PIA : Enseigner la protection des données personnelles dans l'interdisciplinarité

Margo Bernelin
CR CNRS
UMR 6297 Droit et changement social
Nantes Université
margo.bernelin@univ-nantes.fr

Antoine Boutet
INSA Lyon, Inria, CITI
UR3720
69621 Villeurbanne, Lyon, France
antoine.boutet@insa-lyon.fr

***Abstract*—Le module d'enseignement PIA (*Privacy Impact Assesment*), conjuguant informatique et droit, entend créer un dialogue concret entre étudiants en informatique et étudiants en droit afin d'envisager de manière novatrice la protection des données personnelles. Associant l'INSA de Lyon, la Faculté de droit de Nantes Université ainsi que la CNIL, le module PIA, dont la première séance a été organisée en février 2025, doit permettre aux étudiants d'acquérir des connaissances techniques et juridiques centrales pour leur cursus tout en les familiarisant avec l'interdisciplinarité et la nécessité d'engager un dialogue constructif au-delà de leur domaine de compétence.**

***Index Terms*—Protection de la vie privée, droit des données personnelles, CNIL, cybersécurité.**

I. Introduction

La question de la protection de la vie privée et, en particulier celle de la protection des données personnelles, est une thématique qui se prête à des enseignements innovants. En effet, loin d'être cantonnées à un champ disciplinaire particulier, les différentes facettes de la protection des données personnelles débordent le domaine de l'informatique (lequel s'intéresse aux moyens de protection) pour abonder également celui du droit, sous l'angle alors des moyens d'encadrer les pratiques de collecte et d'usage des données personnelles. Actant les possibles passerelles entre ces deux domaines d'enseignement (informatique et droit), le module PIA (*Privacy Impact Assesment*) entend créer un dialogue et une compréhension interdisciplinaire des enjeux de protection des données personnelles [1]. Après avoir présenté le contexte au sein duquel le module PIA a émergé (Section II), nous aborderons le partenariat sur lequel il repose (Section III). Le module et les ressources documentaires utiles seront, ensuite, présentés (Section IV) avant d'aborder le retour d'expérience sur cet enseignement novateur et les perspectives à venir (Section V).

II. Le Contexte

Le module informatique et droit PIA a émergé grâce à la synergie créée entre ces deux disciplines par le projet de recherche IPoP (*Interdisciplinary Project on Privacy*)[1]. Le projet IPoP est issu du PEPR (Programmes et Équipements Prioritaires de la Recherche) Cybersécurité[2]. Le projet entend identifier les nouvelles menaces visant la vie privée introduites par le traitement de données personnelles et proposer des solutions théoriques et techniques pour protéger les données personnelles. Dans cette perspective, les équipes du projet IPoP s'intéressent aux nouvelles formes de collecte de données personnelles, aux systèmes d'IA traitant des données personnelles, aux moyens de les entraîner grâce à des modèles préservant la confidentialité des données, aux techniques d'anonymisation, à la confidentialité différentielles, aux attaques sur les données personnelles ainsi qu'aux ressources du droit pour encadrer la matière. Le projet IPoP, qui s'étale jusqu'en 2028, s'appuie alors sur la pluridisciplinarité et l'interdisciplinarité pour la conduite de ses travaux afin d'offrir des éclairages transversaux questionnant de concert la technique et le droit[3] [2].

Si la recherche est au cœur du projet IPoP, les discussions interdisciplinaires ont mis en lumière la nécessité de construire ou de diffuser ce dialogue au-delà de nos sphères de recherche. En effet, la question de la protection de la vie privée, et des données personnelles en particulier, ne peut se satisfaire d'une étude en silos dans un champ disciplinaire. Les contraintes techniques, légales, éthiques et sociétales imposent une analyse croisée ainsi que la formation des futures promotions d'informaticiens et de juristes à cet exercice. Dans ce cadre, il est apparu utile de penser de manière renouvelée l'enseignement de la protection des données personnelles en proposant un module droit et informatique qui permettrait aux étudiants de ces deux domaines de partager leurs connaissances et d'entamer un dialogue, dialogue qui leur sera utile dans leur parcours professionnel.

III. Les partenaires

Le module informatique et droit PIA s'appuie sur trois partenaires du projet IPoP: l'INSA de Lyon, la Faculté de droit de Nantes, ainsi que la Commission Nationale Informatique et Libertés :

Ce travail a été soutenu par le projet ANR 22-PECY-0002 IPoP (Interdisciplinary Project on Privacy) du PEPR Cybersécurité.

[1]https://files.inria.fr/ipop/.

[2]https://www.pepr-cybersecurite.fr

[3]https://files.inria.fr/ipop/donnees-de-sante/programme/

- INSA-Lyon : L'INSA de Lyon est une école d'ingénieur constituée de plusieurs départements d'enseignement. Ce module a impliqué les 111 étudiants de 4ème année du département informatique et rentre dans le cadre d'un nouveau programme plus large dédié aux Enjeux Environnementaux et Sociétaux du Numérique (EESN) initié en 2023. Le travail a été réalisé en groupe de 6 à 9 élèves sur deux séances de 4 heures.

- Faculté de droit de Nantes Université : La Faculté de droit de Nantes Université est dotée d'une expertise en droit du numérique, en particulier dans le cadre des travaux menés au sein du laboratoire de recherche "Droit et changement social" (UMR 6297). Cette expertise se décline sur le terrain de l'enseignement et notamment au sein du Master 2 Droit de la santé. Ce diplôme comprend un cours magistral en droit du numérique en santé, lequel traite des enjeux spécifiques de protection des données de santé et de la cybersécurité. C'est au titre de ces enseignements que les étudiants de ce Master 2 pour la promotion 2025 ont été conviés à participer à ce module sur un mode optionnel. 8 étudiants ont répondu positivement.

- Commission Nationale Informatique et Libertés (CNIL): Partenaire institutionnel du projet IPoP par l'intermédiaire de son département dédié à l'intelligence artificielle, la CNIL a également embarqué dans ce projet d'enseignement interdisciplinaire. C'est ici, le service de la mise en conformité qui a accepté de participer à ce module en proposant une formation dédiée à notre cas d'étude: l'Analyse d'Impact relative à la Protection des Données personnelles.

IV. Le module PIA

Le module PIA informatique et droit porte sur la création d'une Analyse d'Impact relative à la Protection des Données (AIPD) co-construite par les étudiants en informatique et en droit (SectionIV-A). Il s'organise autour de quatre étapes (SectionIV-C), s'appuie sur l'usage d'outils numériques (SectionIV-B), et sur une documentation disponible en ligne (SectionIV-D).

A. Réalisation d'une Analyse d'Impact relative à la Protection des Données personnelles (AIPD)

Forts de l'expérience de plusieurs initiatives d'enseignement dans le domaine de la cybersécurité [3], [4], il est apparu qu'un terrain propice pour créer un dialogue interdisciplinaire entre étudiants de domaines disciplinaires différents était la question de la constitution d'une analyse d'impact relative à la protection des données personnelles, (*Privacy Impact Assesment*, PIA) en anglais. Ce PIA a pour objectif d'analyser, pour un traitement de données personnelles particulier, "l'origine, la nature, la particularité et la gravité" des risques posés pour la vie privée des personnes concernées par les données[4]. Il s'agit d'une analyse concrète, imposée aux traitements de données personnelles les plus susceptibles de soulever des risques pour la vie privée. Ce PIA doit comprendre les éléments suivants :

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD[5].

Au regard du contenu du PIA imposé par le RGPD, il apparaît évident que sa conduite impose à la fois de mobiliser des connaissances en droit ainsi qu'en informatique, mobilisation qu'un cas pratique en la matière permettrait d'articuler. À cet égard, il convient de noter que les études de droit et d'informatique se retrouvent sur l'emploi de cas pratiques comme outils pédagogiques pertinents [5]. Le module PIA s'appuie alors sur un cas pratique relatif au développement d'une application fictive de coaching bien-être et santé laquelle conduit aux traitements de nombreuses données personnelles (y compris des transferts à des tiers, partenaires commerciaux ou sous-traitants).

B. L'usage de l'outil numérique de la CNIL

Le module PIA s'appuie sur l'outil numérique développé par la CNIL et dédié aux analyses d'impact relatives à la protection des données personnelles et nommé PIA (Figure 1). Il s'agit d'un logiciel en *open source* à l'attention des responsables de traitement de données personnelles pour les guider dans la constitution de leur analyse. Ainsi, le logiciel comprend des cases à remplir par les responsables de traitement lesquelles doivent leur permettre d'identifier aisément les obligations juridiques ainsi que saisir les risques soulevés par leurs traitements de données. Pour ce faire, le logiciel propose des rappels de connaissances sur les notions centrales du RGPD. Le logiciel demande, une fois l'analyse de première intention menée, de valider cette première analyse par une autre personne qui va émettre des commentaires et des demandes de corrections. Cet outil permet alors l'échange entre les étudiants des deux promotions grâce à cette fonctionnalité.

C. Les étapes

Le module PIA s'articule en quatre étapes permettant aux étudiants d'acquérir les connaissances nécessaires,

[4]Considérant 84, Règlement 2016/619 elatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données - RGPD).

[5]Article 35 du RGPD.

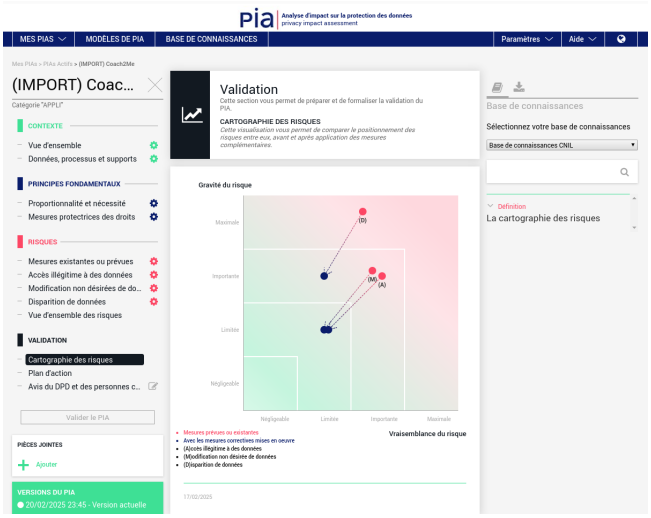

Fig. 1. L'outil PIA permet de suivre la méthode AIPD développée par la CNIL, il intègre 3 axes ((1) contexte, (2) principes fondamentaux, et (3) risques) et permet de décrire l'application en première intention et suivre l'étape de validation et d'amélioration.

de les mettre en pratique ainsi que d'initier un dialogue interdisciplinaire.

La première étape de ce module PIA a consisté en une formation dispensée par Madame Ingrid NKOUENJIN (Chef du service des outils de la conformité de la CNIL) le 14 février 2025. Cette formation, d'une durée de deux heures à l'attention des deux promotions d'étudiants (en droit et informatique) a eu pour objet de présenter le cadre juridique relatif aux analyses d'impact relatives à la protection des données personnelles ainsi que le fonctionnement de l'outil numérique "PIA" de la CNIL, une application qui permet de manière collaborative de constituer une telle analyse d'impact (SectionIV-B). Cette première étape a permis :

- de rappeler le cadre législatif du traitement des données personnelles ;
- de décrire l'objectif d'un PIA ainsi que son contenu ;
- de souligner l'importance d'un travail en équipe entre informaticiens et juristes pour décrire l'application ciblée et son fonctionnement ainsi que pour valider et améliorer sa conformité au RGPD ;
- d'assister à une première mise en pratique grâce à la présentation de l'outil numérique dédié de la CNIL.

Cette formation a été illustrée par des exemples relatifs aux données de santé, exemples utiles aux étudiants pour se projeter dans leur cas pratique.

La deuxième étape a monopolisé les étudiants de l'INSA Lyon pour réaliser une AIPD d'une application de coaching fictive. Les étudiants ont été mis dans la peau de jeunes diplômés rejoignant une startup proposant une application mobile innovante. La question de la régulation avait été omise dans les premières phases de développement de l'application, et le PDG de cette startup leur a demandé de réaliser l'AIPD. Les étudiants commencent donc par remplir l'AIPD en première intention, c'est-à-dire décrivant le fonctionnement de l'application et la formation des données personnelles telles qu'ils sont au début de cette analyse. Cette réalisation en première intention permet d'avoir une cartographie initiale de la gravité des risques et de leurs vraisemblances. Ensuite, les étudiants peuvent identifier les limites ou manques actuels et proposer des contre-mesures pour faire évoluer la cartographie des risques.

La troisième étape fait intervenir les étudiants du Master 2 Droit de la santé de la Faculté de droit de Nantes Université. Ces derniers disposent de trois semaines pour relire chacun deux analyses d'impact dédiées au cas pratique proposé. Ils doivent commenter les descriptions et analyses proposées par les étudiants en informatique et ajouter, lorsque cela leur semble utile et pertinent, des propositions d'amélioration. Ces éléments sont renvoyés aux étudiants en informatique la semaine précédant la séance de restitution.

La quatrième étape consiste en la mise en commun de nos travaux lors d'une séance de restitution laquelle permet de revenir sur les commentaires des étudiants en droit, de prendre connaissance des propositions de correction des étudiants en informatique ainsi que de s'intéresser aux mesures permettant de limiter les risques posés aux personnes concernées par les traitements de données visés par le cas pratique, et de discuter des risques résiduels. Cette séance est cruciale en ce qu'elle scelle le dialogue interdisciplinaire et doit permettre d'envisager en commun la résolution du cas pratique initialement proposé. Cette séance se tiendra la semaine du 24 mars 2025.

D. La documentation

Le module informatique et droit PIA prend appui sur une documentation accessible en ligne et éditée par la CNIL :

- le Guide Analyse d'impact relative à la protection des données personnelles: les bases de connaissance, 2018 [6] ;
- la page de présentation de l'outil PIA de la CNIL [7] ;
- la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise [8] ;
- la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise [9] ;
- les lignes directrices du G29 sur l'analyse d'impact relative à la protection des données - AIPD [10] ;
- une infographie PIA vue d'ensemble des obligations et de la méthode [11].

Ces ressources sont disponibles en libre accès sur le site internet de la CNIL et ont été présentées aux étudiants lors de la formation de la CNIL (étape 1).

V. Retour d'expérience et perspectives

Le module de formation s'est étalé de la mi-février à la fin mars 2025. La séance de restitution a été particulièrement riche d'apports pour les étudiants. Des grands enseignements se sont dessinés d'un groupe à l'autre. Ainsi, la complexité technique de la mise en conformité au RGPD d'une application a constitué l'apport commun principal et attendu de ce module de formation. Les étudiants ont, en effet, conclu que le respect de la vie privée devait être pensé bien en amont de la création d'une application traitant des données personnelles et inclure nécessairement un dialogue interdisciplinaire informatique/droit. Il est à noté que le travail des étudiants en droit intervenants pendant la 3e étape a été souvent facilité, par le fait que les étudiants en informatique aient régulièrement identifié eux-mêmes l'absence de conformité avec le RGPD, prenant rapidement de la distance avec l'énoncé de l'application que nous leur avions transmis. De plus, les étudiants en informatique ont su, pendant la discussion être force de proposition afin de présenter des moyens techniques permettant de protéger les données collectées par l'application. Cela a servi de base de discussion pour aller plus loin dans l'analyse juridique. À cet égard, le logiciel PIA de la CNIL est un très bon outil pédagogique, son déroulé en étapes permettant d'interroger toutes les dimensions des risques pesant sur les données personnelles que ce soit par l'intermédiaire de questionnements sur la nature des données, leur volume, conservation ou encore supports.

Les échanges ont alors conduit à mettre en parallèle les visions du droit et de l'informatique. La question de la nature des données en est une illustration. Alors que le PIA invite à s'interroger sur la nature des données, la réponse du juriste consiste à identifier des données "sensibles" (par exemple des données de santé) lesquelles sont davantage protégées que les autres. Les étudiants en informatique ont proposé une vision technique distinguant les données entrées par les utilisateurs de l'application, celles relevées par des capteurs et, enfin, les données calculées. Cette variété a permis aux étudiants en droit de prendre en compte la multitude des points de collecte des données mais aussi les moyens d'inférer des informations à l'appui des données collecteées. En retour, les étudiants en informatique ont pu interroger la place des données sensibles au sein des trois grands groupes de données identifiés.

Si les bénéfices de ce module sont palpables (ils font l'objet d'un retour des étudiants fin avril 2025), sa mise en œuvre entre des diplômes différents, des formations de tailles différentes (111 étudiants pour l'INSA et seulement 8 étudiants de la faculté de droit) et des emplois du temps contraints a imposé une organisation à distance via l'usage d'outils de visioconférence. Pour cette première année, les écueils, surmontables, ont été multiples:

- difficulté à fixer des créneaux pour le module, les étudiants en droit étant en stage au second semestre,
- une fois les plages horaires dédiées aux modules identifiées, difficultés à synchroniser les groupes d'étudiants en informatique et leurs binômes d'étudiants en droit travaillant sur les mêmes PIA;
- difficultés techniques liées à l'usage d'outils de visioconférence,
- difficultés, du côté des étudiants en droit, à utiliser l'API "PIA" de la CNIL (problèmes d'enregistrement des données, d'extraction des résultats),
- des séances de restitution trop courtes pour les échanges.

Ces difficultés nous ont conduit, ainsi que les étudiants, à faire preuve de patience, d'adaptation rapide et de bonne volonté. Ainsi, l'emploi du temps assez rigide de ce module a été présenté aux étudiants en droit, lesquels avaient le choix de participer ou non au module en fonction de leur disponibilité. La séance de restitution, d'une durée d'une heure et trente minutes s'est avérée trop courte pour nos discussions et, eu égard aux difficultés liées à la visioconférence, les séances ont débordé d'une demi-heure environ (avec l'accord des étudiants présents). Les difficultés de synchronisation des groupes d'étudiants en informatiques et de leurs binômes en droit ont conduit à composer avec une lecture semi-croisée des PIA à savoir la mise en discussion de PIA avec des étudiants en droit n'ayant pas effectué le corrigé le PIA en question mais un autre. Cette stratégie d'adaptation a forcé à dialoguer davantage pour expliquer des commentaires rédigés par d'autres camarades. Du côté des étudiants en droit, les difficultés d'utilisation de l'API PIA ont été résolues par le recourt à un document Word pour restituer les corrections.

Convaincus de la nécessité de proposer des enseignements interdisciplinaires relatifs à la protection des données personnelles et afin de prendre en compte ces écueils, le module sera, de nouveau, proposé en 2026 dans le cadre du même partenariat institutionnel. À cette occasion, le module ne sera plus proposé de manière optionnelle aux étudiants en droit, le module intégrant pleinement la maquette du diplôme M2 Droit de la santé pour la rentrée 2025-2026. En effet, la maquette de ce diplôme sera enrichie de différents cours en droit du numérique (domaine qui intègre la protection des données personnelles) à la rentrée dans le cadre du projet PENSO-DROIT, un projet AMI-CMA dédié à la santé numérique[6].
Cette nouvelle maquette comprendra 10 heures de TD dédiées au module, alors que 7 heures supplémentaires de travail individuel sur le PIA seront également planifiées dans l'emploi du temps des étudiants du M2 droit de la santé qui sera alors en alternance. Ce nouvel ancrage du module dans la maquette du Master 2 Droit de la santé permettra d'organiser des séances de formation et de restitution plus longues. Par ailleurs, et à fin d'intensifier le dialogue interdisciplinaire, nous envisageons d'organiser le module sur deux journées en présentiel à Lyon regroupant l'intervention de la CNIL, et la réalisation de l'AIPD en petits groupes composés d'étudiants de l'INSA Lyon et d'un étudiant en Master 2 Droit de la santé sur une application qui sera développée par le groupe d'étudiants de l'INSA Lyon dans un autre module (une application différente par groupe).

[6]Projet PENSO-DROIT.

REMERCIEMENTS

Ce travail a été soutenu par le projet ANR 22-PERCY-0002 IPOP (Interdisciplinary Project on Privacy) du PEPR Cybersécurité.

REFERENCES

[1] E. Bottini, P. Brunet, and L. Zevounou, *Usages de l'interdisciplinarité en droit*. Presses Universitaires Paris Nanterre, 2014.

[2] M. Bernelin, "La confidentialité : une notion juridique au service de la protection des données de santé ?" in *Cahiers Droit, Sciences & Technologies*, vol. 17, 2023, pp. 21–36.

[3] A. Boutet, M. Cunche, S. Gambs, B. Nguyen, and A. Laurent, "DARC : Data Anonymization and Re-identification Challenge," in *RESSI 2020 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, Nouan-le-Fuzelier, France, Dec. 2020. [Online]. Available: https://inria.hal.science/hal-02512677

[4] A. Boutet and G. Derache, "Simulation de crise -24h dans la tempête," in *RESSI 2022 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, Chambon-sur-Lac, France, May 2022, pp. 1–4. [Online]. Available: https://inria.hal.science/hal-03611184

[5] N. Cayrol and F. Grua, *Méthode des études de droit*. Paris, Dalloz, 2024.

[6] "Guide analyse d'impact relative à la protection des données personnelles," https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-fr-basesdeconnai.

[7] "Présentation de l'outil pia de la cnil," https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

[8] "Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise," https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf.

[9] "Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise," https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf.

[10] "Lignes directrices du g29 sur l'analyse d'impact relative à la protection des données," https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf.

[11] "Infographie pia vue d'ensemble des obligations et de la méthode," https://www.cnil.fr/sites/cnil/files/atoms/files/171002_fiche_risque_fr_cmjk.pdf.