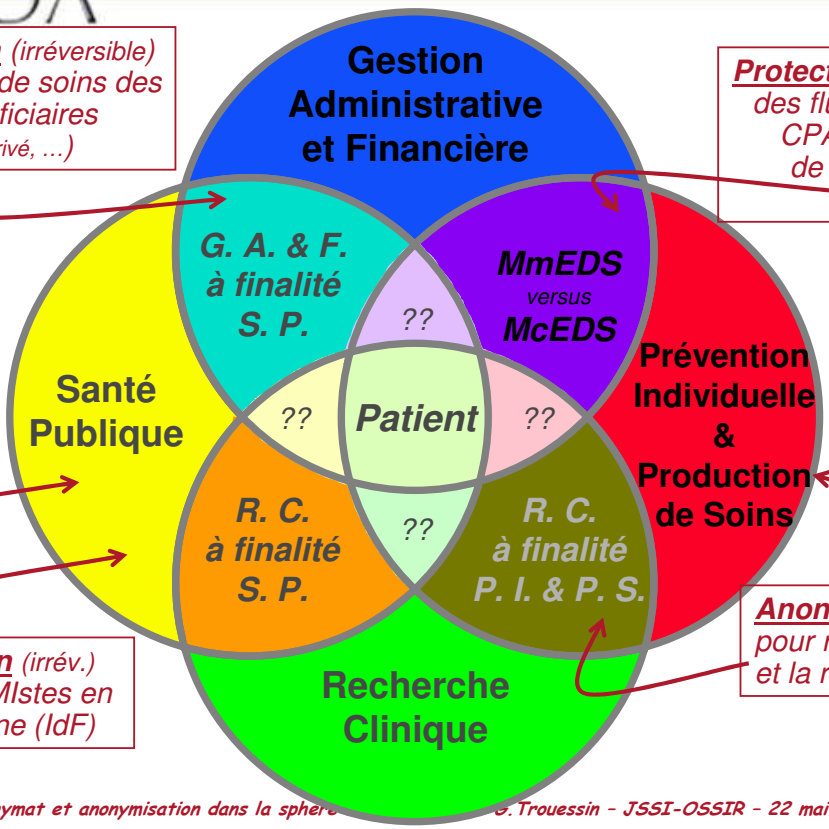
Protection (authenticité) des flux électroniques CPAMs → banques de remboursement aux assurés

Anonymisation des maladies soumises à déclarations obligatoires

Confidentialité des échanges et des extraits de dossiers ~ entre P.S.

Anonymisation (irrév.) du suivi des RMIstes en région parisienne (IdF)

Anonymisation (irrév.) pour réseaux de soins et la recherche



Fil conducteur de la présentation

PREAMBULES

- ☑ **Préambules sur** le respect de… la vie privé — *intimité*
- ☑ **Préambules sur** la sphère Santé/Social — *sécurité*

Sûreté / Sécurité / Confidentialité / Discrétion / Séclusion

- ☑ **Sûreté de fonctionnement** d'un système — *sûreté*
- ☑ **Protection & Sécurité** de l'information — *sécurité*
- ☑ **Confidentialité(s)** des données — *discrétion / séclusion*

Anonymat / Anonymisation / Pseudonymat / Pseudonymisation

- ☑ **Anonymat** des informations — *anonymat*
- ☑ **Anonymisation** des données — *anonymisation*
- ☑ **Pseudonymisation** des identités — *pseudonymisation*

Caractérisation / Caractéristiques

- ☑ **Besoins / Objectifs / Exigences** d'anonymisation — *démarche*
- ☑ **Irréversibilité / Inversibilité / Réversibilité** de l'anonymisation — *X-versibilité*
- ☑ **Chaînage / Robustesse / Inférence / Multiplicité** d'une anonymisation — *propriétés*

Illustrations en Santé & Social

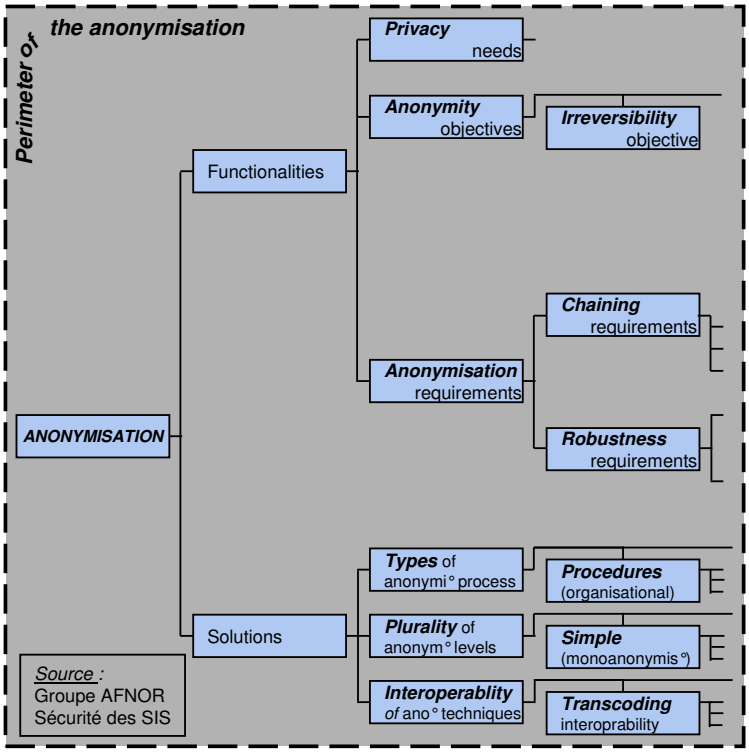
- ☑ **Exemple de double anonymisation** dans la santé — *PMSI*
- ☑ **Exemple de simple anonymisation** dans le social — *Obs.-RMI*

CONCLUSIONS

- ❑ …vers la notion de **TPC d'anonymisation** — *TPC "DMA"*

Démarche d'analyse de risques & technologies pour la confiance

- ❑ **Besoins :**
  - ➢ Authentification ?
  - ➢ Autorisation ?
  - ➢ Authenticité ?
  - ➢ Confidentialité ?
  - ➢ Confidentialité-Discrétion ?
  - ➢ Confidentialité-Séclusion ?
- ❑ **Objectifs :**
  - ➢ Uniformité ?
  - ➢ Spécificité ?
  - ➢ Particularité ?
- ❑ **Exigences :**
  - ➢ Chaînage des *identifiants* ?
  - ➢ Fiabilité des *anonymats* ?
  - ➢ Protection des *clés d'Anonym°*?
  - ➢ Robustesse à l'inférence(s) ?
  - ➢ Tiers de confiance (centralisé) ?



CONCLUSION
vers une nouvelle famille de TPC : les tiers de confiance de "gestion" de l'anonymat

TPC de CONFIDENTIALITE
ou *TTP for "confidentiality"*
ou *Confidentiality-TTP*

TPC de Certification (IGC)
ou Prestataire de Service de Certification
or *Certification-TTP (PKI)*

TPC d'ANONYMISATION
ou Instance de Coordination des Identités
or *Data Matching Agency (DMA)*

- ***Selon les CC (ISO15408)***
  - *f*_anonymat_____OUI
  - *f*_pseudonymat_____non applicable
  - *f*_non-chaînabilité_____OUI/NON
  - *f*_non-observabilité_____non-applicable
- ***Ou bien selon …???***

TPC_de-Pseudo-Anonymisation "réversible"
Pseudo-Annonym._TTP

TPC_d'Anonymisation "irréversible"
Privacy_TTP

TPC_Respect-de-l'-Intimité "inversible"
Anonymity_TTP

… combinable avec...

…du chaînage spatial (seul)

…du chaînage temporel (seul)

…du chaînage spatio-temporel

Je vous remercie pour votre attention…

Questions ?

Remarques ?

Commentaires ?

Avis personnels ?