La réglementation relative aux données à caractère personnel en sciences sociales

Thomas Soubiran

CERAPS - UMR 8026 CNRS-Lille 2

Séminaire du GLISS

Strasbourg, le 6 octobre 2017

La réglementation sur les données à caractère personnel

La réglementation sur les données à caractère personnel (DCP) :

- ensemble de règles juridiques relatives à **l'utilisation** (« traitement ») de DCP, c-à-d de données permettant **d'identifier des personnes physiques**
- définit des **obligations** à respecter lors du traitement de DCP
- ainsi que quelques **interdictions** (mais aussi des **exceptions** à l'interdiction)

Les données à caractère personnel en sciences sociales

Le traitement de DCP est **au cœur** de l'activité des sciences sociales :

- l'utilisation de DCP peut en effet y prendre de **multiples formes** et répond à de **multiples fins** :
  - **collecte de données** (p. ex. pour la réalisation d'enquêtes par questionnaires)
  - **les analyses**
  - ainsi que dans les **publications**, que les personnes soient nommées ou « pseudonymisées »
- l'importance des DCP fait que les traitements en sciences sociales tombent le plus souvent **dans le champ d'application** de la réglementation en vigueur

La réglementation relative aux DCP

En France, le traitement de **DCP** est jusqu'à présent encadré par **la loi informatique et libertés** (LIL) :

- loi votée le 6 janvier 1978
- elle a été modifiée par la suite à plusieurs reprises, notamment en 2004 pour transposer la **directive européenne** sur la protection des données de 1995
- la prochaine modification interviendra **l'année prochaine**

En effet, le 25 mai 2018 prochain,

le règlement européen sur la protection des données entrera en application

- le règlement général sur la protection des données (**RGPD**) est **d'application directe** dans le droit des États membres (pas de transposition)
- il **abrogera** la directive de 1995
- il **n'abroge pas** la LIL mais en rend néanmoins inapplicable les dispositions incompatibles avec le règlement

Le règlement européen sur la protection des données

Depuis sa publication au Journal officiel de l'**UE** le 24 mai 2016, le **RGPD** constitue **le nouveau texte de référence** européen en matière de protection des données à caractère personnel :

- adopté après quatre ans (d'âpres) négociations
- le **RGPD** reprend **les fondamentaux** de la directive, les grands principes restent en effet les mêmes
- les implications sont plutôt d'ordre **pratique**

La situation actuelle est **transitoire** :

- le règlement est en vigueur mais pas encore en application
- un certain nombre de clarifications doivent encore être apportées, notamment par la CNIL
- néanmoins, de par la proximité de la date d'application du règlement, la présentation portera **sur le RGPD** en mentionnant les changements avec la LIL le cas échéant

Plan

- notions et agents de la protection des données en partant de trois notions fondamentales :
  - **données à caractère personnel**
  - **traitement**
  - **finalité**
- mise en œuvre de la réglementation en sciences sociales
  - **interprétation** (et difficultés d'interprétation) des notions dans le contexte spécifique des sciences sociales
  - **mesures** de protection des données

Cette présentation est partiellement issue de notices rédigées **sur la Lil** avec Émilie Masson, juriste au service du CIL du CNRS. Ces notices sont accessibles à cette page :

https://extra.core-cloud.net/collaborations/CIL_Extranet/partage_ESR/GuideSHS/GuideSHS.aspx

Note : l'accès nécessite de s'authentifier via la fédération d'identité de RENATER.

Appréhender la réglementation sur les DCP

Trois écueils :

- faire de la collecte et le l'analyse de **DCP** une question **d'éthique** (personnelle ou professionnelle) ou de **« déontologie »**

  la collecte et le l'analyse de **DCP** une question **juridique**

- ne pas prendre la mesure de la **spécificité** et des **subtilités** du sens donné aux mots par la réglementation (responsable de traitement, anonymisation, pseudonymisation,...)

  - importance de se familiariser avec les notions et leurs **définitions**
  - la réglementation ne fournit qu'**un cadre général**, chaque traitement doit faire l'objet d'**une analyse spécifique**
  - et de garder à l'esprit qu'il s'agit d'une herméneutique de **textes juridiques** : à la fin, c'est la CNIL ou le juge qui a raison

- appréhender la réglementation comme une **construction arbitraire** ou conçue à partir de situations **n'ayant rien à voir** avec les sciences sociales

  - la réglementation est une protection contre des risques **effectifs** pour les personnes et ces risques ont leurs pendants **dans les enquêtes en sciences sociales**
  - de ce point de vue, la réglementation n'est pas seulement **une contrainte** pour les enquêtes en sciences sociales, elle offre aussi **une protection** (elle vous protège en protégeant les personnes)
  - la réglementation vous protège vous aussi en tant que personnes physiques

Appréhender la réglementation sur les DCP

- la réglementation est le produit de **rapports de force** politiques et économiques variables dans le temps qui dépassent largement la seule question des sciences sociales
- la mise en place des réglementations est liée au développement de l'informatique dans l'après-guerre
- dans les années soixante-dix, il s'agissait principalement d'encadrer le traitement de DCP par **les États**
- depuis s'est notamment ajouté la valorisation de DCP par **les entreprises**
- en effet, de nombreuses entreprises ont désormais un *business model* fondé sur **la marchandisation** des DCP et les sommes en jeu sont considérables
- les négociations autour du RGPD ont ainsi généré une intense activité de **lobbying** de la part des GAFAM

Appréhender la réglementation sur les DCP

Pour autant,

- la réglementation n'en est pas contingentée à un contexte précis, du moins dans ses principes
- dès le départ, les réflexions ont visé à établir un cadre **plus général** que les cas concrets qui les ont initiées
- dans certains cas, le caractère général du cadre confère même **au flou** ce qui peut rendre l'analyse juridique difficile (notamment pour certains traitements de DCP en sciences sociales...)
- d'où l'importance des **interprétations** de la CNIL
- la CNIL dispose en effet d'un pouvoir **réglementaire**

Dernières remarques...

...avant de commencer

Chronologie

Chronologie de la réglementation sur les DCP

2018	entrée en application du règlement 2016/679 et fin du délais pour la mise en conformité pour les traitements en cours (25 mai) vote d'une nouvelle loi ?
2016	**règlement 2016/679/UE du Parlement européen et du Conseil 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 (RGPD)** *abroge la directive 95/46/CE* **directive 2016/680/UE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et à la libre circulation de ces données**
2004	traduction dans le droit français de la directive 95/46/CE
1995	**directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**
1981	**convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** *convention du Conseil de l'Europe*
1978	**loi 78-17 relative à l'informatique, aux fichiers et aux libertés (LIL)**

Note : à partir du début des années 70, différents États européens ont commencé à se doter de législations sur les DCP comme le Land de Hesse en 1970 (*Hessisches Datenschutzgesetz*, la première au monde), la Suède (*Datalag*, 1973) ou la RFA (*Bundesdatenschutzgesetz*, 1977)

Autres réglementations

Autres textes traitant de la question des DCP :

2016	**loi** 2016-1321 **pour une République numérique** *succède à la* LCEN et *anticipe le* RGPD
2008	**loi** 2008-696 **du 15 juillet 2008 relative aux archives**
2004	**loi** 2004-575 **pour la confiance dans l'économie numérique** (LCEN)
2002	**directive** 2002/58 **du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques**
1978	**loi** 78-753 **portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal** *création de la Commission d'accès aux documents administratifs* (CADA)
1951	**loi** 51-711 **sur l'obligation, la coordination et le secret en matière de statistiques**

ainsi que : droit à l'image, code du patrimoine,...

Le RGPD

Les changements apportés par le **RGPD** :

- **responsabilité** (*accountability*) : suppression de certaines formalité préalables et inversion de la charge de la preuve
- **protection à la conception** (*privacy by design*) et **sécurité par défaut** (*security by default*) : la protection des données (et pas seulement la sécurité) doit être prise en compte dès la conception du traitement
- réalisation **d'études d'impact** avant la mise en œuvre du traitement pour les traitements « à risque »
- **généralisation du Cil** (délégué à la protection des données)

Anisi que,

- quelques dispositions spécifiques aux traitements à des fins **archivistiques** dans l'intérêt public, à des fins de **recherche scientifique** ou **historique** ou à des fins **statistiques**

Le RGPD

Néanmoins, toutes les implications concrètes de l'application du RGPD ne peuvent pas encore être décrites :

- l'entrée en vigueur du RGPD ouvre une intense période **d'interprétation** pour les autorités nationales de protection des données comme la CIL mais aussi au niveau européen (G29, futur *European Data Protection Board*)
- mais aussi un travail législatif important (cf. projet de nouvelle loi)
- et cela d'autant plus que le texte comporte **57 mentions ou renvois** au droit des États membres

Notions

Notions fondamentales

données à caractère personnel
traitement
finalité
données sensibles
consentement

proportionnalité et de pertinence
licéité, loyauté et transparence
information des personnes
collecte indirecte
conservation et réutilisation

Trois notions fondamentales

Les trois notions fondamentales pour circonscrire le champ d'application de la LIL et du RGPD sont :

- **données à caractère personnel**
- **traitement**
- **finalité**

Pour les personnes physiques **résidant** ou lorsque le responsable de traitement est **établi** sur **le territoire de l'UE**,

la réglementation s'applique à tout **traitement** (informatique ou autre) dont la **finalité** nécessite le recueil d'informations permettant **d'identifier directement ou indirectement** les personnes physiques sur lesquelles ces informations ont été collectées

La loi impose de plus que :

- la finalité soit **déterminée**, **explicite** et **légitime**
- les données collectées soient **proportionnées** et **pertinentes** au regard de la finalité du traitement
- les données soient collectées et traitées de manière **licite**, **loyale** et **transparente**

Données à caractère personnel

Définition : toute information se rapportant à une personne physique identifiée ou identifiable (RGPD art. 4 § 1)

- il s'agit de toute donnée permettant d'identifier une **personne physique** :

  « identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (*ibid.*)

Deux cas de figure :

- **données directement identifiantes :** données nominatives permettant l'identification directe d'une personne comme le nom, l'adresse (postale, électronique,...), téléphone, numéro de bureau,...
- **données indirectement identifiantes :** données permettant d'identifier une personne de manière indirecte, notamment par croisement

Note : si le traitement ne nécessite pas de données identifiantes, le RGPD ne **s'applique pas** (RGPD art. 11 § 1)

Données indirectement identifiantes

Le RGPD porte sur les informations permettant **identifier** une personne et pas seulement la nommer :

- l'application de la réglementation ne se réduit donc pas à la seule question de **« l'anonymat »** *stricto sensu*
- l'expérience ainsi que des travaux en informatique montrent en effet que l'absence ou la suppression de données directement identifiantes (ou leur absence à la collecte) n'est **pas en soi suffisante** pour prévénir toute (ré-)identification
- en pratique, le recoupement d'informations **anodines** (même en nombre limité) peut souvent concourir à l'identification de personnes physiques
- ainsi, **la pseudonymisation** (p. ex. de citations d'entretiens) n'est pas toujours suffisante pour empêcher la ré-identification des personnes

Traitement

Définition : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel (RGPD art. 4 § 2)

- définition **très large**
- recouvre quasiment tout ce qui peut être réalisé dans le cadre **d'enquêtes de terrain** tant du point de vue de la collecte (questionnaires, *data mining* sous toutes ses formes, entretiens, observations, etc.) que de l'analyse
- mais aussi des activités relevant du **fonctionnement des équipes de recherche** comme l'organisation d'événements scientifiques

  Note : dans ce cas, il existe **une norme simplifiée**

De plus,

- pas de distinction entre **collecte**, **analyse** ou encore **publication** : toutes ces opérations font parties du traitement
- le fait que les DCP collectées ne soient **pas utilisées** du tout ou seulement dans une phase du traitement comme l'analyse ne change rien
- pas plus que le **nombre** de personnes identifiables

La finalité

Définition : ?

- la notion de finalité ne semble pas avoir de définition explicite
- pour les sciences sociales, la finalité correspond à la **problématique** de la recherche
- à ne pas confondre avec la **thématique** de la recherche

La notion est toutefois caractérisée dans les textes. La finalité se doit en effet d'être (RGPD art. 5 § 1 (a)) :

- **déterminée** : la finalité du traitement doit avoir été clairement définie avant la collecte
- **explicite**
- **légitime** : la finalité du traitement doit être liée à l'activité du responsable de traitement (p. ex. : réaliser des enquêtes quand on est membre d'une UMR de sociologie)

La finalité

De plus,

- les données ne peuvent être traitées **que pour la réalisation** de la finalité pour laquelle elles ont été collectées
  - le détournement de finalité constitue une **infraction pénale** (art. 226 § 21 (c) du code pénal)
  - la finalité peut néanmoins être **redéfinie** en cours de traitement sous conditions
- **exceptions :** les traitements à fins de recherche et à fins de statistique (cf. *infra*)

La finalité

La notion de finalité est la **pierre angulaire** du **RGPD** :

- le plus important n'est souvent pas tant *en soi* quels types de données sont collectés mais **l'utilisation** qui en sera faite (et à quelle fin)
- la finalité peut **complètement changer** l'analyse juridique d'un même type de données
- **exemple :** l'enregistrement de la voix
  - si l'enregistrement sert à identifier une personne physique, il devient **une données sensible** et, qui plus est, **une données biométrique** avec toutes les contraintes que cela implique
  - mais pas s'il sert à un entretien en vue de sa transcription (pas dispositions spécifiques supplémentaires)

Note : en France, la CNIL considère que l'enregistrement de la voix est une données biométrique, **quelle que soit son utilisation**

- **exception** : **les données sensibles** qui constituent des catégories spécifiques quelle que soit la finalité de leur utilisation

Les données sensibles

Le RGPD distingue des catégories particulières de DCP : **les données sensibles**

En effet, les traitements de DCP qui révèlent :

- **l'origine raciale ou ethnique** (« étant entendu que l'utilisation de l'expression " origine raciale " dans le présent règlement n'implique que l'Union adhère à des théories tendant à établir l'existence de races humaines distinctes » (c51))
- **les opinions politiques**, les convictions **religieuses** ou **philosophiques** ou **l'appartenance syndicale**

ainsi que le traitement :

- des données **génétiques**, des données **biométriques** aux fins d'**identifier** une personne physique de manière unique, des données concernant **la santé**
- des données concernant la **vie sexuelle** ou l'**orientation sexuelle** d'une personne physique

sont **interdits** (RGPD art. 9 § 1) .

À cela s'ajoute le traitement des données à caractère personnel relatives (RGPD art. 10) :

- aux **condamnations pénales** et aux **infractions**
- aux **mesures de sûreté connexes** (mise en détention, peines de prison,...)

Dérogations à l'interdiction de collecte des données sensibles

Cette interdiction peut néanmoins faire l'objet **d'exceptions** (RGPD art. 9 § 2), sauf pour les deux derniers cas :

- la personne concernée a donné son **consentement** explicite au traitement (sauf si le droit national ou de l'UE en vigueur prévoit une interdiction qui ne peut pas être levée)
- le traitement porte sur des données à caractère personnel qui sont manifestement **rendues publiques** par la personne concernée

  Note : cette exception doit être interprétée de façon restrictive, cf. p. ex. l'avis 5/2009 du 12/6/2009 du G29 sur les réseaux sociaux en ligne

- le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de **recherche scientifique ou historique** ou à des fins **statistiques** mais sur le **fondement du droit** de l'UE ou des États membres (c10,c52) entre autres conditions comme la **proportionnalité** à la finalité

Et lorsque : l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée ; la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale ; (. . .)

Consentement de la personne concernée

Définition : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement (RGPD art. 4 § 11)

- **« manifestation » :** pas de consentement tacite, le responsable de traitement doit pouvoir **démontrer** que la personne a donné son consentement (RGPD art. 7 § 1)

  exemple : le fait qu'une personne ait répondu à un entretien ou à un questionnaire ne suffit pas pour attester du consentement (c32) (c42)

- le consentement doit en effet être éclairé : le responsable de traitement doit pouvoir attester qu'un certain nombre **d'informations** ont été fournies à la personne comme la finalité du traitement, identité du responsable de traitement,... (cf. information des personnes)
- avec le RGPD, le consentement doit être **distinct** des autres questions (p. ex. CGU)

Consentement de la personne concernée

De plus,

- il ne peut y avoir de **consentement global**, la personne doit consentir explicitement à chaque traitement s'il y a plusieurs (c32)
- la personne concernée peut **retirer** sont consentement **à tout moment**

  toutefois, le retrait du consentement « ne compromet pas la licéité du traitement avant retrait » (RGPD art. 7 § 3)

- **exemples :** formulaire de consentement (bloquant) avant le questionnaire, entretien

Note : les traitement concernant **les enfants** font l'objet de dispositions spécifiques (RGPD art. 8) qui requièrent notamment le consentement du tuteur légal

Principes de proportionnalité et de pertinence

RGPD art. 5 § 1 (c) : Les données à caractère personnel doivent être [. . .] adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)

- seules les données **directement en lien** et **strictement nécessaires** à la réalisation finalité du traitement peuvent être recueillies
- le type de données à caractère personnel qui va être collecté doit donc être **motivé** et justifié au regard des objectifs poursuivis

Ces deux principes sont généralement interprétés d'une façon très **restrictive** :

- on parle alors de **minimisation** des données
- en pratique, c'est un des aspects les plus **délicats** de l'application de la réglementation aux sciences sociales

Licéité, loyauté et transparence de la collecte des traitements

RGPD art. 5 § 1 (a) : Les données à caractère personnel doivent être [. . .] traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)

- conditions de **licéité** du traitement (RGPD art. 6) :
  - le traitement est nécessaire à l'exécution d'**une mission d'intérêt public**, comme la recherche

    Note : il s'agit d'une condition nécessaire mais **non suffisante**
  - **autres conditions :** consentement, exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux de la personne, . . .
- **loyauté et la transparence** : la personne concernée doit être informée de l'existence du traitement et de ses finalités (c60) ainsi que de ces droits

Information des personnes

La loyauté et la transparence du traitement implique notamment **l'information des personnes** (c39) :

- Le responsable de traitement doit donc fournir **différentes informations** aux personnes concernées (**RGPD art. 13 § 1**) :
  - l'identité du responsable de traitement, des destinataires de données
  - la finalité du traitement
  - la durée de conservation
  - la liste de ses droits (cf. droits des personnes)
- il peut être envisageable **de ne pas décrire précisément** la recherche dans le cas de traitements des données à caractère personnel à des fins de recherche scientifique (c33)

Droit des personnes

Les personnes concernées ont un droit :

- **d'accès** (RGPD art. 15)
- **de rectification** (RGPD art. 16)
- **d'effacement** (RGPD art. 17)
- **de limitation** (RGPD art. 18)
- **d'opposition** (RGPD art. 21)
- introduire **une réclamation** auprès d'une autorité de contrôle
- ainsi que la notification en cas de modification (RGPD art. 19) et le droit à la portabilité des données (RGPD art. 20)

Notes :

- en cas de traitements à des fins de recherche scientifique ou historique ou à des fins statistiques, **l'UE ou les États** peuvent peuvent prévoir **des dérogations** aux droits d'accès (art. 15), de rectification (art. 16), à la limitation du traitement (art. 18), de de modification (art. 19), de portabilité (art. 20) et au droit d'opposition (art. 21) (RGPD art. 89 § 2)
- le droit à l'effacement ne s'applique pas si la mesure est susceptible de compromettre gravement la réalisation des finalités (RGPD art. 17)

Collectes indirectes

La collecte n'est pas toujours réalisée **directement** auprès de la personne :

- **exemples :** fouille (archives, internet, base de données,...), entretiens,...

Note : tout ce que est en **libre accès** n'est pas nécessairement **libre de droits** :

- CGU, licences, droit des base de données,...

Dans ce cas,

- le responsable de traitement est là aussi soumis à une obligations **d'information** des personnes (RGPD **art. 14 § 1**)
- de plus, les informations doivent être fournies dans **un délai raisonnable** après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois RGPD **art. 14 § 3 (a)**

Collectes indirectes

Néanmoins, ces obligations ne s'appliquent pas dans les cas suivants (RGPD art. 14 § 5) :

- information impossible ou exigeant des efforts **disproportionnés**
- en particulier pour les traitements à des fins **archivistiques dans l'intérêt public**, à des fins de **recherche scientifique ou historique** ou à des fins **statistiques**
- si l'information des personnes est susceptible de **compromettre gravement** la réalisation de la finalité du traitement
- dans ces cas de figure, le responsable de traitement doit prendre **les mesures appropriées** pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée
- lorsque l'information des personnes est impraticable, la CNIL recommande de fournir **une information générale**, par exemple sous forme de mention sur le site

Note : ceci ne constitue pas un blanc-seing, il faut bien évidemment motiver l'application de ces exceptions

La conservation et la réutilisation des DCP

Rappel : les données ne doivent être collectées que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités **(limitation des finalités)**

De façon corrélative,

RGPD art. 5 § 1 (e) **:** la conservation est limitée à la durée nécessaire à la réalisation des finalités du traitement

- à l'issue de cette période le responsable de traitement doit, soit **détruire** l'ensemble des données, soit les rendre complément **anonymes**

  Notes :

  - la destruction doit être être **autorisée** par les archives nationales ou départementales
  - attention aux données **indirectement identifiantes** qui peuvent se révéler très difficiles à anonymiser

- la conservation **au-delà** de cette durée est néanmoins possible pour les fins de recherches scientifiques et historiques ou à des fins statistiques (RGPD art. 5 § 1 (e))
- pour autant que **les mesures techniques et organisationnelles** appropriées soient prises pour respecter le principe de minimisation des données
- la conservation est toutefois **distincte** de la réutilisation

La réutilisation des DCP à des fins scientifiques

La LIL prévoit qu'il peut être procédé à des traitements poursuivant une autre finalité :

- si la personne y a **consenti**
- après **autorisation** de la CNIL

Le **RGPD** prévoit que :

- un traitement ultérieur à des fins historiques, statistiques ou scientifiques **« n'est pas réputé incompatible »** (RGPD art. 5 § 1 (b))
- pour autant que, là aussi, **les mesures techniques et organisationnelles** appropriées soient prises pour respecter le principe de minimisation des données

  > le responsable de traitement doit ainsi évaluer s'il est possible d'atteindre ces finalités grâce à un traitement de données qui ne permettent pas ou plus d'identifier les personnes concernées (c156))

- et si et seulement si le traitement sert **uniquement** une finalité de recherche (RGPD art. 89 § 4)
- pour autant, les personnes concernées ont toujours **des droits**

Les agents de la protection des données

responsable de traitement
formalités
responsabilisation
protection des données dès la conception

sous-traitant
Commission nationale informatique et libertés
sanctions
Correspondant informatique et libertés

Le responsable de traitement

Définition : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (RGPD art. 4 § 7)

- le responsable de traitement n'est pas nécessairement une personne physique
- 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 RGPD (RGPD art. 24 § 1)
- le responsable de traitement est **responsable pénalement**

Le responsable de traitement dans l'ESR

Dans le cadre de l'ESR, le responsable de traitement d'un traitement n'est (généralement) **pas** le ou les **(enseignants-)chercheurs** :

- en pratique, les responsables de traitement peuvent varier selon les activités
- **enseignements :** chef d'établissement (p. ex. le président de l'université)
- **recherche :** le directeur de l'entité dont dépend le chercheur (UMR)

Si **plusieurs responsables de traitement** déterminent conjointement les finalités et les moyens du traitement (p. ex. dans le cas d'un projet de recherche associant plusieurs entités) :

- ils sont les responsables **conjoints** du traitement (RGPD **art. 26 § 1**)
- les responsables conjoints du traitement définissent de manière transparente **leurs obligations respectives** (*ibid*)
- par une convention de recherche

Note : le fait que le responsable de traitement soit responsable pénalement ne signifie pas que la responsabilité des différentes catégories de personnels ne puisse pas être engagée à un titre ou un autre

Formalités préalables

Parmi les obligations du responsable de traitement, la LIL impose que :

- si le traitement comporte des **DCP**, il doit faire l'objet de **formalités** (déclarations, autorisations) **avant** la la mise en œuvre du traitement
- les formalités doivent être réalisées auprès de la CNIL ou d'un CIL pour une large partie d'entre elles

Le **RGPD** **supprime (partiellement) cette obligation** :

- le **RGPD** considère en effet que :

  « cette obligation [générale de notifier les traitements de données à caractère personnel aux autorités de contrôle] génère une charge administrative et financière, **sans pour autant avoir** systématiquement **contribué à améliorer la protection des données à caractère personnel** » (c89)

- cependant, toutes les formalités préalables **ne seront pas amenées à disparaître** (p. ex. pour les données relatives aux infractions et aux mesures de sûreté)
- en partie laissé à l'appréciation des États

La responsabilisation

- la contrepartie de la suppression des formalités préalables est **l'inversion de la charge de la preuve** :

  désormais, il incombera donc au **responsable de traitement** de démontrer qu'il est en conformité avec le règlement (RGPD art. 24 § 1)

- le responsable de traitement doit tenir **un registre** actualisé de traitement des données (RGPD art. 30 § 1)

  ce registre comporte les informations suivantes : nom et les coordonnées du ou des responsables du traitement, les finalités, description des catégories de personnes concernées et des catégories de données à caractère personnel, catégories de destinataires, délais de conservation, description des mesures de sécurité

- ce registre peut être tenu par son représentant, **le Cil**

Protection des données dès la conception et par défaut

Parmi les nouvelles obligations du responsable de traitement figurent aussi :

- **la protection des données dès la conception (RGPD art. 25 § 1) :** le responsable de traitement doit mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles **dès la conception** du traitement
- **la protection des données par défaut (RGPD art. 25 § 2) :**
  - cf. finalité : le responsable de traitement doit mettre en œuvre toutes les mesures pour que seules les données **strictement nécessaires** à la réalisation de la finalité soient traitées **par défaut**, -ie : sans intervention de la personne concernée
  - ces mesures doivent garantir que seules **les personnes habilitées** accèdent aux données

Note : au delà des obligations réglementaires, l'expérience montre que la mise en conformité en cours de route est souvent impraticable (ex : collecte directe de données sensibles sans demande du consentement)

Analyse d'impact relative à la protection des données

RGPD art. 35 § 1 : lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies [...] 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

- disposition introduite par le RGPD
- requise « particulièrement » pour le traitements de **données sensibles** (RGPD art. 35 § 3 (b)), les traitements « à grande échelle » (p. ex. sur les réseaux sociaux), ou le traitements de données se rapportant à des condamnations ou des infractions
- **des listes** rendant obligatoire ou dispensant de l'analyse doivent être être dressées par les autorités de contrôle (RGPD art. 35 § 4 et art. 35 § 5)
- si l'analyse révèle un risque particulièrement élevé, l'autorité de contrôle doit être **consultée**
- la Cnil et le G29 ont publié des guides pour réaliser ce type d'études

Le sous-traitant

Définition : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (RGPD art. 4 § 8)

- définition très large : entreprise à qui la réalisation d'une enquête est sous-traitée mais aussi vacations pour des transcriptions d'entretiens

RGPD art. 28 :

- le prestataire doit présenter des garanties suffisantes
- le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique de l'UE
- autorisation de la CNIL si le sous-traitant est établie en dehors de l'UE
- le RGPD s'applique même si le sous-traitant n'est pas établi sur le territoire de l'UE
- formalités ?

Les obligations du sous-traitant

Le contrat de sous-traitance devra contenir un certain nombre de dispositions impératives :

- le sous-traitant ne traite des données personnelles que sur instruction documentée du responsable de traitement
- les données ne doivent être traitées que pour la réalisation de la finalité
- le sous-traitant doit prendre toutes les mesures appropriées pour assurer la confidentialité et la sécurité des données

  Note : les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal)

- les données doivent être détruites ou remise une fois la finalité réalisée (sans conservation de copies)
- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits
- ces obligations doivent se répercuter à ses sous-traitants (*ad lib*)

Champ d'application territorial

Le **RGPD** s'applique si (RGPD art. 3) :

- le responsable de traitement -ou son sous-traitant- **est établi** sur le territoire de l'**UE** (même si les personnes concernées n'y résident pas)
- les personnes concernées **résident** sur le territoire de l'**UE** (même si le responsable de traitement -ou son sous-traitant- n'y est pas établi)

Note : le second cas n'était pas prévu dans la LIL et vise clairement les GAFAM *et. al.*

La Commission nationale informatique et libertés (Cnil)

La Cnil est une **autorité administrative indépendante** crée par la loi de 1978 :

- elle est composée de **18 membres** élus ou nommés principalement issus de différentes instances publiques (Parlement, hautes juridictions de l'État,...) qui sont assistés par près de 200 agents
- la commission dispose d'un pouvoir de **contrôle** et de **sanction** (renforcé par le **RGPD**) mais aussi des missions d'**avis**, de **conseil** et **labellisation**
- elle dispose de plus d'un pouvoir **réglementaire** : la Cnil édicte des normes (normes simplifiées, autorisations uniques, actes réglementaires uniques et méthodologies de référence,...)

Au niveau de l'Union,

- la Cnil est membre du **G29** (Groupe de travail de l'article 29 de la directive 95/46/CE) qui est un organe consultatif de l'UE composé des différentes autorités de protection des données des membres de l'Union
- le **G29** publie régulièrement des avis ainsi que des lignes directrices sur des points précis de l'application de la réglementation

Sanctions

Les infractions à la LIL sont des infractions **pénales** :

- jusqu'à 300 000 d'amendes
- jusqu'à 5 ans d'emprisonnement

Note : personne n'est jamais allé en prison sur le fondement de la LIL

Le **RGPD** augmente considérablement le niveau des sanctions financières encourues en cas d'infraction (RGPD art. 83 § 1) :

- jusqu'à **20 millions d'euros**
- ou **4 % du chiffre d'affaires** annuel mondial
- le plus élevé de ces deux montants est retenu

Le correspondant informatique et libertés (Cil) (futur DPO)

- le CIL a été crée par la modification de 2004 de la LIL en application de la directive européen de 1995 pour prendre en charge une partie des formalités préalables
- le CIL sera remplacé par le **délégué à la protection des données** (**DPO**) à l'entrée en vigueur du **RGPD**
- les fonctions du **DPO** (RGPD art. 39) :
  - **informer** et **conseiller** le responsable de traitement
  - **contrôler** le respect du règlement
  - **coopérer** avec l'autorité de contrôle et faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement

    Note : le **DPO** n'en est pas pour autant une émanation de la CNIL
- le **DPO**, représentant du responsable de traitement, tient à jour **un registre des traitements** (RGPD art. 30 § 1)

  cf. **responsabilisation** et **inversion de la charge de la preuve**

La désignation du DPO

La désignation du **DPO** est obligatoire dans les cas suivant (**RGPD art. 37 § 1**) :

- le traitement est effectué par une **autorité publique** ou **un organisme public** (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle)
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui [...] exigent **un suivi régulier et systématique** à grande échelle des personnes concernées
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de **données sensibles**

Pour **les UMR CNRS-université**, la désignation du CIL doit se faire en fonction de **l'employeur** du **DU** (cf. courrier du 4 septembre dernier de la **CPU** et du **CNRS**) :

- si le **DU** est personnel université, il faut désigner le CIL de l'université
- si le **DU** est personnel **CNRS**, il faut désigner le CIL du **CNRS**

Note : pour les **DU** non-**CNRS**, si le CIL de l'employeur ne peut exercer cette mission, le CIL du **CNRS** peut être nommé à sa place

Le Cil dans vos projets de recherche

Le CIL dans vos projets de recherche :

- l'application de la réglementation peut impacter **ce que vous pouvez collecter** et **la façon** dont vous pouvez le collecter et le traiter
- le **RGPD** renforce de plus considérablement les obligations du responsable de traitement
- l'association de votre CIL à vos projet de recherche est plus que jamais **cruciale**
- et ce, dès **la conception du projet** (*DPO by default*)

Les Cil de vos établissements de tutelle :

- pour l'**UdS** : M^me^ Sarah Piquette-Muramatsu (**spiquette@unistra.fr**)
- pour le **CNRS** : le service du CIL du **CNRS** (**site**)
- **IEP** ?

La mise en œuvre de la réglementation dans les traitements en sciences sociales

La mise en œuvre de la réglementation en sciences sociales

la première mesure à adopter est d'associer
votre CIL **dès la conception de votre enquête**

Pour le reste,

- **tout va dépendre** des données collectées, de leur mode de collecte, de l'utilisation qui en sera faite et des risques que cela fera courir aux personnes sur lesquelles ces données ont été collectées
- de par la diversité des modes de collecte, des populations enquêtées des problématiques de recherche et des risques attenants, il est en pratique difficile de dresser la liste des possibilités et, surtout, de leur combinaison, **du moins en sciences sociales**

La mise en œuvre de la réglementation en sciences sociales

- difficile d'énumérer *a priori* tous les recherches possibles à la différence des traitements de **DCP** dans d'autres contextes
- ce type d'exercice est en effet possible lorsque le nombre de traitements envisageable est **fini** (ex : **le guide** des CIL universitaires)
- difficulté de présenter des **cas pratiques** : problème de l'anonymisation, surtout par rapport aux informations indirectement identifiantes
- en sciences sociales, les choses doivent donc être évaluées **au cas par cas**

  cela dit, dans les traitement en sciences sociales, obtenir **le consentement** est généralement la solution dans les cas collecte de données sensibles auprès des individus, de même que le recours systématique au **chiffrement** des ressources

- cette partie vise plutôt à expliciter certaines des notions vues précédemment : finalité et minimisation

Finalité et minimisation

Rappel

Pour les personnes physiques **résidant** ou lorsque le responsable de traitement est **établi** sur **le territoire de l'UE**,

la réglementation s'applique à tout **traitement** (informatique ou autre) dont la **finalité** nécessite le recueil d'informations permettant **d'identifier directement ou indirectement** les personnes physiques sur lesquelles ces informations ont été collectées

La loi impose de plus que :

- la finalité soit **déterminée**, **explicite** et **légitime**
- les données collectées soient **proportionnées** et **pertinentes** au regard de la finalité du traitement
- les données soient collectées et traitées de manière **licite**, **loyale** et **transparente**

Fins statistiques et fins de recherche scientifique ou historique

Pour les traitement à fins statistiques et fins de recherche scientifique ou historique :

- l'information des personnes peut éventuellement **ne pas être complète** lors de collectes directes
- l'obligation d'information peut même être éventuellement partiellement **allégée** dans le cas de collectes indirectes
- **des données sensibles** peuvent être collectées moyennant, p. ex., le consentement
- les données collectées peuvent être **archivées**
- les données peuvent être **réutilisée** et ce, même si elles n'ont pas été collectées pour une finalité scientifique
  - pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le règlement afin de garantir les droits et libertés de la personne concernée
  - et que les personnes en soit informées

Toutefois,

ces dispositions doivent pour partie encore faire l'objet de clarifications

La finalité du traitement en sciences sociales

La finalité du traitement correspond à la **problématique** du traitement :

- en tant que finalité, la problématique doit donc être **déterminée** et **explicite** (entre autres)
- en pratique, il faut d'abord être en mesure de répondre aux questions suivantes avant le début de la collecte :
  - qui
  - où
  - pourquoi
  - quoi
  - quand
- c-à-d auprès de qui, dans quel contexte et pour quelles raisons quelles DCP vont être collectées

Détermination de la finalité

Ce faisant,

- tout traitement doit d'abord être **problématisé**
- la collecte ne peut pas être une finalité en soi (enquêtes exploratoires ou prosopographiques)

Cepdendant,

- on ne définit souvent une **thématique de recherche** plutôt qu'une problématique pour collecter des données
- la collecte de données et donc de DCP est souvent un **préalable nécessaire** à l'élaboration de la problématique
- démarches inductives (archives, *web mining*, ...)
- la finalité ne peut pas toujours être aussi précisément déterminée que le requière le règlement
- à ce titre, on peut noter que le (c33) fait état de ce que

  > « souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données »

  c'est pourquoi, dans certains cas, l'information des personnes peut ne pas être complète (cf. *supra*)

La minimisation des données

Avoir de (bonnes) raisons (clairement définies) de collecter des données ne suffit pas :

- la collecte est soumise au principe de **minimisation** des données
- la collecte doit être aussi **parcimonieuse** que possible : il faut s'efforcer de collecter le moins de données possible (y compris dans la recherche)

En pratique,

- comme vu précédemment, la finalité n'est pas toujours facile à établir précisément au préalable et donc ce qui est strictement nécessaire à la finalité
- la collecte peut impliquer de collecter plus de $\mathbf{DCP}$ que nécessaire par construction (entretiens semi-directifs)
- de plus, en sciences sociales, l'application du principe de minimisation peut se traduire par un une sorte de **cloisonnement thématique**

La minimisation des données

Exemple (tiré d'un cas concret) : enquêtes par questionnaire sur **les déplacements**

- l'application stricte du principe de minimisation impliquerait de ne collecter des renseignements **exclusivement sur les déplacements** (fréquence, modes de transports,...)
- néanmoins, on peut ici **arguer** que, p. ex., les caractéristiques du ménage (sa composition, ses revenus,...) ont un effet sur les déplacements pour établir la proportionnalité et la pertinence de la collecte d'information sur le ménage et les individus qui le compose relativement à la finalité

La minimisation des données

Exemple (plus délicat) : la religion

- là aussi, l'application stricte du principe de minimisation impliquerait que l'on ne puisse poser des questions relatives aux pratiques religieuses des individus que dans le cadre d'enquêtes sur les pratiques religieuses
- or, d'un point de vue sociologique, la religion apparaît comme un **fait social total** et touche donc à de nombreux autres domaines comme la fécondité, l'éducation, les consommations, la participation politique et associative...
- ainsi, l'étude de la religion implique souvent de s'intéresser à **d'autres pratiques** et, réciproquement, l'études de certaines pratiques nécessite parfois l'intégration de **la dimension religieuse**

La minimisation des données

Problèmes :

- tout ce qui a trait à la religion est considéré comme une **donnée sensible**
- encore mieux (ou pire) : la réalisation de la finalité nécessite de croiser pratiques religieuses et pratiques politiques (**autre donnée sensible**)

Toutefois,

- dans ce cas particulier, on ne peut que se féliciter de ce que **G. Michelat et M. Simon** aient réalisé leurs enquêtes AVANT le vote de la LIL et permettent d'étayer la proportionnalité et la pertinence de la collecte et du traitement de données liant pratiques politiques et religieuses
- préparez-vous néanmoins à devoir batailler...

Fazit

La finalité des traitements (et surtout leur indétermination) peut **parfois** causer des difficultés dans les démarches relatives aux **DCP** :

- il ne s'agit cependant pas du point le plus problématique
- sous condition que vos interlocuteurs aient une **familiarité suffisante** avec les enquêtes en sciences sociales

Mais, en règle générale,

la proportionnalité et la pertinence de la collecte constituent un des principaux points d'achoppement dans l'application de la réglementation relative aux DCP en sciences sociales

et ce, particulièrement lorsque la finalité implique la collecte et, *a fortiori*, le croisement **de données sensibles**

Note : il est important de souligner que ce n'est pas toujours le cas et que la proportionnalité et la pertinence des traitements peuvent être établis dans de très nombreuses situations

Les obstacles à l'analyse juridique

L'analyse juridique des traitements (comme l'appréciation de la proportionnalité) s'appuit notamment sur **les délibérations** de la CNIL

- ces délibérations peuvent être de nature différentes (normes, avis, autorisations, avertissements, sanctions,...)
- mais, quelque soit le type de délibération considéré, les sciences sociales y brillent avant tout par **leur absence**

D'autre part,

- le peu d'intérêt pour la question des **DCP** dans les traitements en sciences sociales ne facilitent pas l'analyse non plus
- les « incidents » ne font pas l'objet de publicité ni de retours réflexifs sur **ce que fait l'enquête aux enquêtés**
- en l'absence d'informations disponibles, les risques effectifs ne sont pas toujours aisés à évaluer, ce qui peut conduire à des postures **très défensives** et parfois trop contraignantes

Les requérants auprès de la Cnil

Les requérants auprès de la Cnil

Globalement,

- une part conséquente des délibérations porte sur des traitements réalisés par **des entreprises**
- mais aussi des traitements dans **le public** (État, administrations, collectivités,. . .)
- les recherches (publiques ou privées) sur **la santé** occupent une place très importante
- parmi les traitements d'organismes publics, on trouve notamment **la statistique publique** (et apparentés) :
  - les Services statistiques ministériels (SSM) : Insee, Drees, Dares,. . .
  - ainsi que l'Ined, le Céreq,. . .

  Note : les enquêtes de la statistique publique passent par un circuit différent et ne nécessite que rarement une délibération de la Cnil
- et quatre délibérations concernant les traitements de **deux UMR** (dont une de science politique)

Interpretatio cessat in claris

- les traitements en sciences sociales apparaissent donc très **peu représentés** dans les délibérations de la CNIL
- or, le **RGPD** ne procure qu'**un cadre général**
- son application n'est possible qu'en référence **aux interprétations** des instances habilitées à le faire comme la CNIL ou le **G29**
- dans les faits, l'application de la réglementation aux traitements de sciences sociales est donc fondée sur des cas souvent **très éloignés** des traitements en sciences sociales
- ce qui complique la prise en compte des spécificités des finalités des traitements en sciences sociales, notamment dans **l'évaluation de la proportionnalité et de pertinence** des données collectées

Caractériser la finalité des traitement en sciences sociales

- les finalités en sciences sociales diffèrent des finalités des entreprises, administrations, associations,. . .
- les sciences sociales n'ont pas directement à faire à des administrés, des assurés sociaux, des usagers, des employés, des clients,. . . mais bien à **des enquêtés**
- généralement, les traitements n'utilisent pas les DCP collectées pour prendre **une décision** sur ces personnes
- les traitements en sciences sociales ne visent souvent des personnes physiques que pour mieux s'en abstraire et produire au final des discours **de portée générale** non contingentés à un échantillon ou un autre
- ce qui ne veut pas dire que les traitements sont nécessairement **sans conséquences** sur les enquêtés, notamment pour ce qui est de la **confidentialité** des données
- nécessité de prendre les mesures adéquates

La protection des personnes

Sécurité des données à caractère personnel

Importance de **la sécurisation** des données collectées, particulièrement lors de la collecte **de données sensibles**

Exemples de mesures prescrites par le RGPD (cf. responsabilité du responsable de traitement) :

- **minimisation**, **anonymisation**
- **la pseudonymisation** et **le chiffrement** des données à caractère personnel (RGPD **art. 32 § 1 (a)**)
- des moyens permettant de garantir **la confidentialité**, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (RGPD **art. 32 § 1 (b)**)
- une procédure visant à tester, **à analyser et à évaluer** régulièrement **l'efficacité** des mesures techniques et organisationnelles pour assurer la sécurité du traitement (RGPD **art. 32 § 1 (d)**)
- **notification**, dans les 72h, des incidents de sécurité (« violation de DCP ») à l'autorité de contrôle ainsi qu'aux personnes concernées (RGPD **art. 33** et **art. 34**)

La pseudonymisation

La pseudonymisation des DCP (RGPD art. 4 § 5) :

- traitement de données à caractère personnel de telle façon que celles-ci **ne puissent plus être attribuées** à une personne concernée précise **sans avoir recours à des informations supplémentaires**
- pour autant que ces informations supplémentaires soient **conservées séparément**
- et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable

La sécurisation en pratique

Sujet très vaste, les mesures à prendre dépendent du type de données , de leur mode de collecte, du contexte de leur utilisation, des risques,. . .

- *a minima*, recourir au **chiffrement** systématique des ressources
- chiffrement **des périphériques** de stockage (chiffrement par blocs) :
  - partitions, `DD` externe, clefs `USB`,. . .
  - soit en utilisant des logiciels proposés par les systèmes d'exploitation : `dm-crypt` sous Linux, `Bitlocker` sous Windows ou `FileVault` sous Mac OS X
  - soit en utilisant des logiciels portables comme `VeraCrypt` (*fork* de `TrueCrypt`)
- chiffrement des **transferts** de données (chiffrement asymétrique) : `GnuGPG`

Note : la meilleure sécurité est évidemment de ne disposer d'aucune **DCP** ou de s'en débarrasser (moins de **DCP**, moins de contraintes)

La sécurisation en pratique

Sécurité au niveau applicatif :

- chiffrement **des connexions** (p. ex. à des serveurs `http`, `ftp`, de données,...) : `TLS`, `VPN`,...
- certaines données ne devraient être accessible que depuis **un réseau local**, voire **pas accessibles du tout**...
- pseudonymisation des données des base de données :
  - pseudonymisation des clefs primaires et secondaires si elles contiennent des **DCP**
  - stockages séparés des **DCP**

    Exemple : gestion des invitations à un questionnaire en ligne distincte de la gestion des réponses
  - cf. l'avis `0829/14` du **G29** du 04/05/2014 sur les Techniques d'anonymisation
- et aussi renoncer **aux services « gratuits »** pour y substituer les services recommandés par vos institutions

La pseudonymisation

- ne pas **confondre anomymisation** et **pseudonymisation** :
  - l'anonymisation est **irréversible**
  - la pseudonymisation permet **la réidentification** en utilisant des informations dont l'accès est restreint
- ne pas confondre anonymisation **des données** et pseudonymisation (ou anonymisation) des citations et des situations dans une **publication** :
  - la collecte comme l'analyse et la publication font parties du traitement
  - à partir du moment où vous avez collecté des DCP, que vous les traitiez ou non, le règlement s'applique
- ne pas confondre pseudonymisation au sens du RGPD et pseudonymisation telle que généralement pratiquée dans **les publications**

La « pseudonymisation » des publications

- les publications contiennent souvent des DCP, qu'elles soient **directement identifiantes** (nominative) ou **indirectement identifiantes** (« pseudonymisées »)
- la pseudonymisation telle qu'elle est mise en œubre ne garantit pas nécessairement **la non-réidentification des personnes**
- ces pratiques ne correspondent d'ailleurs généralement pas à **la définition** qu'en donne le RGPD
- les pseudonymes choisis contiennent souvent plus ou moins explicitement (et de façon plus ou moins équivoque) **des informations** sur le sexe, l'âge, l'origine sociale ou géographique,... et ceci, **à dessin**
- alors que le RGPD prévoit que la réidentification à partir d'un pseudonyme ne soit possible qu'à partir **d'informations supplémentaires** conservées à part
- or, les pseudonymes ainsi que le texte des publications contiennent fréquemment des informations qui, **par recoupement**, peuvent permettre d'identifier les personnes

Conclusion

Conclusion

- la règlementation **encadre** la collecte de DCP et **parfois** la limite
- l'application de la règlementation peut **impacter** ce que vous pouver collecter et la façon dont vous pouvez le traiter
  - implications **pratiques** et même **épistémologiques** (parcimonie, rapport à la population enquêtée,. . .)
  - mais l'impact **varie** considèrablement en fonction du traitement
  - elle affecte avant tout **les modalités** de la collecte et de l'analyse (consentement, sécurisation,. . .)
  - difficultés pratique de l'analyse juridique **dans certains cas**
- l'application de la règlementation doit être intégrée **dès la conception** du projet de recherche (protection des données dès la conception et sécurité par défaut)
- et doit donc **associer votre Cil** dès que possible

Merci pour votre attention