# Transparence vs protection des données – un dilemme dépassé à l'heure de l'administration digitalisée?

**CONFÉRENCE SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES DONNÉES**

**Transparence et protection – deux éléments fondamentaux de la démocratie**

**Tunis/Hammamet, 5 octobre 2022**

**Yves Poullet, Professeur émérite (Namur et Lille), Membre de l'académie royale de Belgique et de l'APD, membre de la CCF d'Interpol; expert auprès du Conseil de l'Europe et de l'UNESCO;**

# Accès à l'information et protection des données

- Une vraie synergie au service de la « Privacy », conçue comme droit au développement individuel dans une société en particulier de l'information:
  - Une approche « collective » de la privacy (loi d'accès à l'information): le droit de connaître et critiquer les actions de l'autorité publique y compris celles impliquant des personnes privées: les premiers textes (y compris celui de 2009) sur l'accès aux données du secteur public.
  - Une approche « individualiste » de la privacy: le droit de connaître les décisions de l'autorité publique relatives à ma personne (physique ou morale), ainsi que leurs motivations (loi de protection des données et loi d'accès à l'information) voire de délivrer les « d'informations essentielles qui permettent aux citoyens d'évaluer les risques pouvant résulter pour elles et leurs proches » (**AFFAIRE GUERRA** ET AUTRES c. Italie, ARRÊT STRASBOURG 19 février 1998)
- La prévalence de l'approche collective: la multiplication des obligations légales de transparence de l'information y compris à caractère personnel.
- L'équilibre d'intérêts …. Au service de la privacy, conçue non dans une optique non propriétaire mais dans une approche d'un individu qui se développe dans une société donnée.

# De nouvelles donnes ou quand la technologie s'en mêle?

- La donnée y compris la donnée à caractère personnel : « the new oil » de l'économie pour le développement de nouveaux services pour les citoyens, les entreprises ET l'autorité publique –
  - Les technologies de l'IA et celles connexes et le mythe d'une administration objective, efficace et prédictive dans ses décisions collectives et individuelles: l'IA Act européen – la tentation de la délégation à l'ordinateur
  - La nécessité de « *big data* »: le dogme du « Data sharing » au sein de l'administration et du secteur privé comme servant l'intérêt général: les « FAIR (Findability, Acessibility, Reusability,)nteroperability, Reusablitlity) principles » - créer un environnement sûr dans lequel les données peuvent être partagées entre les secteurs privés et le secteur public dans l'intérêt de la société et de l'économie. Les différentes mesures de la loi visent à **promouvoir l'accessibilité des données** en vue de leur exploitation, à renforcer les **mécanismes de partage de données** et à améliorer la confiance dans les intermédiaires de données.
- La nouvelle conception des législations sur la transparence:
  - les législations dites « open data » et les règlements européens : en discussion, le Data Act (d'une approche propriétaire des données à une approche fondée sur le droit d'accès), le Data Governance Act (mai 2022) : « "*More data should be available for the common good, for example for improving mobility, delivering personalized medicine, reducing energy consumption and making our society greener.*": le reverse PSI ?: une administration, source mais également destinataire d'informations

# Les nouveaux défis de la transparence

- De l'administration « en silos » à l'administration « en réseaux et plateformes »: la multiplication des flux internes à l'administration
- L'utilisation par l'administration des technologies de l'IA (*machine learning*) et de l'IoT:
  - Des technologies au fonctionnement opaque et dépassant les limites de l'intelligibilité humaine comment discuter la « vérité sortie de l'ordinateur »?
  - De la remise en cause des principes de finalité déterminée et de minimisation
  - Des technologies « acquises »:  Le recours aux opérateurs privés et les risques y attachés
- La réutilisation sans limites (?) par l'entreprise des données et les risques y attachés:
  - Les limites de l'anonymisation: y-a –t-il encore des données anonymes?
  - Le besoin de données au minimum pseudonymisées;
  - Le contrôle des finalités ultérieures (Aff. Satakunnan c. Finlande, CEDH 2017).
  - L' **imposition et la publication des conditions juridiques et techniques** qui devront être respectées pour réutiliser les données du secteur public (sécurité, résultats de la réutilisation, …).

# Pour une transparence « nouvelle » au service de la vie privée et de la démocratie

- Une **transparence publique** renforcée à toute information dont la connaissance par le public en général est jugée d'intérêt général:
  - Le logiciel comme 'document' public (voir contra, le considérant n°30 de la directive « open data ») – publication des algorithmes décisionnels (collectifs et individuels) – problème des droits de PI?
  - Le cadastre des flux au sein du secteur public et la nécessité d'une base légale (légalité, proportionnalité, nécessité dans une société démocratique)
  - Du PIA à l'IAIA – la nécessité d'une prise en compte multidisciplinaire des risques liés à l'utilisation des technologies d'IA et des technologies connexes (robot, IoT) – vers une accessibilité publique du rapport voire au-delà de sa discussion publique (Rapport SAUVE (CE fr): « Consulter autrement, participer effectivement »)
  - L'existence d'un organe de gestion des bases de données publiques et le rôle des plateformes comme outil de contrôle
  - Du rôle essentiel d'une autorité administrative indépendante d'accès aux documents détenus par l'administration.

# Pour une transparence « nouvelle » au service de la vie privée et de la démocratie

- La question particulières de l'accessibilité aux DCP
  - La nécessité d'une base légale en ce qui concerne les données à caractère personnel rendues publiques directement ou indirectement (voir les DCP présentes sur la carte d'identité)
  - La nécessité d'une pseudonymisation garantie – le rôle des intermédiaires de confiance
  - Pour une interdiction du consentement comme seule base de l'accès
  - Les restrictions d'usage et leur contrôle
- La question particulière du reverse PSI: l'altruisme des données
  - Le besoin d'un cadre légal en toute hypothèse contre les logiques du consentement et des besoins exceptionnels de l'état: le respect de la légalité et de la proportionnalité.
  - Vers des « intermédiaires » de confiance?

# Pour une transparence « nouvelle » au service de la vie privée et de la démocratie

- Une **transparence proactive**:
  - Le cadastre des flux dans le secteur public
  - La publication des codes-source des logiciels d'IA utilisés pour les décisions individuelles ou collectives ?
  - Une obligation d'information sur l'existence de l'utilisation d'un système d'aide à la décision
- Une **transparence renforcée lors des demandes d'accès**: vers une égalité d'accès entre agents de l'administration et citoyens (ex: accès aux noms des administrateurs d'une société renvoie vers les autres postes d'administrateurs détenus par ces personnes) – le droit à l'accès de tous, le droit à l'accès sur support numérique lisible et utile
- Une **transparence** renforcée lors de demandes d'accès à leurs dossiers: (personnes physiques et morales!): voir loi DCP + …. (le principe de « réciprocité des avantages du numérique »)
  - L'accès aux dossiers et à leur suivi : l'» audit trail »
  - L'accès aux consultations du dossier (quid de la protection des données des agents de l'administration?)
  - En cas de recours à un système d'aide à la décision automatisée, le droit à une explication humaine et à un recours interne auprès d'un organe indépendant.

# Conclusions

- Nécessité de réfléchir sur une gouvernance globale de l'administration publique
- « Governing with AI and not by AI » (JRC 2020)
- Protection des données et démocratie: deux valeurs à maintenir ensemble: la « privacy » condition de la démocratie et la démocratie comme garantie de la » privacy » – le besoin d'imagination et de solutions technologiques (*Technology is the problem, it might be the solution*).
- Pour une approche « centrée sur l'homme »
- Pour une nécessaire collaboration (voire une fusion) entre les deux autorités administratives indépendantes?

le *Data Governance Act* a été adopté en mai 2022, et sera applicable en septembre 2023. Il vise à favoriser le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation. Ce règlement comporte :

- un encadrement ainsi qu'une assistance technique et juridique facilitant **la réutilisation de certaines catégories de données protégées du secteur public** (informations commerciales confidentielles, propriété intellectuelle, données personnelles) ;
- **une certification obligatoire pour les fournisseurs de services d'**intermédiation de données ;
- **une certification facultative pour les organismes pratiquant l'**altruisme en matière de données.

La proposition législative de la Commission européenne, présentée le 23 février 2022, a pour objectif **d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs de l'économie de la donnée,** notamment liées à l'utilisation des objets connectés et au développement de l'Internet des objets. À ce titre, la proposition de *Data Act* a pour objectifs de :

- **faciliter le partage entre entreprises (B2B) et avec le consommateur (B2C) des données**, en fixant notamment une obligation de rendre accessibles les données générées par l'utilisation des objets connectés et services connexes, en contrepartie d'une compensation juste et équitable ;
- **permettre l'utilisation des données détenues par les entreprises et, sous réserve de justifier d'un besoin exceptionnel**, **par les organismes publics** des États membres et les institutions, agences ou organes de l'Union ;
- **faciliter le changement de fournisseur de services de traitement de données (*cloud* et *edge computing)*** par l'encadrement des relations contractuelles entre les fournisseurs de services et les consommateurs, et notamment par la suppression progressive des frais liés au changement pour le consommateur ;
- prévoir l'élaboration **de normes d'interopérabilité** pour les données et leurs réutilisations entre les secteurs ;
- mettre en place des **garanties contre les accès illicites de gouvernements de pays tiers** aux données non-personnelles contenues dans le cloud.