IDHEAP
POLICY BRIEF

NUMÉRO 6 | MARS 2023

Un outil d'évaluation de l'impact sur la vie privée du traitement de données de l'Internet des objets (IoT)

Unité Management de l'information Prof. Tobias Mettler et Dana Naous

Introduction

Le règlement général de l'UE sur la protection des données (RGPD) a introduit l'analyse d'impact relative à la protection des données (AIPD) comme outil d'évaluation des risques associés à la technologie et au traitement des données pour la vie privée. L'AIPD vise ainsi à identifier et réduire les risques de préjudices pour les personnes physiques. Pour ce faire, l'AIPD est effectuée chaque fois qu'il existe une probabilité considérable que le traitement des données puisse engendrer des risques pour les droits et libertés des personnes précitées. Ce type d'évaluation permet non seulement de mesurer la conformité à la législation mais aussi de s'assurer que les questions de protection des données sont prises en compte dès le début du développement et de l'utilisation des technologies de l'information. Ainsi, l'AIPD permet aux contrôleur·se·s de données d'identifier, de traiter et d'atténuer l'impact négatif des technologies de traitement des données sur les individus. **Cependant, comme la disposition légale du RGPD est abstraite, la conduite de telles évaluations est critiquée car subjective** (Wagner et Boiten 2018). Il est dès lors nécessaire d'introduire des directives concrètes et détaillées dans le processus d'évaluation ainsi que des outils automatisés capables d'accélérer l'analyse.

Démarche de recherche

Dans le but d'améliorer la méthodologie d'évaluation des risques liés à la vie privée, nous avons développé un outil pratique qui permet aux organisations d'effectuer des évaluations plus objectives. Comme ce type d'évaluation varie en fonction du domaine de mise en œuvre, nous abordons un scénario spécifique de traitement de données de l'Internet des objets (IoT) dans la surveillance connectée. Les initiatives IoT, avec des appareils portables et des réseaux de capteurs, permettent d'accéder à différents types de données. Elles sont mises en œuvre dans les organisations pour la surveillance numérique principalement pour détecter et prévenir les problèmes de santé et pour atténuer les risques sanitaires. Cependant, leur mise en œuvre s'accompagne de risques pour la vie privée. **Nous souhaitons ainsi contribuer à la discussion relative à la mise en œuvre de l'AIPD en proposant une aide pratique aux contrôleur·se·s de données sous la forme d'un outil AIPD automatisé pour les projets IoT**. A travers une approche continue de gestion des risques, nous suggérons un processus d'évaluation structuré qui comprend plusieurs phases. Dans la première phase, l'outil répond aux questions liées à l'objectif du projet, au contexte et à la nature du

traitement des données. La deuxième phase comprend des questions détaillées sur l'analyse du flux de données : c.-à-d. la collecte, le stockage et l'utilisation des données. Dans cette phase, les différents rôles sont également identifiés pour documenter les différentes personnes impliquées dans le processus. La troisième phase consiste en une analyse de la vie privée, au cours de laquelle les risques d'atteinte à la vie privée sont identifiés au moyen d'une série de questions pertinentes et évalués par rapport aux principes de protection de la vie privée. La phase finale implique la documentation et la visualisation des résultats dans un rapport analysant l'impact sur la vie privée.

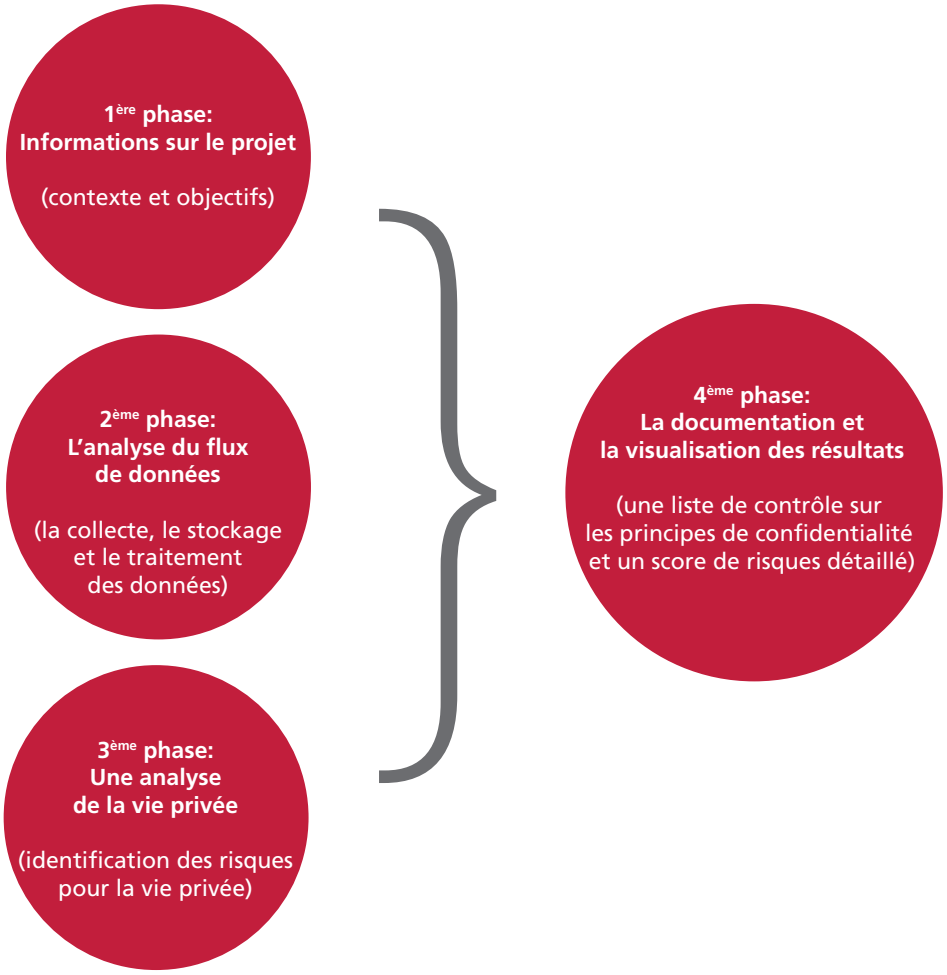

Figure 1 | Le processus d'évaluation du risque pour la vie privée dans notre outil développé.

> " Nous souhaitons ainsi contribuer à la discussion relative à la mise en œuvre de l'AIPD en proposant une aide pratique aux contrôleur·se·s de données sous la forme d'un outil AIPD automatisé pour les projets IoT. "

Résultats, discussions et implications pour les décideuses et décideurs

L'outil développé fournit des conseils sur le processus AIPD et documente les résultats pour permettre aux contrôleur·se·s de données d'identifier et de traiter les risques découlant de l'utilisation de la technologie IoT. De plus, grâce à la liste de contrôles, **nous fournissons une analyse de confirmation sur le processus de mise en œuvre et la disponibilité de garanties dédiées pour préserver la confidentialité des données**. Si cet outil est spécifiquement développé pour le contexte de la surveillance connectée, son champ d'application peut encore être étendu à d'autres technologies comme systèmes d'intelligence artificielle avec gestion algorithmique et à d'autres environnements de mise en œuvre que la santé au travail (ex., gestion des ressources humaines). Pour nos recherches futures, l'outil va être évalué par des praticien·ne·s afin de pouvoir proposer des extensions possibles. Nous souhaitons également tester l'outil auprès des utilisateur·rice·s pour évaluer le rôle du "privacy priming", c.-à-d. obtenir des informations sur les risques pour la vie privée via l'outil, sur l'acceptation de la technologie connectée sur le lieu du travail.

Référence

Mettler, T., & Naous, D. (2022). Beyond Panoptic Surveillance: On the Ethical Dilemmas of the Connected Workplace. In: *European Conference on Information Systems (ECIS)*. Timisoara, Romania

Wagner, I. & Boiten, E. (2018). Privacy Risk Assessment: From Art to Science, by Metrics. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pp. 225-241: Springer.