RGPD-OS : RGPD aware Operating System

Ludovic Pailler

disciplines de recherche
informatique, droit

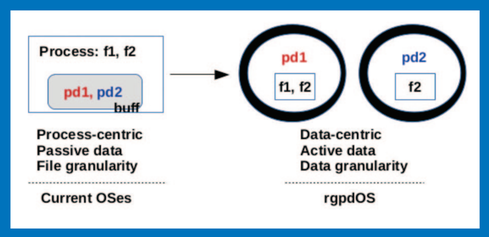
temporalité
Contemporain (XXIe siècle)

Dans l'Union européenne des 27, projection à 2025 :

530 % d'augmentation du volume mondial de données depuis 2018

829 milliards € valeur de l'économie fondée sur les données

10,9 millions de professionnels des données



Les systèmes d'exploitation classiques (à gauche) sont structurés autour des processus d'accès aux fichiers, les données personnelles (pd) étant accessibles à tout moment. Le système rgpdOS, lui, est structuré autour de la donnée, et chacune est protégée par une membrane dans laquelle sont implémentées les conditions d'accès à cette donnée, dite désormais active (source : rgpdOS: GDPR Enforcement By The Operating System, Tchana A. *et al.*, 2022).

lien avec la MSH

Les financements de la MSH ont permis d'offrir les moyens matériels et déterminants pour lancer le projet de recherche. L'accompagnement s'est essentiellement traduit par une aide logistique : commande de fourniture.

RGPD-OS

PROJET DE RECHERCHE

RGPD aware Operating System

LE PROJET

Le projet rgpdOS vise à concevoir un système d'exploitation qui, par son architecture et ses fonctionnalités, contribue, de façon significative, à la protection des données à caractère personnel.

Pour ce faire, le principal moyen envisagé est d'ajouter, autour de la donnée, une couche supplémentaire d'information qui commande l'utilisation qui peut en être faite par quiconque. Les règles de droit et la volonté de la personne concernée par la donnée seraient pleinement performatives. Et le droit de la protection des données devrait lui-même être relu à l'aune d'une donnée conçue désormais comme un véhicule programmable de l'information.

Le règlement général sur la protection des données (RGPD) est un texte européen de 2016 qui pose un cadre juridique uniforme en matière de protection des données personnelles des citoyens. Dans un contexte de fortes évolutions du numérique, il vise à accroître la protection des personnes et à responsabiliser les acteurs du traitement et de la circulation de ces données.

MÉTHODOLOGIE

Pour la partie juridique du projet, la première phase a consisté à dépouiller les **règles de protection des données** pour déterminer celles qui devraient être implémentées telles quelles dans le système d'exploitation, et celles qui doivent prévoir des modularités afin de permettre au responsable de traitement ou à la personne concernée d'adapter l'outil à ses besoins et contraintes. Une seconde phase a consisté à identifier les **sources juridiques et institutionnelles** dans lesquelles des moyens techniques et organisationnels de protection des données avaient pu être définis. Une troisième phase aurait dû consister à déterminer celles des prescriptions d'usage à intégrer dans l'enrobage de la donnée active.

Pour la partie informatique, la première phase a consisté à concevoir, d'une part et de façon schématique, **un nouveau modèle de fonctionnement pour un système d'exploitation**. Il ne s'est pas agi d'en construire un de toute pièce, mais de transformer un système d'exploitation existant et en *open source* pour le modifier dans la mesure nécessaire du projet. D'autre part, il s'est agi de concevoir un langage informatique de haut niveau à partir des exigences tirées du droit de la protection des données. Cela suppose de lister les contraintes juridiques et les notions à implémenter dans la machine, tout en prévoyant que la langue développée puisse également être en mesure d'exprimer les fonctions et implications du code en langage naturel.

Pour la partie transdisciplinaire, il a été nécessaire pour chacun de s'acculturer au vocabulaire, au raisonnement et aux contraintes techniques et juridiques. Ce dialogue entamé dès avant, mais intensifié durant la réalisation du projet, a conduit à une évolution. La cible du RGPD (règlement de l'Union européenne) a été délaissée pour concevoir un outil plus ambitieux, qui offre une **interopérabilité** entre les différents systèmes juridiques du monde et réponde aux besoins des professionnels.

Pour les spécialistes...

Le projet rgpdOS est un projet transdisciplinaire, mêlant principalement les sciences de l'informatique et le droit qui se propose de tirer les conséquences de l'obligation de protection des données dès la conception. Il vise à déterminer une nouvelle conception d'un système d'exploitation qui implémente les règles de la protection des données issues du règlement général sur la protection des données (RGPD).

Il s'agit de traduire et mettre en œuvre les exigences de la protection des données dans un outil technique au niveau du système d'exploitation, c'est-à-dire au point d'origine de la diffusion des données. Ainsi, la donnée active deviendrait l'élément central du système d'exploitation (exemple : Windows, Linux), et on lui implémenterait directement les règles relatives à sa protection de sorte à concrétiser l'ambition même du RGPD qui est de garantir tout à la fois la protection des personnes concernées et la libre circulation des données.

L'économie du droit de la protection des données serait à repenser puisque la donnée pourrait alors être clairement distinguée de l'information. Surtout, son ubiquité, sa rivalité, son excluabilité et sa consomptibilité seraient modulables.

la clé des mots compliqués

Données à caractère personnel : actuellement, toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un identifiant (numéro étudiant, numéro de carte nationale d'identité ou de carte vitale, adresse IP).

Système d'exploitation : un programme qui ordonne l'utilisation des ressources d'un ordinateur par les logiciels applicatifs.

Donnée active : donnée pour laquelle une couche d'information supplémentaire commande l'utilisation qui peut en être faite.

Protection des données dès la conception : obligation faite aux responsables de traitement de penser la mise en œuvre de moyens techniques et organisationnels de protection des données en même temps qu'ils conçoivent le traitement de celles-ci.

Consomptibilité : caractéristique d'une chose qui se détruit par son usage.

Ubiquité : faculté d'une chose d'être présent en plusieurs lieux en même temps.

Excluabilité : caractéristique d'une chose dont on peut interdire ou limiter l'usage.

Rivalité : caractéristique d'une chose dont l'usage par un individu réduit le potentiel d'usage par un autre.

msh Lyon St-Étienne

Projet RGPD-OS
Coordination scientifique Ludovic Pailler (Univ. Lyon 3, EDIEC)
Partenaires Laboratoires EDIEC (EA 4185), LIP (UMR 5668) et IRISA (UMR 6074, Rennes)
Financement MSH Lyon St-Etienne (2022)

UNIVERSITÉ JEAN MOULIN LYON 3 EDIEC ÉQUIPE DE DROIT INTERNATIONAL EUROPÉEN ET COMPARÉ

LIP

UMR IRISA