

Compendium francophone
Law for Computer Scientists (and other folks)
*L'informatique pour les informaticien·nes (et autres
gens lambdas)*

Victor Morel

6 juin 2023

Table des matières

1	Introduction	9
2	Droit, démocratie et État de droit	13
2.1	Qu'est-ce que le droit ?	13
2.1.1	Sources du droit	13
2.1.2	Ce que fait le droit	14
2.1.3	Raisonnement juridique	15
2.2	Qu'est-ce que le droit en démocratie constitutionnelle	16
2.2.1	Droit, morale, politique et nature des règles juridiques	16
2.2.2	Certitude juridique, justice, instrumentalité	17
3	Les domaines du droit	19
3.1	Droit privé, droit public, droit pénal : les différences conceptuelles	19
3.1.1	Droits absolus et droits relatifs	19
3.1.2	Droit privé et droit public	19
3.1.3	Droit privé et droit pénal	20
3.2	Droit privé	20
3.2.1	Droit des biens : transfert de biens mobiliers	20
3.2.2	Droit des contrats et droit des biens : vente et transfert d'un bien immobilier	21
3.2.3	Responsabilité civile	21
3.3	Droit public et droit pénal	21
3.3.1	Droit public	22
3.3.2	Droit pénal	23
4	Droit international et droit supranational	25
4.1	Le concept de juridiction dans les systèmes juridiques occidentaux	25
4.1.1	Un exemple	26
4.1.2	Juridiction nationale	26
4.2	Droit international	27
4.2.1	Sources du droit international	28
4.2.2	Monisme et dualisme en droit international	28
4.3	Droit supranational	29
4.3.1	Transfert de souveraineté	30
4.3.2	Sources du droit de l'UE	30
4.3.3	Jurisprudence de la CJUE	31
4.4	État de droit international	32

5	Protection des données et de la vie privée	33
5.1	Droit relatif aux droits humains	33
5.1.1	Les droits humains comme des droits défensifs face à l'État moderne . . .	33
5.1.2	Des droits de la liberté aux droits sociaux, économiques et autres	34
5.2	Le concept de vie privée	35
5.2.1	Taxonomie et air de famille	35
5.2.2	Vie privée et technologie	36
5.3	Le droit à la vie privée	37
5.3.1	Le droit à la vie privée en droit constitutionnel	37
5.3.2	Le droit à la vie privée en droit international	37
5.3.3	Le droit à la vie privée en droit supranational	37
5.3.4	Article 8 de la CEDH	37
5.3.5	Jurisprudence de la CEDH sur la surveillance	38
5.4	Protection des données et de la vie privée	38
5.4.1	Par défaut : un droit à l'opacité et un droit à la transparence	39
5.4.2	Des droits distincts mais qui se chevauchent	39
5.4.3	Recours juridiques en cas de violation	40
5.5	Droit de la protection des données	40
5.5.1	Droit à la protection des données dans l'EU et aux USA	41
5.5.2	Droit à la protection des données dans l'EU	41
5.6	En bref	48
6	Cybercriminalité	49
6.1	Le problème de la cybercriminalité	50
6.1.1	Criminalité informatique	50
6.1.2	Cybercriminalité	50
6.2	Cybercriminalité et droit public	51
6.2.1	La Convention sur la Cybercriminalité	51
6.2.2	Les limites des pouvoirs d'enquête	54
6.3	Les directives européennes sur la cybercriminalité et la cybersécurité	55
7	Le droit d'auteur dans le cyberspace	57
7.1	Le droit de la PI en tant que droit privé	58
7.2	Vue d'ensemble des droits de la PI	59
7.2.1	Droit d'auteur	59
7.2.2	Brevet	59
7.2.3	Marque déposée	60
7.3	Histoire, objectifs et périmètre d'application du droit d'auteur	60
7.4	Droit d'auteur dans l'UE	62
7.4.1	La Directive Copyright et la Directive relative au respect des droits de PI	62
7.4.2	La Directive concernant la protection juridique des programmes d'ordinateur	63
7.5	Open source et accès libre	64
8	Systèmes informatiques défectueux	67
8.1	Droit de la responsabilité civile en Europe	68
8.2	Responsabilité des tiers en cas de traitement illicite et autres cyberdélits	70
8.2.1	Atteintes à la vie privée	70
8.2.2	Cyberdélits	71

9 Une personnalité juridique pour l'IA ?	73
9.1 Subjectivité juridique	74
9.2 Agentivité juridique	75
9.3 Agents artificiels	76
9.4 Responsabilité de droit privé	77
10 Dès la conception	81
10.1 Apprentissage automatique (ML)	82
10.1.1 Plan de recherche assisté par ML exploratoire et confirmatoire	83
10.1.2 Implications du micro-ciblage	83
10.1.3 Implications du micro-ciblage pour l'État de droit	84
10.2 Technologies de registres distribués (DLT), contrats intelligents et régulation intelligente	86
10.2.1 Contrats intelligents et réglementation intelligente	87
10.2.2 Le statut juridique des <i>contrats intelligents</i> en droit privé	88
10.2.3 Le statut juridique de la <i>réglementation intelligente</i> en droit public	89
10.3 <i>Légal par conception</i> ou <i>Protection juridique dès la conception</i> ?	90
10.3.1 Légal par conception	90
10.3.2 Protection juridique dès la conception	91
10.3.3 La protection juridique dès la conception à la lumière du RGPD	91
11 Fermeture : sur l'éthique, le code et le droit	95
11.1 Distinctions entre le droit, le code et l'éthique	96
11.1.1 Utilitarisme et individualisme méthodologique	96
11.1.2 Raisonnement déontologique : le respect pour l'autonomie humaine	98
11.1.3 Éthique de la vertu : percevoir le bien et faire ce qui est juste	101
11.1.4 Éthique pragmatique : prendre en compte	102
11.1.5 La différence qui fait une différence : la fermeture	103
11.2 La relation conceptuelle entre le droit, le code et l'éthique	104
11.2.1 Justice, certitude juridique et instrumentalité	104
11.2.2 Droit, code et État de droit	106
11.3 L'interaction entre le droit, le code et l'éthique	107
11.3.1 Approches <i>dès la conception en droit et en éthique</i>	107
11.3.2 Équité dès la conception et paradigmes de l' <i>informatique équitable</i>	109
11.4 Fermeture : la force de la technologie et la force du droit	114

Préambule

Cet article est ma première tentative de rédaction d'une note de lecture, ou plutôt d'une *synthèse* de lecture. Car, au-delà d'une note qui serait plus de l'ordre du commentaire, ma motivation première est bien de pouvoir restituer la substance¹ d'un livre à un public qui n'aurait sinon pas pu/voulu le lire, encore moins le comprendre. Ce livre c'est *Law for Computer Scientists* (LfCS) de Mireille Hildebrandt, professeure de droit et philosophe.

LfCS a pour but de sensibiliser un public d'informaticien·nes aux questions juridiques et philosophiques que posent l'informatique au sens général. Bien qu'il ait un but de vulgarisation, il n'en reste pas moins un livre académique et en anglais (juridique) : deux caractéristiques qui peuvent rebuter plus d'un·e lecteurice ! Comme je suis à la fois universitaire (précaire, certes), anglophone et informaticien, la lecture et la compréhension de ce livre restait un défi raisonnable pour moi, d'autant plus que mes thématiques et intérêts de recherche s'orientent de plus en plus vers des problématiques socio-techniques et juridiques. En discutant avec des amis, je me suis rapidement rendu compte que l'objet du livre intéressait, mais qu'il semblait inaccessible : 300 pages en anglais, il faut se les farcir ! Ainsi, je me suis mis à réfléchir à rédiger une synthèse *francophone* de LfCS, c'est-à-dire qui ferait office de résumé et de traduction.

L'aspect résumé semble aller de soi : la pratique est assez commune, bien que j'ai ici l'intention de restituer une bonne partie du contenu ; l'aspect traduction est lui bien plus périlleux. En effet, beaucoup de monde a déjà entendu la méta-anecdote sur le mot italien *traduttore* qui a donné *traduction*, mot qui signifie à la fois *traduire* et *trahir*. C'est encore plus vrai dans un contexte juridique où les termes sont à la fois 1) très précis, 2) chargés de sens et 3) pas forcément traduisibles. Je vous passe les débats sur la traduction de certains termes comme *privacy*, ou le faible emploi du terme français *agentivité* par rapport à son homologue anglais *agency*.

Bref, se lancer dans l'écriture d'une synthèse francophone de LfCS n'est pas une mince affaire. Cependant, la lecture de ce livre m'a été extrêmement utile et j'espère qu'elle puisse l'être pour d'autres, ou à défaut, que puisse être utile la lecture de cette synthèse. Comme l'écrit Hildebrandt sur la première page de l'introduction : « enseigner le droit aux informaticiens sera toujours une tentative, un essai pour combler l'écart entre deux pratiques scientifiques possédant chacune ses exigences de méthodologie et ses contraintes ».²

Quelques explications peuvent être utiles à la lecture :

- les traductions difficiles ont leurs formes d'origine en italique entre parenthèses (*parentheses*)
- certains termes sont simplement accentués en étant mis *en italique* mais pas entre parenthèses, notamment lors de leur première utilisation
- d'autres concepts-clés sont **en gras** pour aider les lecteurices à s'orienter dans la lecture
- je me permet d'enrichir la traduction avec mes propres références et interprétations, c'est généralement sans ambiguïté

1. J'emploie à dessein ce terme à la connotation philosophique.

2. Ma traduction, ce qui sera *a priori* le cas tout au long de cet article, je ne le repréciserai donc plus.

Je souhaite remercier le blog *Mais où va le Web ?* pour l'inspiration qu'ils m'ont donné à lire des ouvrages sur la technologie qui ne soit pas uniquement techniques, ainsi que pour leurs résumés et commentaires toujours pertinents de ces derniers.

Addendum : La traduction à l'ère des chatbots Au terme d'un an de travail, à un rythme pas forcément constant, je fini le travail de relecture en juin 2023. À ce moment, tout le monde a entendu parler d'IA, de chatbots et plus précisément de ChatGPT. Cet agent conversationnel peut notamment faire de la traduction, la question se pose donc : pourquoi traduire «manuelle-ment» si une machine peut le faire. En quelques mots :

- le jargon juridique ne se traduit pas toujours très bien,
- une traduction automatique (sans règles formelles de traduction) ne sera pas toujours cohérente, un même terme peut être traduit de différentes manières,
- ces agents conversationnels, bien qu'impressionnants, ne restent que de simples perroquets stochastiques³, ils ne font qu'obéir à des lois statistiques basées sur des probabilités, on est jamais à l'abri d'une n-ième hallucination,
- je n'ai jamais autant appris sur le droit et la philosophie du droit qu'en traduisant moi-même.

Gardez le contrôle, lisez vous-mêmes.

3. Pour reprendre l'expression de Emily Bender dans son article éponyme *On the Dangers of Stochastic Parrots : Can Language Models Be Too Big ?* <https://dl.acm.org/doi/10.1145/3442188.3445922>.

Chapitre 1

Introduction

L'introduction a pour but de situer l'essor du droit positif moderne en tant qu'*affordance* d'une technologie spécifique d'information et de communication, à savoir la presse écrite.

Le livre ouvre sur une analogie entre le droit et l'informatique, en ce que les deux disciplines ont des *architectures*. L'autrice donne ainsi trois aspects architecturaux du droit et de l'informatique :

- le fait d'être construit (artificiellement donc), plutôt qu'être naturel
- la nature relationnelle et de dimension élevée des constructions (*constructs*)
- la double nature écologique des constructions
 - * en ce qu'elles doivent perdurer dans un environnement spécifique et souvent dynamique
 - * alors que la construction elle-même forme l'environnement pour ses habitant·es

Le caractère hautement dimensionnel d'une construction implique que la moindre modification peut impacter l'ensemble de l'édifice : une jurisprudence dans un cas, un bug dans l'autre.

Le chapitre enchaîne avec une brève histoire de la normativité dans les sociétés orales (*speakerspace*). L'**architecture** de ces sociétés découle alors des affordances du langage. Les justiciables et les exécutant·es étaient les mêmes personnes. Le droit, la religion et l'économie y étaient intrinsèquement liés, sans que les normes ne soient fixées sur le papier.¹ Ces normes fluides et non écrites n'impliquent pas forcément qu'elles soient flexibles.

L'apparition de l'écriture change radicalement le fonctionnement normatif des sociétés. La loi écrite permet à la fois au roi qui l'édite d'assujettir ces sujets et de formaliser le droit coutumier. L'**architecture** de ces sociétés découle alors des affordances des manuscrits écrits à la main. La portée de ces manuscrits est alors bien plus grande que la portée auparavant limitée que pouvait avoir les normes orales. La distanciation occasionnée par le caractère écrit a des implications sur l'interprétation des textes, qui peut se faire dans des circonstances différentes que celles dans lesquelles les textes ont été écrits. L'écriture des normes donnent lieu à une interprétation itérative : on a pu voir des commentaires de commentaires pour assister l'interprétation de droit romain par exemple. La stabilité de l'écrit combinée à l'ambiguïté du langage naturel transforme l'interprétation et la contestation en la marque du droit, que l'on peut considérer comme à la racine de la protection offerte par le droit positif moderne.

Alors que les manuscrits devaient être copiés à la main, permettant des erreurs voire des modifications délibérées, l'invention de l'imprimerie moderne (généralement attribuée à Gutenberg) modifie une fois de plus le paysage normatif. Ici, l'**architecture** des sociétés d'imprimerie est

1. Je vous invite à lire *La société contre l'État* de Pierre Clastres, et notamment son dernier chapitre, pour approfondir la question de la norme fixée sur les corps.

plus complexe, plus systématique et hiérarchique, ainsi que plus explicitement interconnectée que l'architecture des sociétés manuscrites. Cette époque voit aussi naître de nouveaux arrangements politiques. La combinaison du monopole de la violence² avec la capacité à imposer des normes légales abstraites à une population elle-même abstraite³ a donné lieu au droit positif moderne : une loi écrite par un souverain demandant obéissance en échange d'une protection, que l'autrice appelle respectivement les souverainetés *interne* et *externe*. Ainsi, les souverains peuvent maintenant imposer des règles écrites à l'ensemble de leurs sujets, ils peuvent gouverner *par le droit*.⁴ On dit aussi que les souverains *pose* le droit, ce qui a donné le terme droit *positif*, c'est-à-dire le droit explicite en vigueur au sein d'une juridiction. Le droit coutumier est désormais intégré au droit positif, ce qui implique une validation préalable par le souverain. La prolifération des textes légaux est facilitée, ce qui a pour effet d'instiguer une hiérarchie des normes complexe. Enfin, le besoin d'interprétation donne lieu à une indépendance de plus en plus marquée des cours et la création d'une expertise spécifique et déléguée par le roi. Le juge vient alors s'immiscer entre gouvernants et gouvernés, la souveraineté est désormais divisée entre les fonctions législatives, exécutives et administratives : l'État de droit est né.⁵

Nous vivons désormais dans le cyberspace. Le cyberspace a deux caractéristiques propres : son ultra-connectivité et ses préemptions computationnelles (le fait que les calculs aient en quelque sorte un droit de priorité). L'infrastructure d'information et de communication est désormais numérique, elle ne se contente plus de prédire le comportement, mais elle calcule aussi dans quelle mesure son propre comportement influence celui de ses utilisatrices (l'infrastructure *préempte*). Ce changement de paradigme a des effets très concrets tels que l'automatisation de certaines décisions prises par des objets connectés par exemple, ou encore des décisions gouvernementales (prédiction de la récidive) et commerciales (publicité ciblée). L'**architecture** du cyberspace est mené par les données et par le code (*data-driven and code-driven*). L'autrice emploie le terme de monde *onlife*, qui ne serait ni *online* ni *offline*, en ce que la différence entre les deux est désormais artificielle et car les nouveaux systèmes informatiques, de part leur capacités préemptives, peuvent agir sur notre environnement. Le droit positif est lui mené par les écrits (*text-driven*) et les juristes, détenteurs du pouvoir induit par la rédaction des lois, étaient alors les architectes des sociétés. La philosophe du droit écrit que les juristes partagent désormais le pouvoir normatif avec les architectes d'Internet. Au vu de la puissance de certains informaticiens (généralement chefs d'entreprises) on ne saurait la contredire. Ces bouleversements appellent donc de nouvelles manières de produire du droit, afin de garantir la protection que celui-ci offre. Cette tâche prendra nécessairement du temps, mais le temps seul ne suffit pas. Tout comme l'avènement de l'État de droit au temps de l'imprimerie était le résultat de luttes politiques, un cyberspace sujet à l'État de droit demandera un effort concerté entre juristes et informaticien·es (entre autres). En attendant, il est crucial que les informaticien·es aient un avant-goût de ce que sont le droit et la protection juridique, ne serait-ce que pour concevoir des systèmes répondant aux exigences légales.

L'introduction offre ensuite un aperçu du livre, divisé en quatre parties :

1. la première partie couvre les chapitres 2 à 4 et réponds à la question «qu'est-ce que le droit» en posant une autre question : «que fait le droit?»

2. Terme généralement attribué à Max Weber, relié à la naissance de l'État moderne.

3. Je vous invite à lire *L'imaginaire national* de Benedict Anderson pour approfondir.

4. *They rule by law*, ce qui est un double sens car *rule by law* fait clairement référence à un usage instrumentalisé du droit comme arme politique, généralement despotique, voir <https://plato.stanford.edu/entries/rule-of-law/>

5. Hildebrandt parle de transition du *rule by law* au *rule of law*, qu'elle fait remonter à l'adage de Montesquieu *iudex est lex loquens*, "le juge est la loi qui parle". Notez aussi que *rule of law* n'a pas de vrai équivalent en français, cette notion juridique peut aussi être traduite par *primauté de la loi*. J'ai choisi *État de droit* car c'est une traduction largement acceptée et qui fait référence au fait que l'État n'est pas (censé) être au-dessus des lois.

2. la seconde partie couvre les chapitres 5 à 8, elle s'attaque à des grands domaines du *cyber-droit* tels que la protection des données et de la vie privée, le cybercrime, le copyright et la responsabilité de droit privé
3. une troisième partie examine les nouvelles frontières du droit, comme la personnalité juridique d'agents artificiels et la protection juridique dès la conception (*legal protection by design*)
4. enfin la quatrième partie conclut le livre sur les relations entre le droit, le code et l'éthique, avec un accent sur l'équité algorithmique (*algorithmic fairness*, dont Hildebrandt est spécialiste).

Chapitre 2

Droit, démocratie et État de droit

Le droit ne peut pas se résumer à des ordres donnés sous la menace, ni à de simples normes sociales. Bien que la morale fasse aussi partie prenante du droit, toute loi n'y est pas sujette. Ce chapitre examine les sources du droit, la nature du raisonnement juridique ainsi que les relations entre droit, démocratie et État de droit.

2.1 Qu'est-ce que le droit ?

L'historien du droit Uwe Wesel écrivait «Essayer de définir le droit est aussi vain qu'essayer de clouer un pudding sur un mur». Ce *pudding* juridique possède en effet une fluidité intrinsèque qui, plutôt qu'un *bug*, doit être considérée comme une caractéristique du droit. La **certitude juridique** — une des trois valeurs constitutives du droit avec la **justice** et l'**instrumentalité** selon le philosophe du droit Gustav Radbruch — ne doit d'ailleurs pas tant être comprise comme le fait de fixer la signification des normes, mais plutôt comme l'équilibre entre des attentes légitimes et la capacité à reconfigurer et contester ces normes.

2.1.1 Sources du droit

Alors qu'une source peut être thermale, journalistique, ou encyclopédique, une source de connaissance fait référence, plus précisément, au lieu (pas forcément physique) où l'on peut trouver la réponse à une question. En droit, le terme *source du droit* a une signification très précise, en ce qu'il fournit les normes légales à partir de leurs origines et qu'il rend ces normes contraignantes (*binding*). Ainsi, un article Wikipédia sur un article de loi n'est pas considéré comme une source du droit. Pour répondre au principe de certitude juridique mentionné ci-avant, seules les sources suivantes sont considérées comme source du droit :

les traités ils contraignent les États qui les signent et ratifient

la législation (dont la Constitution fait partie), elle promulgue prohibitions et obligations au sein d'une juridiction (bien souvent un État-nation)

la jurisprudence (*case law*), qui est l'ensemble des décisions rendues par les cours de justice. Il est intéressant de noter que c'est à la fois une source du droit et le résultat de l'application du droit.

la doctrine c'est un ensemble de textes publiés par les avocats avec intérêt à agir (*lawyers of standing*, qui ont un motif permettant de prévaloir d'un intérêt lésé), elle développe une interprétation spécifique d'un cadre juridique.

les principes fondamentaux du droit ce sont les principes implicites d'autres sources du droit, ce ne sont pas exactement des règles mais plutôt une forme de philosophie du droit.

le droit coutumier décrit l'ensemble des pratiques juridiques non-écrites, il est pris en compte lorsque des sujets de droit agissent d'une manière qu'ils considèrent légitimes. Il nécessite *usus* (une habitude d'agir) et *opinion necessitatas* (l'opinion partagée que ladite habitude correspond à un devoir d'agir).

2.1.2 Ce que fait le droit

Effet juridique

Le droit attribue un *effet juridique* à partir de conditions spécifiques, il a ce qu'on appelle une force *performative*. Par exemple, un employé de mairie qui déclare deux personnes mariées *performe* du droit et rends ces deux personnes mariées (si certaines conditions sont réunies). Cet effet juridique est ce qui différencie les normes morales et les normes juridiques : il ne dépend pas des inclinaisons morales mais bien du droit positif. C'est pour ça qu'on dit que le droit n'est pas une *science douce* (*soft science*), il a de vrais effets dans le vrai monde, la définition d'un terme juridique a donc une importance primordiale.

Un exemple illustre concrètement cet effet juridique. Dans une décision de la cour de justice États-Unienne de 2012 (*US v. Jones*), la Cour Suprême¹ a unanimement décidé que le traçage par GPS sans mandat était une violation du quatrième amendement de la constitution,² avec pour effet juridique que toute preuve obtenue de cette manière ne peut être utilisée devant une cour états-unienne. Dans cette affaire, un traceur GPS avait été mis en place après expiration d'un mandat. La Cour peut rédiger trois types d'opinions pour expliquer leur position :

- l'opinion de la Cour, qui explique les principales raisons de la décision
- l'opinion concordante, qui explique la même décision mais avec un raisonnement différent
- l'opinion dissidente, qui explique les raisons de contester la décision de la majorité.

L'opinion de la Cour argumentait que la voiture fait partie des effets personnels, ainsi l'apposition d'un traceur violait le quatrième amendement. Une opinion concordante elle soutenait que l'analyse des *patterns* de mobilité dérivés des données de géolocalisation violait une attente raisonnable de vie privée. Bien que les deux opinions atteignent la même conclusion, l'impact n'est pas le même. Dans le premier cas, la jurisprudence a une portée limitée car elle ne s'applique qu'aux cas où il y a intrusion physique ; tandis que le second cas prends en compte toute violation de la vie privée à partir d'analyse de mobilité. En résumé, l'effet juridique est double :

1. la décision clarifie le fait que la police ne peut pas placer de traceur GPS sans mandat
2. mais aussi qu'en cas de gain de popularité de l'opinion concordante, de futures décisions de justice pourraient offrir une meilleure protection dans le monde *onlife*.

L'effet juridique le plus évident est donc la décision d'une action ou d'une situation comme étant **légale** ou **illégal**. Un effet juridique peut aussi concerner l'attribution d'obligations légales — lors de la conclusion d'un contrat de vente, une partie a pour obligation de payer tandis que l'autre a pour obligation de fournir le produit — et de droits — toujours sur le même exemple, la première partie obtient le droit de propriété et l'autre le droit de recevoir son paiement.

1. La plus haute institution judiciaire des USA.

2. Le quatrième amendement institue le droit des personnes à se prémunir de recherches excessives dans leurs personnes, foyers, effets personnels etc.

Droits individuels effectifs et pratiques

Un droit, au sens juridique, fournit à un sujet de droit soit des pouvoirs spécifiques pour agir en relation avec les autres, soit la liberté d'assurer que d'autres vont se retenir d'interférer avec l'objet de leur droit. On peut penser qu'on sait intuitivement ce qu'est un droit, mais sa définition peut poser plus de problèmes qu'elle n'en résout. Hohfeld propose une de ces définitions et soutient qu'un droit tel que le droit de propriété est en fait une combinaison :

de revendications (*claim right*) corrélées à des **devoirs**. Si je revendique mon droit de propriété sur un livre que je t'ai acheté, tu as le devoir de me transférer le droit de propriété de ce livre (et le livre, bien entendu).

de privilèges ou libertés (*liberty*) corrélées à la **non-revendication**. Si je possède un livre, personne ne peut revendiquer que je n'ai pas le droit de le jeter à la poubelle.

de pouvoirs ou autorités/compétences corrélés à des **responsabilités** (*liabilities*). En tant qu'employeur, si j'exige de mes employé·es qu'ils effectuent une tâche dans le cadre de leurs fonctions, ceux-ci sont responsables d'effectuer la tâche en question.³

d'immunités corrélées à des **défauts d'autorité**. En tant qu'employé je possède une immunité contre des demandes illégales de mon employeur, qui lui-même n'a pas autorité ici.

Cette définition ne résout pas les problèmes que l'on peut rencontrer dans le vrai monde. Elle a par ailleurs été largement critiquée comme étant parfois incohérente, notamment car sa terminologie entre en contradiction avec celle du droit positif (comme le terme *liability* par exemple).⁴ Cependant, elle a le mérite de mettre en évidence que les droits sont des relations entre sujets de droit, telles qu'une **revendication** ou une **compétence** ; et que ces droits correspondent à des **devoirs** ou des **absences de droits**.

Par contre, Hohfeld ne tient pas ou peu compte de :

- la différence entre droits *erga omnes* — que l'on peut invoquer contre toutes (tels que le droit de propriété) — et droits *ad personam* — que l'on ne peut invoquer que contre des sujets spécifiques, comme le droit des contrats.
- la différence entre un droit qu'une ou plusieurs personnes agissent d'une certaine façon et un droit que certain·es se retiennent d'interférer avec un objet spécifique.
- la différence entre les droits d'entités privées basés sur le droit privé et les droits des autorités publiques, que tout le monde est censé suivre, basés sur le droit public.

Hildebrandt met un accent sur le fait que les droits individuels entre personnes sont une invention récente, généralement attribuée à Hugo Grotius au XVI^{ème} siècle, en aucun cas un attribut naturel.

Les droits individuels dépendent donc de l'institution de l'État de droit, c'est-à-dire d'une distribution des compétences publiques par le biais d'un système constitutionnel de freins et de contrepoids, ainsi que de droits fondamentaux effectifs et pratiques dont la mise en application est désarticulée du pouvoir décisionnel arbitraire du gouvernement.

2.1.3 Raisonnement juridique

Si l'on comprends le droit en termes de conditions et d'effets juridiques, la prééminence de l'interprétation et de l'argumentation devient clair. Le raisonnement juridique n'est pas simplement une affaire de méthode, mais plutôt de justification. Ceci implique d'établir les faits,

3. Vous m'excuserez de l'exemple malheureux.

4. Bien que les contextes soient différents.

identifier les normes légales en vigueur, interpréter les faits au regard de ces normes et interpréter les normes au regard des faits. Parfois, certaines normes peuvent avoir des conséquences contradictoires, ce qui conduit à prendre des décisions donnant la priorité à certaines normes sur d'autres. La justification peut aussi être vue comme un syllogisme :

- Si a alors b (norme)
- On est dans le cas a (faits)
- Conclusion : b (effet juridique)

Cependant, le raisonnement juridique ne doit pas être vu comme un acte mécanique : c'est avant tout un problème d'argumentation plutôt que de logique pure, qui se base sur l'expérience et l'expertise. On peut dire que l'étude du droit est l'étude des conditions et des effets juridiques, ou encore que c'est savoir anticiper les décisions des cours de justice (et le raisonnement ayant mené à une décision). Oliver Wendell Holmes écrivait à ce sujet «Les prophéties de ce que feront les cours dans les faits, rien de plus prétentieux, sont ce que j'entends par *le droit*.»

2.2 Qu'est-ce que le droit en démocratie constitutionnelle

Le droit est intimement lié à la politique (qui décide du droit ?) ainsi qu'à la morale (qu'est-ce qui doit prévaloir ?). À bien des égards, le droit, la politique et la morale sont *mutuellement constitutifs*, c'est-à-dire que chaque domaine participe à la constitution des deux autres. Cependant, au sein d'une démocratie constitutionnelle, le droit, la politique et la morale ne peuvent pas être reliés n'importe comment.

Tout d'abord, le droit façonne le terrain politique. Les pouvoirs législatifs, administratifs et juridictionnels sont donc à la fois contraints et permis par le droit : il fournit le cadre pour leur fonctionnement.

Ensuite, dans une certaine mesure, le droit façonne le terrain qui permet aux individus, aux entreprises et aux gouvernements d'agir de manière éthique. Le droit n'est pas équivalent à l'éthique, qu'il n'impose pas de manière univoque par ailleurs, mais offre un cadre qui doit favoriser la réflexion éthique (en théorie).

Enfin, en démocratie constitutionnelle, le droit contraint et autorise à la fois la politique et l'éthique de manière spécifique. Selon Hildebrandt, la démocratie n'est pas la dictature de la majorité mais un système de freins et de contrepoids, dont la majorité gouvernante se doit de considérer que les minorités peuvent devenir majoritaires.

2.2.1 Droit, morale, politique et nature des règles juridiques

Un des philosophes du droit les plus connus, Herbert Hart, explique dans *Le concept du droit* le sens du droit, et notamment en quoi il diffère de la morale et de la politique. Il pose pour cela trois questions :

En quoi le droit est-il comparable et en quoi diffère-t-il d'ordres sous la menace, autrement dit du commandement ?

Le droit est comparable au commandement car :

- il a du pouvoir (*it has teeth*),⁵
- il suppose une autorité étatique et,

5. On pourrait aussi le traduire par le fait qu'il ait suffisamment de pouvoir et de support de la part des autorités pour contraindre à l'obéissance ou pour punir les contrevenant·es.

— il dépend de la souveraineté mais la constitue par là-même.

Une différence entre les deux, qu'il cite parmi d'autres, réside dans le fait que le droit s'applique à celles et ceux qui le promulgue (du moins en principe).

En quoi l'obligation légale se rapporte et diffère-t-elle de l'obligation morale ?

Le droit diffère de l'obligation morale en ce que :

- il a du pouvoir,
- il intègre des règles primaires, avec des règles secondaires qui déterminent la validité des règles primaires (définies ci-après).

Les deux notions sont comparables car avoir une obligation légale comme morale suppose :

- l'existence d'un standard,
- l'application à une personne en particulier,
- application qui peut contrevenir aux intérêts de la personne en question.

Que sont les règles et en quoi le droit est-il une affaire de règles ?

- Les règles légales sont des règles au sens de l'*obligation* et non pas au sens de *régularités*.
- Les règles répondent à un point de vue interne, *i.e.* violer une règle n'empêche pas de rester obligé de s'y soustraire : la possibilité de désobéir est constitutive au droit.

Ce qui amène une quatrième et dernière question :

Qu'est-ce qui détermine la validité des règles légales ?

D'après Hart, c'est le droit lui-même qui détermine cette validité. Pour cela, il propose deux types de règles (déjà mentionnées plus-haut) :

Les règles primaires Ce sont les règles qui *régulent* nos interactions en imposant une prescription ou une prohibition («Tu ne tueras point»)

Les règles secondaires Ce sont les règles constituantes qui déterminent la validité des règles primaires et l'effet légal en cas de violation.

Toujours selon Hart, les règles secondaires confèrent du pouvoir, par exemple celui pour un parlement de décider ce qui doit se passer en cas de meurtre. Tout ceci met en évidence la nature systémique et architecturale du droit positif qui consiste en 1) un système complexe et cohérent de règles primaires qui clarifient ce qui est attendu, supporté par 2) des règles secondaires qui permettent de tester si une règle primaire est effectivement valide.

2.2.2 Certitude juridique, justice, instrumentalité

La philosophe conclut le chapitre grâce aux travaux de Radbruch (le droit comme **certitude juridique, justice** et **instrumentalité**). Radbruch a servi comme Ministre de la Justice dans les années 1920, il a donc vécu la montée du nazisme et pour lui, la tension entre ces trois buts du droit n'est donc pas du pinaillage.

La **certitude juridique** fait référence au besoin de fournir une réponse prédictible à l'action d'une personne afin de créer de la confiance sociale (*societal trust*). Cette certitude implique donc la notion d'équité de la loi.

La **justice** quant à elle fait référence à l'égal traitement de cas égaux et au traitement inégal de cas inégaux, dans la mesure de leur inégalité. Ce but est directement connecté à la certitude

juridique en ce que cela permet aux individus de planifier et d'anticiper comment leurs actions seront interprétées par la loi et répondues par le gouvernement. Certains (*e.g.* Dworkin) disent même que la justice va au-delà de la simple cohérence : elle répond à l'intégrité des règles, des principes et des politiques, assurant par là que chaque décision juridique prise le soit en accord avec la philosophie qui fonde le droit.

Enfin, l'**instrumentalité** fait référence au fait que le droit est un instrument pour accomplir divers buts qui sont en partie externes à ces propres opérations. Ces buts peuvent être à un niveau politique (telle que la législation) ou au niveau des sujets du droit (au sens large) qui peuvent donc s'en servir pour leurs intérêts propres (comme le droit privé), leurs droits et libertés.⁶

À la fin de la seconde guerre mondiale, Radbruch écrivit un court texte intitulé «5 minutes de philosophie du droit», dans lequel il explique en quoi ces trois buts peuvent être parfois antinomiques, en s'appuyant sur le cas concret du nazisme qui, selon lui, a instrumentalisé le droit au détriment de la justice et de la certitude juridique.

Ce chapitre est conclut en précisant que dans une démocratie constitutionnelle, les règles juridiques qui confère du pouvoir contraignent ce dernier de manière simultanée ; elles fournissent des fonctionnalités protectrices, servant ainsi la double instrumentalité du droit comme outil pour le gouvernement et comme protection.

6. Pour approfondir, je vous invite à lire le cours d'Alain Supiot au Collège de France *Du gouvernement par les lois à la gouvernance par les nombres* disponible librement à https://www.college-de-france.fr/media/alain-supiot/UPL2335835739398687161_supiot.pdf. Le cours traite avec une perspective orthogonale cette question de l'instrumentalité.

Chapitre 3

Les domaines du droit : droit privé, droit public et droit pénal

L'informatique peut être divisé en plusieurs sous-disciplines, telles que l'ingénierie logicielle, ce qui a trait aux sciences cognitives ou à l'apprentissage automatique. Le droit quant à lui est généralement divisé entre le droit privé, le droit public et le droit pénal ; chaque domaine possédant son vocabulaire spécifique, ses principes et ses structures. Ce chapitre examine tout d'abord les différences conceptuelles entre ces domaines, ce qui permet par la suite d'introduire leurs caractéristiques. Ce tour d'horizon est central à la compréhension de domaines plus spécifiques comme le droit à la protection des données ou le copyright qui constituent la seconde partie du livre.

3.1 Droit privé, droit public, droit pénal : les différences conceptuelles

Le droit peut être vu comme un système de *relations légales* entre *sujets de droit* à l'égard d'*objets juridiques*.

3.1.1 Droits absolus et droits relatifs

Le droit de propriété est souvent décrit comme la relation entre un sujet de droit (*e.g.* une personne physique) et un objet juridique (*e.g.* une maison), en énonçant que le sujet a un droit sur l'objet. Lorsqu'un sujet de droit impose un devoir de non-interférence sur un objet juridique à *tous* les autres sujets de droit, on dit qu'il possède un **droit absolu** sur cet objet juridique. Ici absolu ne veut pas forcément dire illimité : un propriétaire immobilier ne peut pas rentrer à sa guise dans une maison qu'il loue ; il est par contre le seul propriétaire face à toutes les autres personnes. Un **droit relatif** lui ne concerne qu'un nombre limité de sujets. C'est le cas d'un contrat qui n'engage que les parties signataires.

3.1.2 Droit privé et droit public

Plusieurs critères ont été proposés pour établir une démarcation entre le droit privé et le droit public, mais aucun n'est vraiment satisfaisant. Au final, on définit généralement le droit public comme étant constitué du **droit constitutionnel**, du **droit administratif** ainsi que

du **droit public international**. Hildebrandt en déduit que le droit public est le domaine où le gouvernement agit *en tant que tel*, c'est-à-dire en tant qu'autorité publique soumise au principe de légalité; il suit que le droit privé est le domaine où le gouvernement n'agit pas *en tant qu'autorité publique*. Elle observe aussi que le gouvernement est censé agir dans l'intérêt général, ce qui soulève la question du but du droit privé. Ce dernier fournit un cadre pour les actes des individus : le droit privé est intimement lié à la notion d'**autonomie individuelle**, mais aussi à celle de **confiance sociétale**. En prenant en exemple le droit de la protection des consommateurs, elle ajoute que le droit privé est aussi lié à la *fairness*.¹ Pour revenir à la question de l'intérêt général comme but du droit public, celui-ci est contraint par le principe de légalité, qui impose qu'un acte d'un gouvernement soit régi par une base légale (généralement compris comme étant validé par une Constitution).

3.1.3 Droit privé et droit pénal

Pour bien comprendre la différence entre droit privé et droit pénal, il faut s'intéresser à la différence entre un acte illégal et un acte répréhensible (*punishable*). Un acte répréhensible est forcément illégal, mais ce n'est pas tout le temps réciproque. Le droit pénal exige non seulement qu'un acte soit répréhensible, mais aussi qu'il ait préalablement été défini en tant que crime. Ainsi une violation de contrat, bien qu'illégale, n'est pas criminelle et ne réponds donc pas du droit pénal.² Un acte criminel doit être défini en tant que tel dans le **droit objectif** qui est constitué de l'ensemble des règles primaires et secondaires (voir Section 2.2.1) ainsi que des principes implicites valides au sein d'une juridiction.³

3.2 Droit privé

Le droit privé peut être divisé en tant que :

- droit de la famille (non traité dans l'ouvrage)
- droit des contrats
- droit des biens
- droit de la responsabilité civile (*tort law*)

Petit rappel : nous avons vu ci-avant que le droit privé régissait les interactions entre sujets de droit (à l'exception du gouvernement) de manière horizontale.

3.2.1 Droit des biens : transfert de biens mobiliers

La question de propriété est centrale en droit des biens : est-ce qu'avoir un *urnom* est la même chose qu'avoir un *livre*? Vendre un livre qu'on nous a prêté entraîne-t-il un transfert de propriété? Pour répondre à ces questions, on définit généralement le transfert de la propriété d'un bien mobilier par trois caractéristiques cumulatives⁴ : la **transmission** en vertu d'une **base légale** par la personne détentrice du **pouvoir de disposition**. Pour revenir à l'exemple, la vente du livre prêté, bien que remplissant les conditions de transmission et de base légale (imaginons un contrat de vente), ne réponds pas à l'exigence de pouvoir de disposition : elle est donc *a priori* caduque. Cependant, certaines juridictions (comme aux Pays-Bas) valident juridiquement un transfert sans pouvoir de disposition, mais à condition que : le bien soit **mobilier**, que le

1. *Fairness* peut être traduit par équité ou justice, mais a un sens à part dans la langue anglaise.

2. Notons qu'un acte illégal peut être répréhensible sans être criminel.

3. Le droit objectif attribut ce qu'on appelle des **droits subjectifs**.

4. Cumulative signifie que les trois caractéristiques doivent être remplis, et pas l'une OU l'autre.

transfert ne soit **pas gratuit** et que la partie acquérante soit de **bonne foi**. Toujours dans notre exemple, si l'acheteur sait que le vendeur ne possède pas le livre, alors le transfert est caduque.

3.2.2 Droit des contrats et droit des biens : vente et transfert d'un bien immobilier

Que signifie juridiquement vendre une maison? La vente d'un bien immobilier est régie par le droit des contrats, celui-ci demande à ce qu'un accord consiste en : un **acte juridique** établi **multilatéralement**, par **une des parties ou plusieurs** avec une **obligation envers une partie ou plus**. Un acte juridique exige l'intention par la personne agissante d'établir un effet juridique (voir Section 2.1.2) et cette intention doit être exprimée par une déclaration (pas forcément écrite). Dans le cadre d'un contrat de vente, celui-ci doit remplir deux conditions supplémentaires : l'acheteur doit payer le prix convenu et le vendeur doit transférer la propriété. Adoptons l'exemple vu plus haut à la vente d'une maison dont le vendeur ne possède pas la propriété (il n'est que locataire). Ici, le transfert de propriété ne peut être effectué : on est confrontés à une violation de contrat, qui peut entraîner une responsabilité pour les dommages éventuellement causés. On notera que la propriété d'un bien immobilier est constatée dans un registre public (car on ne peut pas se balader avec, par définition).

3.2.3 Responsabilité civile

Pour comprendre le droit de la responsabilité civile (*tort law*), il faut distinguer un acte juridique d'un fait juridique. Nous avons vu plus haut qu'un acte juridique est une action qui cherche l'effet juridique que le droit attribut, par exemple la validité d'un contrat, la validité d'une volonté (*will*) ou la législation en vigueur. Un fait juridique est quant à lui une occurrence, un statut ou un acte qui est juridiquement pertinent en ce que le droit lui attribut un effet juridique, et ce, indépendamment d'une intention (*intent*), telle qu'une naissance (qui attribut la subjectivité juridique), une mort (héritage) ou un délit civil (*tort*).

La complexité du droit de la responsabilité civile est illustré avec l'affaire *de la trappe de la cave*, dans laquelle un client est tombé dans un cellier laissé ouvert par un employé de Coca-Cola négligent. Bien qu'on considère généralement qu'une personne soit responsable de ses actes (ici, de tomber dans la trappe) et qu'on ne puisse attribuer sa propre malchance à d'autres, il y a quelques exceptions telles que les délits civils. Un délit civil est défini (en droit néerlandais) comme un acte délictuel (illégal) causé par une personne (à laquelle on peut attribuer cet acte) envers une autre personne qui souffre de dommages suite à cet acte. Une omission peut tout à fait être considérée comme un acte en soit, la responsabilité peut découler d'une culpabilité directe ou d'une responsabilité plus ou moins directe (Coca-Cola en tant qu'employeur par exemple). Reprenons notre exemple : est-ce que Coca-Cola est responsable des dommages induits par la chute du client dans la trappe? Un premier jugement a déterminé que ce n'était pas le cas, l'employé aurait dû faire plus attention. Un second jugement a contredit le premier en indiquant que l'employé de Coca-Cola aurait dû mettre en place des mesures pour prévenir cet incident (les clients ne font pas forcément aussi attention que nécessaire). En conclusion : un jugement est une chose cruciale bien que complexe!

3.3 Droit public et droit pénal

Nous avons vu plus haut que le droit public doit pouvoir être justifié par l'intérêt général. L'État peut agir dans ses intérêts au nom de l'intérêt général, mais les deux ne doivent pas être confondus. Dans une démocratie constitutionnelle, l'État doit non seulement agir en vue de

l'intérêt général, mais aussi en fonction du principe de légalité ainsi que de l'égal respect pour ses citoyen·nes. Ces exigences sont aussi vraies pour le droit pénal, qui implique une des compétences les plus invasives de l'État : le *ius puniendi* (le droit de sanction). Le droit pénal est souvent classé comme un sous-domaine du droit public en ce qu'il constitue et régule les relations entre l'État et ses concitoyen·nes.

3.3.1 Droit public

Le droit public considère d'un côté les relations État-citoyen·nes et d'un autre côté les relations d'État à État. Le premier aspect est constitué du droit constitutionnel et administratif, tandis que l'autre est constitué du droit public international. Le droit constitutionnel et le droit public international ont plusieurs liens entre eux : la constitution détermine (en partie) dans quelle mesure le droit international peut avoir priorité sur le droit national en cas de conflit ; le droit international peut aussi définir lui-même la priorité, en cas de crime contre l'humanité par exemple. Le droit international sera discuté dans le prochain chapitre.

Droit constitutionnel

Le droit constitutionnel attribue les compétences :

- de légiférer et de réguler ;
- d'agir et de décider sur la base de son autorité publique (gestion du trafic, protections environnementales ...) ;
- de statuer (droit pénal, droit privé, droit administratif).

Ces compétences sont attribuées au législateur (parlement, municipalités), aux autorités publiques (cabinets ministériels, agences environnementales etc) et aux cours de justice. Le droit constitutionnel restreint les compétences qu'il attribue en exigeant des garde-fous qui limitent les pouvoirs alloués.⁵

Droit administratif

Le droit administratif régule la conduite du gouvernement et d'autres agences d'autorité publique, par exemple dans les domaines du droit environnemental, du droit de la santé publique ou du droit fiscal. Il répond au principe de légalité et exige donc un fondement juridique pour chacune des actions et décisions effectuées ou prises par les autorités publiques. Cette base légale constitue les compétences des autorités pour prendre des décisions qui peuvent concerner tant la voirie que les taux d'émissions réglementaires de véhicules motorisés. Les citoyen·nes concerné·es ont le devoir d'obéir aux décisions prises, décisions qui sont souvent considérées comme légitimes bien que cela puisse être contestable (moralement, comme légalement devant un tribunal). Ce principe de légalité limite ainsi les compétences des autorités publiques en même temps qu'il fonde leurs pouvoirs. En plus de ça, certaines juridictions ont développées des principes implicites qui peuvent avoir force de loi, tels que les principes de *confiance et d'attente légitime*, de *proportionnalité* ou de *subsidiarité*.⁶

Les recours juridiques forment un garde-fou crucial dans le contexte du droit administratif, car ils donnent la compétence aux citoyen·nes de faire appel aux décisions prises par les autorités

5. On parle ici de la théorie du droit, en pratique tout ceci peut être sujet à débat.

6. Notons qu'on peut voir en droit international et supranational ces principes inscrits de manière explicite. Par exemple, le Traité sur l'Union européenne, aussi appelé traité de Maastricht, mentionne les principes de proportionnalité et de subsidiarité dans son Article 5, article auquel le RGPD fait référence, RGPD que l'on discutera plus loin dans le document.

publiques. L'autrice conclut cette section en démystifiant l'idée qu'un gouvernement est forcément tout puissant face à des contre-pouvoirs : les freins et contrepoids de l'État de droit doivent être constamment réinventés, ni tenus pour acquis ni niés dans leur impact.

3.3.2 Droit pénal

Le droit pénal est habituellement divisé en droit substantiel et en droit procédural. Le premier définit les droits et obligations dans un système juridique donné (quelles actions peuvent être qualifiées de criminelles), tandis que le second précise comment on peut faire valoir ces droits. Autrement dit : le droit procédural permet aux règles substantives de s'exercer.

Droit pénal substantiel

Le droit pénal substantiel détermine quelle conduite est punissable et quelle est la sanction à appliquer. Le principe de certitude juridique (vu dans la Section 2.2.2 notamment) implique que l'infraction soit précisément définie. Ce principe est par ailleurs renforcé et protégé par le principe de légalité du droit pénal, encore plus rigoureux que le principe général de légalité. On appelle ce principe en droit pénal *lex certa*, il garantit une définition raisonnablement précise des infractions, afin de ne pas inclure outre mesure des comportements, ainsi qu'une protection contre une application rétroactive.

Mais le *lex certa* n'est pas tout le temps absolu. Ainsi, un ingénieur a été condamné à 40 mois de prison ferme suite à l'affaire Volkswagen, au sein de laquelle il a été jugé coupable (en partie) bien que n'étant pas la tête pensante.⁷ La condamnation a été perçue comme sévère, on voit ici que le jugement n'était pas seulement basé sur la rétribution du crime, mais aussi sur la volonté de dissuasion : plutôt que de chercher à traduire en justice toutes les suspectes d'infractions, le jugement participe à inciter certains comportements. Un acte criminel peut ne pas être condamné en vertu des justifications et excuses invoquées. Ainsi, par exemple, une personne en tuant une autre volontairement peut ne pas être condamnée si la légitime défense est justifiée. Ce qui nous amène à la **structure** d'une infraction criminelle, qui détermine sa punissabilité. Une infraction est composée de :

L'*actus reus* (l'acte et sa qualification), elle-même définit par :

- une action (ce qui concerne le droit de la preuve dans une procédure criminelle)
- qui tombe sous la coupe d'une infraction criminelle (la qualification d'une conduite comme criminelle dans une procédure criminelle).

Ainsi que des *mens rea* (les éléments), définits par :

- l'illicéité (*wrongfulness*) (ici, qui concerne la justification) ;
- la culpabilité (qui a trait à la disculpation ou à l'excuse dans ce contexte).

Procédure pénale et enquête de police

La structure d'une infraction pénale est intimement entrelacée avec la procédure pénale qui l'accompagne. En effet, une condamnation doit répondre positivement aux questions suivantes :

- la conduite imputée doit être prouvée au-delà d'un doute raisonnable, une défense réduite au cas minimale étant : *ce n'est pas moi*
- la conduite doit être qualifiée de criminelle (au nom du principe de légalité), une défense étant : *la conduite n'est pas condamnable*

7. Le groupe allemand a été condamné en 2017 pour avoir triché sur les émissions de gaz polluants.

- l'action était injustifiée, une défense étant : *j'avais une permission*
- lae justiciable est coupable (ne peut être excusé·e), une défense étant : *j'avais une excuse*.

Dans le contexte d'une procédure pénale, le terme *principe de légalité* est utilisé pour l'ensemble des corps impliqués (police, procureur), mais il revêt une signification particulière en ce qu'il réfère aussi à l'idée que toutes les conduites criminelles doivent être traduites en justice. Cette interprétation s'oppose à l'idée que seul le procureur général a le pouvoir discrétionnaire de décider d'entamer des poursuites ou non. La jurisprudence a ainsi clarifié que le procureur général (en tout cas dans la législation néerlandaise) doit développer une politique spécifiant le critère utilisé pour déterminer ou non une poursuite judiciaire. Dans la législation néerlandaise, le procureur général a publié une doctrine concernant la (non-)criminalisation des drogues douces.

Certaines théories de la justice souligne que la sanction est la juste rétribution pour la violation de normes ; d'autres que la sanction est là pour prévenir de futurs crimes. La plupart des juridictions combinent ces deux interprétations. En Europe, tout jugement doit résulter d'un procès équitable (Article 6 de la Convention européenne des droits de l'homme), ce qui se traduit par six principes :

- la présomption d'innocence
- le droit à un tribunal indépendant et impartial
- l'égalité de moyens entre le procureur et le défendeur
- l'immédiateté de la présentation et de l'analyse des preuves devant la cour
- la publicité externe (*external publicity*)
- le droit a une décision dans un temps raisonnable.

Ces droits garantissent que le justiciable peut contester la légalité d'une enquête de police, et que la charge de la preuve repose sur le procureur général. Cela garantit aussi qu'en principe, toutes les mesures prises avant un jugement ne doivent pas l'être pour sanctionner.

Le chapitre se conclut sur quelques considérations à propos des procédures de droit privé. **Tout d'abord**, les principes de procès équitable (énoncés ci-dessus) s'appliquent aussi à la détermination des droits et obligations civils d'une personne. **Ensuite**, dans les procédures de droit privé, la règle de base est que quiconque initie une procédure porte la charge de la preuve. **Troisièmement**, tandis que le standard de preuve en droit pénal est *au-delà du doute raisonnable*, la simple plausibilité en droit privé peut suffire. **Enfin**, la requête du plaignant est normalement accordée si le défendeur ne conteste pas la preuve : en droit privé, les parties sont considérées comme autonomes, capables de décider entre elles du périmètre et de la forme du conflit ; tandis que cette autonomie des parties n'existe pas en droit pénal, où la sanction d'une personne innocente est à éviter même si le défendeur et le procureur concluent un accord.

Chapitre 4

Droit international et droit supranational

Le droit international a été considéré dans le passé comme un sujet mineur et un objet d'étude à part. Aujourd'hui, il est clair que l'étude du seul droit national n'est pas seulement *provinciale*, mais traduit aussi le manque d'exigence que requiert l'étude du droit positif. En effet, le droit positif, c'est-à-dire le droit applicable à un moment donné sur un territoire donné, dépend bien souvent de lois internationales, voire supranationales comme c'est le cas en Europe. Par exemple, les droits fondamentaux ne font pas seulement partis de constitutions nationales, mais peuvent aussi être invoqués sur la base de la Convention européenne des droits de l'homme¹ (CEDH), ou depuis 2009 la Charte des droits fondamentaux de l'Union européenne (CDFUE). Notons au passage que les droits humains ne sont pas les seuls concernés, puisque d'autres sujets sont aussi concernés : la cybercriminalité avec la Convention sur la Cybercriminalité (Convention de Budapest, CC), ainsi que tout le corps législatif européen.

Ce chapitre est d'autant plus crucial pour les informaticien·nes que les systèmes étudiées en informatique sont rarement cantonnés à un seul pays. Nous nous focaliserons ici sur le droit international dans le contexte du Conseil de l'Europe², et dans le droit supranational de l'Union Européenne (UE). Ça ne veut pas dire que ce passage n'intéressera pas les informaticien·nes d'autres continents³, car en effet nous nous intéresserons à fournir un cadre pour comprendre *comment le droit opère*, et ce grâce à des exemples tirés du droit international et supranational.

Nous aborderons ce chapitre en présentant le concept de juridiction, puis nous nous présenterons une vue d'ensemble du droit international et supranational.

4.1 Le concept de juridiction dans les systèmes juridiques occidentaux

Le concept de juridiction est apparu au début du XIV^{ème} siècle et bien qu'il soit étroitement lié au concept de territoire, ce dernier concept est lui apparu un peu plus tard au début du XV^{ème} siècle. Le terme juridiction a deux significations :

1. Notons ici la particularité linguistique française qui est une des rares à voir choisi un terme genré, quand par exemple le nom anglais est très clairement *humain*.

2. À ne pas confondre avec le Conseil Européen et le Conseil de l'Union Européenne. Désolé ce n'est pas moi qui choisit la terminologie.

3. Je doute cependant qu'ils lisent cette synthèse.

- la compétence du juge de rendre justice (légiférer, statuer, mettre en application)
- par extension, le territoire sur lequel une entité a juridiction au sens premier du terme.

On peut même ajouter une autre distinction entre :

- la juridiction interne, qui est la compétence de rendre justice au sein de son État
- la juridiction extra-territoriale, qui est la compétence de rendre justice sur le territoire d'un autre État.

Petit point linguistique : le terme *power* est utilisé aux États-Unis alors qu'on préfère *competence* en Europe. Le contour de cette compétence (ou de ce pouvoir) soulève des questions stimulantes bien que difficiles, comme la mesure avec laquelle un État peut décider des limites entre sa propre juridiction et une juridiction internationale sur son territoire. Pour compléter ce point linguistique, notons que l'essentiel de l'étude juridique sur la définition de ce contour ayant été effectuée par des germanophones, on appelle cette question la *kompetenz-kompetenz*⁴.

4.1.1 Un exemple

Pour illustrer la *kompetenz-kompetenz*, rien de tel qu'un exemple matrimonial. Que se passe-t-il si Alice (néerlandaise) se marie à Bob (états-unien) au Japon alors qu'ils vivent en Russie ? Quel droit s'applique pour leur mariage : le droit néerlandais, états-unien, japonais ou russe ? Même question pour un éventuel divorce ? Poussons le vice un peu plus loin : qu'en est-il s'ils veulent faire reconnaître leur divorce néerlandais en Iran ? Cet exemple soulève trois types de questions, à savoir : 1) le droit applicable, 2) la cour compétente et 3) la mise en application.

Les questions relatives au droit applicable demandent quel droit national détermine les conséquences légales du mariage. Ça dépend de plusieurs choses mais le droit national prévaut ultimement, on appelle ça la *primauté du droit national*. Son implication dans le cas présent est qu'une personne est considérée comme mariée dans son pays de résidence même après un divorce (juridiquement valide) au sein d'une autre juridiction.

Le second type de questions concerne la juridiction au sens de la compétence juridictionnelle. Si quelqu'un se marie en Russie sous le droit japonais, quelle cour est compétente pour décider d'un divorce ? Est-ce que ça dépend du droit du pays de résidence, de la nationalité de la personne concernée ou du pays dans lequel le mariage a eu lieu ?

Le troisième type de question, assez proche du second, concerne la reconnaissance et la mise en application. Dans quelles conditions un divorce est-il reconnu et mis en application dans un autre pays ?

L'exemple choisi ici parle de droit de la famille, mais les questions sus-citées se posent tout aussi bien dans des domaines tels que le commerce de biens et de services, l'investissement, les conditions de travail au sein de multinationales etc. Ces questions peuvent être complexes et mettent en évidence la nécessité de traités internationaux simplifiant ces questions en clarifiant leurs réponses.

4.1.2 Juridiction nationale

Que se passe-t-il si les Pays-Bas décide de supprimer le premier article de leur Constitution ? Ou plus plausiblement, de protéger ses citoyens·nes de cyber-attaques russes ou états-uniennes ? On mentionnait plus haut la primauté du droit national, on discutera ici de ses limites ainsi que de ses relations avec le droit international et supranational. En effet, comment assurer la certitude juridique (concept vu à la Section 2.2.2) dans un contexte où les normes juridiques

4. Terme non-traduit par l'autrice, que nous conserverons ici pour le distinguer de la signification vulgaire du terme compétence.

peuvent être incompatibles ? La manière la plus simple est de considérer que le droit est un système hiérarchiques de règles juridiques, dans lequel certaines règles prévalent sur d'autres. Par exemple, la Constitution prévaut sur les Actes du Parlement, qui eux-même prévalent sur les règles provenant d'autres autorités publiques (telles que les municipalités). Cette hiérarchie fonctionne assez bien au sein d'un seul État, du fait qu'il ait à la fois une souveraineté interne et externe. Le concept de souveraineté dans ce sens particulier découle des traités de 1648 dits de Westphalie, qui ont mis fin à une sanglante période de guerre en Europe au XVI^{ème} et XVII^{ème} siècles. Ces guerres étant notamment des guerres de religion entre catholiques et protestants, les traités déclaraient que la religion était une affaire privée, établissant ainsi l'idée d'État-nation doté de frontières, au sein desquelles le souverain exerce une souveraineté dite **interne**, tandis qu'il doit respecter les autres souverains et leur souveraineté (on parle alors de souveraineté **externe** ou de principe de non-interférence).⁵ Ces deux concepts sont en fait les deux faces de la même pièce : l'une ne peut exister sans l'autre. Ainsi, le droit international devient le droit entre États souverains (et indépendants), il dépend donc du consensus entre ces États. On touche ici du doigt la différence fondamentale entre le droit international et le droit supranational : le second dépend d'un transfert partiel de souveraineté.

Résumons :

- les États ne sont contraints par le droit international et supranational que s'ils le décident, cependant
- le jeu de pouvoir entre les États et d'autres entités dotées de puissance (telles que des multinationales) conteste cette hypothèse, de plus
- de nombreuses règles en droit international ne dépendent pas du consentement des États, mais plutôt de ce qui constitue une conduite légitime (les crimes contre l'humanité par exemple)

Dans le cadre du droit supranational, ça devient encore plus complexe car les États cèdent une partie de leur souveraineté afin de permettre une collaboration et une coordination au sein de la juridiction de l'UE. Rappelons enfin que :

- alors que les juridictions nationales sont mutuellement exclusives entre les États, les juridictions nationales, supranationales et internationales se superposent souvent, et
- la souveraineté des États dépend d'un système de droit international qui à la fois *suppose* et *attribue* cette souveraineté (comme nous le verrons en détails plus tard).

4.2 Droit international

La section précédente exposait que les principaux acteurs du droit international sont les États souverains. Cependant, d'autres entités participent aussi à ce domaine, telles que les organisations internationales (e.g. l'Organisation Mondiale du Commerce ou les Nations Unies), les multinationales (e.g. Alphabet, Total), les ONGs (e.g. Greenpeace) et même des individus.

5. Note personnelle : ces traités établissant formellement des concepts de souveraineté et de territoire, ils sont décisifs dans la création de ce qu'on appelle l'État *moderne*. J'invite les lectrices intéressées à lire le recueil de cours au Collège de France *Sur l'État* de Pierre Bourdieu, ainsi que divers livres et interventions d'Alain Supiot (je pense en particulier à sa chaire au Collège de France *État social et mondialisation : analyse juridique des solidarités*, qui traite de manière extensive du féodalisme et de la genèse de l'État moderne). Je préviens toutefois que ces ouvrages ne sont pas exactement accessibles, notamment à des informaticien·nes.

4.2.1 Sources du droit international

Les sources du droit ont la même fonction en droit international qu'en droit domestique, c'est-à-dire qu'elles déterminent l'identification des normes juridiques applicables. Puisque le droit international dépend du consentement des États souverains, une source évidente est donc les traités internationaux. Citons quelques exemples tels que la Convention sur la Cybercriminalité (2001) et la Convention de Bern (notamment connue pour avoir été amendée en 1952 sur le droit d'auteur).

Cependant, les traités ne sont pas la seule source du droit international. L'Article 38 du Statut de la Cour Internationale de Justice de la Haye⁶ énonce ainsi que le droit applicable l'est en fonction de :

- les conventions internationales, soit générales, soit spéciales, établissant des règles expressément reconnues par les États en litige ;
- la coutume internationale comme preuve d'une pratique générale, acceptée comme étant le droit ;
- les principes généraux de droit reconnus par les nations civilisées ;
- sous réserve de la disposition de l'Article 59, les décisions judiciaires et la doctrine des juristes publicistes les plus qualifiés des différentes nations, comme moyen auxiliaire de détermination des règles de droit.

La plupart des livres sur le droit international résume les dites sources à :

- le droit coutumier (*usus, opinio necessitatis*)
- les traités (déjà mentionnés dans ce texte à plusieurs reprises)
- les principes généraux du droit (promotion des droits humains, auto-détermination des peuples, limitation de l'usage de la force entre les États, etc)
- les jugements et la doctrine (les décisions de corps spécialisés des Nations Unies)
- les actions unilatérales (le droit international doit accepter certaines pratiques comme le rejet de certaines coutumes, ou le rejet par certains États de jugements par des juridictions qu'ils ne reconnaissent pas)
- le *jus cogens* et les obligations *erga omnes* (le droit contraignant et les obligations absolues, indépendant du consentement des États, ça concerne les violations les plus flagrantes de la dignité humaine telles que les génocides).

4.2.2 Monisme et dualisme en droit international

Comment le droit international s'impose-t-il à un État sujet à sa juridiction ? Sous quelles conditions est-ce que le droit international a un effet direct, c'est-à-dire qu'il fournit directement des droits aux citoyen·nes ? La doctrine fait une distinction analytique entre deux approches de la relation entre le droit national et international : l'approche *moniste* et l'approche *dualiste*.

Une approche **moniste** ne reconnaît qu'un seul ordre hiérarchique juridique, dans laquelle le droit international prévaut sur le droit national. La conséquence de cette approche est que les traités internationaux prévalent sur les lois nationales, les citoyens peuvent en appeler directement au droit international, droit international que les cours nationales ont obligation d'appliquer.

Une approche **dualiste** nie que le droit national et international puisse faire partie de la même juridiction, ils sont considérés comme étant deux ordres juridiques séparés. Pour pouvoir

6. La Cour internationale de Justice constitue l'organe judiciaire principal des Nations Unies. Elle a été établie à la suite immédiate de la seconde guerre mondiale. Elle ne juge que les États, qui doivent l'avoir formellement reconnue.

être appliqué au niveau national, le droit international doit d'abord être transposé en droit national. Cette approche implique que les citoyen·nes ne peuvent pas faire directement appel au droit international, ils doivent attendre sa transposition.

En pratique, ces deux approches peuvent être vues comme les deux extrémités d'un spectre, avec par exemple le Royaume-Uni d'un côté qui prends une approche dualiste, tandis que les Pays-Bas prennent plutôt une approche moniste modérée.

Cette distinction entre les deux approches ne doit pas seulement être vue comme un débat pour spécialistes, car elle a en effet des implications concrètes et d'une grande portée. Ainsi, un système juridique moniste se doit d'appliquer un traité international de manière à ce que les citoyen·nes sous sa juridiction puisse s'y référer dans sa cour national; tandis qu'un système juridique dualiste peut se permettre de ne pas considérer directement le traité en question.

Prenons par exemple un traité avec un effet direct comme la CEDH. Son Article 94 montre clairement qu'il doit être appliqué directement dans un système moniste tel que les Pays-Bas (dans le cas présent), même s'il en résulte l'inapplicabilité du droit national néerlandais. Ça a de vastes implications sur les compétences du Parlement dont les Actes peuvent être supplantés, dans la mesure où ils seraient en conflit avec la CEDH! Cependant, les Pays-Bas ne peuvent pas être contraints par des traités internationaux à moins d'y avoir consenti (comme vu plus haut). Ainsi, après son accord et sa signature sur un traité, le Parlement doit décider si le pays y sera contraint ou non. Si le Parlement consent, le chef de l'État (le Roi en l'occurrence) doit ratifier le traité, et c'est là seulement que l'État devient contraint par le traité en question.

Voyons maintenant un exemple d'un traité avec effet direct comme la Convention sur la Cybercriminalité. La CC oblige les États contractants (dont de nombreux pays du Conseil de l'Europe) à promulguer un certain nombre d'infractions pénales et de mesures d'investigations liées à la cybercriminalité. La police ou de simples individus ne peuvent par contre pas s'y référer directement devant une cour de justice, ils doivent se référer à sa traduction en droit national (dans le Code Pénal par exemple).

Enfin, pour complexifier la question, l'application de traités internationaux soulève la question de leur interprétation et de qui décide de cette interprétation : une cour nationale, internationale, ou les deux? Bien souvent, l'interprétation d'un traité implique l'utilisation de document préparatoire clarifiant les intentions des parties contractantes et des buts du texte. De telles informations peuvent notamment être trouvées dans le préambule d'un traité, qui consiste bien souvent en des *considérants* qui articulent hypothèses, buts et explications du traité. Alors que les articles d'un traité font juridiquement foi (ils ont un effet direct soit sur les citoyen·nes soit sur les États contractants), les considérants n'ont pas un tel pouvoir. Les considérants sont cependant une importante source de droit en ce qu'ils fournissent des informations importantes sur l'interprétation des articles, d'autant plus que les traités peuvent être le résultat de compromis donnant lieu à des articles formulés de manière vague (la version plus radicale d'une version préliminaire est souvent déplacée dans ces considérants afin de conserver une partie de la signification d'un article). On verra un peu plus tard le rôle que peuvent avoir ces considérants.

4.3 Droit supranational

Comme nous l'avons vu à plusieurs reprises, le droit supranational est différent du droit international. Plus précisément, dans le cas du droit supranational, un ensemble d'États membres (EM) se mettent d'accord pour transférer une partie de leur souveraineté à une organisation supranationale. En pratique, ça fait référence au droit de l'Union Européenne. Ce droit n'est pas seulement entre les EM, mais aussi entre les différents corps de l'UE et ses citoyens car en effet, certains instruments juridiques ont un effet direct *peu importe que les EM choisissent une*

approche moniste ou dualiste. Rappelons qu'historiquement, l'UE s'est construite sur une volonté d'harmoniser le marché en Europe pour assurer une interdépendance économique entre ses États. Aujourd'hui, on peut considérer que l'objectif est un peu plus large que ça et que l'UE a aussi pour but d'instituer une aire de sécurité, de liberté et de justice.⁷

4.3.1 Transfert de souveraineté

Un transfert de souveraineté impacte substantiellement la souveraineté nationale. La décision *Van Gend en Loos* de 1963 marque un tournant dans ce processus de transfert, en ce que le jugement rendu mentionne de manière explicite cet nouvel ordre juridique sur la base du Traité de Rome (traité instituant la Communauté économique européenne). Rappelons enfin que les limites entre les souverainetés nationales et supranationales est un sujet épineux (la fameuse *kompetenz-kompetenz*).

4.3.2 Sources du droit de l'UE

On parle d'*acquis* pour désigner une partie des sources du droit dans le contexte de l'UE.⁸ C'est un ensemble de droits et d'obligations en évolution constante, qui comprends notamment :

- le contenu, les principes et les objectifs politiques des traités
- la législation adoptée à la suite des traités
- la jurisprudence de la CJUE
- les déclarations et les résolutions adoptées par l'UE
- les instruments sous la politique étrangère et de sécurité commune (PESC)
- les instruments sous la coopération policière et judiciaire en matière pénale (encore parfois nommée JAI car ex-Justice et affaires intérieures)
- les accords internationaux conclus par la Communauté.

L'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE⁹) spécifie le degré d'applications de différents textes issus de l'UE (je cite) :

- *Pour exercer les compétences de l'Union, les institutions adoptent des règlements, des directives, des décisions, des recommandations et des avis.*
- *Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre.*
- *La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens.*
- *La décision est obligatoire dans tous ses éléments. Lorsqu'elle désigne des destinataires, elle n'est obligatoire que pour ceux-ci.*
- *Les recommandations et les avis ne lient pas.*

Notons que la différence entre les règlements et les directives sont un bon exemple de la difficulté de la mise en application du droit supranational : l'UE n'est pas un *super-État* ni une forme de collaboration internationale, c'est un peu quelque chose entre les deux. On a d'un côté de

7. Sans vouloir rentrer dans des considérations politiques, qui ne sont pas le sujet de cette partie descriptive, notons que cette aire peut se construire en excluant les citoyen·nes qui n'en feraient pas partie·es. Je pense notamment aux différents scandales de l'agence européenne de garde-frontières et de garde-côtes Frontex, qui érodent assez visiblement cette image d'épinal d'une Europe bienveillante.

8. C'est le terme dédié, ouf pas de problème de traduction cette fois !

9. Le nouveau nom du traité de Rome, ndt.

la législation qui s'applique uniformément — une régulation — et de l'autre de la législation qui laisse la main aux EMs. Une directive peut rendre plus complexe certaines situations aux yeux d'acteurs multinationaux, mais peut mieux s'adapter aux contextes locaux. Cependant, une régulation peut aussi avoir des interprétations légèrement différentes entre les juridictions nationales.

4.3.3 Jurisprudence de la CJUE

Pour éviter les interprétations contradictoires du droit de l'UE, les cours des EMs peuvent consulter la CJUE dans ce qu'on appelle des actes préliminaires.

Prenons ici un exemple qui devrait parler au lectorat, sur une décision de la CJUE sur la validité de la Directive 2006/24/CE sur la conservation des données. La cour européenne a jugé illégale la Directive (décision Digital Rights Ireland), mais comme c'est une directive, ça n'affecte pas forcément son implémentation nationale. Chaque EM a donc du vérifier si l'interprétation nationale de cette directive était en conformité avec les conditions légales en rapport avec la décision de la cour. Pour être qualifiées comme des restrictions juridiquement valides, les mesures prises pour implémenter la Directive doivent être proportionnelles, même si elles ont un but légitime. Selon la CJUE, ça veut dire que :

- les mesures sont suffisamment circonscrites, limitées au strict nécessaire
- le périmètre des mesures de rétention doit être différenciée
- les limitations, ainsi que des critères objectifs pour s'assurer que les données ne sont utilisées que pour les délits les plus graves, doivent être prévues à l'avance
- la période de rétention doit être différenciée en fonction des catégories de données
- le stockage en dehors de l'UE doit être interdit

Après une telle décision, chaque EM a du vérifier sa législation et sa politique à l'aune de ces critères. Certains EMs étaient déjà en conformité, alors que d'autres se sont aperçus que leur transposition violait les Articles 7 et 8 de la CDFUE.¹⁰ En effet, deux décisions de justice ont fait référence à cette décision de la CJUE, notamment *Tele2 Sverige AB v. Post-och telestyrelsen* et *Secretary of State for the Home Department v. Watson*. Dans les deux cas la CJUE a jugé que les législations nationales violait le droit de l'UE.¹¹ L'argument principal de la CJUE joue sur le fait sur la législation nationale doit être en conformité avec l'Article 15 de la ePrivacy Directive (ePD), directive qui concerne la protection des communications électroniques. Cet article permet aux EMs de restreindre l'applicabilité de certains articles à conditions que des garde-fous soient mis en place, et que ces restrictions soient nécessaires et proportionnelles. Selon la CJUE, le critère de proportionnalité n'était pas rempli dans les législations nationales. Enfin, pour conclure sur cette notion de jurisprudence, notons l'importance qu'ont eu les considérants dans la décision :

La portée des dispositions des articles 5 et 6 et de l'article 9, paragraphe 1, de la directive 2002/58, qui visent à garantir la confidentialité des communications et des données y afférant ainsi qu'à minimiser les risques d'abus, doit en outre être appréciée à la lumière du considérant 30 de cette directive, aux termes duquel « [l]es systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires ».

10. Ces articles concernent la vie privée et la protection des données.

11. En France, c'est toujours en suspens, malgré le travail acharné des camarades de La Quadrature du Net pour faire invalider le droit national existant et les futures lois concernant la conservation généralisée des données de connexion, cf <https://www.laquadrature.net/?s=tele2>.

Les considérants, bien que ne faisant pas juridiquement foi, sont quand même une source importante du droit !

4.4 État de droit international

Ce chapitre se conclut sur la remarque que le droit international dépend du droit national pour deux raisons. Tout d'abord parce que le second détermine dans quelle mesure les États sont liés au premier. Ensuite parce que la mise en application du droit international dépend des corps nationaux (à l'exception du *ius cogens* rencontré plus haut). Cependant, la réciproque est aussi vraie : le système d'États souverains est basé sur la reconnaissance mutuelle des souverainetés internes et externes de chacun.

Chapitre 5

Protection des données et de la vie privée

Travailler avec des systèmes informatiques implique la plupart du temps de travailler avec des données. Ces données sont parfois personnelles, et certains systèmes peuvent avoir un impact majeurs sur les personnes qu'ils ciblent (tels les *data brokers*, aussi appelés courtiers de données) et les personnes qui utilisent ces systèmes (comme les médias sociaux).¹ Ce chapitre va investiguer ce vaste champ d'étude du droit qu'est la protection des données et de la vie privée, qui comprends une série d'exigences légales pour le développement, le design, les paramètres par défauts et l'usage des architectures informatiques au sens large. Ce chapitre ne va cependant pas automatiquement vous transformer en juriste : il a plutôt vocation à fournir de vrais morceaux de droit pertinents pour l'informatique. Le droit à la vie privée est un droit subjectif attribué par le droit objectif. Ce droit peut être national, international ou supranational. Nous ferons d'abord un panorama des droits humains à différents niveaux législatifs, qui sera suivi par une discussion sur le concept de *vie privée*, nous verrons ensuite le droit à la vie privée tel que décrit par la CEDR et la CDFUE, pour finir sur ce nouveau droit fondamental qu'est la protection des données (notamment garanti par le RGPD).

5.1 Droit relatif aux droits humains

Quand on retrace l'histoire des droits humains, on rencontre tout d'abord le *Bill of Rights* britannique de 1689, suivi en 1789 par la *Déclaration des Droits de l'Homme et du Citoyen* révolutionnaire et le *Bill of Rights* états-uniens de 1791. La *Magna Charta* de 1215 pourrait apparaître comme un exemple précoce de charte des droits humains, mais elle assurait plutôt la restriction du pouvoir royal par les seigneurs féodaux.

5.1.1 Les droits humains comme des droits défensifs face à l'État moderne

L'établissement de l'État moderne doit être situé au début de ce que les historien·nes appellent comme ère la *modernité*, c'est-à-dire autour du XV^{ème} ou XVI^{ème} siècle. Cette époque voyait la montée de l'État moderne et bureaucratique, garantissant de nouvelles protections contre les

1. Je préfère médias sociaux à réseaux sociaux, car en dehors de tout pédantisme : nos réseaux sociaux ne se limitent tout simplement pas à quelques plateformes d'acteurs monopolistiques !

pouvoirs monopolistiques du Roi. Le concept de droits humains coïncide ainsi avec la montée du concept de souveraineté (discuté à la Section 4.1.2). Les déclarations mentionnées ci-avant fournissaient des droits civils et politiques aux sujets d'un État souverain, émulant ainsi leurs statuts de porteuses de droits individuels constituant-es d'un régime politique. Être sujet d'un souverain devint alors être sujet de droit. Et bien que ça puisse nous surprendre aujourd'hui, c'était nouveau pour l'époque ... et difficile à mettre en place.

Dans le contexte du droit international, les droits humains ont plutôt été considérés comme des droits du citoyens dû à la protection constitutionnelle offerte par la citoyenneté, ce qui impacte négativement la protection que peuvent offrir les *États voyous* (*rogue states*).² Après les atrocités de la Seconde Guerre Mondiale, les États décidèrent d'élever la protection des droits humains au niveau du droit international, en commençant par la Déclaration Universelle des Droits de l'Homme (DUDH).³

5.1.2 Des droits de la liberté aux droits sociaux, économiques et autres

Les droits humains étaient originellement axés sur la protection des citoyen-nes contre les États, ces droits étaient appelés *droits humains de première génération*. Ils peuvent être décrits comme le *droit subjectif à ce que l'État s'abstienne d'intervenir au sujet de biens juridiques considérés par les dits droits*, c'est pour cela qu'on les appelle aussi *droits de la liberté*. Les biens juridiques en question sont : la **vie privée**, la **non-discrimination**, l'**intégrité physique**, la **liberté de mouvement**, la **présomption d'innocence**, le **procès équitable**, la **liberté d'expression**, la **liberté d'association**, la **liberté de religion** et le **droit de vote**. On considère ces biens juridiques comme étant dignes de protection en tant que biens publics car une société qui ne les protégerait pas peut difficilement se réclamer de la démocratie (dans un sens assez convenu du terme). Ces droits supportent l'indépendance d'esprit et le développement des identités individuelles comme de groupes, on les appelle ainsi des droits **civils et politiques**. L'accent est donc mis sur la protection des individus en tant qu'agents autonomes dans un régime politique démocratique, ainsi que sur les obligations *négatives* de l'État envers ses citoyen-nes.

Une deuxième génération de droits humains a vu le jour quand on s'est aperçus que la non-interférence ne suffisait pas forcément, et qu'un certains nombre d'autres biens juridiques étaient absents de la liste sus-citée. Les biens considérées par cette nouvelle génération sont, entre autres, l'**emploi**, l'**alimentation**, le **logement**, la **sécurité sociale** (au sens large), l'**accès aux soins**, ainsi que l'accès à certains services de base comme l'électricité, la poste et les transports publics. Ces droits, souvent appelés *droits sociaux et économiques*, ne peuvent être assurés simplement par la non-interférence de l'État, qui est doté pour ce faire d'obligations *positives*. Pour garantir l'accès à l'emploi, il faut qu'un système économique soit mis en place afin de permette un tel droit : cette deuxième génération de droits humains nécessite que les États créés des institutions capable de mettre en application ces droits. Ces droits de deuxième génération sont par contre plus des normes d'instructions envers les États que des droits directement applicables au niveau individuel, bien qu'on puisse être témoins à la fin du XX^{ème} de plaidoyers en faveur d'une *troisième génération de droits humains* (sous-entendu : directement applicables).

2. Rogue state et sa traduction État voyou doivent être pris avec des pincettes : ce sont des termes employés notamment par les USA pour décrire d'autres États commettant des attentats (guerre en I *tousse* rak) ... ou ne remboursant pas le FMI comme la Grèce (c'est assez *subjectif* dirons-nous).

3. Même constat que précédemment sur l'adoption d'un terme genré en français.

5.2 Le concept de vie privée

Avant d'investiguer le droit à la vie privée, nous allons nous intéresser au concept de vie privée (*privacy*) en soi.⁴ En effet, l'informatique a une relation particulière avec l'informatique et notamment dans un contexte où l'on a développé la sécurité numérique et la cryptographie. On voit souvent la vie privée comme un sous-domaine de la sécurité informatique, qui cherche principalement à masquer le lien entre des données et les personnes associées, ou à chiffrer des données ou communications afin de se protéger respectivement d'yeux ou d'oreilles indiscretes. Cette vision a souvent restreint la vie privée à soit 1) l'anonymisation ou la pseudonymisation de données personnelles en les supprimant ou en les séparant de ses identifiants, ou bien 2) en cachant du contenu grâce à des techniques de chiffrement ou d'autres mesures de sécurité. Bien que la recherche sur ces sujets soit cruciale, il ne faut pas se contenter de réduire la vie privée à quelques problèmes techniques tels que l'identifiabilité (i.e., l'étude de la robustesse de l'anonymisation).

5.2.1 Taxonomie et air de famille

Plusieurs universitaires ont essayé de définir la vie privée comme la somme de ce qu'on considère généralement être ses parties, ce qui s'est retrouvé être une entreprise douteuse du fait de l'insaisissabilité du terme. Une autre manière de définir les contours du concept de vie privée est de le définir en termes de ressemblance familiale (*family resemblance*). Ainsi, le juriste Daniel Solove s'est employé à cette tâche en fournissant six catégories qui peuvent parfois se recouper :

- le droit d'être laissé·e seul (*right to be left alone*)
- l'accès limité au soi (*limited access to self*)
- le secret - la dissimulation (*secrecy - concealment*)
- le contrôle sur les informations personnelles (*control over personal information*)
- l'identité individuelle et sa protection (*personhood - protection of identity*)
- la dignité
- l'intimité

Certaines de ces catégories sont des buts, d'autres de moyens, en tout cas chaque catégorie prise indépendamment ne peut définir le concept de vie privée. Solove nous avertit donc que ce n'est pas une taxonomie au sens propre du terme⁵, mais bien une tentative de définition par ressemblance familiale au sens Wittgensteinien du terme.⁶

Lorsqu'on définit la vie privée comme une liberté à ne pas être importuner, on se réfère au **droit d'être seul**. La vie privée peut être comprise à travers le concept d'**intimité** lorsqu'on cherche à tracer des limites entre un groupe de proches avec qui l'on partage des informations, et d'autres personnes. Si l'on considère à la fois les concepts d'**accès limité**, de **secret** et d'**anonymat**, on peut aborder la notion de divulgation aux tiers dans son interprétation juridique. Aux USA, cette interprétation se traduit, ou plutôt se traduisait en 1967, par une doctrine qui spécifie que la transmission de données à des tiers (comme une banque) vaut abandon des attentes au regard de la protection de ces données vis-à-vis du gouvernement. Ce n'est pas le

4. On utilise parfois la traduction *intimité numérique*, mais ici *privacy* est pris dans un sens pas uniquement numérique.

5. Bien qu'il ait aussi introduit une taxonomie du terme dans un autre article intitulé *A taxonomy of privacy*.

6. Dans ses *Investigations philosophiques*, Wittgenstein propose une manière d'appréhender le langage qu'il nomme *air de famille*. Selon cette définition, différents mots classés dans le même groupe linguistique peuvent être reliés entre eux par des similitudes sans que ces dernières soient nécessairement communes à tous les mots.

cas en Europe, les USA ont par ailleurs révisé leur doctrine en la matière depuis (voir la décision *US v. Jones* Section 2.1.2). Définir la vie privée en termes de contrôle nous rapproche de l'idée d'*information personnellement identifiable* (*personally identifiable information*, terme employé aux USA alors qu'on emploie données personnelles - *personal data* en Europe) en tant que propriété, ce qui n'est pas sans poser quelques problèmes. En effet, l'idée de propriété sur les données personnelles implique très rapidement la possibilité de les vendre : c'est une boîte de Pandore qu'il vaut mieux ne pas ouvrir.⁷ Enfin, on peut connecter le concept de vie privée à celui d'**identité individuelle** (*personhood*), en ce que la construction de l'identité se réfère à la manière que l'on a de se présenter aux autres.

S'il fallait ne garder qu'un seul concept clé pour définir la vie privée, c'est bien que c'est un terme mouvant qu'il est difficile de définir précisément. En fin de compte, on affine la définition de la vie privée notamment lorsque celle-ci est violée.

5.2.2 Vie privée et technologie

Maintenant que le concept de vie privée a été débroussaillé, on peut s'attaquer à ses relations avec la technologie.

Le psychologue environnemental Altman⁸ disait que la vie privée est une histoire de négociation des barrières entre soi et les autres : c'est une relation plus qu'une propriété. Selon lui, la vie privée est un processus continu de partage et d'exclusion basé sur des pratiques sociales qui elles-mêmes dépendent des *affordances* de la technologie. En ce sens, la vie privée peut-être décelée dans la plupart des sociétés humaines, sous différents noms.

Le droit à la vie privée (*right to privacy*) est par contre une invention plus récente, qui fait suite aux progrès de la photographie. Dans un article devenu célèbre, les juristes Warren et Brandeis discutent de la nécessité de pouvoir se protéger juridiquement de la publication de photos à son encontre, arguant d'un droit à être laissé·e seul (*right to be left alone*). Ce droit à la vie privée, surprenamment introduit comme un droit privé et non comme un droit constitutionnel, favorise la vie privée comme une liberté négative : le droit que les autres s'abstiennent d'interférer.

L'apparition suite à la seconde guerre mondiale d'infrastructures technologiques, notamment sous la forme de base de données, aboutit à la collecte et au stockage d'une grande quantité d'informations concernant les citoyen·nes. Le juriste Alan Westin écrit à ce sujet, dans son article séminal *Privacy and Freedom*, que la vie privée est :

la prétention des individus, des groupes ou des institutions à déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées aux autres.

Cette définition du droit à la vie privée comme contrôle sur l'information, favorise une liberté positive : la liberté de définir comment nos informations personnelles peuvent être utilisées.

L'essor d'Internet combiné au big data et aux techniques dites motivées par les données (*data-driven*) met en évidence la définition d'un nouveau droit à la vie privée, plus complexe et contextuel. Une liberté définit négativement ne suffit plus car le contrôle sur les données devient illusoire ; tandis qu'une liberté définit positivement semble tout aussi inatteignable du fait du volume de données généré. Une définition pratique de la vie privée se doit de combiner les deux approches, tout en mettant l'accent sur la question de la construction de l'identité. Les chercheurs en sciences de l'information Agre et Rotenberg définissent ainsi la vie privée : comme le droit d'être libre de contraintes déraisonnables sur la construction de son identité.

7. En France, certains libertariens tels que Gaspard Koenig défende cette idée malheureuse.

8. Rien à voir avec le fondateur d'OpenAI Sam Altman.

5.3 Le droit à la vie privée

La vie privée est une valeur, un intérêt, un droit ou un bien. On peut l'analyser d'un point de vue éthique (comme une vertu ou un devoir), économique (en tant qu'utilité, préférence), ou encore par le prisme de la théorie politique (comme un bien public et un bien privé). On s'intéressera ici au point de vue juridique en traçant les contours de l'applicabilité du droit positif sur les questions de vie privée, respectivement par les perspectives constitutionnelles, internationales et supranationales, avant de conclure par une discussion sur l'Article 8 de la Convention Européenne des Droits de l'Homme (CEDH).

5.3.1 Le droit à la vie privée en droit constitutionnel

Le droit à la vie privée est un droit subjectif attribué par le droit objectif, dont la branche la plus évidente à cet égard est le droit constitutionnel, notamment en ce qu'il protège les citoyen·nes contre certains pouvoirs de l'État. À l'origine, les droits humains ont été conçus dans une optique de réguler *verticalement* les relations entre l'État et ses sujets, mais la révolution industrielle et l'essor du capitalisme a donné lieu à la naissance de puissants acteurs dont les capacités de nuisance étaient comparables à celles de l'État. Ça a donné lieu à ce qu'on appelle un **effet horizontal** des droits constitutionnels tels que le droit à la vie privée, dont on distingue deux tendances. L'effet horizontal indirect signifie que les citoyens peuvent poursuivre l'État en justice pour avoir négligé ses obligations relatives au contrôle du secteur privé. L'effet est dit *indirect* car on ne peut pas l'invoquer directement. Selon les juridictions nationales, certaines cours attribuent cependant un effet horizontal *direct* : à ce moment-là, une violation de la vie privée peut être invoqué directement contre une entreprise privée. Par exemple, la Constitution des USA, bien que ne le mentionnant pas forcément de manière explicite, a été souvent interprétée comme sauvegardant le droit à la vie privée (notamment sur la base du quatrième Amendement, comme vu précédemment).

5.3.2 Le droit à la vie privée en droit international

Parmi les différents garde-fous prévus pour protéger la vie privée, le droit international n'est pas en reste. Par exemple, l'Article 17 du Pacte international relatif aux droits civils et politiques (PIDCP) ainsi que l'Article 8 de la CEDH mentionne spécifiquement le droit à la vie privée. Tandis que le premier texte a un périmètre mondial mais des mécanismes d'application faibles, le second fournit un recours direct aux citoyen·nes via son Article 34 mais ne concerne que la juridiction du Conseil de l'Europe.

5.3.3 Le droit à la vie privée en droit supranational

Depuis 2009 et la mise en application de la Charte des droits fondamentaux de l'Union européenne, la protection des droits humains a d'autant plus gagné en popularité, notamment via son Article 51.

5.3.4 Article 8 de la CEDH

L'Article 8 de la CEDH est une des provisions les plus importantes discutée dans ce livre. En effet, le droit à la vie privée qui y est articulé est notamment pertinent pour l'intégrité corporelle, le respect des décisions et d'autres aspects de la vie privée, mais aussi car il affecte directement des questions de cybercriminalité (fuite de données) et de copyright (dissémination illégale de photos ou de textes), notamment lorsque les mesures de protections enfreignent le droit à la vie

privée. On va tout d'abord s'attarder sur les *conditions* juridiques stipulées par l'Article 8 de la CEDH, puis on s'intéressera aux *effets* juridiques qu'elles génèrent.

Cet article consiste en deux paragraphes, le premier concerne la question de savoir si la vie privée est enfreinte, tandis que le second clarifie sous quelles conditions une infraction est justifiée.

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Ici les conditions qui qualifient une enfreinte à la vie privée sont listées une à une, et la Cour de justice de l'EU s'est positionnée pour une interprétation large de ces conditions. Notons qu'une *infraction* de la vie privée n'est pas forcément une *violation* de celle-ci : une infraction peut être justifiée, c'est à la CrEDH de juger.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

Ce deuxième paragraphe nous apprend qu'une infraction peut être justifiée (selon les critères mentionnés). Il faut donc passer un test triple pour justifier d'une infraction (afin qu'elle ne devienne pas *violation*) : avoir un but légitime, avoir un fondement juridique et être proportionnelle au but visé.

5.3.5 Jurisprudence de la CEDH sur la surveillance

Cette sous-section se conclue par des explications détaillées sur les décisions de la CEDH en matière de surveillance. Ces explications, bien qu'intéressantes, sont principalement constituées de citations des décisions de la Cour. Ainsi, j'ai choisi de ne pas les inclure ici.

5.4 Protection des données et de la vie privée

Depuis la mise en application de la Charte des droits fondamentaux de l'Union européenne (CDFUE) en 2009, l'EU possède deux droits fondamentaux en ce qui concerne le traitement des données personnelles, explicités dans les articles suivants :

- Article 7. Respect de la vie privée et familiale : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.
- Article 8. Protection des données à caractère personnel :
 - 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
 - 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
 - 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

C'est une situation nouvelle pour les droits humains, car aucune autre constitution ou traité n'attribue un tel droit à la protection des données personnelles.

L'Article 52 de la CDFUE clarifie la relation entre son Article 7 et l'Article 8 de la CEDH, les deux faisant référence au droit à la vie privée.

- 3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

Ce qui signifie en l'espèce que l'Article 7 de la CDFUE ne peut être interprété comme fournissant des protections moindres comparé à l'Article 8 de la CEDH ; il peut cependant être interprété comme en attribuant de meilleures. Dans la mesure où l'Article 8 de la CDFUE correspond à l'Article 8 de la CEDH, le premier peut aussi être interprété comme fournissant plus de protection que le second (mais pas l'inverse).

Avant de se plonger dans le Règlement Européen sur la Protection des Données (RGPD), qui fournit plus de détails quant aux règles et aux principes régissant la collecte et le traitement des données personnelles, nous allons tout d'abord investiguer comment le droit fondamental à la protection des données peut être comparé au droit fondamental à la protection de la vie privée.

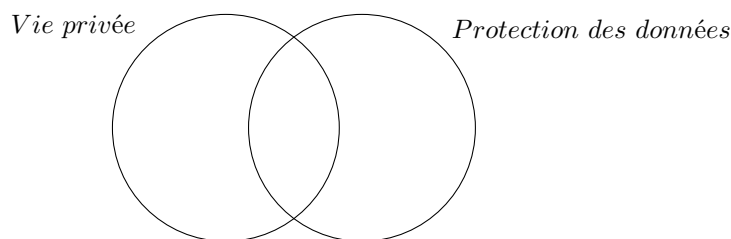
5.4.1 Par défaut : un droit à l'opacité et un droit à la transparence

Certaines auteures ont argué que par défaut, le droit à la vie privée est avant tout un *droit à l'opacité*, alors que le droit à la protection des données est un *droit à la transparence*. En tant que droit à l'opacité, le droit à la vie privée a pour objectif de préserver une sphère intime pour les citoyen·nes (notamment face à l'État). On rejoint ici la conception de la vie privée comme un droit à la liberté, comme un droit négatif. En tant que droit à la transparence, le droit à la protection des données cherche lui à s'assurer que tout traitement de données personnelles (comprendre ici : la collecte, l'accès, la manipulation et tout autre usage) doit être fait de manière transparente et en adéquation avec un ensemble de conditions qui assurent un traitement juste et légitime (*fair and lawful*).

Notons ici que l'opacité fait référence à la sphère privée des individus tandis que la transparence concerne l'État ainsi que d'autres puissants acteurs, ce qui fait écho à un principe central de l'État de droit (i.e., que le gouvernement doit être aussi transparent que possible alors que les citoyen·nes doivent être protégé·es contre les intrusions du gouvernement). Notons aussi que bien que la vie privée soit un droit à l'opacité requérant que l'État s'abstienne d'intervenir (c'est donc une *liberté négative*), il peut néanmoins imposer des *obligations positives* à l'État pour permettre aux citoyen·nes de jouir de leurs droits. De manière symétrique, bien qu'on puisse considérer le droit à la protection des données comme un droit à la transparence qui permet aux individus d'agir sur leurs données personnelles (*liberté positive*), il peut néanmoins imposer des *obligations négatives* en ce qui concerne le traitement de ces données.

5.4.2 Des droits distincts mais qui se chevauchent

Il peut être tentant de voir le droit à la protection des données comme un sous-ensemble du droit à la vie privée, mais ce n'est pas exactement correct. Dans le contexte de l'EU, leurs périmètres se recoupent partiellement, ainsi on peut les représenter par un diagramme de Venn.



Lorsque le traitement de données personnelles constitue une interférence au droit à la vie privée, il y a chevauchement. Il ne faut cependant pas oublier que le droit à la vie privée concerne aussi l'interférence à l'intégrité physique, la prise de décision (*decisional privacy*), la vie intime (*privacy of the home*), sans qu'il n'y ait nécessairement de traitement de données personnelles.

De manière similaire, le droit à la protection des données concerne aussi le traitement des données personnelles quand il n'y a pas d'interférence avec la vie privée, par exemple, lorsque l'on demande que nos données bancaires soit traitées afin de payer un bien. Ce qui ne veut pas dire non plus que ces données ne tomberont jamais sous le couperet du droit à la vie privée : leur réutilisation à des fins de ciblage marketing nous situerait à l'intersection du diagramme de Venn.

5.4.3 Recours juridiques en cas de violation

Le droit à la vie privée peut être invoqué devant une cour de justice nationale. Comme on a pu le voir plus haut, les citoyen·nes peuvent présenter des plaintes à la CEDH, mais seulement après avoir épuisé les recours nationaux. Ce qui signifie que si l'on échoue à se réclamer d'une violation de l'Article 8 de la CEDH au niveau national, ou si l'on échoue à faire appel à un jugement qui nie une telle violation, alors l'application devant la CEDH sera inadmissible (comme précisé dans les Articles 34 et 35 de la CEDH).

5.5 Droit de la protection des données

L'histoire de la protection des données remonte aux années 1970, quand plusieurs pays ont émis des législations afin d'assurer un traitement juste des informations personnelles par leurs gouvernements. Un exemple notable est le *US Privacy Act* en 1974, ou encore en 1980 lorsque l'OCDE a émis ses *Fair Information Principles* (FIPs) dont on peut lister un aperçu ici :

- | | |
|-------------------------------------|-------------------------------------|
| 1. Limitation de la collecte | 5. Garanties de sécurité |
| 2. Qualité des données | 6. Ouverture (des pratiques) |
| 3. Spécification du but de collecte | 7. Participation des individu·es |
| 4. Limitation de l'utilisation | 8. Responsabilité (des contrôleurs) |

De nombreux États ont promulgué des législations de protection des données depuis 1980, souvent en suivant l'exemple des FIPs. La Directive sur la Protection des Données (DPD) dans l'EU en 1995 est un exemple typique d'une législation qui met en application ces principes de manière concrète. La DPD a été supplanté en 2018 par le RGPD, mais les principes fondamentaux restent les mêmes.

5.5.1 Droit à la protection des données dans l'EU et aux USA

Aux USA et a contrario de l'EU, la protection des données fait partie du droit à la vie privée, elle est sujette à des législations sectorielles, avec par exemple des spécificités liées à la finance, la santé, la protection des enfants ou la protection des consommatrices. Il n'y a pas de droit général à la protection des données, seul le Privacy Act de 1974 a un effet général (et encore, il ne s'applique qu'aux Agences Fédérales). Cela signifie que la protection des données varie selon le contexte de traitement. Par exemple, dans un contexte commercial, la majeure partie des protections offertes dépend des compétences de la Federal Trade of Commerce (FTC) (voir la section 5 du FTC Act). Une attente raisonnable du respect de la vie privée est un principe fondamental intimement lié au fonctionnement du marché en ligne. La FTC s'occupe des violations au cas par cas, mais elle peut aussi émettre des décisions (*rulings*) si certains types de violations sont prévalents. On considère généralement la FTC comme l'organe de régulation de la vie privée (*informational privacy*) du à son rôle central dans l'élaboration des politiques concernant la protection des données.

La situation est bien différente dans l'EU où l'applicabilité du droit à la protection des données est générale et ne dépend pas de si une violation peut être considérée comme *un acte injuste et trompeur affectant le commerce*. On pourrait alors dire qu'aux USA, le traitement d'information personnelles est autorisé à moins qu'il n'ait été explicitement interdit, tandis que dans l'EU tout traitement est conditionné par un ensemble de règles et de principes qui imposent des obligations au responsable de traitement et attribuent des droits aux personnes concernées.

Voyons voir maintenant un peu plus en détail le contenu principal du droit à la protection des données dans l'EU.

5.5.2 Droit à la protection des données dans l'EU

Le RGPD est basé sur l'Article 16 du TFUE, qui précise que toute personne a le droit à la protection de ses données personnelles, que l'EU doit émettre des règles pour permettre cette protection et que ces règles doivent être sujettes à un contrôle par des autorités indépendantes. Ainsi, le RGPD protège le droit fondamental à la protection des données (stipulé dans l'Article 8 de la CDFUE). On peut même dire qu'il va plus loin dans le sens où il protège *tout droit fondamental et toute liberté* impliquée par le traitement de données personnelles. Cependant, ce n'est pas l'unique but du Règlement qui cherche aussi à harmoniser les différents niveaux de protection offerts par les États Membres, dans l'optique d'assurer une libre circulation des données au sein du marché européen (ce qui est explicité dans son Article 1).

Sources du droit de l'EU en matière de droit à la protection des données

On a vu jusqu'à maintenant que les sources du droit consistaient en les législations, les traités, le droit jurisprudentiel, la doctrine, le droit coutumier ainsi que les principes fondamentaux. Dans le cas de l'UE plus précisément, on trouve les Traités fondateurs, la Charte, le RGPD, la Directive « Police-Justice » (DPJ), la Directive ePrivacy (ePD), ainsi que d'autres régulations et directives dont on ne parlera pas ici. On trouve à côté de ça la jurisprudence de la CJUE et une grande variété de sources moins contraignantes (discussions dans des journaux etc). Une particularité de l'UE est cependant ce qu'on appelle les Opinions du Groupe de Travail 29 (*WP29*), qui se nomme désormais Comité Européen de la Protection des Données (EDPB en anglais). Ces Opinions fournissent des interprétations pertinentes au regard du droit européen, bien que non contraignantes.

Champ d'application matériel et territorial

Le champ d'application matériel du RGPD (décrit dans son Article 2) est limité au traitement de données à caractère personnel⁹, le terme traitement ayant par contre une définition très large comme le démontre l'Article 4(2) :

« traitement », 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, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Notons cependant que le RGPD ne s'applique pas au traitement de données personnelles dans le cadre familial ni dans un contexte de lutte contre la criminalité (c'est la DPJ qui prends le relais ici). En plus des exceptions au champ d'application listées dans l'Article 2, on peut lire dans l'Article 33 que les États Membres peuvent aussi émettre des lois afin de restreindre l'applicabilité de certaines provisions du RGPD, dans la mesure où ces décisions seraient nécessaires dans une société démocratique et répondraient à des exigences de proportionnalité¹⁰.

Le champ d'application territorial du RGPD est quant à lui défini par son Article 3 :

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

Le paragraphe 2 précise même que :

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

En bref : peu importe que l'on le responsable de traitement soit européen ou non, le RGPD a un effet **extra-territorial**.

Données à caractère personnel et personnes concernées

Ici encore, citons directement le texte pour définir précisément ce que sont les données à caractère personnel :

« données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un 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 ;

9. Que j'appellerais indifféremment ici données personnelles, c'est à la fois plus court et très largement utilisé même au sein des milieux juridiques.

10. Notons que l'interprétation des notions de nécessité et de proportionnalité est une question subtile qui fait souvent débat.

Tout comme la définition du traitement vue plus haut, la définition des données personnelles est très large, le Considérant 26 précise même que :

Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.

Ainsi, la CJUE a caractérisé dans l'arrêt *Breyer v. Germany* les adresses IP dynamiques comme étant des données personnelles, celles-ci pouvant être dé-anonymisées par les fournisseurs d'accès Internet.

On a vu plus haut que le champ d'application du RGPD concerne les données personnelles, ce qui peut laisser penser qu'anonymiser des données permet d'éviter d'avoir à appliquer le RGPD. Il y a cependant deux réserves à cette idée simpliste : tout d'abord, l'anonymisation est en soi une forme de traitement, l'opération nécessite ainsi un fondement juridique ; en outre, anonymiser des données n'est pas chose facile, on arrive bien (trop) souvent à dé-anonymiser les données, à moins de les rendre si anonymes qu'elles perdent toute utilité.

Le RGPD parle aussi de pseudonymisation dans son Article 4(5) :

«pseudonymisation», le 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 ;

On voit clairement que les données pseudonymisées sont un sous-ensemble des données personnelles, il faut donc comprendre ce processus comme un moyen de se conformer au droit et non pas de s'y soustraire. Par exemple, des données chiffrées mais pas de bout-en-bout (c'est-à-dire que des tiers autres que les personnes concernées seraient en mesure de déchiffrer) seraient très probablement qualifiées de données pseudonymisées.

Responsable de traitement et sous-traitant

Continuons sur des définitions avec celle du responsable de traitement :

«responsable du traitement», 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 ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ;

Cette définition est cruciale car c'est l'entité responsable de la conformité au RGPD. Il détermine les moyens de traitement des données, moyens qu'il peut cependant externaliser à un sous-traitant (tout en gardant la responsabilité juridique) :

«sous-traitant», 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 ;

Il existe aussi un cas spécifique de responsables conjoints du traitement :

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement [...].

Cette définition permet d'établir des responsabilités partagées lorsque c'est nécessaire, au-delà d'un simple dichotomie responsable/sous-traitant.

Fondement juridique pour la licéité du traitement

Le traitement de données personnelles n'est autorisé que sur la base d'un des six fondements juridiques (parfois appelés *bases légales*) décrits dans le RGPD. Le premier est le consentement : *la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*

Nous reviendrons un peu plus loin sur les spécificités du consentement.

Le deuxième fondement se lit : *le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;*

Une implication de cette définition est que les données ne peuvent plus être traitées sur cette base une fois le contrat exécuté.

Le troisième fondement : *le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*

Ce cas est typique des obligations légales relatives aux impôts ou à la sécurité sociale.

Le quatrième : *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;*

On parle ici de situations de vie ou de mort, dans lesquelles le traitement de données médicales est nécessaire.

Le cinquième fondement : *le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;* Cette base légale est comparable à la troisième, à ceci près qu'elle relève plus de traitement par des agences gouvernementales (dans le cadre de développement de politiques publiques par exemple).

Enfin, le sixième et dernier fondement : *le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.*

Cette base est importante pour de nombreux cas, notamment ceux relatifs au secteur commercial, il a par ailleurs été utilisé à outrance sous prétexte que les intérêts économiques sont légitimes en soi. Cependant, ce n'est pas aussi facile que ça : cette base requiert un test d'ajustement (*balancing test*), qui évite que les droits fondamentaux soient bafoués sur de simples motifs économiques.

Ça a deux conséquences : 1) le responsable doit évaluer *a priori* si les intérêts économiques au traitement des données peuvent supplanter les intérêts et les droits des personnes concernées par le micro-ciblage et 2) les personnes concernées peuvent s'opposer au traitement dans ce cas particulier (ce droit d'opposition est décrit dans l'Article 21). Plus concrètement, un tel test doit entre autres prendre en considération la nature et la source de l'intérêt (prétendument) légitime, l'impact sur les personnes concernées ainsi que leurs *attentes raisonnables*, ainsi que les garanties additionnelles qui peuvent être apportées afin de limiter cet impact : minimisation de la collecte,

amélioration de la transparence, mise en place de technologies respectueuses de la vie privée (*privacy-enhancing technologies*), etc.

Principes de licéité, loyauté et transparence

En plus d'avoir un fondement juridique, le traitement de données personnelles doit obéir à un ensemble de règles, selon l'Article 5 du RGPD. Contrairement à la DPD qui régissait précédemment le traitement aux données personnelles, les principes du RGPD sont à la fois explicites et contraignants. Examinons un par un les différents principes qui régissent le traitement des données :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

Ici le terme *licite* fait référence à l'Article 6 certes, mais aussi plus généralement au respect de l'État de droit. Ainsi, un simple fondement juridique ne peut suffire, le traitement doit s'accompagner d'attentes raisonnables de la part des personnes concernées ainsi que de freins et de contre-mesures. Notons l'emploi du terme *transparence*, décrit plus précisément dans les Articles 13 et 14, sur lequel nous reviendrons.

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

La limitation des finalités est un des principes les plus importants dans le droit européen à la protection des données. Une finalité supplémentaire est permise si celle-ci n'est pas incompatible avec la finalité initiale, en revanche, le traitement est alors soumis à des obligations supplémentaires : mise en évidence des liens entre les finalités, indication de la nature et de la sensibilité des données, existence de garanties etc. Notons qu'un traitement supplémentaire à des fins de recherche scientifique ou statistique ou d'archivage dans l'intérêt public est considéré comme *compatible par défaut* (les détails sont précisés dans l'Article 89).

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

La minimisation des données est un autre principe fondamental, il sous-tend la limitation des finalités et de la conservation. Alors que la DPD précisait *non-excessives*, le RGPD lui parle de limitation à *ce qui est nécessaire*. On peut interpréter ça comme une restriction supplémentaire, en direction d'une stricte proportionnalité et subsidiarité.

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

Ici le principe d'exactitude est formulé comme une obligation pour le responsable de traitement, et est lié aux droits à l'effacement et à la rectification.

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins

*archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (**limitation de la conservation**) ;*

Le principe de limitation de la conservation exige des responsables qu'ils engagent un cycle de gestion des données qu'ils traitent, par exemple en les supprimant lorsque le but de la collecte est rempli. L'exception à des fins de recherche dont on a parlé plus haut doit être rigoureusement encadré par des mesures techniques et organisationnelles, afin de protéger les libertés des personnes concernées.

*f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (**intégrité et confidentialité**) ;*

Ce principe est lié aux exigences de sécurité dès la conception décrit dans l'Article 32, ainsi qu'aux obligations de notifications en cas de violation (voir les Articles 33 et 34).

*2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (**responsabilité**).*

Ce dernier principe, en filigrane de tous les autres, considère que le responsable de traitement est responsable en dernier ressort.¹¹ Ce principe de responsabilité est détaillé dans l'Article 30, ainsi que dans le Chapitre VIII. Le rôle du responsable du traitement (conjoint ou non) est lui spécifié dans les Articles 24, 26 et 28.

Consentement valide

Le RGPD contient un article spécifique aux conditions applicables au consentement, l'Article 7. Celui-ci précise que le responsable porte la charge de la preuve de l'obtention du consentement (¶1), que le consentement ne doit pas être caché dans des politiques de confidentialité, il doit au contraire être présenté sous une forme compréhensible (¶2), les personnes concernées doivent pouvoir retirer leur consentement à tout moment, aussi simplement qu'ils l'ont donné (¶3), que l'exécution d'un contrat n'est pas subordonnée à un consentement qui lui ne serait pas nécessaire à l'exécution dudit contrat (¶4). Notons que le Considérant 43 apporte des précisions à ce sujet.

Catégories spéciale de données

L'Article 9 définit un ensemble de données qui exigent un traitement spécial, dites à *catégories particulières* ou *sensibles*. Par exemple, les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, etc. Le traitement de ces données est **interdit par défaut** (¶1), la suite de l'article précise cependant des conditions qui permettent de lever cette exemption (un consentement *explicite*, des intérêts vitaux pour la personne etc).

Protection des données dès la conception et protection des données par défaut

On a vu dans l'Introduction la nature du droit moderne, basé sur sa représentation textuelle (*text-driven*). L'essor d'environnements basé sur le code et les données (*code- and data-driven*) confronte le droit à de nombreux problèmes. Le simple fait de poser sur le papier et d'émettre des

11. *The controller is accountable*, ça sonne un peu mieux en anglais on va pas se mentir.

normes juridiques ne suffit pas si l'architecture technique et organisationnelle génère une normativité à leur encontre. Autrement dit : l'architecture technique peut présenter à ses utilisatrices une architecture de choix qui limite la compréhension des systèmes.

L'Article 25 exige des responsables de traitement qu'ils conçoivent le traitement des données en conformité avec le droit à la protection des données. On parle ainsi de protection des données dès la conception (*Data Protection by Design*) ainsi que de protection de la vie privée dès la conception (*Privacy by Design*), il ne faut cependant pas confondre les deux concepts : le second relève d'un devoir éthique et pas forcément d'une obligation légale, et l'on a vu plus haut que la vie privée et la protection des données ne sont pas des concepts interchangeables. La protection des données par défaut est une obligation légale qui n'existait pas sous la DPD.

Le premier paragraphe de l'Article 25 décrit un ensemble de mesures techniques et organisationnelles qui intègrent les principes fondamentaux du droit à la protection des données dans la conception de l'architecture de traitement des données. Ces mesures sont censées atténuer les risques pour les droits et libertés des personnes (en anglais, l'article ne parle pas de *data subjects* contrairement au reste du texte, mais bien de *natural persons*, bien que la version française ne fasse pas de différence). Ces mesures peuvent être la pseudonymisation, des interfaces de consentement utilisables, etc. Elles ne sont pas forcément faciles à mettre en œuvre et peuvent impliquer des coûts substantiels.

Le second paragraphe décrit ce que doit être la protection des données par défaut, c'est-à-dire la protection des données dès la conception appliquée à la minimisation des données. Il insiste sur le fait qu'aucun traitement superflu ne doit avoir lieu.

Enfin, le troisième paragraphe déclare qu'un mécanisme de certification peut contribuer à la démonstration d'une conformité avec les exigences de protection dès la conception.

Analyse d'impact relative à la protection des données

La protection des données dès la conception est intimement liée à un nouveau mécanisme de conformité : l'analyse d'impact. En gros, les responsables de traitement ont pour obligation d'évaluer les violations potentielles au RGPD lorsqu'ils mettent en œuvre des nouvelles technologies. Un critère important dans la décision de mener ou non une telle analyse est la possibilité que le traitement soit *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*.

Pour se faire, le responsable de traitement peut aller faire appel à un délégué à la protection des données (DPD) s'il y en a un. Les Articles 37 à 39 précisent sous quelles conditions un DPD est obligatoire et pour quels types de responsables.

Si une analyse d'impact doit être menée, elle doit au moins contenir :

- a) 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 ;
- b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et
- d) 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 présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Mise en conformité et mise en application

De manière générale, le RGPD renforce le principe de responsabilité. Pour cela, de nouvelles obligations sont introduites, telles que la protection des données dès la conception et les analyses d'impact. D'autres obligations sont renforcées ou améliorées, par exemple la facilité du retrait du consentement, l'accent mis sur la pseudonymisation, le droit à la portabilité etc.

En plus de ces obligations, la régulation se donne les moyens de mettre en application ces mesures. En effet, on a souvent pu reprocher aux précédentes législations leur manque d'application (*enforcement*). Le RGPD quant à lui dédit un chapitre entier à ces questions, le numéro VIII, sous le titre *Voies de recours, responsabilité et sanctions*.

Entre autres, les Articles 77 et 78 fournissent aux personnes concernées la possibilité d'introduire une réclamation auprès d'une autorité de contrôle. L'Article 79 fournit un accès direct aux cours de justice. L'Article 80 stipule que les personnes concernées peuvent mandater un organisme, une organisation ou une association à but non lucratif pour faire valoir leurs droits. L'Article 83 a beaucoup fait parler de lui car il stipule que les autorités de supervision peuvent imposer des amendes jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

5.6 En bref

Dans ce chapitre, nous avons exploré le droit des droits de l'humain et étudié les *rouages* du droit à la vie privée dans le contexte de la CEDH, et du droit à la protection des données dans le contexte de la CFREU, tel que protégé par le RGPD.

Au chapitre 10, nous reviendrons sur la législation européenne en matière de protection des données en tenant compte de la nature de plus en plus codifiée de notre environnement, en soulignant la nature unique des droits de protection des données de l'UE en ce qui concerne les décisions automatisées basées sur le traitement des données à caractère personnel.

Chapitre 6

Cybercriminalité

La dépendance croissante envers le numérique implique une augmentation de l'impact de la cybercriminalité. Alors qu'on peut compenser les dommages faits aux individus grâce au droit privé, les dommages structurels causés aux infrastructures exigent une approche complémentaire qui rétablit la confiance envers les fondations des rapports sociaux. C'est dans une certaine mesure le rôle du droit administratif, qui impose des sanctions en cas de violations des normes légales afin de protéger ce qu'on appelle en théorie politique et en philosophie du droit des *biens communs*.¹ On parle de biens communs dans ce sens quand on fait référence à quelque chose qui bénéficie à la société de manière générale, que ce soit exclusif ou non, rival ou non. On peut citer par exemple la santé publique, la liberté d'expression, l'accès à l'énergie, à l'éducation. En philosophie du droit, on considère les droits humains comme des biens communs. Ainsi, le RGPD est un exemple issu du droit administratif qui protège des biens communs comme la vie privée, la non-discrimination et la liberté d'expression. Cependant, dans une approche administrative du droit, on peut avoir tendance à confondre une sanction et le paiement d'une amende pour ne pas avoir à respecter la loi : «il ne faut pas dépasser les limites de vitesse sous peine d'amendes» peut devenir «on peut dépasser les limites de vitesse si on est prêt à payer une amende».

Le droit pénal ne cherche pas à définir le prix à payer pour violer les normes légales, il cherche plutôt à créer une forme de censure que l'on pourrait qualifier de bienveillante. Le droit pénal est bien plus qu'un simple calcul utilitariste conçu pour dissuader un prétendu *homo economicus* de violer la loi, ce n'est pas non plus un moyen de déshonorer des agents afin qu'ils se comportent correctement. Le droit pénal est une forme de censure qui cherche à s'adresser aux citoyen·nes comme des personnes responsables de leurs actes et non pas comme des pions manipulables.

Les souverainetés internes et externes (que l'on a vu dans la Section 1) impliquent qu'un gouvernement qui ne protège pas ses concitoyen·nes contre la criminalité risque de perdre sa légitimité.² Dans le cadre de la cybercriminalité, les autorités compétentes font face à une cible mouvante. Les développements technologiques, tant du côté des auteurs de crimes que du côté du maintien de l'ordre, vont bien souvent plus vite que les stratégies légales qui cherchent à cerner le caractère spécifique de la cybercriminalité. Ce chapitre s'intéressera d'abord à la question de savoir ce qui rend la cybercriminalité *cyber*, puis présentera les cadres juridiques internationaux et supranationaux destinés à lutter contre la cybercriminalité. Enfin, nous fournirons une analyse plus détaillée de la Convention sur la cybercriminalité, comprenant une réflexion sur l'image de

1. En terme économiques, le terme de *biens communs* fait référence à des biens non-exclusifs (car ils ne peuvent être monopolisés, tel que l'air) et non-rivaux (car leur usage par une personne n'amointrit par leur valeur d'usage, telle que l'information).

2. Ça fait partie de ce que l'on appelle le *contrat social*.

la balance lorsqu'il s'agit de trouver un équilibre entre la sécurité et les droits et libertés.

6.1 Le problème de la cybercriminalité

Dans son *Internet Security Threat Report* de 2018, Symantec rapporte que non seulement le nombre de cybermenaces³ augmente année après année, mais aussi que ces menaces deviennent de plus en plus variées. Toujours d'après son rapport, une requête web sur treize (1 sur 13) conduit à un programme malveillant, 24 000 applications malicieuses sont bloquées par jour en moyenne, que les programmes malveillants sur Mac ont augmentés de 80% par rapport à l'année précédente, etc. On peut bien sûr remettre en questions ces chiffres (toutes ces attaques ont-elles un fort impact ?), mais la tendance elle est indéniable : la cybercriminalité est une menace.

Symantec est une entreprise experte en cybersécurité, ce qui n'est pas la même chose que la cybercriminalité. La cybersécurité est généralement définie en termes de confidentialité, d'intégrité et de disponibilité (CIA) des données, des systèmes informatiques ou des deux. Examinons dans un premier temps ce que l'on entend par criminalité informatique et cybercriminalité, ainsi que leur lien avec la cybersécurité.

6.1.1 Criminalité informatique

Quand les ordinateurs étaient encore des appareils autonomes, ce qu'on appelle cybercriminalité aujourd'hui portait alors le nom de *criminalité informatique*. Afin de le justifier en tant que sous-domaine spécifique du droit, il consistait en un ensemble de crimes commis *avec* les ordinateurs, *contre* les ordinateurs et *dans un contexte* informatique. Le premier sous-ensemble traitait par exemple de hameçonnage, le second de programmes malveillants, tandis que le troisième de pornographie infantile distribuée en ligne.

Une autre distinction analytique permet de différencier 1) les crimes traditionnels assistés par ordinateur, où la nature du crime est différente en raison de la nature des environnements en ligne ; et 2) les nouveaux types de crimes, impliquant la confidentialité, l'intégrité ou la disponibilité des données numériques ou des systèmes informatiques (ici, la criminalité informatique se superpose à la sécurité numérique), impliquant à la fois des crimes avec et des crimes contre un ordinateur.

6.1.2 Cybercriminalité

L'essor d'Internet et du Web, l'interconnexion des systèmes informatiques et l'utilisation accrue d'hyperliens entre diverses informations au sein d'un réseau marqua le passage de la criminalité informatique à la cybercriminalité. On peut dire sans se tromper que l'on vit dans un monde bien différent d'il y a vingt ans, cela étant dû à la croissance exponentielle des capacités de calculs et à l'hyperconnectivité des machines. Cela rend la cybercriminalité différente dans **six dimensions** des rapports humains, et ce de manière hautement pertinente pour le droit pénal :

la distance La cybercriminalité n'appréhende pas les frontières et les territoires de manière traditionnelle

l'échelle La possibilité d'automatiser les attaques changent de manière drastique l'échelle des ces dernières

la vitesse On parle ici des capacités de calculs des ordinateurs et de leur hyper-connectivité

le caractère distribué Il est attaché à la nature réticulaire des systèmes informatiques

3. Va falloir vous faire au fait que beaucoup de termes seront préfixés par *cyber* dans ce chapitre.

l'invisibilité Cette dimension fait référence à la difficulté que peuvent avoir les utilisatrices finales·aux à déterminer ce qui relève des interfaces (*front-end*) et de la partie terminale (*back-end*)

la visibilité Cette dernière différence fait référence aux possibilités d'inférence du *big data* et aux nouvelles menaces que cela permet.

Ces nouvelles frontières du crime rendent la tâche difficile pour les États, qui peinent à combattre la cybercriminalité à cause des dimensions sus-citées. De nouvelles collaborations supra- et inter-nationales sont donc nécessaires.

6.2 Cybercriminalité et droit public

Comme on l'a vu plus haut, le droit public est constitué du droit constitutionnel, du droit public international et du droit administratif. Le droit constitutionnel est pertinent pour la cybercriminalité en ce qu'il détermine le droit à un procès équitable, le principe de légalité du droit pénal et le droit à la vie privée. Le droit public international lui est pertinent car la cybercriminalité a une nature internationale qui requière une coopération entre États. Enfin, le droit administratif est pertinent dans la mesure où la cybersécurité impose des obligations sur les États membres.

6.2.1 La Convention sur la Cybercriminalité

La Convention sur la Cybercriminalité (CC) a été initiée par le Conseil de l'Europe bien que certains pays en dehors de l'Europe furent impliqués dès le début, tels que les USA, le Canada, le Japon et l'Afrique du Sud. C'est aujourd'hui le traité sur la cybercriminalité à la portée la plus importante au niveau mondial. Il a été signé le 23 novembre 2001. Ses idées principales sont 1) un accord sur les nouvelles compétences permettant d'enquêter sur la cybercriminalité, 2) des définitions communes de ce que sont les comportements criminels dans le cyberspace, tout en 3) s'assurant que le principe de certitude juridique est garanti au travers des frontières et que 4) un niveau de protection juridique pour les droits humains est garanti.

Le fait que la CC relève du droit international et non supranational signifie qu'elle a un effet direct en fonction de si les EMs possèdent un système moniste ou dualiste. En pratique, la CC ne possède pas vraiment d'effet direct et doit tout d'abord être implémentée en droit national. Ce manque d'effet direct soulève des questions telles que :

- Est-ce que la police peut baser ses enquêtes relatives à la cybercriminalité sur la CC ?
- Est-ce qu'une victime de fraude bancaire peut poursuivre en justice le coupable ?
- Est-ce qu'une cour néerlandaise peut traduire en justice sur la base de la CC ?

Si on a été attentif à ce qui a été dit jusque-là, les réponses devraient être claires : elles sont négatives dans tous les cas, il faut d'abord une interprétation en droit national de la CC.

Voyons maintenant brièvement le contenu de la CC.

Droit substantiel

Tout d'abord, rappelons que la CC se base sur le *principe de légalité du droit pénal* : pas de sanctions sans criminalisation.

Le premier ensemble d'infractions pénales concerne les crimes liés au trio CIA, à savoir les accès illégaux, les interceptions et les attents à l'intégrité de systèmes comme de données. Un **accès illégal** est criminalisée par l'Article 2 de la CC, il faut pour cela avoir commis un acte

d'intrusion *intentionnel et sans droit à tout ou partie d'un système informatique*. Un EM peut aussi exiger des conditions supplémentaires pour qualifier un acte de criminel, telles que l'enfreinte à des mesures de sécurité, l'intention d'obtenir des données informatiques de façon malhonnête et la relation avec un système informatique connecté à un autre système informatique. On peut alors se poser la question de ce qu'il en est du hacking éthique, qui a vocation à tester la sécurité des systèmes en essayant de s'y introduire afin de mieux les protéger ? D'un point de vue éthique, on fait la différence entre les black hats⁴ (aux intentions malveillantes), les white hats (aux intentions bienveillantes et dotés de permissions) et les grey hats (aux intentions bienveillantes mais sans permission). Cependant, d'un point de vue juridique, l'intention importe peu : c'est essentiellement la permission qui compte (sauf dans certains cas exceptionnels, comme la police qui peut avoir certaines prérogatives). On distingue alors trois cas pour prévenir les sanctions en cas de grey hat hacking (les deux autres types sont généralement sans ambiguïtés).

Dans le premier cas, le procureur peut décider de ne pas poursuivre en justice s'il n'y trouve pas d'intérêt, ça peut être le cas si le hacker a suivi un processus de divulgation responsable. Dans le second cas, la sanction est empêchée car une justification juridique est trouvée (bien que l'intrusion n'ait pas été permise). On peut alors imaginer qu'un devoir plus élevé a supplanté le devoir de non-intrusion, c'est alors à la cour de décider (ce qu'elle fait de manière prudente du fait des potentielles implications). Enfin dans le troisième cas, la cour peut décider de reconnaître le hacker coupable sans lui administrer de sanction, ce qui envoie très clairement des signaux de désaccord avec l'acte sans toutefois trouver de raisons suffisantes pour administrer une sanction.

Une autre infraction pénale liée au trio CIA est spécifiée dans l'Article 3 de la CC, l'**interception illégale**, ce qui correspond à *l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques*. Pour être criminalisée, une interception doit avoir été commise intentionnellement, sans en avoir le droit et par des moyens techniques. Comme pour l'accès illégal, un EM peut exiger certaines conditions supplémentaires, à savoir l'intention malhonnête et la relation avec un système informatique connecté à un autre système informatique.

L'Article 4 de la CC stipule la criminalisation de l'**attente à l'intégrité des données**, ce qui correspond au fait *d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques*. Les conditions juridiques sont alors l'intention de l'acte sans droit, et une seule condition supplémentaire peut être ajoutée : si l'acte *entraîne des dommages sérieux*.

Enfin, l'Article 5 de la CC criminalise l'**attente à l'intégrité des systèmes**, c'est-à-dire *l'entrave grave [...] au fonctionnement d'un système informatique*, si celle-ci est intentionnelle et sans droit, et commise par *l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques*.

La CC décrit aussi des infractions plus traditionnelles telles que la fraude à l'identité, la pornographie infantile et les violations de copyright, que nous ne décrivons pas plus en détail ici.

Droit procédural

La seconde partie de la CC concerne le droit procédural, qui stipule les pouvoirs attribués aux autorités de police et de justice : la conservation accélérée (*expedited*) des données informatiques (de trafic et de contenu), les ordres de production, la perquisition et la saisie, ainsi que l'interception (de métadonnées comme de contenu). On fournira ici une analyse de l'ordre de production et du pouvoir juridique à conduire des perquisitions, le reste étant laissé aux lectrices intéressées.

4. Je ne traduis pas car on utilise les termes tels quels en français.

On a vu dans la Section 2.2.1 que les normes juridiques peuvent être primaires ou secondaires. Le premier ensemble de règles régulent les rapports entre humains grâce à des prohibitions et des obligations, tandis que le second ensemble constitue les compétences pour faire appliquer le premier ensemble. Le droit pénal substantiel peut être vu comme un ensemble de règles secondaires qui imposent des sanctions lorsque les normes primaires sont violées. Alors que la première partie de la CC stipule les normes primaires à protéger (en criminalisant certains comportements), la seconde partie peut être comprise comme un ensemble de règles secondaires qui définissent sous quelles conditions les autorités compétentes peuvent exercer leurs pouvoirs judiciaires afin de combattre la cybercriminalité.

Ainsi, l'Article 18 de la CC exige que les parties contractantes adoptent des pouvoirs judiciaires permettant à leurs autorités compétentes de *demandeur des données informatiques et des informations sur les abonnés*. Le principe de légalité est ici à l'œuvre : l'Article précise en effet que les autorités ne peuvent agir que sur un fondement juridique, certaines actions telles que les enquêtes requièrent même des fondements détaillés. Les compétences juridiques ont une fonction double : elles attribuent un pouvoir en même temps qu'elles le limitent. L'Article 18 exige aussi que les parties attribuent des pouvoirs juridiques spécifiques, en partant du principe que les autorités compétentes ne peuvent agir que dans les limites de la spécification qui constitue le pouvoir. Le deuxième paragraphe confirme cette affirmation en se référant aux Articles 14 et 15, qui limitent la portée des compétences d'enquête et stipulent que des garanties pertinentes doivent être mises en place.

Voyons maintenant rapidement le contenu de l'Article 19, qui exigent des parties contractantes qu'elles adoptent un pouvoir de *saisie et de perquisition des données informatiques stockées*. Le ¶4 donne la compétence d'exiger un mot de passe pour accéder à un système informatique, ou pour déchiffrer du contenu. Cependant, cette compétence (toutes celles précisées à vrai dire) est restreinte par des garde-fous (précisés dans les Articles 14 et 15), afin de s'assurer du principe de légalité. Dans ce cas précis, ça implique qu'une telle demande ne peut pas être dirigé à l'encontre d'un suspect, car ça violerait le principe de *nemo tenetur (se ipsum accusare)*, c'est-à-dire le *privilège contre l'auto-incrimination* (que l'on appelle aussi droit au silence). La CrEDH a par le passé lu ce droit dans l'Article 6 de la CEDH, bien qu'il n'y soit pas explicité. Ce droit protège en principe contre les contraintes justifiées, mais seulement dans une certaine mesure : il n'est pas absolu. Par exemple, il n'est pas parfaitement clair sous quelles conditions la CrEDH considérerait qu'une exigence de mot de passe est une violation de l'Article 6, ça dépendrait des garanties juridiques, des exigences de proportionnalité etc.

Notons enfin que la CC n'impose à aucun moment une obligation aux parties contractantes d'adopter un pouvoir permettant à la police un accès distant à des systèmes d'information. Ce n'est pas interdit non plus, mais **il n'y a aucune obligation de permettre l'accès à distance**.

Jurisdiction extra-territoriale pour l'application et l'enquête

Une autre réserve concerne la limitation d'accès au territoire d'enquête d'un État, tout d'abord dans le ¶1.b, qui limite la recherche aux bases de données sur le territoire de la partie contractante concernée; ensuite, selon le ¶2, une recherche dans un système distant dont on a déjà l'accès est restreinte aux cas où les autorités *ont des raisons fondées de croire que les données recherchées sont stockées sur un autre système informatique, ou sur une partie de celui-ci, localisé sur son propre territoire*. On touche ici à un principe fondamental du droit international, à savoir l'interdiction d'appliquer une juridiction extra-territoriale. Ce principe découle des deux souverainetés interne/externe qu'on a déjà évoqué à plusieurs reprises. L'interdiction de conduire une enquête sur le territoire d'un autre État est en vigueur depuis la fameuse affaire du Lotus

en 1927, et l'arrêt de la Cour permanente de justice internationale (CPJI) sur cette affaire. Dans cette affaire, il a été décidé que cette compétence d'exécution extra-territoriale n'est autorisée qu'en cas de permission accordée par l'État sur le territoire duquel les enquêtes ont lieu. Cette autorisation peut être ad hoc, mais elle peut également être fondée sur des traités d'assistance juridique mutuelle. L'Article 32 de la CC confirme cette interdiction à conduire une enquête extra-territoriale.

6.2.2 Les limites des pouvoirs d'enquête

Nous l'avons vu plus haut, le principe de légalité exige que les gouvernements agissent d'une manière non-arbitraire, suffisamment prévisible, proportionnelle et intégrée dans des garanties adéquates. Ça inclut le respect des droits humains, ainsi qu'une approche pro-active pour prévenir les potentiels risques envers la démocratie et l'État de droit. Comme mentionné brièvement, l'Article 15 exige de manière explicite que les parties contractantes implémentent les provisions concernées de la CC en accord avec les exigences que l'on peut attendre d'une démocratie constitutionnelle. En gros, l'Article 15 intègre le droit jurisprudentiel de la CrEDH (la plus haute cour du Conseil de l'Europe, qui a initié la CC) dans la CC.

Test de proportionnalité pour l'accès de la police à des données personnelles

Un exemple intéressant d'un test de proportionnalité concernant un accès par la police de données personnelles détenues par un Fournisseur d'Accès Internet (FAI) a été conduit par la CJUE lors de son jugement d'octobre 2018. Cette affaire concernait une demande policière d'obtenir des informations identifiantes sur des personnes ayant été en contact avec un smartphone volé, durant une période de 12 jours après qu'il ait été volé. La question était de savoir si ça constituait une interférence *sérieuse* avec les droits et libertés fondamentales des personnes concernées. Le ¶60 du jugement aborde un début de test de proportionnalité : y est fait mention le risque minimal d'intrusion dans la vie privée, pesé à l'aune des bénéfices potentiels. Le ¶61 conclut ainsi que la requête n'est pas une infraction *sérieuse*.

Test de proportionnalité, test d'équilibre et l'image de la balance

Pour terminer cette section, nous allons brièvement discuter de cette image de la balance, si souvent invoquée quand on soulève des questions de proportionnalité. Dans beaucoup d'ouvrages, on trouve l'idée que la sécurité et la liberté sont deux notions mutuellement exclusives, ce qui suggère qu'on ne peut pas avoir le beurre et l'argent du beurre : il y a forcément un compromis (*trade-off*) à faire, avoir plus de l'une implique qu'on a moins de l'autre. Ce n'est pas correct au regard de la sécurité numérique : des mesures telles que le chiffrement vont souvent établir ou renforcer les capacités d'une personne à faire des choix libres et bien informés quant au partage de ses données personnelles. Cependant, le contraire est tout aussi incorrect : certaines mesures nécessitent de la divulgation, des tests de pénétration, ou encore de l'inspection profonde de paquets réseau (*deep packet inspection*), afin de faciliter le monitoring d'attaques, ce qui entraîne nécessairement une violation des droits et des libertés des individus (notamment quand ces mesures sont invisibles ou tenues secrètes).

L'idée que des mesures sécuritaires et les droits à la liberté doivent être comprises en tant que compromis n'est pas restreinte au domaine de la cybersécurité. Cette idée traverse l'ensemble des sciences politiques où l'on fait référence à la sécurité nationale ou publique, au combat contre le terrorisme transnational ou contre les agences d'information étrangères qui visent les infrastructures critiques et les processus démocratiques. Dans ce domaine, la sécurité fait référence aux menaces envers l'autonomie et l'intégrité corporelle d'une personne, à la résilience d'une

organisation, à l'existence même d'un État ou à sa santé économique, en fonction de ce qui est visé. Dans ce sens, la sécurité (*security*) est un sous-domaine de la sûreté (*safety*), sous-domaine qui fait aussi référence à des menaces, cependant pas forcément fondées sur des cibles délibérées.

Dans le contexte du droit de la cybercriminalité, la discussion plus large d'un compromis entre la sécurité et les libertés se retrouve chaque fois que les mesures d'investigation portent atteinte aux droits humains tels que la vie privée, la liberté d'expression ou encore le privilège contre l'auto-incrimination. La CC, comme nous l'avons vu précédemment, exige la proportionnalité entre les mesures d'infractions et l'objectif que l'on veut protéger. Il est essentiel de reconnaître que cette proportionnalité n'est pas équivalente au compromis qui est souvent suggéré lorsque l'image de la balance est invoquée (plus de protection de la sécurité exige moins de protection des droits humains), mais nous ne devons pas non plus adopter la position inverse selon laquelle un tel compromis n'arrive jamais.

Dans un article fondamental, écrit peu après les attentats du 11 septembre 2001 contre le World Trade Center de New York, le philosophe du droit Jeremy Waldron a formulé six mises en garde contre l'invocation de cette image de la balance :

1. la diminution des libertés n'augmente pas automatiquement la sécurité (le compromis n'est pas un donné) ;
2. la balance suggère une précision qui est absente, parce qu'un *tertium comparationis* est généralement absent ;
3. les libertés ne peuvent pas être échangées à volonté, elles sont la condition préalable à un gouvernement légitime ;
4. négocier de la liberté contre la sécurité génère souvent un effet distributif (échange de la liberté d'un groupe pour augmenter la sécurité d'un autre groupe) ;
5. la diminution des libertés augmentera l'insécurité par rapport à l'État ;
6. la balance a une valeur symbolique élevée ; elle peut ne contenir aucune garantie effective.

Parfois, une sécurité accrue nécessite une atteinte à la vie privée, mais ce n'est pas nécessairement le cas. Certaines mesures de sécurité numérique peuvent en effet accroître la protection de la vie privée, comme par exemple le chiffrement de bout en bout. Cependant, dans le domaine des enquêtes policières sur la cybercriminalité, alors que la police peut utiliser ces mesures pour sa communication interne, les consommatrices qui les emploient peuvent être considérées comme une obstruction aux enquêtes policières. Dans le contexte de la cybercriminalité, les mesures de sécurité concernent l'accès de la police aux systèmes informatiques, les ordres de production et l'interception. Le premier point soulevé par Waldron souligne que le simple fait que ces mesures portent atteinte à la vie privée n'implique pas automatiquement qu'elles renforcent la sécurité publique : *si a alors b* n'implique pas que *si b alors a*. Tout cela est également lié à son sixième point : les mesures de sécurité promettent souvent plus qu'elles ne peuvent effectivement réaliser. Il faut s'y attendre en soi, mais lorsqu'on procède à un test d'équilibre, on doit accepter que des mesures inefficaces ne peuvent être nécessaires, et donc non proportionnelles.

6.3 Les directives européennes sur la cybercriminalité et la cybersécurité

Au sens strict du terme, la Directive relative aux attaques contre les systèmes d'information (2013/40/UE) est la Directive européenne contre la cybercriminalité. Tant dans ses objectifs que dans sa valeur instrumentale, elle recoupe la CC, qui exige des États membres de l'UE qu'ils criminalisent l'accès illégal, les attaques contre les systèmes d'information et les données informatiques, ainsi que l'interception illégale (droit pénal substantiel). À l'exception de la CC, elle ne

concerne pas la criminalisation de la fraude, de la pédopornographie ou des violations des droits d'auteur, se concentrant clairement sur les infractions liées au trio CIA. De même, contrairement à la CC, elle n'impose pas d'obligations en matière de procédure pénale et d'enquêtes criminelles. Le but de la Directive est une harmonisation minimale, ce qui signifie que les EMs peuvent aller plus loin que ce qui est exigé, mais pas en deçà.

De manière intéressante, cette directive oblige les EMs à imposer des sanctions *minimales et maximales* pour des cybercrimes spécifiques. Le droit pénal est souvent considéré comme essentiel à la souveraineté interne, ce qui signifie que les États résistent à l'ingérence supranationale dans leur politique pénale. En stipulant des peines minimales et maximales, le droit européen réserve une marge de manœuvre aux EMs qui rejettent les peines minimales ou autorisent la condamnation sans peine. La Directive accorde une attention particulière à la responsabilité pénale des personnes morales et aux questions de compétence, et prévoit divers types de collaboration transnationale au sein de l'Union (par exemple, l'échange d'informations via des points de contact nationaux et la collecte de statistiques pertinentes).

Outre la *vraie* directive européenne sur la cybercriminalité, l'UE a également adopté une directive sur la cybersécurité, la Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (2016/1148), qui n'a pas de surnom en français mais que l'on appelle NIS comme en anglais.

La Directive NIS ne concerne pas le droit pénal, qui - comme le montre l'Article 2, ¶6 - peut même être en contradiction avec l'échange d'informations qui est au cœur de la Directive NIS. Cela montre bien qu'il ne faut pas confondre cybersécurité et cybercriminalité. Les cybercrimes liés à la CIA concernent essentiellement la criminalisation des attaques contre la cybersécurité, telles que l'accès illégal, les attaques contre les systèmes d'information et l'interception illégale. En ce sens, la Directive NIS recoupe la CC et la Directive sur la cybercriminalité dans son objectif d'identification, de prévention et de dissuasion des menaces pour la cybersécurité.

Notez que l'Article 2 de la Directive NIS stipule que les données à caractère personnel traitées en vertu de cette directive relèvent du champ d'application de la DPD (aujourd'hui le RGPD), ce qui signifie qu'elles ne relèvent pas du champ d'application de la Directive Police Justice (qui est axée sur le traitement des données à caractère personnel *par les autorités compétentes à des fins de prévention, d'enquête, de détection ou de poursuite des infractions pénales ou d'exécution des sanctions pénales, et sur la libre circulation de ces données*). Ceci, une fois de plus, clarifie la différence entre la cybersécurité et la cybercriminalité.

En définissant la sécurité en terme de résilience contre *toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité*, la Directive NIS s'ancre bien dans les préoccupations CIA qui définissent la cybersécurité.

Chapitre 7

Le droit d'auteur dans le cyberspace

Pour les informaticien·nes, la partie la plus importante du droit d'auteur concerne les programmes informatiques, qu'on appelle plus communément logiciels. Dans ce chapitre, on fournira une introduction à la propriété intellectuelle (PI), dont le droit d'auteur (*copyright*) est un exemple important. Avant de s'attarder sur le droit d'auteur appliqué aux logiciels, qui est la condition préalable pour la General Public Licence (GPL) et l'initiative open source en général, on s'intéressera tout d'abord à la position qu'a la PI dans le contexte d'une démocratie constitutionnelle et on clarifiera ce qu'est la PI en droit privé.

On a vu dans la Section 2 que le rôle du droit et de l'État de droit était à la fois constitutif et limitatif. Son rôle constitutif se retrouve dans la constitution d'une architecture qui permet aux individu·es de s'épanouir en société, grâce aux principes de **certitude juridique**, de **justice** et d'**intentionnalité du droit**. Une partie de cette architecture cherche à créer des incitations tel qu'un marché économique, qui stimule les transactions qui en échange stimulent la productivité des biens et des services. L'État de droit implique que les pouvoirs juridiques qui constituent cette architecture soient simultanément restreints, introduisant ainsi les freins et contrepoids pour un marché économique juste et ouvert.

L'attribution d'une propriété intellectuelle crée supposément une structure incitant à la création de travaux, d'inventions intellectuelles, de marques déposées et de conceptions. Puisque ces droits fournissent à la fois du contrôle et la capacité à récolter les récompenses financières pour les auteurices ou inventeurices, ils incitent à la création de bien immatériels qui ne seraient pas protégés autrement. La raison est que si ce contrôle n'était pas protégé par le droit, il serait très difficile de protéger les travaux et inventions autrement que par le secret.¹

À la différence des biens tangibles et des biens matériels, les biens intellectuels ne sont ni rivaux ni exclusifs : une personne accédant à des travaux n'implique pas que d'autres ne puissent plus y accéder, un raisonnement similaire peut s'appliquer à l'utilisation d'une invention.

Le rôle limitatif du droit qui cherche à protéger les citoyen·nes, en tant qu'ils méritent un respect et une considération égale, peut être retracé au fait que la PI diffère d'autres droits de propriété en deux points principaux :

1. Bon, je ne vous cache pas que je suis assez en désaccord avec cette vision. Par souci d'honnêteté intellectuelle je laisse le texte en l'état, mais je vous conseille urgemment d'aller voir la série de vidéos de Philoxime <https://www.youtube.com/playlist?list=PLyh4DKd62N23iaCKQungwsv1JSLXVwcCN> sur le sujet de la propriété intellectuelle. C'est un philosophe du droit qui fait des vidéos accessibles, et en l'occurrence qui tempèrent un peu ce paradigme comme quoi les brevets incitent à la création intellectuelle.

- ils sont limités dans le temps
- une œuvre entre dans le domaine public au bout d'une certaine période de temps

En gros, la création des droits relatifs à la PI assure que les ayant-droits ont une incitation à partager leurs œuvres grâce aux récompenses qu'ils peuvent en tirer, tout en s'assurant que les œuvres en question deviennent disponibles après une certaine période de temps. Le droit de la PI a aussi un rôle limitatif en ce qu'il impose certaines restrictions à l'exercice des droits liés à la PI, par exemple la doctrine de *common law* dite d'usage raisonnable (*fair use*) ou la doctrine européenne d'usage personnel (*home copy*).

7.1 Le droit de la PI en tant que droit privé

On a vu dans la Section 3.1.1 la différence entre droits absolus et relatifs en droit privé en se représentant un système juridique comme une architecture de relations juridiques, à la fois entre l'État et ses sujets juridiques, mais aussi entre ces sujets. La propriété est un droit absolu dans le sens où elle peut être appliquée à l'encontre de quiconque : tout un·e chacun·e se doit de respecter le droit du ou de la propriétaire. Un contrat, lui, crée des droits relatifs qui ne peuvent être appliqués qu'envers les parties contractantes, puisqu'il est basé sur le consentement et ne contraint ainsi que ceux qui consentent audit contrat. Un contrat crée ainsi deux droits relatifs, par exemple dans le cas d'un contrat de vente :

- le droit de la partie acquérante à bénéficier du bien
- le droit de la partie cessionnaire à être rétribuée

Le droit de la PI fournit aux autrices, inventeurices et autres ayant-droits un droit de propriété sur le *bien intellectuel* qu'ils ont créé ou inventé (éventuellement acheté). Le droit de la PI relève donc du droit privé, bien que le droit international public joue un rôle important en exigeant des États qu'ils protègent les droits de PI. Comme un droit absolu doit être appliqué à l'encontre de quiconque, tout le monde doit en être informé, on a besoin d'une forme de publicité. Dans le cadre de biens tangibles, la possession physique va de soi, et pour ce qui est des biens immobiliers et de PI, cela se fait par le biais d'un enregistrement. Dans le cadre du droit d'auteur, cette publicité est souvent indiquée par un signe ©. Notons que ça ne fait qu'indiquer le droit d'auteur, ça ne le constitue pas en tant que tel.

Le droit d'auteur fournit ainsi la liberté à disposer d'un droit absolu sur un travail. Une licence copyright est par contre un droit relatif. Quiconque détient le droit absolu sur une œuvre peut décider d'accorder une licence à une autre personne pour qu'elle exerce certains de ses droits, par exemple le droit de reproduire et de publier. Cela crée une relation juridique entre le concédant et le licencié (*licensor and licensee*).

Un autre droit relatif qui peut être en jeu dans le cas du droit d'auteur est le droit à une indemnisation, ou le droit à une mesure injonctive dans le cas d'un délit. Ce droit est très important lorsque des tiers violent le droit d'auteur d'un titulaire de droits en téléchargeant illégalement des œuvres sur lesquelles ils n'ont aucun droit. Cette responsabilité délictuelle exige du titulaire du droit qu'il apporte la preuve de l'illicéité, du dommage et du lien de causalité (s'il intente une action en réparation), tandis que le défendeur peut faire valoir une excuse (par exemple, qu'il ne savait pas qu'il violait le droit d'auteur car il a supposé, à tort mais raisonnablement, que l'œuvre était tombée dans le domaine public par le titulaire du droit ou en son nom).

Plus actuel encore, un détenteur de droits peut poursuivre un intermédiaire pour avoir indûment facilité la tâche d'autres personnes qui violent le droit d'auteur. Pensez à The Pirate Bay (TPB) et aux nombreuses tentatives pour obtenir des décisions de justice interdisant à TPB

de permettre le téléchargement de contenus protégés, ou des décisions de justice imposant aux FAIs l'obligation de filtrer et/ou de bloquer tout le trafic vers TPB. Notez que les titulaires de droits d'auteur sont souvent représentés officiellement par une personne morale qui a pour but statutaire de défendre leurs droits, car ils n'ont souvent pas les moyens de porter plainte eux-mêmes.

L'interaction entre les droits absolus et relatifs sur une œuvre peut être complexe. Par exemple, comme nous le verrons un peu plus bas, une licence GPL oblige ceux qui partagent une œuvre à le partager uniquement sous les conditions de cette licence spécifique. Si un·e licencié·e viole cette obligation, le concédant peut engager des poursuites pour rupture de contrat, mais sans droit d'auteur, le concédant ne pourra pas faire appliquer les conditions pertinentes envers les tiers.

Précisément parce que le droit d'auteur est un droit absolu, il suit le *droit de suite* (en français dans le texte), peu importe le type de licence ultérieur. En ce sens, la protection de *logiciels libres* offerte par la licence GPL dépend du droit de propriété qui sous-tend la licence.

7.2 Vue d'ensemble des droits de la PI

Comme on a vu plus haut, les droits de la PI forment un ensemble fermé. Bien que ce chapitre se focalise sur le droit d'auteur, cette section offre une vue d'ensemble rapide sur les différents types de PI pertinents ici. Notez bien que ni une découverte ni une idée ne peuvent être protégées ; la protection est limitée à *l'expression d'une idée au travers d'un médium spécifique* ou à une *invention*, invention qui ne peut se résumer à une simple découverte.

7.2.1 Droit d'auteur

On distingue de manière générale deux types de droits d'auteur. Tout d'abord, le droit moral d'un·e auteur·ice à être crédité de la parentalité (*authorship*) de l'œuvre. Ce premier type de droit est absolu dans le sens où il peut être appliqué envers n'importe qui et n'est de plus pas transférable. On distingue ensuite deux types de droits économiques :

- un droit absolu applicable envers quiconque et transférable, qui permet la vente ou l'octroi de licence
- un droit relatif qui ne peut être appliqué qu'envers le concédant, donnant ainsi la possibilité de faire des licences logicielles par exemple.

Mais la différence est parfois floue entre ces deux types de droits. Ainsi dans l'arrêt *Oracle v. UsedSoft*, la CJUE a jugé que la vente d'une copie d'un programme logiciel avec des droits d'utilisations illimités doit être considérée comme une vente stricto sensu (avec transfert de propriété), même si le contrat parle bien de licence d'utilisation.

7.2.2 Brevet

Comme le droit d'auteur, un brevet a une durée limitée dans le temps, cette durée dépend bien sûr de la juridiction nationale. Pour être considéré comme un brevet, un bien intellectuel doit remplir de manière cumulative les conditions suivantes : 1) **être une invention**, 2) **innovatrice** avec 3) **une application industrielle**.

L'effet légal de l'octroi de brevet est que l'ayant-droit obtient le droit exclusif de l'exploitation commerciale, mais ce seulement si une *quatrième condition* juridique est remplie. Cette condition stipule qu'**une demande doit être faite**, cette demande doit divulguer la nouvelle invention et son application dans l'industrie. La première personne à en faire la demande obtient

le brevet. On voit ici qu'un brevet diffère substantiellement d'un droit d'auteur, ce dernier est en effet octroyé automatiquement à la création d'une œuvre, alors qu'un brevet n'est pas automatiquement attribué lors de la création d'une invention même si celle-ci est innovante et a une application industrielle. Notons que la politique de *premier arrivé premier servi* n'est pas vérifiée par le bureau des brevets, en cas de suspicion de *vol* de l'invention il faut engager une action en justice (et être en mesure de le prouver). Il est courant que plus d'un brevet s'applique à une seule application industrielle, dans ce cas, chaque ayant-droit peut empêcher l'exploitation commerciale par d'autres, ce qui signifie que quiconque souhaitant développer un modèle économique pour cette application doit s'assurer de la permission des autres ayant-droits. D'une certaine manière, un brevet comprend un *droit d'exclusion* qui prime sur le *droit d'exploitation* d'un autre (il en va de même pour le droit d'auteur conjoint).

Comme on peut se l'imaginer cependant, la définition même d'un brevet n'est pas sans soulever de questions :

- Qu'est-ce qui qualifie quelque chose d'invention ? Est-ce qu'une découverte d'un gène spécifique est une invention ou une découverte au sens large du terme ? La réponse a des implications fortes, qui soulève de vifs débats aujourd'hui.²
- À partir de quel moment une invention est-elle considérée comme innovante ? En droit américain, le caractère innovant signifie que l'invention est **nouvelle, utile et non-évidente**.
- Qu'est-ce qu'on entend par une application *industrielle* ?

7.2.3 Marque déposée

Une marque déposée est définie comme *des signes propres à identifier et à distinguer un produit ou un service*, et le droit de la PI sur une marque implique l'utilisation exclusive de ces signes. Comme pour un brevet, une marque doit être déposée (une demande doit être faite).

7.3 Histoire, objectifs et périmètre d'application du droit d'auteur

On l'a vu dans l'introduction, la production de documents était faite à la main avant l'invention de l'impression par Gutenberg en 1450. La prolifération de copies identiques de documents écrits donna lieu à une combinaison surprenante de censure et de privilège. En effet, les textes imprimés servaient notamment de support à des pamphlets et à des opinions pas forcément au goût des autorités (religieuses), qui s'empressèrent de contrôler la dissémination de telles idées. Ainsi, l'église catholique compila un Index des documents pécheurs soumis à la censure. Les souverains prirent le contrôle sur les éditeurs, en octroyant des privilèges à certains (ceux prêts à s'accorder sur la censure royale). Une lutte contre la censure s'instaura alors durant plusieurs siècles, et donna finalement lieu à un droit subjectif des auteurs. Ce qui est protégé est alors l'*œuvre* : ce n'est pas l'idée abstraite en soit, ni une instance matérielle, mais bien l'expression de l'idée sur un support.

Au cours du XVIII^{ème} siècle, l'idée que le choix de disséminer une œuvre devait être du ressort de l'auteur, et non pas de celui de l'éditeur, fut consolidée par divers décrets royaux en Angleterre, en France et aux USA. Ces actes furent les premiers à attribuer un *droit d'auteur*, fournissant ainsi des revenus aux auteurs tout en garantissant que les œuvres tombent dans le domaine public au bout d'une certaine période de temps. En droit d'auteur, le *domaine public*

2. Pensons aux luttes contre le brevetage du vivant.

7.3. HISTOIRE, OBJECTIFS ET PÉRIMÈTRE D'APPLICATION DU DROIT D'AUTEUR⁶¹

a un sens bien spécifique, il fait référence à toute œuvre sans droit exclusif, ce qui signifie que le public est libre d'accéder, de reproduire, de distribuer et de reproduire une telle œuvre.

Le droit d'auteur moderne coïncide donc avec l'essor des droits humains tels que la liberté d'expression. Ce processus aboutit en 1886 à la convention de Berne, qui permet la protection du droit d'auteur au-delà des frontières grâce à une harmonisation des droits nationaux.

La protection de la PI devint au XX^{ème} siècle une partie essentielle du commerce international, donnant ainsi un rôle prééminent à l'Organisation Mondiale du Commerce (OMC). On présentera cependant le droit de l'UE en la matière dans ce livre, ainsi que quelques comparaisons avec le droit américain.

Avant d'étudier le droit d'auteur de l'UE, on examinera d'abord brièvement comment la loi sur le droit d'auteur du Royaume-Uni et des États-Unis diffère de celle de l'Europe continentale. Dans la tradition de l'Europe continentale, l'accent a été mis sur l'auteurice et l'œuvre. Cette conception du droit des auteurs s'appuie sur le Romantisme du XVIII^{ème} et du XIX^{ème} siècle, où la singularité de l'imagination créative d'un·e auteurice individuel·le primait sur les intérêts commerciaux courants d'un éditeur. L'idée était que le droit d'auteur fait partie du droit naturel plutôt que d'être posé par un législateur (droit positif). Le droit des auteurs, dans cette ligne de pensée, est constitué par l'acte de création original de l'auteurice et ne devrait pas être lié à des formalités (telles que l'enregistrement), tandis que l'œuvre qui est créée appartient au domaine de l'auteurice. Il s'agit d'une question de droit de la personnalité (droit moral), et non de propriété (comme le voudrait Locke).

Dans la common law qui a inspiré le Royaume-Uni et les États-Unis, l'accent n'était pas mis sur l'auteurice et son œuvre, mais sur l'original et la copie. C'était moins une question de personnalité et d'imagination qu'une question de pragmatisme. Le droit d'auteur était simplement un choix fait par un législateur (toujours en droit positif), plutôt qu'un droit naturel inhérent à l'acte de création de l'auteurice. Cela a conduit à l'obligation d'enregistrement et à l'accent mis sur le droit d'auteur en tant que droit économique (et non pas en tant que droit moral). Ici, le droit d'auteur concerne le domaine de l'œuvre plutôt que celui de l'auteurice, et une telle œuvre est considérée comme *originale* dans le sens où elle ne peut être copiée, plutôt qu'*originale* dans le sens où elle est créative ou nouvelle.

Malgré ces différences, on considère généralement que la loi sur le droit d'auteur - tout comme la loi sur les brevets - a quatre objectifs, tant dans le domaine du droit anglo-américain que dans celui du droit européen continental :

1. récompenser l'auteurice ou l'inventeurice
2. fournir à l'auteurice et à l'inventeurice un contrôle d'exclusion sur l'utilisation que d'autres peuvent faire de leur travail ou de leur invention
3. encourager l'investissement dans l'expression créative, l'invention et l'innovation
4. assurer l'avantage sociétal d'avoir une telle expression ou invention dans le domaine public après une période de temps déterminée

Quant à l'étendue du droit d'auteur, nous pouvons résumer les droits de contrôle suivants : 1) publication (communication au public), 2) reproduction (faire une copie), 3) distribution (de l'original tangible ou de la copie), 4) droit d'interdire les droits 1, 2, 3, et 5) droit d'autoriser des tiers à exercer les droits de 1, 2, 3.

Notez que le droit exclusif de distribution du titulaire du droit est épuisé après la première vente, ce qui permet le partage de copies individuelles de livres (et la vente de livres d'occasion). En vertu de la directive européenne sur le droit d'auteur, cela ne s'applique pas à un livre électronique, car le droit de distribution ne concerne que les copies tangibles. Il en va autrement dans le cas d'un programme d'ordinateur qui relève du champ d'application de la directive européenne sur le droit d'auteur des logiciels, qui doit être interprétée comme stipulant que le

droit d'auteur est épuisé après la première vente, même si le logiciel a été téléchargé au lieu d'être fourni sur un support tangible.

7.4 Droit d'auteur dans l'UE

Comme on l'a vu ci-avant, le droit d'auteur relève du droit privé et fait partie des juridictions nationales des EMs. Il n'y pas vraiment de droit privé européen, mais plusieurs types de traités internationaux proposent des solutions aux interprétations inter-juridictionnels. Il n'y a pas plus de droit privé de l'UE, bien qu'il y ait des exceptions quand les EMs doivent intégrer des responsabilités de droit privé dans leurs juridictions nationales (sur des questions environnementales ou de droit à la protection des données par exemple).

Le cadre juridique de l'EU sur le droit d'auteur cherche à harmoniser le droit applicable au sein des EMs, de manière à assurer une protection équivalente pour les ayant-droits au sein du marché interne, stimulant ainsi les transactions économiques entre les frontières. Récemment, la Directive Copyright a subi une mise à jour majeure impliquant notamment deux mesures hautement controversées imposés aux FAIs (dites de *taxe de liaison* et une obligation de *police privée*, que nous discuterons peu après).

7.4.1 La Directive Copyright et la Directive relative au respect des droits de PI

Le cadre juridique de l'EU sur le droit d'auteur est basé sur la Directive Copyright et sur la Directive relative au respect des droits de PI. Les deux directives sont des *lex specialis*, ce qui signifie qu'elles fournissent de la législation spécifique sur le droit d'auteur appliqué aux logiciels et appliqué aux bases de données. On l'a vu plus haut, une *lex specialis* est prioritaire sur une *lex generalis*, tout comme *lex posterior derogat legi priori* : le droit le plus récent est prioritaire sur d'autres législations.

Le périmètre de protection (restrictions)

La Directive Copyright exige de EMs qu'ils offrent le périmètre d'application suivant, formulée en termes de *restrictions* :

- le droit exclusif à autoriser et à interdire la reproduction d'une œuvre (Article 2)
- le droit exclusif à autoriser et à interdire la publication et la *communication au public* d'une œuvre (Article 3)
- le droit exclusif à autoriser et à interdire la distribution d'une œuvre ou d'une de ses copies (Article 4) (le droit à la distribution étant épuisé après la première vente)
- de manière intéressante, la directive fournit aussi des mesures juridiques de protection contre le contournement de mesures techniques tels que les DRMs (*Digital Rights Management*) (Articles 6 et 7).

Les limites

Les limites, définies dans l'Article 5, concernent elles la reproduction, la distribution et la possible publication à des fins d'enseignement, de recherche scientifique, la caricature, la parodie ou le pastiche. Les limites signifient donc que les droits (restrictions) sont eux-mêmes limités. Une limite importante du droit d'auteur s'applique à l'usage privé, défini dans l'Article 5.2(b) *lorsqu'il s'agit de reproductions effectuées sur tout support par une personne physique pour un*

usage privé et à des fins non directement ou indirectement commerciales, à condition que les titulaires de droits reçoivent une compensation équitable.

7.4.2 La Directive concernant la protection juridique des programmes d'ordinateur

Cette directive a pour objet de protection un certain type d'œuvres littéraires que l'on appelle communément programmes informatiques. Comme pour les autres droits de PI vus jusque-là, c'est bien l'expression qui est protégée et non pas l'idée ou le principe, et la protection fait foi seulement si le programme est original, c'est-à-dire que c'est la création intellectuelle propre à un·e auteur·rice.

En bref, les Articles 2 et 3 détermine que l'ayant-droit est l'auteur·rice du programme, défini·e comme la·e créateur·rice du programme (modulo les liens de subordination salariaux). L'Article 4 définit les actes soumis à restriction (le périmètre de protection) au regard d'un programme. L'Article 5 définit de manière exhaustive les exceptions aux actes soumis à restrictions. L'Article 6 aborde la *décompilation* d'un programme, il stipule que la reproduction et la traduction de code (au sens de l'Article 2) est permise sans autorisation pour permettre l'interopérabilité (sous certaines conditions cependant).

Voyons maintenant deux affaires qui illustrent comment cette directive a été interprétée.

Exceptions au droit d'auteur exclusif sur les logiciels : *SAP v. WPL*

Cette affaire concernait les lignes de démarcation entre le droit d'exclusion de l'objet de la protection et les exceptions pertinentes lorsqu'on cherche à découvrir les idées et les fonctionnalités sous-jacentes du programme. SAS avait développé un programme d'analyse de données, dont une partie du programme aide les utilisateur·ices à construire leurs propres modules qui peuvent ensuite être utilisés avec cette même partie du programme d'analyse de SAS. World Programming Languages (WPL) vendait alors un programme qui imite la partie centrale du programme de SAS, créant ainsi une alternative pour les utilisateurs du programme de SAS. Pour protéger sa part de marché, SAS poursuivit WPL en justice pour violation du droit d'auteur de son logiciel. Il s'agissait essentiellement de savoir quand l'ingénierie inverse constitue une violation du droit d'auteur et quand elle entre dans le champ des exceptions pertinentes.

La CJUE a pour cela posé 3 questions, résumées avec leurs réponses ici :

1. *La fonctionnalité d'un programme d'ordinateur, le langage de programmation et le format des fichiers de données peuvent-ils être interprétés comme une forme d'expression, et donc être protégés par le droit d'auteur ?*

Ce a quoi elle a répondu que toute forme qui permet la reproduction d'un programme est protégée (le code donc) ; l'interface graphique, la fonctionnalité, le langage et le format de fichier ne l'est pas.³

2. *Quelle est la responsabilité d'un licencié - même s'il s'agit d'un concurrent - qui agit en dehors du cadre de cette licence pour observer et étudier le fonctionnement d'un programme d'ordinateur afin de déterminer les idées et les principes qui sous-tendent ce programme ?*

La CJUE répond en concluant qu'un·e licencié·e a le droit d'observer, d'étudier ou de tester le fonctionnement d'un logiciel afin de déterminer les idées et les principes qui sous-tendent tous les éléments du programme, pour autant qu'il ne viole pas le droit d'auteur, par exemple en utilisant le code source ou le code objet.

3. En tant qu'informaticien je trouve ça très étrange : une interface graphique peut tout à fait être du code.

3. *La reproduction dans un programme (ou dans le manuel d'utilisation de ce programme) de matériel décrit dans le manuel d'utilisation d'un autre programme (protégé par le droit d'auteur) constitue-t-elle une violation du droit d'auteur ?*

La CJUE conclut que la reproduction d'éléments particuliers dans un manuel d'utilisation d'un programme d'ordinateur peut constituer une violation du droit d'auteur, si le matériel reproduit constitue une expression de la création intellectuelle de l'auteur. Alors que les mots-clés, la syntaxe, les commandes, les combinaisons de commandes, les options, les valeurs par défaut et les itérations constituées de mots, de chiffres ou de concepts mathématiques ne sont pas protégés par le droit d'auteur en eux-mêmes, ils peuvent l'être s'ils sont combinés d'une manière qui constitue une création intellectuelle.

Exceptions au droit d'auteur exclusif sur les logiciels : Microsoft

Cette affaire concerne l'interprétation des Articles 4.2, 5.1 et 2 de la Directive, elle est survenue dans un contexte de procédure pénale (une vente illégale d'objets protégés par copyright sur un support non-original).

La Cour rappelle les conditions de ce qu'est une *vente*, puis que ces conditions ne font pas de distinction selon la forme (matérielle ou immatérielle) d'une copie. Cela implique qu'une copie téléchargée légalement doit être considérée comme équivalente à une copie stockée sur un DVD, en ce qui concerne l'épuisement de la première vente. Notez la différence avec la directive générale sur le droit d'auteur, qui limite cette limitation à la première vente de copies tangibles.

Les faits en l'espèce concernent toutefois la revente d'une copie de sauvegarde du logiciel concerné, car MM. Ranks et Vasiļevičs n'avaient plus accès à la copie originale. Ils ont fait valoir que, comme ils avaient le droit de faire une copie de sauvegarde afin d'utiliser la copie originale (Article 5.2), ils pouvaient vendre une telle copie de sauvegarde en vertu de l'exception d'épuisement après la première vente de l'Article 4.2. La CJUE estima cependant que *la copie de sauvegarde d'un programme d'ordinateur ne peut être réalisée et utilisée que pour répondre aux seuls besoins de la personne ayant le droit d'utiliser ce programme et que, par conséquent, cette personne ne peut pas - même si elle a endommagé, détruit ou perdu le support matériel original - utiliser cette copie pour revendre ce programme à un tiers* (¶43).

7.5 Open source et accès libre

En 1983, Richard Stallman lance le projet GNU et publie le manifeste éponyme dans lequel il explique :

GNU, l'acronyme de GNU's Not Unix (GNU N'est pas Unix), est le nom du système complet de logiciels, compatible avec Unix, que je suis en train d'écrire pour pouvoir le donner [give away free] à qui en aura l'usage. J'ai l'aide de plusieurs autres bénévoles. Les contributions en temps, en argent, en logiciel et en équipement nous sont indispensables.

Il fonde en 1985 la Free Software Foundation (FSF), qui a pour but de développer et de partager du logiciel sous licence publique générale GNU (*GNU General Public License*, abrégé GPL).

En 1991, Linus Torvalds développe le noyau Linux, cherchant ainsi à permettre des interactions entre les parties logicielles et matérielles. Avec la suite logicielle GNU développée dans le cadre du projet du même nom, Linux⁴ forme un système d'exploitation. Linux est libre d'utili-

4. Oui oui je sais on dit GNU/Linux.

sation, chacun·e est libre de contribuer à son développement.⁵

En 1998, l'Open Source Initiative (OSI) est créée, elle ne fait pas seulement référence à la liberté d'utiliser du logiciel : elle inclut aussi la nécessité d'ouvrir le code source.

La FSF définit ainsi quatre libertés fondamentales pour du logiciel libre :

- *la liberté de faire fonctionner le programme comme vous voulez, pour n'importe quel usage (liberté 0) ;*
- *la liberté d'étudier le fonctionnement du programme, et de le modifier pour qu'il effectue vos tâches informatiques comme vous le souhaitez (liberté 1) ; l'accès au code source est une condition nécessaire ;*
- *la liberté de redistribuer des copies, donc d'aider les autres (liberté 2) ;*
- *la liberté de distribuer aux autres des copies de vos versions modifiées (liberté 3) ; en faisant cela, vous donnez à toute la communauté une possibilité de profiter de vos changements ; l'accès au code source est une condition nécessaire.*⁶

Pour s'assurer que le logiciel reste libre au sens défini plus haut, un ensemble de licences a été défini, exigeant que le logiciel ne puisse être développé et partagé qu'avec une licence équivalente. Cette exigence peut être **absolue**, dans le sens où la liberté devient *virale* ; ajouter des restrictions au code devient impossible pour les utilisateurices ultérieures ; chaque œuvre dérivée devienne contaminée par les mêmes exigences au moyen de la même licence (on appelle aussi ça le *copyleft*). Cette exigence de liberté peut aussi être **relative** : l'effet viral n'est pas jugé nécessaire, et on permet alors aux versions ultérieures de faire partie de logiciels sous licences propriétaires.

En 2001, le juriste Lawrence Lessig lance l'initiative des Creative Commons (cc), transposant ainsi l'idée de l'open source à des créations non-logicielles. Les Creative Commons ont développé un ensemble de licences différentes, permettant un contrôle plus granulaire des versions ultérieures de la même expression créative (voir Figure 7.1).

Aujourd'hui, de nombreux modèles d'accès libre (*open access*) ont été développés dans le domaine du droit des brevets, par exemple en créant des bases de données accessibles au public (recherche scientifique, par exemple le projet du génome humain) pour alimenter le domaine public, et comme stratégie de défense, puisque la diffusion publique empêche le brevetage. Cela peut être combiné avec l'interdiction des restrictions en aval par le copyleft, par exemple avec HAPMAP (concerne uniquement les données, pas les applications dérivées), BIOS (application à l'invention brevetée, bien que les améliorations puissent être brevetées).

En ce qui concerne plus particulièrement les pays en développement, une licence d'accès équitable et une licence pour les maladies négligées ont été proposées. Enfin, nous pouvons observer une consolidation de cet élan dans l'Open Science Initiative de Budapest de 2001, la Déclaration de Berlin de 2003 sur l'accès libre à la connaissance dans les sciences et les humanités, et le Science Commons de 2007.

Le noyau commun de toutes ces variétés de modèles de sources ouvertes, de logiciels libres et d'accès ouvert est le suivant :

- 1) l'affirmation du droit de propriété intellectuelle, 2) l'utilisation inversée de l'exclusivité, et 3) l'absence de discrimination.

Il est essentiel de se rappeler que les licences Creative Commons n'ont aucun sens sans le droit de propriété sous-jacent sur l'œuvre qui est développée et partagée.

5. En pratique la contribution est structurée, tout le monde ne peut pas faire n'importe quoi et heureusement, cela peut par contre donner lieu à une certaine asymétrie de pouvoir.

6. Les valeurs de logiciel libre prônées par la FSF comprennent donc l'ouverture du code, ce qui ne l'empêche pas de s'opposer à l'open source, je cite : *Associer GNU avec le terme open source est une erreur dans la mesure où ce terme fut inventé en 1998 par des gens en désaccord avec les valeurs éthiques du mouvement du logiciel libre. Ils l'utilisent pour promouvoir une approche amoral du même domaine.*








LOGO	LICENCE	SIGLE
	Zero (domaine public)	CC0
	Attribution	BY
	Attribution/pas de modification	BY ND
	Attribution/pas d'utilisation commerciale/pas de modification	BY NC ND
	Attribution/pas d'utilisation commerciale	BY NC
	Attribution/pas d'utilisation commerciale/partage dans les mêmes conditions	BY NC SA
	Attribution/partage dans les mêmes conditions	BY SA

FIGURE 7.1 – Les combinaisons des licences CC.

Chapitre 8

Responsabilité de droit privée pour les systèmes informatiques défectueux

Imaginons qu'une nouvelle version d'un système d'exploitation soit lancée, permettant ainsi le choix entre une mise à jour manuelle et automatique. Est-ce qu'une mise à jour aura alors un effet légal ? On peut en effet se dire que les utilisatrices effectuant la mise à jour manuelle encourent des risques de sécurité si une mise à jour n'est pas faite à temps. Peut-être même que certaines versions du système d'exploitation ne seront plus supportées au bout d'un certain temps, laissant ainsi certaines utilisatrices à découvert. Ou encore que les mises à jour automatiques installent des logiciels espions par inadvertance.

On peut imaginer une autre situation dans laquelle un frigo connecté communique avec certains fournisseurs de composants ou responsables d'applications. Est-ce que ces communications ont alors un effet légal ? Le frigo peut être confronté à des coupures d'électricité causant ainsi des électrocutions, alors que ça aurait pu être prévu par son logiciel. Le frigo peut être basé sur un *smart contract* implémentée dans une blockchain, contrat qui déconnecte le frigo suite à un défaut de paiement causant cette fois un court-circuit. Il peut aussi commander plusieurs fois la même nourriture à plusieurs services de livraison à cause d'un bug, sans que ces commandes puissent être annulées.

La lectrice peut facilement imaginer d'autres cas où des technologies de l'information et de la communication (TIC) - qu'elles soient adaptatives ou auto-exécutives - causent des dommages physiques, matériels, économiques ou émotionnels. Par exemple, que se passe-t-il si l'on rate un rendez-vous important parce que la machine à laver prend feu (dommage matériel à la machine, à la salle de bain), ce qui entraîne l'inexécution d'un contrat et une perte de revenus (dommage économique), ou si l'on est témoin d'imposantes lésions corporelles ou du décès d'un proche parent à cause de l'incendie, ce qui entraîne un syndrome de stress post-traumatique (dommage émotionnel) ? Peut-être que le fait que les données personnelles d'une personne aient été divulguées par une compagnie d'assurance dans le cadre d'une importante violation de données provoque une anxiété durable, à propos de qui a pu accéder à ces données, les vendre ou les partager d'une autre manière.

La question de savoir si le fait d'avoir causé un tel dommage peut avoir des effets juridiques relève du droit de la responsabilité civile. Les conditions juridiques d'un tel effet juridique exigent que ces préjudices puissent être attribués, par exemple, au fabricant, au fournisseur du système

d'exploitation, au détaillant, à la compagnie d'assurance où une violation a eu lieu, au fournisseur du service d'assistance qui a donné un mauvais conseil, ou à l'entreprise qui a loué la voiture, la machine à laver ou le réfrigérateur (car cette entreprise peut avoir modifié les paramètres par défaut du fabricant, causant ainsi le préjudice).

Peut-être, en revanche, la machine à laver ne fonctionne-t-elle tout simplement plus aussi bien qu'avant, depuis qu'une mise à jour a été installée. Peut-être que les freins d'une voiture connectée sont en turbulence à cause d'un bug dans l'OS. Se pose alors la question de savoir si l'on peut poursuivre le vendeur sur la base de la non-conformité du produit ou du service à ce que l'on pouvait raisonnablement attendre, compte tenu de sa fonction et de son prix, ou sur la base d'un défaut.

Dans ce chapitre, on se concentrera sur la responsabilité civile comme un exemple important de la manière dont la responsabilité de droit privé peut intervenir pour dissuader les développeurs, les fabricants, les vendeurs et les utilisatrices de TIC de développer, vendre ou utiliser des TIC défectueuses.

8.1 Droit de la responsabilité civile en Europe

En Europe continentale, ainsi que dans certaines parties de l'Afrique, de l'Amérique latine et de l'Asie influencées par ses systèmes juridiques, le droit privé a été codifié par le législateur. On peut par exemple trouver en France le Code Civil, le Bürgerliches Gesetzbuch en Allemagne, ou encore le Burgerlijk Wetboek aux Pays-bas. Ces systèmes juridiques sont généralement désignés par la tradition du *droit civil*. En Grande-Bretagne, aux USA, au Canada, en Australie et en Inde, le droit privé fait partie du droit commun (*common law*), qui se base sur les *précédents* ou la jurisprudence, plutôt que sur une codification. Ça peut mener à la conclusion que le code (le droit codifié) est la seule chose qui importe dans la tradition de droit civil, alors que dans la *common law* tout dépend de l'adhésion aux précédents ou à la jurisprudence. Ce n'est plus vrai aujourd'hui.

Alors que le droit civil s'inspire de la législation, l'interprétation du code exige une attention particulière à la jurisprudence antérieure; alors que la *common law* s'inspire des antécédents jurisprudentiels, son interprétation exige une attention particulière des règles implicites et des principes qui implique une systématisation similaire à celle recherchée par la codification. De plus, une myriade de lois statutaires ont été promulguées dans les juridictions de *common law*.

Dans cette section, on révisera rapidement les principales conditions juridiques à remplir pour parler d'un acte délictueux (n'hésitez pas à relire la Section 3.2.3). On prendra en compte les diverses juridictions civiles comme de *common law* qui *composent* l'Europe, car du fait que le Royaume-Uni ait quitté l'UE, les échanges économiques au sein de l'UE et entre le Royaume-Uni et l'UE bénéficieront d'une reconnaissance mutuelle et d'une bonne compréhension des principaux piliers du droit de la responsabilité civile. À la lumière de l'accès et du contrôle à distance, permis par l'hyperconnectivité et la puissance de calcul, le droit de la responsabilité civile devra s'adapter à la responsabilité lorsque qu'une action délictuelle a des effets hors des juridictions au sein de laquelle cette action a été initiée.

Passons maintenant en revue les exigences en matière de *dommages*, de *causalité*, de *responsabilité pour faute* et de *responsabilité stricte*, pour terminer par des questions relatives à la compensation et à la dissuasion.

Le **dommage** est la première condition du succès d'une action en responsabilité civile, dans la mesure où l'on souhaite obtenir une indemnisation. Il peut s'agir d'un préjudice économique, d'un dommage corporel ou d'une violation des droits de la personnalité. Des dommages et intérêts peuvent être demandés pour le préjudice moral, pour l'atteinte à la dignité et pour le décès d'une

personne aimée.

Le lien de **causalité** est la deuxième condition, puisque le dommage doit avoir été causé par l'acte délictueux incriminé pour donner droit à une indemnisation. Habituellement, l'établissement du lien de causalité se réfère à la *conditio sine qua non*, qui signifie que sans l'acte pertinent, le dommage ne se serait pas produit. Il s'agit de toute action impliquée dans la chaîne d'événements qui a conduit au dommage, dans la mesure où l'on peut prouver que c'est une cause pertinente. Ainsi, la décision du grand-parent du présumé auteur du dommage de s'installer dans un autre pays où il a rencontré son futur conjoint est également une *conditio sine qua non*, mais ne sera pas prise en compte. Il faut pour cela une conception normative de la causalité.

La réduction de l'espace ouvert par le critère de la *conditio sine qua non* est souvent obtenue en tenant compte de la prévisibilité du dommage. Par exemple, la jurisprudence néerlandaise exige que les automobilistes prévoient que les autres usagers d'une voie publique ne respecteront pas les règles de circulation. Cela signifie que les voitures doivent anticiper les cyclistes sans lumière après la tombée de la nuit.

La **responsabilité pour faute** est fondée sur la maxime selon laquelle chaque victime supporte (*bears*) son propre dommage, à moins qu'une raison particulière ne permette de transférer la charge à un autre sujet de droit qui a causé le dommage. Ces raisons particulières peuvent être :

- la faute, qui suppose un acte répréhensible intentionnel, ou
- la négligence, qui suppose un manque de diligence raisonnable.

La **responsabilité stricte** s'écarte du principe de base selon lequel chaque victime doit supporter ses propres dommages. Ici, le dommage est attribué sans avoir à prouver la faute ou la négligence de l'auteur du délit. Cette exception est souvent appliquée à une personne morale qui profite du danger qu'elle crée, considérant qu'elle est en mesure de se prémunir contre toute responsabilité.

On peut parler de responsabilité stricte pour des activités, des biens ou des personnes inhéremment dangereuses mais pas illégales (un conducteur qui cause un accident impliquant une piétonne), ou des produits ou objets qui ne sont pas intrinsèquement dangereux mais qui s'avèrent défectueux pour l'usage pour lequel ils ont été conçus (typiquement les produits défectueux, y compris les produits ou services avec de l'IA appliquée).

Dans le droit de la responsabilité civile, on peut distinguer les réparations qui offrent une compensation ou une dissuasion (ou les deux). Le droit de la responsabilité civile exige essentiellement que les gens agissent comme des personnes raisonnables. L'attribution d'une responsabilité en cas de manquement à cette obligation permet de faire passer les dommages causés de la victime à l'auteurice du délit, ou du moins d'exiger une compensation financière. En même temps, cela incite les auteurices potentiel·les de délits à s'abstenir de tout comportement susceptible de causer des dommages.

Comme nous l'avons vu, le droit de la responsabilité civile est parfois utilisé pour indemniser les victimes de dommages causés par des activités dangereuses que la société trouve légitimes, comme la conduite d'une voiture. Cela implique que la responsabilité délictuelle ne doit pas être confondue avec la punition et n'implique pas nécessairement l'illicéité (caractère de ce qui est interdit par la morale ou la loi, ce n'est pas nécessairement un synonyme d'illégalité). Elle doit donc être distinguée de la responsabilité pénale, mais aussi de la sécurité sociale ou de l'assurance privée du côté de la victime, qui peuvent toutes deux indemniser les victimes pour les préjudices et les dommages mais n'auront aucun effet dissuasif sur les auteurices potentiel·les de délits (qui peuvent alors penser qu'ils peuvent s'en tirer avec une conduite dangereuse et ainsi externaliser les coûts de leurs décisions).

8.2 Responsabilité des tiers en cas de traitement illicite et autres cyberdélits

La responsabilité civile est définie comme la responsabilité en l'absence de contrat, lorsque la victime et l'auteurice du délit n'ont pas de relation directe, ce qui peut, par exemple, rendre difficile l'identification de l'auteurice du délit. La distance entre la victime et le tiers peut être euclidienne (géographique) ou autre, par exemple en raison du type d'effets de réseau que les applications *cyber* génèrent. L'émergence de la cybercriminalité et les six différences pertinentes que nous avons identifiées par rapport à la criminalité traditionnelle s'appliquent également aux cyberdélits civils : les différences de distance, d'échelle, de vitesse, de distribution, d'invisibilité et de visibilité, induites par l'automatisation et l'hyperconnectivité sous-jacentes des systèmes informatiques en réseau (voir Section 6.1.2).

Une question importante dans le domaine de la responsabilité civile est que les tentatives individuelles de poursuivre les grands acteurs peuvent ne pas être efficaces pour maintenir la confiance sociétale que le droit privé vise à atteindre. Cela peut être dû au fait qu'aucun préjudice concret ne peut être identifié, que les coûts d'une action en justice l'emportent sur les avantages d'une indemnisation, ou au simple fait que les petits acteurs n'ont peut-être pas la compréhension, le temps ou l'argent nécessaires pour savoir comment faire valoir leurs droits. L'une des façons de résoudre ce problème est l'action collective, par exemple en permettant aux gens de mandater leurs demandes auprès d'associations à but non lucratif, ou en permettant à une association à but lucratif de poursuivre les grands acteurs en leur propre nom.

8.2.1 Atteintes à la vie privée

Enfin, abordons brièvement deux exemples de jurisprudence concernant les *délits relatifs à la vie privée* dans les juridictions de *common law*, juridictions qui – comme indiqué ci-dessus – ont un *droit des délits* granulaire plutôt qu'un *droit des délits général* tel que les juridictions de droit civil peuvent avoir.

Le délit canadien d'intrusion dans la vie privée

Dans l'affaire *Jones v. Tsige*, la Cour d'appel de l'Ontario s'est prononcée pour la première fois sur un *délit d'intrusion dans la vie privée*. Les faits de l'affaire sont les suivants :

En juillet 2009, l'appelante, Sandra Jones, a découvert que l'intimée, Winnie Tsige, avait subrepticement consulté les dossiers bancaires de Jones. Tsige et Jones ne se connaissaient pas malgré le fait qu'elles travaillaient toutes deux pour la même banque et que Tsige avait formé une union de fait avec l'ancien mari de Jones. En tant qu'employé de la banque, Tsige avait un accès total aux informations bancaires de Jones et, contrairement à la politique de la banque, a consulté les dossiers bancaires de Jones au moins 174 fois sur une période de quatre ans.

L'affaire est éclairante car elle vise à établir si la *common law* reconnaît ce type de délit d'atteinte à la vie privée, sur la base d'une enquête approfondie dans les juridictions de *common law* (notamment au Canada, aux États-Unis et au Royaume-Uni). La Cour soutient que les développements technologiques ont effectivement entraîné la nécessité de reconnaître un tel délit en *common law*.

Ils estiment que l'effet juridique d'un acte qualifié de *délit d'intrusion dans la vie privée* dépend des trois conditions juridiques suivantes :

- le comportement du défendeur ou de la défenderesse doit être intentionnel (ce qui inclut l'imprudence)

8.2. RESPONSABILITÉ DES TIERS EN CAS DE TRAITEMENT ILLICITE ET AUTRES CYBERDÉLITS⁷¹

- le défendeur ou la défenderesse doit avoir envahi, sans justification légale, les affaires ou les préoccupations privées du plaignant ou de la plaignante
- une personne raisonnable considérerait l'invasion comme très offensante, causant détresse, humiliation ou angoisse.

Le délit britannique d'abus d'informations privées

Dans l'affaire *Murray v. Express Newspapers plc and another*, des photographies ont été prises secrètement (avec un objectif à longue focale) du jeune fils de J.K. Rowling dans une poussette, avec ses parents marchant dans une rue. Elles ont été prises par une agence photographique, pour être vendues aux parties intéressées, comme en l'espèce l'éditeur du magazine The Sunday Express qui a publié l'une des photos. La question de savoir si cela peut constituer un délit d'*utilisation abusive d'informations privées* a été résolue en se référant aux conditions juridiques suivantes :

1. le demandeur fait valoir de manière convaincante qu'il avait une *attente raisonnable en matière de respect de la vie privée* pour ces informations ; et
2. le défendeur ne peut pas faire valoir de manière convaincante qu'il existe une justification pertinente, par exemple en invoquant un *intérêt public* prépondérant pour la publication.

Il faut en conclure que, dans le contexte de la *common law*, d'anciens et de nouveaux types de délits relatifs à la vie privée se développent, en raison de l'évolution du paysage technologique.

8.2.2 Cyberdélits

En présentant la cybercriminalité, nous avons discuté de la différence qui existe entre les cybercrimes et les crimes traditionnels. Comme mentionné ci-dessus, des différences similaires s'appliquent à l'idée de cyberdélits. Nous pouvons, par exemple, penser aux dommages causés par les logiciels malveillants, l'accès illégal, la fraude d'identité, le piratage de domaine, par l'intimidation, la traque, la diffamation, l'humiliation, le toilettage, par le blocage de l'accès ou de la disponibilité, et par les communications chronophages et irritantes telles que le spam. Les atteintes à la vie privée causées par des systèmes informatiques hyperconnectés pourraient facilement entrer dans le champ d'application des délits cybernétiques.

Les **types de délits** pourraient inclure : les violations de données, le traitement illégal de données à caractère personnel, mais aussi la responsabilité civile pour les dommages causés par la non-conformité dans la vente de biens ou de services, les atteintes à la réputation et les risques pour la sécurité.

Les **types de dommages** peuvent être les suivants : dommages compensatoires ou punitifs ; dommages directs et indirects ; perte de revenus, perte de capacité de gain ou manque à gagner ; dommages matériels et immatériels ; et préjudice présent ou futur.

Les exemples donnés au début de ce chapitre, qui mettent en évidence les dommages causés par les voitures connectées, les réfrigérateurs intelligents et les lave-linge intelligents, à l'aube de la robotique, de la robotique en nuage et de l'IoT, soulèvent clairement un certain nombre de questions sur la portée du devoir de diligence, le rôle de la prévisibilité lors de la définition de l'intention dans le contexte des applications d'apprentissage automatique, les problèmes de causalité distribuée dans le cas de composants logiciels et matériels intégrés, la responsabilité de l'utilisateur final pour les éventuels dommages consécutifs causés à autrui, et la mesure dans laquelle le traitement illégal de données à caractère personnel pourrait en soi être qualifié de dommage immatériel en vertu de la législation de l'UE sur la protection des données, indépendamment de l'expérience subjective d'une personne concernée.

Prof. Hildebrandt conclut le chapitre en affirmant qu'elle s'attend à ce que la responsabilité de droit privé, ainsi que le droit de la protection des données, le droit de la concurrence et la protection des consommateurs, prennent l'initiative de reconfigurer le paysage juridique du monde *onlife*. Cela devrait contribuer à une protection juridique plus adaptative et à une meilleure répartition des freins et contreponds entre les développeurs de technologies, les fabricants, les détaillants, les fournisseurs de services et les utilisatrices finals-aux.

Chapitre 9

Une personnalité juridique pour l'IA ?

L'auteur de science-fiction Isaac Asimov énonça en 1942 dans la nouvelle *Cercle Vicieux* les Trois lois de la robotique :

1. Un robot ne peut porter atteinte à un être humain ni, restant passif, laisser cet être humain exposé au danger,
2. Un robot doit obéir aux ordres donnés par les êtres humains, sauf si de tels ordres entrent en contradiction avec la première loi,
3. Un robot doit protéger son existence dans la mesure où cette protection n'entre pas en contradiction avec la première ou la deuxième loi.

Ces *lois* soulèvent plus de questions qu'elles n'apportent de réponses, ce qui en fait une tentative très intéressante pour faire face à l'imprévisibilité des systèmes informatiques autonomes.

Le premier type de question concerne la séquence des lois, cette séquence n'étant pas arbitraire (voir le dessin humoristique <https://xkcd.com/1613/>, je n'en ai pas trouvé de version français). Le deuxième type de question prouve en fait le bien-fondé de la caricature : ces lois (et leur séquence d'application) ne sont pas seulement pertinentes pour le choix individuel mais impliquent la société dans son ensemble. Il en va de même pour la question de savoir comment la société dans son ensemble permet ou limite le choix individuel.

En fait, Asimov a formulé une quatrième loi, ou loi zéro, qui devait précéder les autres :

Un robot ne doit pas nuire à l'humanité ou, par son inaction, permettre à l'humanité de lui nuire.

Aujourd'hui, l'essor des systèmes autonomes (des voitures connectées et de la robotique industrielle aux moteurs de recherche et aux technologies financières) a atteint un point où les paradoxes implicites de ces lois deviennent apparents.

Le MIT a ainsi développé un outil en ligne pour réfléchir aux choix éthiques que peut avoir à faire un véhicule autonome.¹ Mais tout cela soulève d'autres questions encore : peut-on coder *en dur* de tels choix ? Est-ce le rôle du fabricant de véhicule, ou celui du ou de la conductrice ?

Un examen attentif soulève cependant au moins deux objections à la manière dont peuvent être formulées ces questions. Tout d'abord, de nombreux·ses expert·es pointent que le niveau d'autonomie requis par les véhicules ne sera peut-être jamais atteint. Deuxièmement, les questions sont formulées en termes utilitaristes quelque peu naïfs, définissant le problème en termes

1. <https://www.moralmachine.net/h1/fr>

de préférences individuelles qui peuvent ensuite être agrégées et décidées, en fonction de ce que la majorité d'une communauté d'utilisatrices spécifiques préfère. Ce type de calcul utilitaire suppose que les préférences sont données, qu'elles ne fluctuent pas dans le temps, qu'elles concernent des variables indépendantes et qu'elles peuvent être évaluées hors contexte.

Ici, on s'intéressera à la question de la personnalité juridique plutôt que de l'agentivité morale. En 2017, le Parlement européen (PE) a voté une résolution, demandant à la Commission européenne (CE) de se pencher sur le potentiel de *règles de droit civil sur la robotique*. La résolution a été adoptée avec 396 voix contre treize, et quatre-vingt-cinq abstentions. Ce chapitre aborde les questions juridiques liées aux systèmes autonomes, en posant la question de savoir si ces systèmes devraient se voir attribuer le statut de personnalité juridique, et si oui, sous quelles conditions. Il convient de noter que le statut de personnalité juridique peut être attribué dans le contexte de différents domaines juridiques : il est possible, par exemple, d'accorder le statut de personnalité juridique aux sociétés de droit privé, tout en limitant la responsabilité pénale aux personnes physiques. Il doit être clair que la responsabilité pénale, qui met l'accent sur la censure, suppose un type d'agentivité morale qui n'est pas évident dans le cas des systèmes autonomes actuels. La responsabilité stricte en droit privé, cependant, ne serait pas nécessairement concernée par le blâme moral. Pour étudier ces questions, nous allons d'abord discuter du concept de subjectivité juridique et de l'agentivité juridique, puis du concept d'agentivité artificielle, pour aboutir à une première évaluation du potentiel de la responsabilité civile des systèmes autonomes.

9.1 Subjectivité juridique

En droit positif moderne, on distingue deux types de personnalités juridiques :

- les personnes physiques (*natural persons*)
- les personnes morales (*legal persons*)

Les humains sont considérés comme des personnes physiques, mais ça n'a pas toujours été ainsi : par le passé, les esclaves et les femmes n'étaient pas considérés comme tels dans de nombreuses sociétés. La décision selon laquelle tous les êtres humains sont des sujets de droit est une décision politique qui découle de l'idée que les gouvernements doivent traiter chaque individu comme méritant un respect et une attention égaux. La subjectivité juridique est attribuée par le droit positif, tout comme les droits subjectifs (les droits des sujets de droit) dépendent du droit objectif.

Outre les êtres humains, la loi peut attribuer et attribue effectivement la qualité de personne morale à d'autres entités, par exemple aux sociétés, associations et fondations ou aux municipalités et à l'État. Ainsi, les organismes privés et publics peuvent être qualifiés de personnes morales si le législateur (ou le précédent en *common law*) leur attribue une subjectivité juridique. Si tel est le cas, ils peuvent agir en droit : posséder des biens, conclure des contrats, ils peuvent être tenus responsables des dommages causés en vertu du droit privé et ils peuvent même être accusés d'une infraction pénale. Toutefois, si les êtres humains sont des sujets de droit en vertu du droit privé, constitutionnel et pénal, ce n'est pas nécessairement le cas des personnes morales telles que les sociétés. Cela varie selon les juridictions ; dans certaines d'entre elles, une société est une personne morale de droit privé, mais pas de droit pénal.

Le concept de personne dérive du latin *persona*, qui signifie masque. Un masque a deux fonctions : il permet de jouer un rôle et il protège l'entité qui se cache derrière le masque. Le masque offre donc à son porteur ou sa porteuse une liberté positive (le rôle qu'il peut désormais jouer) et une liberté négative (empêcher l'identification entre le masque et son porteur). D'une part, le *masque* de la personne morale permet à une entité d'agir en droit (de créer des effets juridiques) et d'être tenue pour responsable ; d'autre part, le *masque* protège cette entité. Le

masque empêche d'identifier une personne de chair et de sang avec le rôle que cette personne joue en droit, excluant ainsi qu'une personne soit définie par son statut juridique. De cette façon, la loi laisse la place à la réinvention du soi. L'idée de la *persona* est centrale pour le rôle instrumental et protecteur du droit : elle est instrument lorsqu'elle permet à une entité d'agir en droit ou d'être tenue responsable et elle protège lorsqu'elle empêche d'assimiler le statut juridique à la personne vivante.

Cela soulève la question de savoir s'il existe des critères qui conditionnent l'attribution du statut de personne morale. De nombreux auteurs estiment que les êtres humains sont naturellement des sujets de droit, alors que les sociétés sont des sujets de droit en raison d'une fiction juridique. Elles sont traitées comme si elles étaient des personnes morales (en tant que fiction juridique), alors qu'elles ne sont pas *réellement* des personnes ou des sujets. Comme l'a observé John Dewey dans un célèbre article sur la personnalité juridique, une fiction juridique telle que la personnalité juridique est réelle même si elle est artificielle. Tout comme un lac artificiel est un lac réel, et non un lac imaginaire : ici, le caractère artificiel importe peu.

Le caractère artificiel de la personnalité juridique est lié au fait que la subjectivité juridique est par définition attribuée par le droit positif (loi ou *common law*) et ne peut être présumée, alors que la capacité juridique des sujets de droit peut être limitée par le droit positif (par exemple, dans le cas des mineur·es, ou dans le cas de la tutelle).

Il convient de noter que la terminologie est telle que le terme *sujet de droit* est utilisé tant pour les personnes physiques que pour les personnes morales, tandis que le terme *personnes morales* n'est utilisé que pour les sujets de droit qui ne sont pas des personnes physiques. Par conséquent, les personnes morales ont toujours besoin d'être représentées ; une société ne peut agir que par l'intermédiaire de ses représentants légaux. En clair, si une personne morale est responsable pénalement, elle ne peut pas être mise en prison, mais d'autres sanctions s'appliqueront (comme des amendes, la fermeture des activités, voire la cessation de l'organisation).

Tout ceci devrait conduire à la conclusion qu'en principe, le droit positif peut attribuer la personnalité juridique à n'importe quelle entité, selon que le législateur (ou la *common law*) juge cette attribution nécessaire pour protéger les droits, libertés et intérêts légalement pertinents.

9.2 Agentivité juridique

En ce qui concerne la terminologie, il est logique de faire une distinction entre :²

- la personne humaine, utilisée comme un terme biologique (qui distingue les humains des autres animaux, mais qui soulève également la question de savoir à partir de quand un cyborg cesse d'être considéré comme une personne humaine)
- la personne morale, utilisée comme un terme moral (qui soulève la question de savoir si, et si oui, dans quelles conditions, un agent artificiel peut être qualifié de personne morale, capable d'agir à tort ou à raison)
- la personne physique ou morale, utilisée comme un terme juridique fondé sur le droit positif (qui soulève la question de savoir quels animaux ou agents artificiels pourraient être qualifiés de personne morale, en notant que cela impliquera une décision politique).

Ces questions peuvent également être formulées en termes d'agentivité (*agency*) plutôt que de personnalité, par exemple en termes d'agentivité morale, qui est généralement comprise comme la capacité de s'engager dans une action intentionnelle, ce qui suppose la capacité de donner

2. Le livre n'en fait pas trop mention, mais l'attribution de la personnalité juridique aux individus d'autres espèces animales fait l'objet de vifs débats, et à mon humble avis de la plus haute importance. Notons aussi que la Nouvelle-Zélande a octroyé une personnalité juridique ... à un fleuve, notamment pour fournir une meilleure protection écologique.

des raisons à ses actions ; ou en termes d'agentivité juridique, généralement comprise comme la capacité, attribuée par la loi, d'agir en droit et d'être responsable de ses propres actions (subjectivité juridique). Il est toutefois intéressant de noter qu'il existe une deuxième signification du concept d'agentivité juridique, qui fait référence à la capacité, attribuée par la loi, d'agir au nom d'une autre personne (agir en tant que mandataire, représentant).

Ce second sens de la notion d'agentivité suppose une relation juridique spécifique entre un agent (ou mandataire) et son mandant (*principal*, que l'on peut aussi traduire par commettant en français), dans laquelle l'agent agit au nom d'un mandant. Cette relation est généralement fondée sur une relation contractuelle entre l'agent et son mandant, d'une part, et l'agent et un tiers, d'autre part, créant ainsi une relation contractuelle entre le mandant et le tiers.

Par exemple, une société qui exploite des boutiques de mode dans différents endroits peut être représentée par des vendeurs qui vendent effectivement des vêtements aux visiteurs de la boutique. Dans ce cas, le vendeur est l'agent et la société est le mandant. Notez qu'en vertu du droit actuel (dans la plupart des juridictions), le mandant et l'agent doivent tous deux être des sujets de droit pour que le tiers soit lié par les actions de l'agent.

En droit de l'agentivité, il est crucial d'établir l'autorité de l'agent (c'est-à-dire la mesure dans laquelle l'agent est autorisé à agir pour le compte du mandant). On distingue l'étendue de l'autorité et son origine. En ce qui concerne l'étendue, la loi fait la différence entre les agents universels (qui ont l'autorité pour tous les actes), les agents généraux (qui ont l'autorité pour tous les actes concernant une fonction spécifique), et les agents spéciaux (avec l'autorité pour un type spécifique d'acte).

En ce qui concerne l'origine de l'autorité, la loi fait la distinction entre :

- l'autorité réelle (implicite ou expresse)
- l'autorité ostensible, ou apparente (estoppel³)
- l'autorité ratifiée (où le mandant confirme l'autorité malgré le fait que l'agent a agi *ultra vires*, c'est-à-dire au-delà de l'autorité stipulée).

Une question importante est de savoir si le mandant est responsable des actions d'un agent qui agit *ultra vires*. En d'autres termes, l'effet juridique d'un contrat avec un tiers, conclu par le mandataire pour le compte du mandant, s'applique-t-il au mandant si le mandataire a outrepassé ses pouvoirs et que le mandant n'a pas ratifié ? La réponse à cette question dépend des éléments suivants. Le mandant est lié :

- si le tiers était fondé à faire confiance au mandataire pour agir dans le cadre de son autorité, **et**
- le mandant a agi ou omis d'une manière qui a généré une confiance justifiée, **ou**
- si le risque est pour le mandant, sur la base de principes généralement acceptés.

Si ces conditions ne s'appliquent pas, l'agent est responsable.

9.3 Agents artificiels

Avant d'approfondir la question de savoir si les logiciels ou les systèmes embarqués peuvent ou doivent être qualifiés de personnes morales, nous devons définir ce que l'on entend par agent artificiel. Luc Steels (un scientifique renommé travaillant sur l'IA), définit un agent comme :

- un système (un ensemble d'éléments ayant des relations entre eux et avec l'environnement)

3. L'estoppel est une exception procédurale destinée à sanctionner, au nom de la bonne foi, les contradictions dans les comportements d'un État, celui-ci étant considéré comme lié par son comportement antérieur, et dès lors *estopped* à faire valoir une prétention nouvelle.

- remplissant une fonction pour un autre agent
- capable de faire sa propre maintenance.

Il fait ensuite la différence entre un agent automatique, qui s'autogère sur la base de lois externes, et un agent autonome, qui est à la fois autoguidé et autogouverné.

Dans d'autres travaux, l'autrice a proposé une distinction entre l'agentivité automatique, autonome et autonome (où l'agentivité est définie comme une combinaison de la perception et de la capacité d'agir sur ce qui est perçu, tandis que la perception est informée par une action potentielle) :

- l'agentivité automatique implique que la conduite de l'agent est entièrement prédéfinie, par exemple, un thermostat ou un contrat intelligent ;
- l'agentivité autonome implique que l'agent est capable d'autogestion, d'autoréparation, d'autoconfiguration. Par exemple, un système nerveux central biologique, la gestion de l'énergie dans un centre de données, des réseaux de capteurs sans fil coopératifs qui *fonctionnent* (*run*) tout seuls (une maison intelligente)
- l'agentivité autonome implique à la fois la conscience (tout court) et la conscience de soi, ce qui signifie que l'agent est capable d'autoréflexion, d'action intentionnelle, d'argumentation et de développement de désirs de second ordre, par exemple, et notamment les êtres humains. Les désirs de second ordre sont des désirs concernant nos désirs, comme le désir de ne pas désirer fumer.

Les agents automatiques de Steels ne correspondraient pas à cette définition de l'agentivité autonome. Notez que l'agentivité autonome n'implique pas nécessairement la conscience et que de nombreux organismes, y compris des animaux conscients, entreraient dans son champ d'application, alors que l'agentivité autonome exige une conscience de soi d'une manière qui échappe aux agents autonomes. Il semble que la personnalité morale soit subordonnée à l'agentivité autonome. Si, et dans la mesure où l'état de personne morale nécessitait une conscience de soi, les agents autonomes ne seraient pas concernés. Cependant, les sociétés qui jouissent du statut de personne morale ne sont pas conscientes d'elles-mêmes, même si elles peuvent être représentées par des êtres humains qui le sont. Cela implique qu'il n'y a pas de réponse juridique catégorique à la question de savoir si un système informatique autonome (généralement un système autonome dans le sens susmentionné) devrait être doté de la personnalité juridique.

La question à laquelle il faut répondre lorsqu'on s'interroge sur l'opportunité d'attribuer le statut de personne morale à des agents artificiels est une question pragmatique portant sur :

- quel problème l'introduction d'une telle attribution résout
- quel problème elle ne résout pas
- quels problèmes elle crée.

9.4 Responsabilité de droit privé

On peut maintenant se concentrer sur la question de l'attribution de la personnalité juridique aux agents artificiels qui permet la responsabilité de droit privé de ces agents. Si l'on suit la définition de Luc Steels, où un agent artificiel agit pour le compte d'un autre agent, combinée à la question d'un agent artificiel agissant pour le compte d'une personne physique ou morale, le problème suivant apparaît : en vertu du droit actuel, être un agent légal implique d'être un sujet de droit, alors qu'un agent artificiel serait un objet juridique, un outil, mais pas un sujet de droit. Cela signifie qu'un agent artificiel ne peut lier le sujet de droit au nom duquel il opère, autrement qu'en tant qu'outil. De nombreux spécialistes ont soulevé la question d'un

agent artificiel qui cause un préjudice ou des dommages d'une manière qui était imprévisible pour son *mandant*, car ils craignent que cette imprévisibilité ne fasse obstacle à la responsabilité du *mandant*.

Dans le cas de contrats entre machines à l'aide d'agents logiciels entièrement déterminés par leurs algorithmes, ceux qui emploient les *agents* peuvent prévoir les types de contrats qui seront conclus. Dans le cas de contrats de machine à machine avec des agents logiciels qui agissent de manière autonome (en affichant, par exemple, des comportements émergents), ceux qui les emploient ne peuvent pas prévoir toutes les conséquences. Dans la mesure où cela impliquerait que ceux qui emploient de tels agents échappent à toute responsabilité (puisque leur propre comportement peut ne pas avoir été fautif, précisément parce qu'ils ne pouvaient pas prévoir le préjudice), on pourrait faire valoir que les victimes seraient avantagées si l'agent lui-même pouvait être tenu responsable. Afin de protéger les victimes potentielles contre des dommages pour lesquels elles ne peuvent être indemnisées, les agents artificiels dont le comportement ne peut être prévu par ceux qui les emploient pourraient être certifiés et enregistrés en tant que personnes morales à condition qu'ils aient accès à des fonds permettant d'indemniser les victimes potentielles en cas de préjudice ou de dommage. On pourrait même imaginer une interdiction des agents artificiels ayant une propension à causer des dommages, à moins qu'ils ne soient certifiés, enregistrés et assurés ou dotés de fonds suffisants pour indemniser les victimes réelles.

Si le problème à résoudre est que les dommages imprévisibles excluent la responsabilité de celui qui emploie l'agent, on peut prévoir les solutions suivantes :

1. L'agent peut être considéré comme un outil (comme dans le droit actuel) :
 - les tribunaux ou les législateurs pourraient assouplir l'exigence d'intention ou de négligence de la part de celui qui emploie l'outil (une évolution vers une responsabilité délictuelle stricte)
 - la loi pourrait refuser la validité des transactions générées par des agents autonomes qui sont imprévisibles (ce qui pourrait, cependant, étouffer l'innovation).
2. L'agent artificiel peut être enregistré comme une personne morale (dans une loi future ?)
 - cela permettrait d'attribuer une autorité réelle ou ostensible à l'agent, rendant ainsi son mandant responsable (ce qui soulève la question de la différence par rapport à la responsabilité objective)
 - cela permettrait cependant aussi de rendre les agents responsables pour leur propre compte (certification, fonds propres, etc.) si, par exemple, ils outrepassent leur autorité.

La question de la personnalité juridique des agents artificiels montre clairement que même si son attribution résout certains problèmes, elle en crée d'autres. De nombreux juristes et autres spécialistes mettent en garde contre le fait que cette attribution ne devrait pas permettre à ceux qui développent et emploient des agents artificiels d'externaliser et d'échapper à la responsabilité, les incitant ainsi à prendre des risques et à externaliser les coûts parce qu'ils savent qu'ils ne seront pas responsables. En 2019, un groupe d'expert·es sur la responsabilité et les nouvelles technologies (mis en place par la Commission européenne), a publié son rapport sur la responsabilité en matière d'intelligence artificielle, en réponse à la résolution du Parlement européen, mentionnée dans l'introduction de ce chapitre. Le groupe d'expert·es a élaboré les recommandations suivantes :

- Une personne exploitant une technologie autorisée qui comporte néanmoins un risque accru de préjudice pour autrui, par exemple des robots pilotés par l'IA dans les espaces publics, devrait être soumise à une responsabilité objective pour les dommages résultant de son exploitation.

- Dans les situations où un prestataire de services assurant le cadre technique nécessaire a un degré de contrôle plus élevé que le propriétaire ou l'utilisatrice d'un produit ou d'un service réel équipé d'IA, cela devrait être pris en compte pour déterminer qui exploite principalement la technologie.
- Une personne utilisant une technologie qui ne présente pas un risque accru de préjudice pour autrui devrait néanmoins être tenue de respecter les obligations de sélection, d'exploitation, de surveillance et de maintenance appropriées de la technologie utilisée et, à défaut, être responsable de la violation de ces obligations si elle est fautive.
- Une personne utilisant une technologie dotée d'un certain degré d'autonomie ne devrait pas être moins responsable du préjudice qui en résulte que si ce préjudice avait été causé par un auxiliaire humain.
- Les fabricants de produits ou de contenus numériques incorporant une technologie numérique émergente devraient être responsables des dommages causés par les défauts de leurs produits, même si le défaut a été causé par des modifications apportées au produit sous le contrôle du producteur après sa mise sur le marché.
- Pour les situations exposant les tiers à un risque accru de préjudice, l'assurance responsabilité obligatoire pourrait donner aux victimes un meilleur accès à l'indemnisation et protéger les auteurs potentiels de délits contre le risque de responsabilité.
- Lorsqu'une technologie particulière accroît les difficultés à prouver l'existence d'un élément de responsabilité au-delà de ce qui peut être raisonnablement attendu, les victimes devraient avoir droit à une facilitation de la preuve.
- Les technologies numériques émergentes devraient être dotées de fonctions d'enregistrement, lorsque les circonstances l'exigent, et le fait de ne pas enregistrer ou de ne pas fournir un accès raisonnable aux données enregistrées devrait entraîner un renversement de la charge de la preuve afin de ne pas porter préjudice à la victime.
- La destruction des données de la victime doit être considérée comme un dommage, indemnisable dans des conditions spécifiques.
- Il n'est pas nécessaire de doter les dispositifs ou les systèmes autonomes d'une personnalité juridique, car les dommages qu'ils peuvent causer peuvent et doivent être imputables à des personnes ou organismes existants.

Il semble que le groupe d'expert·es cherche à résoudre les problèmes causés par le comportement émergent et l'imprévisibilité subséquente des agents artificiels en adaptant les exigences de la responsabilité de droit privé, **sans recourir à la personnalité juridique** de ces agents. La principale préoccupation des expert·es semble être que ceux qui fabriquent, exploitent, utilisent ou mettent à jour ces agents doivent être tenus pour responsables des dommages causés, afin de prévenir l'emploi dangereux d'agents artificiels. En faisant en sorte que les victimes puissent demander des comptes à ceux qui prennent le risque d'utiliser des agents artificiels imprévisibles, cette approche particulière peut stimuler l'innovation, car elle augmentera la fiabilité des agents artificiels qui sont mis sur le marché.

Chapitre 10

Légal par conception ou protection juridique dès la conception ?

Les décideurs politiques, les juristes et bien d'autres parlent souvent de *réglementation des technologies* (*regulating technologies*). Il s'agit d'une expression intéressante, car elle peut signifier beaucoup de choses, selon la façon dont on la comprend. Autrefois, la plupart des juristes et des responsables politiques l'entendaient dans le sens où les technologies faisaient l'objet d'une réglementation légale. La loi peut, par exemple, imposer des exigences en matière de fabrication, de conception, de vente et d'utilisation de voitures, de couteaux, d'armes à feu, de logements, de bureaux, de machines à laver, de jouets ou d'instruments médicaux. Ces exigences peuvent concerner la sécurité, la vie privée ou le potentiel d'une technologie à violer les droits d'auteur, à diffuser de la pornographie infantine ou à polluer l'environnement. Elles peuvent viser à protéger les personnes les plus faibles, les infrastructures critiques, la sécurité nationale ou publique, ou l'environnement. La réponse par défaut selon laquelle les technologies font l'objet d'une réglementation pourrait toutefois être en train de changer.

La même expression, *technologies régulatrices* (*regulating technologies* mais prise dans un sens différent) peut également désigner la technologie comme un *sujet* qui régule le comportement humain, par exemple par le biais de dos d'âne, de technologies de gestion des droits numériques (DRM), d'algorithmes de flux d'informations qui déterminent les informations que nous percevons, et d'autres paramètres par défaut qui déterminent notre *architecture de choix*. Ici, l'objet de la réglementation n'est pas une technologie mais le comportement humain. Ainsi, la technologie peut être soit l'objet, soit le sujet de la réglementation (et peut-être les deux), alors que le droit n'est généralement considéré que comme un sujet de la réglementation (ce qui réglemente).

Cela pourrait être sur le point de changer en raison des effets omniprésents de deux types de technologies qui ont un impact sur l'environnement du droit : les applications d'apprentissage automatique (ML pour l'acronyme anglais) qui, par exemple, décident de la solvabilité ou de l'employabilité d'une personne, et les technologies de registres distribués (DLT pour l'acronyme anglais) qui exécutent prétendument elles-mêmes des transactions et des accords sans et au-delà de la loi.

Dans ce chapitre, l'accent sera mis sur la façon dont le ML et les DLT transforment l'environnement du droit, la substance des biens juridiques (tels que la sécurité juridique, l'égalité devant la loi, l'inaliénabilité des droits de la personnalité, l'équité et la dignité humaine) et la

mesure dans laquelle cela affecte la protection juridique. L'un des principaux défis à cet égard concerne les effets réglementaires de ces nouvelles technologies et l'incompatibilité potentielle entre la protection juridique et la techno-réglementation (définie comme les effets réglementaires d'une technologie, qu'ils soient prévus ou non).

10.1 Apprentissage automatique (ML)

Pour comprendre la pertinence du ML en matière de protection juridique, il peut être utile de prendre un exemple très simple, comme les tests AB. Imaginons que le fournisseur d'un site web veuille l'optimiser pour obtenir de meilleures performances en termes d'influence sur les comportements d'achat, les habitudes de lecture ou la politique de ses visiteurs.

Pour ce faire, le fournisseur peut employer un logiciel qui permet le processus suivant :

1. la page web actuelle est appelée version A
2. sa conception est modifiée de manière minimale, par exemple, la couleur ou l'emplacement d'un bouton, la position d'un bloc de texte, le type et le nombre de clics nécessaires pour accéder à d'autres pages web du site
3. la page légèrement transformée est appelée version B
4. 50 % des visiteurs sont dirigés vers la version A, les autres 50 % vers la version B
5. le logiciel mesure automatiquement les comportements des visiteurs en matière de parcours de clics, y compris éventuellement ceux capturés le jour suivant (éventuellement sur d'autres sites web sur la base de cookies de traçage)
6. le logiciel calcule quelle version a généré les comportements les plus souhaitables
7. la version la plus efficace est alors utilisée comme page par défaut
8. l'ensemble du processus est répété avec une autre légère modification
9. les tests AB peuvent être ciblés sur des types spécifiques de personnes ou même être personnalisés

Voyons si cela peut être considéré comme un exemple de ML. Dans son manuel sur l'apprentissage automatique, Tom Mitchell raconte qu'on dit d'un programme informatique qu'il apprend 1) à partir de l'expérience **E**, 2) en ce qui concerne une certaine classe de tâches **T**, 3) une mesure de performance **P**, si 1) ses performances pour les tâches de **T**, 2) telles que mesurées par **P**, 3) s'améliorent avec l'expérience **E**.

Quant au type de tâche **T** : il est clairement établi que les machines n'apprennent rien si aucune tâche n'est définie. Dans ce cas, la tâche sera définie par le propriétaire du site web, en collaboration avec le fournisseur de logiciels, car la définition de ce qui constitue un comportement souhaitable doit être traduite en langage lisible par la machine. Une boutique en ligne peut trouver souhaitable d'augmenter le comportement d'achat, mais elle peut aussi formuler des tâches plus complexes, basées sur une segmentation des visiteuses : elle peut préférer augmenter le comportement d'achat des personnes qui achètent des produits chers, ou des personnes qui sont susceptibles d'acheter plus d'un produit au cours d'une période donnée.

Quant à l'expérience **E** : notez que l'expérience de ce logiciel est limitée aux comportements de clickstream¹ des visiteurs de la page, même s'ils peuvent être suivis sur d'autres sites. Il se peut que leurs comportements sur d'autres sites n'entrent pas dans le champ de suivi du fournisseur du logiciel (par exemple, dans des magasins hors ligne ou via un autre navigateur), alors

1. Que l'on traduirait maladroitement par *chemin de clics* en français.

que ces comportements inconnus sont en fait plus pertinents pour une inférence sur leurs préférences. L'expérience du logiciel est toutefois nécessairement limitée aux données d'apprentissage disponibles.

Quant à la mesure de performance P , il se peut qu'une simple mesure de performance, telle que *clique sur un produit* ou *achète au moins deux produits*, n'en dise pas beaucoup sur les préférences des visiteurices, car ces comportements sont des exemples de comportements situés qui dépendent de nombreux autres facteurs. Ces autres facteurs peuvent être plus révélateurs de leurs préférences. Pour tester les deux versions l'une par rapport à l'autre, il peut être nécessaire de tester six ou sept mesures de performance différentes pour obtenir une meilleure image de ce qui constitue une mesure précise de l'obtention d'un comportement souhaitable.

10.1.1 Plan de recherche assisté par ML exploratoire et confirmatoire

Les tests AB peuvent être effectués au moyen d'un plan de recherche (*research design*) exploratoire, destiné à générer des hypothèses sur le type de comportement le plus lucratif pour la boutique en ligne. Cela implique de reconnaître que ces tests AB relèvent de l'expérimentation en temps réel. Comme l'écrivent Hofman, Sharma et Watts :

Dans les analyses exploratoires, les chercheuses sont libres d'étudier différentes tâches, d'ajuster plusieurs modèles, d'essayer plusieurs règles d'exclusion et de tester plusieurs paramètres de performance. Toutefois, lorsqu'ils présentent leurs résultats, ils doivent déclarer de manière transparente la séquence complète de leurs choix de conception afin d'éviter de donner la fausse impression d'avoir confirmé une hypothèse plutôt que d'en avoir simplement généré une. Dans le même ordre d'idées, ils doivent rendre compte des performances en fonction de plusieurs paramètres afin d'éviter de donner une fausse impression de précision.

Prétendre au succès sur la base d'un tel test AB est une très mauvaise idée, et équivaut généralement à ce que les statisticiens appellent le piratage de la qualité. Pour une prédiction fiable, il faut un modèle de recherche confirmatoire, qui fournit des hypothèses testées et vérifiables sur les préférences des visiteurs. Comme l'écrivent Hofman, Sharma et Watts :

Pour qualifier une recherche de confirmatoire, les chercheuses devraient toutefois être tenus de préenregistrer leurs plans de recherche, y compris les choix de prétraitement des données, les spécifications des modèles, les paramètres d'évaluation et les prédictions hors échantillon, dans un forum public tel que l'Open Science Framework (<https://osf.io>).

Comme on peut le comprendre, les fournisseurs de logiciels de marketing permettant le micro-ciblage ou sous-tendant la publicité comportementale ne seront pas enclins à déposer leur plan de recherche, y compris les choix de prétraitement, auprès de l'OSF.

Nous pouvons conclure de tout cela que :

- le ML est utilisée pour influencer ou pousser les gens à adopter des comportements qui sont souhaitables du point de vue de celui qui paie le logiciel
- un tel logiciel n'est peut-être pas aussi efficace que certains l'espèrent ou le craignent.

10.1.2 Implications du micro-ciblage

Au lieu de cela, le résultat du micro-ciblage basé sur un plan de recherche défectueux peut être que les visiteurices de sites Web sont confrontées à une architecture de choix personnalisée destinée à les attirer vers ce que d'autres considèrent comme un comportement désirable. Cela a deux conséquences involontaires :

1. un espace public fragmenté qui pourrait favoriser algorithmiquement les contenus extrêmes pour retenir l'attention des gens ; et
2. une discrimination indésirable fondée sur des points de données qui désavantagent systématiquement certaines catégories de personnes.

Ces conséquences ne sont pas nécessairement envisagées par les développeuses ou les utilisatrices du logiciel ; elles sont dues au fait que l'on a confondu un plan de recherche exploratoire, potentiellement médiocre, avec un plan de recherche confirmatoire robuste.

Cela soulève des problèmes de protection juridique. Par exemple, l'extraction et l'inférence de données comportementales peuvent interférer avec certains droits fondamentaux, tels que la vie privée, la protection des données, la non-discrimination et la liberté d'expression. Les données comportementales sont souvent des données personnelles, ainsi l'extraction de ces données peut porter atteinte à la vie privée de ceux qui ne sont pas conscients de la richesse des profils qui peuvent être construits à partir de ces données, souvent combinés avec des caractéristiques qui sont déduites de ces données. Cela peut constituer une violation directe du droit fondamental à la protection des données, selon la manière dont les données sont extraites et partagées, sur quelle base et dans quel but. Sur la base du micro-ciblage, l'extraction et l'inférence des données comportementales peuvent également violer la liberté d'expression, puisque ce droit inclut la liberté de recevoir des informations sans censure.

Un exemple de ce type de biais est le logiciel propriétaire COMPAS, vendu par Equivant (anciennement Northpointe), où COMPAS signifie *Correctional Offender Management Profiling for Alternative Sanctions*. COMPAS est utilisé par les tribunaux des États-Unis pour évaluer le risque de récidive d'un délinquant (c'est-à-dire le risque qu'il commette une autre infraction après sa libération). Ce risque co-détermine les décisions de libération conditionnelle ou de condamnation. Le score de risque est basé sur un nombre limité de points de données qui se sont avérés corrélés avec la récidive. COMPAS est le résultat d'un plan de recherche assisté par ML qui a testé 137 caractéristiques pour en déduire les six caractéristiques réellement prédictives. Après avoir mené ses propres recherches sur des données d'entraînement similaires, Julie Angwin a affirmé que le COMPAS était discriminatoire à l'égard des personnes en raison de leur ethnicité (*race*).

Selon Equivant, cela résultait du fait que les personnes noires avaient en moyenne un risque plus élevé de récidive. Equivant a accusé Angwin d'avoir utilisé des méthodologies défectueuses, impliquant que les lois de la statistique étaient responsables du résultat disparate du score de risque. En tant que cas d'utilisation, l'accusation de discrimination raciale a généré un flot de littérature scientifique sur l'équité dans l'apprentissage automatique, étayant les demandes de transparence et de responsabilité, exigeant essentiellement que les entreprises et les gouvernements emploient des applications d'apprentissage automatique équitables, responsables et transparentes (que l'on appelle en anglais par son acronyme FAT ML).

10.1.3 Implications du micro-ciblage pour l'État de droit

Le deuxième aspect de la protection juridique concerne la mesure dans laquelle les décisions fondées sur des inférences du ML violent les principes fondamentaux de l'État de droit, tels que la transparence et la responsabilité.

Ou, plus précisément :

1. l'explicabilité du processus décisionnel
2. la justification de la décision
3. la contestabilité de la décision.

Les deuxième et troisième exigences concernent la décision. Dans l'administration publique, les décisions doivent être prises dans le respect du principe de légalité, ce qui signifie que la justification doit être fondée sur le droit et que les citoyens ont le droit de contester la décision devant un tribunal. Dans le secteur privé, en revanche, la liberté contractuelle et la liberté de disposer de ses biens comme on le souhaite peuvent fournir la justification. Ces libertés sont toutefois restreintes, par exemple en raison de l'interdiction de toute discrimination dans le cadre de l'emploi, ou de toute discrimination fondée sur le sexe ou l'ethnicité. Tant dans l'administration publique que dans les entreprises commerciales, la prise de décision fondée sur le ML peut entraîner une discrimination invisible qui est en fait interdite, par exemple sur la base de l'ethnicité. Cette discrimination sera souvent involontaire et invisible parce qu'elle est fondée sur un ensemble concerté de caractéristiques qui sont en corrélation avec l'ethnicité et agissent donc comme des proxys de l'ethnicité. Cela signifie que cette discrimination ne doit pas nécessairement être fondée sur une tentative délibérée d'utiliser l'ethnicité comme caractéristique pertinente ; même si l'on supprime complètement l'ethnicité comme caractéristique, les proxys maintiendront probablement la discrimination.

Juridiquement parlant, cela peut être qualifié de discrimination indirecte (ou disparate), qui est souvent explicitement définie et interdite par la loi (sauf justification). Ce qui importe ici, c'est qu'en l'absence de ML explicable, il peut être très difficile de vérifier l'ampleur de la discrimination.

Outre la discrimination interdite, la prise de décision fondée sur l'application de la classification des risques peut avoir d'autres répercussions. Imaginons que le profil de risque appliqué à une personne soit basé sur le risque moyen d'une catégorie déterminée de personnes, alors que ce risque moyen ne s'applique pas à chaque membre de cette catégorie. Dans ce cas, les individus sont essentiellement traités sur la base d'un score qui ne leur est probablement pas applicable. Même si cette classification des individus n'implique pas une discrimination interdite, elle peut être considérée comme injuste. Par exemple, les femmes ont en moyenne un risque sur huit de souffrir d'un cancer du sein. En fonction de l'âge de la femme, de l'occurrence du cancer du sein dans son ascendance et sa famille, de son mode de vie et d'autres facteurs, son risque passera de *un sur huit* à un risque potentiellement beaucoup plus élevé ou plus faible. Il serait donc peu judicieux de traiter chaque femme comme si son risque était de un sur huit et, dans le cas, par exemple, d'une prime d'assurance maladie, on pourrait dire que c'est injuste. Cela explique pourquoi l'explicabilité des décisions fondées sur l'application du ML est devenue une question importante de protection juridique.

En ce qui concerne le RGPD, le ciblage personnalisé (ou profilage) fondé sur le ML relèverait le plus souvent de l'Article 4(4), qui le définit comme

toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

L'Article 21 du RGPD stipule que les personnes concernées ont un *droit d'opposition* au profilage fondé sur les motifs de l'Article 6 (e) et (f), c'est-à-dire fondé sur une mission publique ou une autorité publique, ou sur l'intérêt légitime du responsable du traitement, ainsi qu'un droit d'opposition au profilage *dans la mesure où il est lié au marketing direct*.

En outre, les personnes concernées ont le *droit de ne pas être soumises* au profilage lorsque celui-ci entraîne une prise de décision automatisée qui les affecte de manière significative (Article 22). Nous verrons plus tard dans quelle mesure le droit de ne pas être soumis à des décisions automatisées fournit une *protection juridique par conception* contre les applications de ML bia-

sées. Il convient de noter que ce droit n'est pas seulement applicable au profilage, mais aussi à d'autres types de décisions automatisées, telles que celles impliquant un code auto-exécutoire.

10.2 Technologies de registres distribués (DLT), contrats intelligents et régulation intelligente

Le développement et l'utilisation des DLT et/ou des blockchains étant en pleine évolution, il en va de même pour la terminologie. En dehors des discussions sur l'exactitude de l'un ou l'autre terme, nous utiliserons le terme DLT pour couvrir toute la gamme des technologies encadrées comme :

1. des bases de données distribuées (*ledgers*)
2. qui stockent des transactions basées sur
3. des infrastructures décentralisées (le code central)
4. qui permettent un code auto-exécutable, basé sur
5. une combinaison spécifique de technologies de la sécurité (notamment le hachage et le chiffrement)
6. qui incitent les *mineurs* ou les *validateurs* à participer à un mécanisme de consensus raisonnablement fiable
7. qui est censé garantir l'intégrité des données stockées dans le ledger, et de la séquence de ce stockage.

Les DLT sont souvent présentés comme offrant une informatique *sans confiance* (*trustless*) qui permet un stockage immuable, transparent et sécurisé des transactions, avec une garantie contre la manipulation a posteriori des transactions précédentes, assurant ainsi l'intégrité à la fois de la séquence et du contenu des transactions (où l'intégrité de la séquence protège contre la *double dépense*). Les DLT sont souvent *vendus* comme permettant la désintermédiation, ce qui signifie que les utilisatrices n'ont pas besoin de se connecter à une institution traditionnelle (comme les banques) pour effectuer des transactions fiables avec des parties qu'ils ne connaissent pas ou auxquelles ils ne font pas confiance. L'idée est que le ledger leur permet d'interagir avec d'autres personnes de manière totalement transparente, avec la certitude que ni l'autre partie ni aucun tiers ne peut manipuler les transactions stockées. En un sens, la promesse est que la technologie peut assumer le rôle d'un intermédiaire de confiance par le biais d'une séquence d'événements entièrement prévisible qui exécute elle-même des transactions inviolables.

Avant d'examiner ces affirmations, il est essentiel de faire la distinction entre les DLT publics et privés, et entre les DLT avec et sans autorisation, ainsi que leurs combinaisons. La différence entre les DLT publics et privés peut être définie comme dépendant de qui peut *lire* le contenu, et la différence entre les DLT autorisés et non autorisés peut être définie comme dépendant de qui peut ajouter ou *écrire* du nouveau contenu. Bitcoin repose sur des DLT publics non autorisés, ce qui signifie que tout le monde peut vérifier le contenu et en soumettre de nouveaux. À l'heure actuelle, les entreprises commerciales, les institutions financières et les agences gouvernementales étudient les arguments commerciaux en faveur des DLT, en recourant souvent à des versions privées avec autorisation qui ne présentent pas l'attrait d'un système décentralisé, car avec les DLT privés avec autorisation, seul un ensemble spécifique d'acteurs est autorisé à lire et à écrire sur le ledger.

Notons d'emblée que cela signifie que les DLT privés non autorisés exigent essentiellement que les utilisatrices fassent confiance :

1. à l'intermédiaire traditionnel qui emploie le DLT et

2. à ceux qui écrivent le code pour un type particulier de transaction et
3. à ceux qui écrivent les protocoles qui constituent l'infrastructure (développeurs de base)

Si l'on tient compte du fait que la plupart des utilisateurices ne comprennent pas le code informatique, ces DLT renforcent fondamentalement le rôle des institutions qui les emploient ; elles requièrent plus de confiance, pas moins, et ne réalisent certainement pas la désintermédiation.

10.2.1 Contrats intelligents et réglementation intelligente

Dans le cadre de ce chapitre, la pertinence des DLT concerne ce que l'on appelle les contrats intelligents et la réglementation intelligente, c'est-à-dire l'utilisation des DLT pour exécuter automatiquement soit un contrat convenu, soit une politique spécifique fondée sur la compétence réglementaire. En ce qui concerne le premier point, on peut penser à un contrat de vente qui s'exécute de lui-même une fois déclenché (lorsque le système détecte un paiement, il transfère l'objet, ou l'inverse). Notez que cela peut fonctionner parfaitement si le paiement (par exemple, une crypto-monnaie) et les actifs (par exemple, une preuve électronique de propriété) sont tous deux à l'intérieur du système (souvent appelé *on-chain*). Les paiements hors chaîne ou le transfert d'actifs hors chaîne, cependant, nécessiteront l'utilisation d'**oracles**, c'est-à-dire d'applications logicielles qui assurent l'interface entre le ledger et le monde réel, ou d'autres systèmes.

Quant à l'auto-exécution des politiques réglementaires, elle suppose qu'une autorité compétente traduise sa politique en code lisible par une machine (un acte d'interprétation) et définisse le type de données qui déclenche l'exécution du code (un autre acte d'interprétation).

Certaines ont fait remarquer que cela confond la législation avec son exécution et même avec l'adjudication (en cas de désaccord sur le contenu du contrat). Cela signifierait que les freins et contrepoids de l'État de droit, notamment la séparation des pouvoirs de législation, d'administration et d'adjudication, sont perturbés. Cela nécessiterait à son tour de nouveaux types de garanties (recours juridiques) pour permettre la contestation des décisions qui en découlent – garantissant ainsi que la réglementation et les contrats intelligents restent sous l'égide du droit.

Un rapide tour d'horizon des critiques concernant certaines des affirmations faites à propos des DLT, notamment en ce qui concerne les contrats intelligents et la réglementation intelligente :

L'immutabilité Cette caractéristique peut être remise en question selon la gouvernance du DLT (distribué ne veut pas forcément dire décentralisé). L'immutabilité peut être un problème si une des parties ne comprends pas le code exécuté.

L'informatique sans confiance Il faut de toute manière faire confiance au code, et dans le cas des DLT privés à autorisation, les utilisateurices doivent faire confiance 1) à ceux qui contrôlent le DLT, 2) aux protocoles qui forment sa *constitution* et 3) au code qui est exécuté en leur nom ou au nom de l'autre partie.

Les transactions transparentes La transparence est une caractéristique dans la mesure où les parties ont accès au code source de l'infrastructure et au contrat intelligent, mais ce n'est pas le cas dans le cadre de DLT privés

La sécurité Celle-ci est questionable en cas de bugs de mauvaise implémentation, ou en cas d'attaque (e.g., attaque des 51 %²).

L'anonymat L'anonymat n'est jamais absolu, par exemple dans le cas où on l'on utilise de l'analyse comportementale à des fins de ré-identification.

La sûreté La sûreté des contrats peut être remise en question si le système sous-jacent ou le code du contrat intelligent est piraté, si les données saisies hors chaîne sont incorrectes ou si le fournisseur ne peut être tenu responsable, une ou plusieurs parties au contrat peuvent

2. https://fr.wikipedia.org/wiki/Attaque_des_51_%

perdre leurs données. De plus, la nature auto-exécutoire du code peut créer des résultats dangereux pour les utilisatrices, surtout s'ils ne peuvent pas identifier ou poursuivre la personne responsable.

L'exactitude Dans la mesure où l'entrée hors chaîne est incorrecte, l'erreur ou la fausse entrée est automatisée (en raison de l'immutabilité, cela peut être difficile à corriger).

Du point de vue du droit, l'utilisation des DLT soulève de nombreuses questions. Dans le cadre de ce chapitre, on se concentre sur la question de savoir si l'exploitation d'un code auto-exécutoire via un DLT doit être considérée comme *légal par conception* ou comme une *protection légale par conception*.

Les contrats intelligents ou les réglementations intelligentes garantissent-ils que le comportement des parties au contrat ou des destinataires de la réglementation est *légal par conception* ou *conforme à la loi par conception*? Explorons tout d'abord la question de savoir si les contrats intelligents sont des contrats au sens juridique, puis si la réglementation intelligente est une loi au sens juridique.

10.2.2 Le statut juridique des *contrats intelligents* en droit privé

En ce qui concerne les contrats au sens juridique du terme, il convient d'examiner les conditions juridiques à remplir pour que *quelque chose* puisse être considéré comme un contrat juridiquement contraignant. Ces conditions juridiques peuvent être trouvées dans le droit privé, qui, en Europe, est principalement constitué par le droit national, puisqu'il n'existe pas de droit privé européen contraignant.

Bien que d'autres juridictions puissent avoir des conditions juridiques différentes, certaines des hypothèses sous-jacentes restent les mêmes. Tout d'abord, un accord obligatoire est un acte plus poussé dans lequel les parties visent à établir des effets juridiques spécifiques, tels qu'une obligation légale de payer un prix en échange du transfert d'un bien ou de la fourniture d'un service. En common law, un contrat nécessite une contrepartie pour être valide (un prêt pour un rendu). L'intention d'être lié par le contrat peut être déduite des déclarations des parties, mais parfois elle peut aussi être déduite de leurs actions – si ces actions ont généré la confiance légitime que l'on a consenti au contrat. Dans la plupart des juridictions, si ce n'est dans toutes, un contrat valide nécessite une offre suffisamment précise de la part d'une partie, qui est acceptée par l'autre partie. Si l'acceptation a été déduite à tort de certains comportements, alors qu'en fait il n'y a pas eu d'acceptation, le contrat sera considéré comme nul (car l'une des conditions constitutives ne s'applique pas). En revanche, si la partie qui offre a légitimement déduit l'acceptation du comportement de l'autre partie, le contrat peut néanmoins être valide.

Mais un contrat intelligent peut-il être considéré comme un contrat légal? Sur la base de ce qui précède, il y a au moins trois questions :

1. Peut-on supposer que l'envoi d'un message à un contrat intelligent (code sur le ledger) implique la volonté d'y être lié (et donc d'accepter une offre)?
2. Le code informatique compte-t-il comme une expression du contenu d'un contrat (et donc comme une offre suffisamment spécifiée)?
3. Une partie peut-elle invoquer l'annulation parce qu'elle ne peut pas lire le code?

Le fait que la plupart des contrats n'ont pas d'exigences formelles pourrait être utilisé comme argument pour dire que l'envoi d'un message spécifique au code sur le DLT peut compter comme l'expression de l'intention de conclure le contrat tel que défini dans le code. Toutefois, la question de savoir si le code informatique est considéré comme l'expression du contenu d'un contrat, au même titre qu'un contrat écrit, n'est toujours pas tranchée. Pour compter comme une telle expression, le code doit être suffisamment déterminé pour que les deux parties comprennent

l'effet juridique du contrat (c'est-à-dire les obligations juridiques qu'il génère). Si la partie qui accepte ne lit pas le code, elle peut soit

- faire valoir qu'elle n'a pas accepté le contenu du code parce que ses attentes légitimes concernant ce contenu – telles que déduites des négociations, de la publicité ou d'autres expressions de la partie offrante – ne correspondent pas au code, ce qui signifie que le contrat est nul, ou
- faire valoir que le contrat est annulable en raison, par exemple, d'une erreur ou d'une fraude.

Si nous supposons que le contrat est valide, nous devons encore examiner l'effet juridique d'un contrat valide, car dans la plupart des juridictions, cet effet juridique n'est pas limité à la formulation littérale du contrat.

Cet effet s'étend souvent à

- ce que les deux parties devraient raisonnablement attendre, compte tenu des circonstances
- tandis qu'un certain nombre de contraintes juridiques peuvent s'appliquer qui codéterminent le contenu du contrat.

10.2.3 Le statut juridique de la *réglementation intelligente* en droit public

Le terme *réglementation* fait référence aux règles promulguées par l'administration publique ou par des contrôleurs indépendants institués par un acte législatif (généralement appelés *régulateurs* aux États-Unis et au Royaume-Uni, par exemple la Federal Trade Commission ; dans l'UE, on peut penser au CEPD ou aux autorités nationales de protection des données).

Ces règles sont soit :

- une partie d'une compétence explicitement attribuée pour créer et imposer des règles ; ou
- un moyen de fournir la transparence sur la façon dont un régulateur fera usage de sa compétence discrétionnaire (dans ce cas, ces règles forment une politique).

De nombreuses décisions gouvernementales affectent les citoyens, comme l'octroi d'un permis, la sécurité sociale ou une décision sur la fiscalité. De nombreux arguments fournis dans la section précédente peuvent être répétés ici, et ne s'appliquent pas seulement à la mise en œuvre via les DLT mais aussi à d'autres formes de prise de décision algorithmique (automatisée). Cela signifie simplement que les règles pertinentes sont interprétées et traduites en un code non ambigu, afin de permettre leur auto-exécution.

Comme pour les contrats de droit privé, la réglementation intelligente sera nécessairement surinclusive et sous-inclusive (ou les deux), en raison de son manque de flexibilité adaptative.

La nécessité de formaliser figera, en un sens, les réponses futures dans un modèle qui ne tient pas nécessairement compte de l'évolution des circonstances et peut ne pas refléter l'évolution de la jurisprudence, ce qui pourrait aboutir à ce que le code viole des droits au lieu d'imposer la conformité. À cet égard, il est crucial de se rappeler que ces règles et politiques, ainsi que leur automatisation machinale, relèvent de l'État de droit.

Au lieu de comprendre la réglementation intelligente comme une sorte de loi, il est donc préférable de la comprendre comme une administration publique.

Cela signifie que ces règles et politiques, ainsi que leurs traductions machiniques, doivent à un moment donné être contestables devant un tribunal. Les personnes soumises à des décisions fondées sur la réglementation intelligente doivent pouvoir demander une justification de la décision conformément au principe de légalité. Notons toutefois qu'une justification n'est pas équivalente à une explication, qui sert plutôt à rendre la décision contestable quant à sa justification.

10.3 *Légal par conception ou Protection juridique dès la conception ?*

Certaines auteurices affirment que le code auto-exécutoire pourrait être utilisé pour garantir que la conduite des sujets de droit sera *légal par conception* (*legal by design*, LbD). Ce qu'ils veulent dire, c'est qu'il est possible d'interpréter le contenu d'un contrat, le contenu des directives politiques ou même le contenu de la législation de manière à pouvoir le traduire en code informatique. Des langages Turing-complet ont été développés dans le domaine des DLT pour écrire des contrats intelligents qui, comme nous l'avons vu précédemment, sont censés exécuter eux-mêmes ce qui a été convenu par les parties. On peut imaginer des tentatives similaires pour assurer la conformité au niveau des règles réglementaires.

10.3.1 Légal par conception

La LbD est un sous-ensemble de ce que d'autres auteurices ont appelé la *techno-réglementation*. Il s'agit du fait que les technologies induisent ou inhibent souvent certains types de comportements et les appliquent ou les excluent, ce qui a un effet régulateur *de facto*.

La LbD est donc un sous-ensemble spécifique de la techno-réglementation qui est :

1. le résultat de choix de conception délibérés, où
2. ces choix visent à garantir le respect des obligations légales par le biais d'une application technique.

La LbD comporte deux étapes :

1. elle implique une interprétation spécifique (non ambiguë) de la norme juridique pertinente
2. et elle implique la traduction de cette interprétation dans un langage de programmation.

Notez que ces étapes peuvent être distinguées analytiquement, mais qu'elles peuvent être confondues dans la pratique (masquant ainsi l'acte d'interprétation). En raison de la nécessité de sélectionner une interprétation qui peut être traduite en langage machine non ambigu, ces interprétations peuvent être trop ou pas assez inclusives par rapport à la norme juridique pertinente.

Par exemple, l'obligation légale pour un employé de conduire un camion de A à B dans un délai raisonnable pourrait faire partie d'un contrat intelligent entre un employeur et un employé. Comme l'exécution du contrat a lieu hors chaîne, un oracle doit être mis en place pour fournir des signaux clairs indiquant si cette obligation légale a été remplie ou non. Pour définir quelle performance est considérée comme *raisonnable*, en tenant compte de différents types de circonstances, le contrat doit être interprété au préalable et traduit en un ensemble de variables d'entrée pour l'oracle. Comme nous l'avons vu plus haut, le *caractère raisonnable* n'est pas un concept subjectif en droit des contrats, car il doit être interprété conformément à la jurisprudence pertinente, tout en tenant compte des circonstances particulières du cas d'espèce. Il est donc très improbable qu'un contrat intelligent puisse être assimilé à une *conformité juridique par conception*, en raison de la rigidité du comportement du code informatique par rapport à l'adaptabilité du sens du langage naturel.

La LbD semble dans cet exemple être un terme inepte pour ce qui est réellement réalisé. Tant que l'on garde cela à l'esprit, en intégrant des contrôles et des équilibres (y compris des recours juridiques si la légalité est contestée), les contrats intelligents et la réglementation intelligente peuvent néanmoins contribuer à la conformité (sans toutefois la garantir).

10.3.2 Protection juridique dès la conception

La protection juridique dès la conception (LPbD) est une autre question. Elle ne vise pas à garantir l'application d'une norme juridique, quelle qu'elle soit, mais plutôt à faire en sorte que la protection juridique ne soit pas exclue par les possibilités de l'environnement technologique qui détermine si nous jouissons ou non de la substance des droits fondamentaux.

Le terme *juridique* implique ici deux exigences importantes du droit dans le contexte d'une démocratie constitutionnelle :

- le champ d'application de la LPbD doit être déterminé par le biais d'une participation démocratique, par exemple dans le cadre d'une évaluation technologique participative et de l'implication du corps législatif démocratique
- les personnes soumises à cette LPbD doivent être en mesure de contester son application devant un tribunal.

La techno-réglementation en général n'inclut pas ces exigences et la LbD non plus, qui se concentre souvent sur l'exclusion de l'implication (*excluding the involvement*) de tiers de confiance. Ces deux exigences distinguent donc la LPbD d'autres types de solutions *dès la conception*, par exemple la conception sensible à la valeur (*value sensitive design*) ou la protection de la vie privée dès la conception (*privacy by design*).

Ces dernières sont souvent proposées comme des exigences éthiques, ce qui est problématique pour deux raisons. **Tout d'abord**, comme les normes éthiques ne peuvent pas uniformiser les règles du jeu (*level the playing field*), les entreprises qui appliquent une telle conception éthique peuvent être évincées du marché. **Deuxièmement**, les approches éthiques par conception font dépendre la protection des inclinations éthiques de ceux qui développent et commercialisent l'architecture de choix des citoyens, au lieu d'exiger que cette architecture de choix réponde à des normes minimales qui fournissent une protection efficace et pratique.

10.3.3 La protection juridique dès la conception à la lumière du RGPD

Trois exemples intéressants de LPbD peuvent être trouvés dans le RGPD.

Analyse d'impact relative à la protection des données

Tout d'abord, l'obligation légale de réaliser une analyse d'impact (DPIA pour l'acronyme anglais) à l'Article 35, qui est obligatoire si l'introduction d'une nouvelle technologie est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées.

L'Article 35 exige essentiellement que les responsables du traitement fassent preuve de prudence en prévoyant les risques pour les droits et libertés des personnes physiques. On pourrait qualifier cela d'introduction du principe de précaution dans le droit de la protection des données. Il convient de noter que l'évaluation ne porte pas uniquement sur les violations potentielles des droits et obligations stipulés dans le RGPD, mais se concentre sur les *droits et libertés* dans un sens plus général, ce qui correspond à l'objectif du RGPD tel qu'il est formulé à l'Article 2(2) :

[l]e présent règlement protège les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel.

En outre, l'évaluation d'un tel risque ne se limite pas aux personnes concernées mais se réfère aussi aux personnes physiques, ce qui inclut les individus qui courent le risque d'être discriminés même si leurs données personnelles ne sont pas (encore) traitées.

Protection des données par défaut et dès la conception (DPbDD)

L'Article 35(7)(d) indique clairement qu'une DPIA incorpore une évaluation de la nécessité d'une protection des données par défaut et dès la conception (DPbDD), puisqu'il exige un inventaire des *mesures envisagées pour faire face aux risques, y compris les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel et à démontrer la conformité au présent règlement en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes concernées*. Cela nous amène à l'Article 25, qui exige de concevoir les systèmes qui traitent des données à caractère personnel de telle sorte que la minimisation des données soit réalisée par défaut, tout en intégrant toutes les autres obligations du RGPD dans la conception du système.

Bien que la DPbDD ne soit pas à prendre à la légère, elle n'exige pas ce qui n'est pas faisable. L'obligation prend en compte *l'état de l'art, le coût de la mise en œuvre et la nature, la portée, le contexte et les finalités du traitement* (¶1), ce qui signifie que les mesures doivent être réalisables, y compris à la lumière du modèle d'entreprise. Toutefois, cela ne signifie pas que tout est permis si le modèle d'entreprise ne peut pas fonctionner sans prendre des risques disproportionnés avec les droits et libertés des personnes physiques. Là encore, comme pour la DPIA, ces risques doivent être pris en compte lors de la conception des opérations de traitement. La proportionnalité dépend des *risques de probabilité et de gravité variables*, ce qui signifie que plus les risques sont élevés, plus la protection doit être mise en œuvre dès la conception.

Il est clair que la DPIA et la DPbDD adoptent tous deux une approche du risque pour la protection des données à caractère personnel. Bien que certain·es aient interprété cela comme un signe que le législateur européen favorise une compréhension cybernétique du risque et de la réglementation plutôt qu'une approche fondée sur les droits, il semble plus probable que l'approche du risque vise à introduire certaines précautions légalement requises du côté des contrôleurs de données, afin de soutenir et de permettre une protection efficace et pratique des droits et libertés des personnes physiques. À la lecture des exigences soigneusement élaborées, équilibrées et raisonnablement complexes visant à intégrer les normes juridiques pertinentes dans l'architecture du traitement des données à caractère personnel, il est évident que ni la DPIA ni la DPbDD ne visent à produire des systèmes de traitement qui soient légaux par conception. Au contraire, elles justifient et introduisent des obligations légales pour incorporer la protection juridique par la conception dans des systèmes techniques qui, autrement, rendraient illusoire la protection des droits et libertés d'une personne.

Décisions automatisées

Ceci nous amène à un troisième exemple de LPbD dans le contexte du RGPD qui est très pertinent pour les applications de ML et les DLT, car il vise les implications des décisions automatisées. L'Article 22 du RGPD spécifie ainsi :

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Quand une décision produit-elle un effet juridique ? L'EDPB précise que c'est le cas si la décision *affecte les droits légaux d'une personne, tels que la liberté de s'associer avec d'autres, de voter lors d'une élection ou d'intenter une action en justice. (. . .) affecte le statut juridique d'une personne ou ses droits en vertu d'un contrat.*

Dans le cas d'une décision fondée sur un traitement automatisé nécessaire à l'exécution d'un contrat ou d'une décision fondée sur le consentement, l'accès à une intervention humaine est nécessaire, tant pour exprimer son point de vue que pour contester la décision. Le considérant 71 nous apprend ainsi que :

10.3. LÉGAL PAR CONCEPTION OU PROTECTION JURIDIQUE DÈS LA CONCEPTION ?93

En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

Nous trouvons ici le droit d'obtenir une explication de la décision, que de nombreux auteurs interprètent comme étant une condition préalable pour pouvoir contester la décision (comme l'exige l'Article 22(3)). À l'heure actuelle, un certain nombre d'articles scientifiques ont été publiés sur le *droit à une explication* et l'*IA explicable (XAI)*, qui sont jugés très pertinents notamment en raison de la possibilité d'une partialité injustifiée. Ce *droit à l'explication* peut également être interprété dans les exigences de transparence des Articles 13(2)(f), 14(2)(g) et 15(1)(h).

Les responsables du traitement ont l'obligation légale de fournir ces informations, tant lorsque les données ont été fournies par la personne concernée (Article 13) que lorsque les données n'ont pas été collectées auprès de la personne concernée (Article 14), tandis que les personnes concernées ont le droit d'obtenir ces informations (Article 15). Il convient de noter que l'obligation de fournir ces trois types d'informations ne dépend pas d'une demande de la personne concernée mais doit être fournie de toute façon.

Chapitre 11

Fermeture : sur l'éthique, le code et le droit

Ce dernier chapitre examine la distinction entre le droit, le code et l'éthique, leurs relations mutuelles et leur interaction. Il s'agit d'un chapitre bonus pour celles et ceux qui s'intéressent au lien entre le droit et l'éthique, à la lumière des infrastructures d'information et de communication (IIC) axées sur le code et les données.

Dans l'introduction du Chapitre 10, nous avons rencontré l'expérience de pensée de la *moral machine* du MIT, qui visait à extraire des opinions sur l'éthique des choix que les voitures à conduite autonome pourraient être amenées à faire. Hildebrandt qualifiait l'expérience comme correspondant à un type *naïf* d'utilitarisme. Dans ce chapitre, on va expliquer les hypothèses qui sous-tendent la formulation du problème de ces *machines morales* et on discutera d'autres façons traditionnelles de formuler les dilemmes éthiques. C'est nécessaire parce qu'elles font partie de notre sens commun et servent donc souvent de prémisses cachées à l'éthique dans l'IA et de tentatives similaires de faire le bien (*do good*) lors du développement de systèmes basés sur le code ou les données. Ces hypothèses cachées jouent un rôle important, même si l'on n'en est pas conscient, et il faut donc les signaler.

Après avoir donné une vue d'ensemble, on précisera ce qui différencie le droit de l'éthique, car il s'agit d'un livre sur le droit et non principalement sur l'éthique. Spoiler : l'une des principales différences est que le droit fournit une fermeture (*closure*) alors que l'éthique reste dans le domaine de la réflexion en ce qu'elle n'a pas force de loi. Cependant, une deuxième différence renverse l'affirmation précédente : alors que le droit et la règle de droit introduisent des contrôles et des équilibres et exigent une participation démocratique (du moins dans les démocraties constitutionnelles), l'éthique peut être décidée par des développeuses ou derrière les portes closes de la salle du conseil d'administration d'une entreprise commerciale. Elle peut ainsi obtenir la force de la technologie.

Cela impliquerait que ce n'est plus la loi mais aussi la technologie qui fournit la fermeture, mais pas par le biais d'une législation démocratiquement légitimée. La fermeture est plutôt assurée par l'éthique, telle qu'elle est incarnée dans la boîte noire de la R&D, les salles de conseil des grandes entreprises technologiques et les communautés de développeuses qui écrivent et maintiennent le code source ou les registres distribués.¹

Pour bien comprendre le rôle de l'éthique, du code et du droit dans le développement technologique, nous devons aller au-delà des distinctions analytiques. Comme démontré au Chapitre 2,

1. Bien que ces derniers ne soient pas une boîte noire pour ceux qui s'y connaissent sur le plan technique, ils sont des boîtes noires pour ceux qui ne peuvent pas lire le code.

il existe une relation particulière entre l'éthique et la règle de droit, ce qui implique que le droit et l'éthique interagissent. L'exemple que l'on utilisera tout au long de ce chapitre ne concerne pas les dilemmes éthiques des voitures sans conductrice, mais la question de l'équité algorithmique (qui concerne évidemment aussi les décisions prises par ceux qui construisent le code des voitures sans conducteur). Cela confrontera la force de la loi à la force de la technologie, nécessitant un nouveau type d'interaction entre les juristes et les informaticien·nes sur la manière de garantir que le design éthique ne l'emporte pas sur les freins et contreponds de la règle de droit. En ce sens, certaines des notions présentées au Chapitre 10 referont surface lors de la discussion sur la relation entre le code et la loi.

Dans le contexte de ce chapitre, on utilisera le terme éthique pour faire référence à la fois à la moralité (agir d'une manière moralement justifiée) et à la philosophie morale (s'interroger sur les types de justification morale que l'on pourrait développer). Cela signifie également que, pour les besoins de ce chapitre, on utilisera les termes *éthique* et *moral* comme synonymes.

11.1 Distinctions entre le droit, le code et l'éthique

Faire de l'éthique peut signifier deux choses différentes :

- être engagé dans la sous-discipline philosophique de l'éthique, ou
- agir d'une manière qui soit éthique.

Bien qu'il puisse être tentant d'inventer une éthique pour le monde onlife, comme si ce que des siècles de recherche en philosophie morale nous ont apporté n'avait pas d'importance, on se laisse facilement entraîner par des hypothèses cachées. Par exemple, l'expérience de pensée du MIT (vu au Chapitre 10) est présentée comme si elle n'avait rien à voir avec les débats savants sur les différentes écoles de philosophie morale, mais sa formulation du problème repose sur une variante spécifique de l'utilitarisme et incorpore un certain nombre d'hypothèses qui sont considérées comme allant de soi sans examen approfondi.

Pour agir de manière éthique en tant qu'individu·e, il n'est pas nécessaire d'avoir étudié l'éthique, mais lorsqu'on réfléchit aux implications éthiques de la partialité dans l'apprentissage automatique par exemple, il est crucial de prendre du recul avant d'avancer.

11.1.1 Utilitarisme et individualisme méthodologique

L'utilitarisme se concentre sur les conséquences de nos actions. Pour cette raison, il est souvent assimilé au conséquentialisme. L'utilitarisme est toutefois un type particulier de conséquentialisme, fondé sur l'*individualisme méthodologique*. Cela signifie que les choix individuels sont supposés être indépendants, de sorte que le choix collectif n'est rien d'autre que l'agrégat des choix individuels. Il s'agit d'une position très controversée, car le choix individuel dépend de l'anticipation du choix d'autrui et est en partie constitué d'architectures de choix qui dépendent à leur tour des IIC et sont informées par les relations de pouvoir.

Les interdépendances entre les choix individuels et collectifs dans des systèmes complexes tels que la société humaine sont nombreuses et, en partie, émergentes. Les simplifier en supposant un choix individuel indépendant peut être commode d'un point de vue informatique, mais totalement inadéquat quant à l'interaction avec le monde réel. C'est pourquoi la théorie du choix rationnel peut sembler un bon outil pour réfléchir aux choix éthiques, mais elle ne tient pas compte du fait qu'en tant qu'outil, elle codétermine en fait ce qu'elle est censée étudier. Cela crée un problème de cadrage. Ceci est lié à la deuxième hypothèse intenable de l'individualisme méthodologique, à savoir que les **moyens** et les **fins** peuvent non seulement être distingués analytiquement (une très bonne idée), mais aussi *exister* séparément dans notre monde (une idée très problématique).

Pour des raisons de brièveté, on abordera quatre types d'utilitarisme qui se recoupent, en laissant inévitablement de côté de nombreuses nuances : l'utilitarisme des **actes** et des **règles**, et l'utilitarisme **maximal** et **moyen**. Tous les quatre soulignent que le choix éthique doit être fait sur la base de l'utilité qu'il génère. C'est pourquoi l'utilitarisme se nourrit d'évaluations coûts-avantages qui, à leur tour, alimentent un calcul utilitariste ; il constitue l'hypothèse cachée de l'évaluation des risques comme moyen viable de faire face à l'impact des nouvelles technologies. Comme les gens peuvent ne pas s'entendre sur ce qui constitue l'utilité, les conséquences sont généralement discutées en termes de préférences ou de bien-être plutôt que d'utilité. Cela soulève toutefois la question de savoir si ces préférences sont données ou encadrées, en fonction de l'architecture de choix présentée par l'environnement. Le bien-être soulève des questions similaires, car il n'est pas nécessairement une fonction objective des choix éthiques (des individus, groupes, cultures et sociétés différents peuvent définir le bien-être de manière contrastée, voire incompatible). Par conséquent, on s'en tiendra au concept d'utilité, en prenant note qu'il s'agit du point de fuite de l'utilitarisme et, à bien des égards, d'une boîte noire.

L'**utilitarisme des actes** dit que le bon acte est celui qui maximise l'utilité. La question est évidemment *l'utilité de qui ?*, car la maximisation peut être comprise comme un agrégat : plus l'utilité des gens est satisfaite, mieux c'est ; ou comme une moyenne : plus l'utilité moyenne est élevée, mieux c'est. De nombreuses modulations sont possibles. Le philosophe du droit John Rawls pourrait exiger que le résultat optimise au moins l'utilité des *moins favorisés*, tout en récompensant ceux dont les actions ont augmenté la portée globale de l'utilité. C'est ce que l'on appelle le principe de **maximin**, qui sera expliqué plus loin dans le cadre du raisonnement déontologique (Section 11.1.2) et dans celui de la justice, de la certitude juridique et de l'instrumentalité (Section 11.2.1), puisque Rawls n'est pas un utilitariste pur et dur. Le point le plus important ici est que dans l'utilitarisme des actes, chaque acte est isolé comme s'il s'agissait d'un *dispositif* autonome. L'expérience de la machine morale demandait aux visiteurs de donner une préférence morale sur la base d'un accès limité au contexte, à l'historique et aux circonstances - comme si les situations se produisaient dans le vide.

L'**utilitarisme des règles** a été conçu pour résoudre les problèmes générés par l'utilitarisme des actes. Il proclame essentiellement que l'acte juste est celui qui s'aligne sur une règle qui permettrait - si tout le monde la suivait - d'atteindre l'utilité maximale. Comme pour l'utilitarisme des actes, certaines peuvent préférer l'utilité moyenne à l'utilité maximale, ou suivre le principe du maximin de Rawls. L'utilitarisme des règles partage avec l'utilitarisme des actes les hypothèses de l'individualisme méthodologique et de la séparation des moyens et des fins. Il en résulte une propension à quantifier le problème au moyen de la théorie des jeux (en supposant des agents rationnels) ou de l'économie comportementale (en supposant que si les agents humains peuvent être irrationnels, leurs comportements irrationnels sont néanmoins prévisibles).

On peut maintenant expliquer pourquoi Hildebrandt pense que l'expérience de la *moral machine* du MIT repose sur un type naïf d'utilitarisme. Soit elle vise à découvrir les préférences morales des visiteuses d'un site web quant aux conséquences souhaitables d'une série d'actes particuliers, auquel cas toutes les hypothèses problématiques de l'utilitarisme de l'acte s'appliquent. Soit elle vise à découvrir les préférences morales des visiteuses du site web quant au type de règles qui devraient informer le comportement des véhicules autonomes, en ce qui concerne un acte spécifique. Dans ce cas, l'utilitarisme des actes est confondu avec l'utilitarisme des règles, car l'idée même de l'utilitarisme des règles est de parvenir à une orientation à un niveau d'abstraction plus élevé (non pas basée sur des cas mais sur des règles).

Les chercheuses pourraient objecter que leur étude n'est qu'une enquête objective, basée sur des données, sur les préférences morales de 40 millions de visiteurs du web, et qu'elle ne doit pas être confondue avec une enquête éthique. Iels pourraient affirmer que l'étude ne cautionne aucune théorie de l'éthique et ne contient aucun biais en faveur de l'utilitarisme. Le philosophe des

sciences Karl Popper répondrait que la cognition et même la perception ne sont pas possibles sans une théorie sous-jacente qui encadre les questions étudiées. Dans le cas présent, l'individualisme méthodologique qui sous-tend l'utilitarisme encadre clairement l'expérience et configure le type de choix proposé aux internautes. Ces choix sont ensuite qualifiés de préférences données et traités comme des variables indépendantes qui peuvent être corrélées avec, par exemple, des *traits culturels*, des *prédicteurs économiques* et la *proximité géographique*. Comme l'ont écrit Michel Callon et John Law, la quantification (via des données numériques) est nécessairement précédée d'une qualification (un regroupement d'instances spécifiques sous la même rubrique d'une variable ou d'une caractéristique spécifique). Bien qu'il n'y ait rien de mal à cette qualification, nous devons prendre conscience des choix de définition qu'elle implique et des problèmes de cadrage qu'elle engendre. Je donnerai ci-dessous un exemple d'évaluation de l'équité algorithmique qui met en évidence ces choix et montre certaines de leurs implications (dans la Section 11.1.5).

Il suffit ici de souligner que les deux types d'utilitarisme nécessiteraient en fin de compte un moyen de mesurer et peut-être même de pondérer les préférences, par exemple, une préférence pour sauver les blancs plutôt que les gens de couleur compterai-elle ? En général, ces types de préférences dépendent de l'agent, car mon choix pour une règle de comportement ou une action peut dépendre du fait que je sois dans la voiture ou à l'extérieur. La manière dont les internautes ont développé leurs préférences n'est absolument pas claire, ce qui fait de l'ensemble de l'expérience une tentative plutôt hasardeuse de contribuer à un débat éclairé sur l'éthique des voitures à conduite autonome. Pour comprendre sérieusement les préférences pertinentes sur le plan éthique, nous devrions imposer un voile d'ignorance, nous obligeant à décider sans savoir si nous serons la victime ou non. Cependant, cela peut rapprocher l'utilitarisme des règles des impératifs déontologiques, puisque les raisons qui informent mon choix indépendant de l'agent peuvent différer de celles qui informent mon choix dépendant de l'agent, ce qui introduit un critère moral qui ne fait pas partie des notions d'utilité, d'acte ou de règle.

Passons maintenant à l'équité algorithmique, en nous demandant comment elle se comporterait sous différents types d'utilitarisme. Le problème est que ni l'utilité maximale ni l'utilité moyenne ne résoudre le problème de l'impact disparate de divers types de biais dans l'apprentissage automatique. Dans l'ensemble, un parti pris injuste peut augmenter l'utilité (qu'elle soit maximisée ou moyenne), mais certaines catégories de personnes individuelles peuvent trouver que leurs préférences sont ignorées ou diminuées. Il est clair que l'équité est un critère moral qui ne peut pas être facilement intégré dans la logique de l'utilitarisme des actes ou des règles.

11.1.2 Raisonnement déontologique : le respect pour l'autonomie humaine

Le raisonnement déontologique concerne les personnes qui font la bonne chose pour la bonne raison, sans tenir compte des effets. Le raisonnement déontologique porte sur les devoirs, et non sur les conséquences, et peut être rattaché à l'**impératif catégorique** de Kant. Kant distingue l'impératif *hypothétique*, qui fait dépendre une décision des conséquences qu'elle est censée engendrer (souvent évaluées du point de vue de l'intérêt personnel), et l'impératif *catégorique*, qui fait dépendre une décision de la justification morale qu'elle implique (notamment le respect de l'autonomie d'autrui).

Kant a formulé différentes versions de l'impératif catégorique. Je les cite ici à partir de la célèbre Stanford Encyclopedia of Philosophy,² pour donner aux lectrices un aperçu des complexités que le raisonnement déontologique peut impliquer, ce qui le rend apparemment moins propice à une traduction informatique qu'un calcul utilitaire (bien que le problème de la définition de l'utilité crée les mêmes types de problèmes). Notez que l'accent mis sur l'autonomie

2. On utilisera ici la traduction de l'article du Larousse.

morale individuelle ne dépend pas de l'individualisme méthodologique de l'utilitarisme, puisque les maximes à discuter ne dépendent pas d'une utilité globale, mais de la mesure dans laquelle une maxime implique que l'autonomie de chacun·e soit respectée.

1. *Agis uniquement d'après la maxime qui fait que tu puisses vouloir en même temps qu'elle devienne une loi universelle.*

Selon la Stanford Encyclopedia of Philosophy, cela implique :

- Premièrement, formulez une maxime qui consacre votre raison d'agir comme vous le proposez.
- Deuxièmement, reformulez cette maxime comme une loi universelle de la nature régissant tous les agents rationnels, et donc comme voulant que tous doivent, par loi naturelle, agir comme vous vous proposez d'agir dans ces circonstances.
- Troisièmement, examinez si votre maxime est même concevable dans un monde régi par cette loi de la nature. Si elle l'est, alors,
- quatrièmement, demandez-vous si vous voudriez, ou pourriez, rationnellement vouloir agir selon votre maxime dans un tel monde. Si vous le pouvez, alors votre action est moralement admissible.

- 2 *Agis de façon telle que tu traites l'humanité, aussi bien dans ta personne que dans toute autre, toujours en même temps comme fin, et jamais simplement comme moyen.*

Selon la Stanford Encyclopedia of Philosophy, cela implique :

- Premièrement, la formule de l'humanité n'exclut pas d'utiliser les gens comme des moyens pour atteindre nos fins.
- Deuxièmement, ce ne sont pas les êtres humains en soi mais *l'humanité dans les êtres humains* que nous devons traiter comme une fin en soi.
- Troisièmement, l'idée de fin a trois sens pour Kant, deux sens positifs et un sens négatif.
- Enfin, la formule de l'humanité de Kant exige le respect de l'humanité des personnes.

- 3 *L'idée de la volonté de tout être raisonnable conçue comme volonté instituant une législation universelle.*

Selon la Stanford Encyclopedia of Philosophy, cela implique :

- dans ce cas, nous nous concentrons sur notre statut de donneur de loi universelle plutôt que de suiveur de loi universelle.
- C'est bien sûr la source même de la dignité de l'humanité dont parle Kant dans la deuxième formulation.
- Une volonté rationnelle qui serait simplement liée par des lois universelles pourrait agir en conséquence à partir de motifs naturels et non moraux, tels que l'intérêt personnel.
- Mais pour être un législateur de lois universelles, de tels motifs contingents, des motifs que des agents rationnels comme nous peuvent avoir ou non, doivent être mis de côté.
- 4 Agis selon les maximes d'un membre qui légifère universellement en vue d'un règne des fins simplement possible.

Selon la Stanford Encyclopedia of Philosophy,

- cela implique que nous devons conformer nos actions aux lois d'une législature morale idéale,
- que cette législature établit des lois universelles, liant toutes les volontés rationnelles, y compris la nôtre, et

- que ces lois sont d'un *royaume simplement possible* dont chacun des membres possède également ce statut de législateur de lois universelles, et doit donc toujours être traité comme une fin en soi. L'idée intuitive qui sous-tend cette formulation est que notre obligation morale fondamentale consiste à n'agir que sur la base de principes qui pourraient être acceptés par une communauté d'agents pleinement rationnels, dont chacun a une part égale dans la législation de ces principes pour sa communauté.

En résumé, ce type de raisonnement déontologique est fondé sur un respect fondamental de l'autonomie de chaque personne, ce qui nous oblige à agir selon des règles que toute personne pourrait accepter comme la bonne règle. Notez que *pourrait* n'est pas équivalent à *ferait*, car *ferait* peut dépendre de l'intérêt personnel, alors que *pourrait* dépend de raisons morales valables pour convenir de la règle, en tenant compte de l'autonomie des autres personnes. Cela permet de faire abstraction des préférences personnelles et de la simple acceptation des règles, en exigeant que les règles soient au contraire acceptables du point de vue d'un consensus universel rationnel sur la meilleure façon de respecter l'autonomie de chaque personne. Cela implique une moralité *reconstructive* en ce sens que les actions d'une personne devraient pouvoir être justifiées comme étant conformes à une règle générale que n'importe qui accepterait derrière un voile d'ignorance (ne sachant pas ce qui serait dans son intérêt personnel, transformant ainsi le *pourrait* ci-dessus en *voudrait*).

Il est clair que l'hypothèse d'un consensus universel rationnel est problématique, non pas parce que les gens ont des intérêts différents (le voile de l'ignorance résout ce problème), mais parce que les gens ont des idées différentes sur la valeur de ces intérêts et sur leur classement (par exemple, préférer la communauté à la liberté, ou l'égalité à la communauté). Nous reviendrons sur ce point lors de la discussion sur le pragmatisme.

Comment l'équité algorithmique s'inscrirait-elle dans le cadre du raisonnement déontologique? Une façon d'aborder la question serait de se demander si le biais dans les systèmes de décision algorithmique viole l'autonomie de certains agents humains, tout en respectant l'autonomie des autres. L'inégalité est au cœur de la question, puisque l'impératif catégorique ne permet pas de respecter plus ou moins l'autonomie d'une personne; soit on la respecte, soit on ne la respecte pas. Du point de vue de Kant, l'autonomie n'est pas respectée s'il n'existe pas de règle universelle qui justifie un traitement disparate. Pour évaluer si c'est le cas, nous devons nous demander si l'on consentirait à un traitement différent si l'on ne savait pas si l'on bénéficierait ou perdrait de l'algorithme.

Cette expérience de pensée a été proposée par John Rawls sous le nom de **voile de l'ignorance**. Ce voile d'ignorance a inspiré le principe éthique du maximin de Rawls qui explique dans quelles conditions l'inégalité n'est pas injuste. Imaginons qu'il y ait un seul gâteau, à partager entre plusieurs personnes. Certaines d'entre elles peuvent trouver le moyen d'agrandir le gâteau. Puisque l'on se trouve derrière le voile de l'ignorance, il n'y a aucun moyen de savoir si l'on fait partie de ceux qui pourraient *agrandir* le gâteau ou non. Selon le principe de maximin, par défaut, tout le monde devrait obtenir une part égale du gâteau. Toutefois, il serait juste que ceux qui parviennent à agrandir le gâteau reçoivent une part plus importante que les autres. Cela ne devrait toutefois pas avoir pour conséquence que ceux qui ont les plus petites parts se retrouvent avec encore moins qu'avant. En fait, ils devraient bénéficier de l'élargissement du gâteau, mais pas dans la même mesure que ceux qui l'ont fait grossir. De cette façon, ceux qui ont augmenté le gâteau partagé sont récompensés pour leur contribution (juste dû), tout en veillant à ce que les moins favorisés participent à l'augmentation (répartition équitable).

Rawls combine essentiellement deux types de justice en tant qu'équité dans son principe maximin : la justice distributive et la justice correctrice. Nous y reviendrons lorsque nous discuterons de la justice (Section 11.2.1). Il y a peut-être une question préliminaire qui est encore plus pertinente ici : l'application automatisée d'un algorithme peut-elle jamais être respectueuse de

l'autonomie des personnes soumises à ses décisions ? Se pourrait-il que les algorithmes n'utilisent nécessairement les personnes que comme un moyen et ne puissent jamais respecter leur autonomie, en raison de la nature même de la prise de décision machinique ? Il s'agit d'une question cruciale et l'autrice pense que la réponse dépend d'un certain nombre de facteurs liés à la mesure dans laquelle la surveillance et l'intervention humaines sont exclues. On ne rejettera pas catégoriquement la prise de décision algorithmique, car on peut faire valoir que s'abstenir de l'utiliser pourrait entraîner un traitement injuste invisible de la part des êtres humains (que ce soit délibéré ou non). Dans ce cas, on pourrait soutenir que s'abstenir de recourir à la prise de décision algorithmique témoigne d'un manque de respect pour l'autonomie des personnes soumises à la décision.

11.1.3 Éthique de la vertu : percevoir le bien et faire ce qui est juste

L'utilitarisme des règles et le raisonnement déontologique fondé sur l'impératif catégorique recherchent une orientation éthique dans des règles abstraites qui devraient être applicables indépendamment des caractéristiques personnelles ou des inclinations de l'agent agissant. L'éthique de la vertu est moins empreinte de justification abstraite, car elle se concentre sur le caractère moral développé par l'acteur. Il ne s'agit pas de raisonner en fonction de l'intérêt personnel de l'agent, mais de souligner la nécessité pour les agents individuels de pratiquer et de développer leur boussole morale. L'idée est que les agents humains ne naissent pas avec une telle boussole, mais qu'ils doivent acquérir de l'expérience dans des situations de la vie réelle, en construisant ce qu'Aristote appelait la *phronesis*, ou sagesse pratique. Dans le contexte de l'éthique de la vertu, il ne s'agit pas de se soumettre à des règles abstraites mais de dégager la bonne règle pour la situation en cours. C'est une question d'acuité et de jugement plutôt que l'application de règles existantes ou un calcul d'utilité.

Alors que l'utilitarisme et l'éthique déontologique se concentrent sur le raisonnement concernant la bonne décision à prendre face à des devoirs contradictoires ou des conflits d'intérêts, l'éthique de la vertu concerne la perception de ce qui est bon et l'action en conséquence.

Comme l'écrit Varela dans son ouvrage sur la sagesse éthique :

En première approximation, permettez-moi de dire qu'une personne sage (ou vertueuse) est une personne qui sait ce qui est bon et qui le fait spontanément.

C'est cette immédiateté de la perception et de l'action que nous voulons examiner de manière critique. Cette approche contraste fortement avec la manière habituelle d'étudier le comportement éthique, qui commence par analyser le contenu intentionnel d'un acte et se termine par l'évaluation de la rationalité de jugements moraux particuliers.

Aristote distingue deux types de connaissances : la connaissance théorique ou *épistème*, et la sagesse pratique ou *phronesis*.

Alors que l'épistème, selon Aristote, est une question de raisonnement et de perspicacité théorique, la *phronesis* est une question d'expérience, d'action et de perception. Les jeunes hommes (Aristote ne s'intéresse pas aux femmes) sont excellents pour atteindre la connaissance épistémique, alors que la *phronesis* ne peut être atteinte qu'au cours d'une vie. L'éthique de la vertu est peut-être le type d'éthique le plus intéressant dans un monde onlife, où les agents non humains remettent en question notre compréhension de l'agence morale. Il semble évident que les machines peuvent développer quelque chose d'apparenté à la connaissance épistémique. Cependant, elles seront, par définition, exclues du développement de vertus ou de sagesse pratique. Ceci est lié à la différence entre la connaissance et la sagesse, et entre la rationalité et le caractère moral. La sagesse et le caractère moral exigent un type d'acuité qui implique à la fois l'ambiguïté et les bonnes intentions, ainsi qu'une intuition habile, une sorte de connaissance tacite qui intègre des vertus telles que la prudence, la tempérance, le courage et la justice. Il est difficile d'imaginer

qu'un algorithme d'apprentissage profond développe l'une de ces caractéristiques dans sa relation avec d'autres agents, même s'il bat les grands maîtres aux échecs, au go et à tout autre jeu fermé aux règles bien définies.

Comment l'équité algorithmique s'accorderait-elle avec l'éthique de la vertu ? Peut-on définir la vertu de justice de telle sorte qu'elle puisse être formalisée et calculée ? La distinction d'Aristote entre justice distributive et justice correctrice (Section 2.2.2) pourrait-elle se prêter à des modèles de recherche qui détectent les biais injustes, tout en réparant le bug qui a conduit à la violation de la justice ?

Il semble que l'éthique de la vertu soit basée sur un type spécifique d'incompatibilité, notamment en ce qui concerne la nature relationnelle de l'agence humaine et des relations humaines, confirmant ainsi que l'équité ne peut pas être calculée (bien qu'elle puisse - paradoxalement - être formulée et calculée de nombreuses manières, dont aucune ne peut prétendre à une réponse unique et correcte). Cela pourrait indiquer que le concept d'algorithme éthique est un oxymore qui ignore l'indécidabilité de l'action vertueuse et de la prise de décision équitable. Non pas parce que les humains ont plus souvent raison que les machines, mais parce que la nature relationnelle de l'action vertueuse n'a pas sa place dans un système qui ne peut jamais qu'exécuter du code (que ce soit sous la forme d'un code déterministe auto-exécutoire ou sous la forme de moteurs d'inférence inductive).

11.1.4 Éthique pragmatique : prendre en compte

Le père fondateur du pragmatisme, Charles Saunders Peirce, a élaboré la *maxime pragmatiste* :

Considérez quels effets, qui pourraient avoir des implications pratiques, nous concevons que l'objet de notre conception ait. Ensuite, notre conception de ces effets est la totalité de notre conception de l'objet.

Il devrait être clair que le pragmatisme est profondément conséquentialiste, dans la mesure où le sens des mots que nous utilisons est défini en termes d'effets anticipés de leur usage. Cela conduit le pragmatisme, en fin de compte, à reconnaître que les moyens codéterminent ou reconfigurent les fins d'une manière qui fait de leur séparation une expérience de pensée naïve bien que parfois productive (en termes philosophiques, cela implique que les moyens et les fins peuvent être analytiquement distingués mais pas ontologiquement séparés).

Cela a clairement des implications pour l'éthique, car cela souligne que la manière dont nous essayons d'atteindre nos objectifs les façonne, également dans le domaine de l'éthique. Dans le contexte de l'utilitarisme, les technologies sont souvent considérées comme des outils neutres, ignorant la manière dont elles permettent et limitent les effets voulus et non voulus. Dans le contexte de l'éthique déontologique, tout ce qui semble compter, ce sont les devoirs moraux de chacun envers les autres agents, sur la base d'un consensus rationnel abstrait qui ne tient pas compte de la situation de l'agence humaine. Il en résulte des devoirs moraux qui s'abstraient des moyens matériels de les exécuter, manquant ainsi leur impact sur l'autonomie humaine. À l'exception de Kant, un pragmatiste de l'éthique ne supposerait pas ou ne postulerait pas un sujet humain autonome, mais chercherait à découvrir les conditions réelles de l'agence autonome.

L'éthique de la vertu semble très pertinente dans le domaine de la conception sensible aux valeurs, car le succès de la *conception éthique* dépendra des compétences nécessaires pour faire fonctionner la conception sensible aux valeurs. Mais c'est le pragmatisme qui a la compréhension la plus claire des implications normatives de la conception d'une technologie d'une manière ou d'une autre, précisément parce qu'il est déjà conscient de la manière dont les moyens façonnent les objectifs. Une éthique pragmatiste partage avec l'éthique de la vertu la conscience de la

situation de l'agent humain, ainsi qu'une sensibilité à l'importance de l'expérience, puisque le pragmatisme souligne la nécessité d'anticiper les conséquences (même si ce n'est pas au sens utilitaire). Comme pour l'éthique de la vertu et l'utilitarisme, une éthique pragmatiste est moins impressionnée par les devoirs moraux universels du raisonnement déontologique, et elle soutient une compréhension plus située de l'autonomie humaine.

D'un point de vue pragmatique, l'équité algorithmique est clairement une préoccupation éthique, puisque le pragmatisme reconnaît que toute technologie utilisée comme un outil pour atteindre un objectif spécifique :

1. entraînera ce que l'on appelle habituellement des effets secondaires,
2. redéfinira l'objectif en termes de moyens pour l'atteindre,
3. reconfigurera ainsi les affordances de l'environnement du ou des agents humains,
4. ce qui aura probablement des effets normatifs pouvant nécessiter une évaluation morale.

Nous pouvons citer les travaux d'Helen Nissenbaum, notamment son heuristique d'*intégrité contextuelle* (CI pour l'acronyme anglais), qui retrace les implications des nouveaux types de technologies, en fournissant une évaluation étape par étape de la manière dont l'environnement est modifié et dont cela peut affecter les attentes légitimes et contextuelles des agents humains. L'une des conséquences de l'introduction de nouvelles technologies peut être une redistribution des risques et des avantages dans et entre les contextes, ce qui peut renforcer les inégalités existantes ou même créer de nouveaux types d'inégalité. Son analyse s'inscrit dans les hypothèses fondamentales d'une éthique pragmatiste, elle va au-delà de la vie privée et fournit un cadre cohérent pour évaluer l'équité en tant que valeur éthique susceptible d'être perturbée.

Notez que l'intégrité contextuelle n'assimile pas l'équité à l'égalité. Comme nous l'avons vu ci-dessus, lors de l'examen du principe de maximin de Rawls, traiter des personnes différentes de manière égale peut en fait être injuste. Pensez au célèbre constat d'Anatole France selon lequel :

Dans sa majestueuse égalité, la loi interdit au riche comme au pauvre de dormir sous les ponts, de mendier dans les rues et de voler des miches de pain.

L'équilibre qui doit être trouvé entre l'égalité corrective et l'égalité distributive exige des choix qui supposent une évaluation morale et politique de ce qui est considéré comme juste dans quelles conditions. Il peut y avoir des indications claires d'un traitement injuste, mais il n'est pas facile de se mettre d'accord sur ce qui constitue un traitement équitable.

En fin de compte, il s'agit d'un choix moral sur lequel les individus et les sociétés devront se prononcer, et d'un choix politique, par exemple en promulguant des normes juridiques qui interdisent certaines actions comme étant injustes et donc illégales.

11.1.5 La différence qui fait une différence : la fermeture

Que pouvons-nous apprendre de ce qui précède sur la différence entre la loi, le code et l'éthique ?

1. L'étude de l'éthique concerne une réflexion sur la justification (qu'elle soit utilitaire ou déontologique) de la prise de décision qui affecte les agents humains et les sociétés humaines, et/ou le développement de la sagesse pratique (éthique de la vertu), et/ou l'étude de la manière dont les moyens d'atteindre des objectifs souhaitables reconfigurent ces objectifs ainsi que les valeurs qu'ils incorporent (éthique pragmatiste). L'étude de l'éthique et le développement de la sagesse pratique n'ont pas force de loi ; ils ne fournissent pas (et ne devraient pas fournir) une conclusion sur la façon d'agir ou de concevoir nos IIC.
2. Le droit positif moderne fournit une fermeture d'une manière que l'éthique ne peut et ne devrait pas faire, puisqu'une démocratie constitutionnelle exclut l'imposition d'une position

éthique spécifique. C'est précisément parce que *nous* ne sommes pas d'accord sur l'éthique, que nous avons besoin du droit pour coordonner notre comportement d'une manière qui assure la certitude juridique et la justice – d'une manière qui soutient le rôle instrumental du droit (Section 2.2.2). La fermeture du droit moderne est directement liée à sa *positivité* (il est promulgué par le législateur, son interprétation est décidée par des tribunaux indépendants, dont les verdicts sont exécutoires en raison du monopole de la violence). Le fait que le droit permette de fermer la porte n'implique pas pour autant qu'il n'existe aucune relation entre le droit et l'éthique. L'exigence fondamentale de justice constitue l'interface avec l'éthique et détermine la moralité interne de l'État de droit, qui est un type spécifique de méta-éthique. Nous y reviendrons dans la section suivante (Section 11.2.1).

3. Agir de manière éthique consiste à prendre la bonne décision, tant au niveau du choix individuel qu'au niveau de la conception des architectures de choix juridiques, politiques et techniques qui encadrent ce choix. Les deux types de décisions interagissent, et elles sont fermées dans la mesure où elles excluent les effets qu'une autre décision aurait pu générer. Dans le cas des choix de conception, l'impact peut être substantiel.
4. Le développement et l'implémentation du code informatique dans une variété de systèmes algorithmiques de prise de décision peuvent aboutir à la fermeture, en raison des architectures de choix qu'ils présentent. À l'heure actuelle, une telle fermeture ne fait pas partie de la participation démocratique et il n'y a aucun moyen de garantir que les freins et contrepoids de l'État de droit sont intégrés.

On pourrait conclure que, si l'éthique n'est pas un concurrent du droit, les systèmes de décision algorithmiques le sont.

11.2 La relation conceptuelle entre le droit, le code et l'éthique

L'éthique est à la fois plus et moins que le droit : elle est plus parce que de nombreuses préoccupations éthiques ne sont pas traitées par le droit et moins parce que les résultats des considérations éthiques ne sont pas nécessairement transformés en normes juridiques et ne sont donc pas applicables par le biais du droit. Comme indiqué ci-dessus, étant donné que nous ne sommes souvent pas d'accord sur les règles, les valeurs ou les choix éthiques, le droit intègre principalement les principes et les considérations éthiques à un méta-niveau – par exemple, pour s'assurer que le choix éthique n'est pas systématiquement annulé par l'intérêt économique. L'idée est que le droit, et en particulier l'État de droit, crée un espace pour développer la sagesse pratique de chacun et pour agir conformément au type de règles que l'on croit que tout le monde devrait suivre (vu de derrière un voile d'ignorance).

Je vais maintenant revenir à la Section 2.2.2 pour clarifier une fois de plus la relation entre le droit et l'éthique au niveau de l'architecture fondamentale du droit. Ensuite, j'expliquerai comment cette architecture fondamentale est liée à l'utilisation du code informatique pour prendre des décisions juridiquement pertinentes.

11.2.1 Justice, certitude juridique et instrumentalité

Les objectifs de l'éthique peuvent se résumer à *agir de la bonne manière*, ce qui suppose d'avoir pris les bonnes décisions, tout en sachant que ces décisions peuvent être implicites dans nos actions, car une grande partie de nos connaissances éthiques sont tacites et difficiles à expliciter. L'étude de l'éthique espère expliquer comment nos actions peuvent être justifiées, en se référant,

par exemple, à des valeurs telles que la liberté, l'égalité et l'autonomie. Bien qu'une partie de la philosophie morale suppose qu'un consensus rationnel universel sur ce qui constitue une action juste est possible, le problème de l'éthique est précisément qu'un tel consensus n'existe pas (et qu'il n'y a pas non plus de consensus sur le fait que nous devrions essayer de raisonner vers un tel consensus rationnel universel). En fait, les démocraties constitutionnelles considèrent qu'il serait contraire à l'éthique d'imposer l'éthique d'une majorité aux minorités, et encore moins que l'éthique d'une minorité règne sur une majorité. Mais, comme certains nous le rappellent, cette position elle-même est précisément le type de règle universelle dont nous avons besoin dans un cadre méta-éthique.

Le droit ne peut pas se dissocier complètement de l'éthique. Au contraire, le droit et l'État de droit embrassent une méta-éthique pragmatique qui intègre un système de contrôles et d'équilibres institutionnels qui préservent la liberté de vivre selon sa propre éthique – mais dans les limites nécessaires pour garantir des protections équivalentes pour les autres. Cela signifie que le droit est concerné par un type spécifique de justice, étroitement aligné mais non équivalent à la certitude juridique. Comme nous l'avons vu dans la Section 2.2.2, le droit doit servir trois objectifs différents, qui se chevauchent en partie et sont souvent incompatibles : ceux de la justice, de la sécurité juridique et de l'instrumentalité.

La justice concerne la combinaison de la justice distributive et correctrice qui garantit que la loi :

1. traite des cas similaires de manière égale dans la mesure de leur similitude ; et
2. prévoit un juste dû en proportion de ce qui le suscite (par exemple, la commission d'un délit ou d'une infraction pénale ou la création d'une valeur ajoutée pour la société).

Bien que nous puissions convenir que les gens doivent être traités de manière égale, nous ne sommes pas toujours d'accord sur ce qui est considéré comme égal et nous devons également admettre que le fait de traiter tout le monde de manière égale ne correspond pas à notre sens de la justice, car cela ne peut être mérité.

Plus haut, dans la Section 11.1.2, nous avons discuté du principe de maximin de Rawls comme d'un moyen de combiner les deux types de justice, sous le titre *justice as fairness*. Même dans ce cas, nous devons prendre une série de décisions sur la manière dont cet équilibre peut ou doit être atteint, en laissant une marge de choix, d'interprétation et de contestation.

En fin de compte, des décisions politiques doivent être prises, par exemple sur ce qui constitue un marché équitable, en promulguant la législation correspondante, suivies de décisions juridiques qui appliquent ce que le législateur a promulgué. À partir de ce moment, le droit prendra le relais et veillera à ce que l'instrumentalité du droit en termes d'objectifs politiques fixés par le législateur soit réalisée dans le respect de la sécurité juridique (prévisibilité) et de la justice (égalité distributive et proportionnelle). Là encore, les tribunaux devront prendre des décisions sur ce qui est considéré comme égal et ce qui est mérité. Parfois, une décision peut être juste mais imprévisible, prévisible mais injuste, ou elle peut résister à l'instrumentalité pour sauvegarder la prévisibilité ou violer l'équité pour assurer l'instrumentalité.

Il n'y a aucun moyen de résoudre – à un niveau abstrait – la tension entre les trois objectifs du droit : la justice, la certitude juridique et l'instrumentalité. Ce qui importe, c'est que toute décision juridique doit pouvoir être justifiée comme s'efforçant de servir ces trois objectifs, entretenant ainsi la tension entre eux au lieu de la résoudre. Cette *demande* peut être qualifiée de méta-éthique qui permet essentiellement aux gens de développer leurs propres compétences morales. Par exemple, si les valeurs éthiques telles que la vie privée et l'équité sont laissées au *marché*, les entreprises qui construisent leurs systèmes conformément à ces valeurs risquent d'être évincées du marché (parce qu'elles doivent supporter des coûts que les autres entreprises externalisent). En revanche, si la loi fixe un seuil sur le marché en exigeant et en obligeant les

entreprises à intégrer ces valeurs dans leurs systèmes, les entreprises peuvent se *permettre* d'agir de manière éthique.

11.2.2 Droit, code et État de droit

Dans la sous-section précédente, nous avons vu que le rapport entre le droit et l'éthique peut être retracé dans le fait que l'éthique informe une règle de droit qui :

1. exige que l'instrumentalisation du droit soit un moyen d'atteindre les objectifs fixés par le législateur,
2. est contrainte à la fois par la prévisibilité et la stabilité du droit et par son application égale (sécurité juridique),
3. repose sur l'idée que les gouvernements doivent faire preuve d'un respect et d'une préoccupation égaux pour tous les citoyens (justice).

Bien que la justice soit une valeur éthique, son rôle dans le droit est limité par l'instrumentalité de la loi (une orientation vers des objectifs définis par le législateur ou, dans le cas d'un contrat, par les parties contractantes) et par les exigences de la sécurité juridique (la *positivité* de la loi, destinée à garantir à la fois l'applicabilité de la loi et l'intégrité de la loi dans son ensemble).

Cela confirme que le droit est à la fois plus et moins que l'éthique. Cela soulève la question de la relation entre le droit et la règle de droit, d'une part, et le code, d'autre part, une question déjà abordée au Chapitre 10, notamment à la Section 10.3 où nous avons distingué le *légal par conception* de la *protection juridique dès la conception*. Ici, nous examinons plus largement les systèmes de décision algorithmiques, que ce soit dans le secteur privé ou public, sans nous concentrer sur les systèmes censés exécuter des normes juridiques.

Que se passe-t-il si un code informatique est utilisé pour trancher des affaires individuelles pour des raisons d'efficacité, de rapidité et d'échelle? Comment cela se rapporte-t-il au droit et à l'État de droit, ainsi qu'à l'éthique?

1. Premièrement, comme nous l'avons vu plus haut, la prise de décision algorithmique modifie la relation entre le droit et l'éthique dans la mesure où les choix éthiques peuvent acquérir la force de la technologie, devenant ainsi un concurrent du droit en termes d'applicabilité.
2. Deuxièmement, bien que les deux types d'applicabilité aient une nature fondamentalement différente, ils affectent tous deux les personnes soumises à leurs décisions, réduisant potentiellement l'espace de choix éthique.

La mise en application technologique réduit l'espace du choix éthique, car le choix éthique suppose la liberté d'agir autrement et la possibilité de développer des positions éthiques alternatives. L'espace du choix éthique peut être occupé soit par des obligations légales, soit par le code informatique. Dans la mesure où les normes juridiques imposent des choix éthiques particuliers, le comportement pertinent est transformé en conformité juridique. On peut dire la même chose du code informatique qui impose des choix éthiques à des personnes ou à des entreprises, puisque dans ce cas, les choix ne sont plus faits par ces personnes ou ces entreprises.

La différence entre le droit et le code informatique, cependant, est qu'une norme juridique peut en principe être désobéie, alors que le code qui parvient à limiter les options comportementales des personnes ou des entreprises peut ne laisser aucune place à la désobéissance. Il s'agit là d'une différence importante entre le droit et la technologie : le droit laisse une marge de manœuvre pour les choix éthiques même lorsqu'il impose ses normes (pensez à la désobéissance civile), alors que le code informatique peut ne laisser aucune marge de manœuvre. Pensez à un algorithme qui permet automatiquement aux publicitaires de cibler les hommes blancs pour des emplois mieux rémunérés, excluant ainsi les femmes et les personnes de couleur d'être informées sur ces

emplois. Le choix éthique qui est en jeu ici est le choix, par exemple, d'un propriétaire de site web de refuser ce type de ciblage injuste. Étant donné que l'algorithme est formé pour augmenter les recettes publicitaires, il peut être difficile, voire impossible, d'éliminer ce type de résultats algorithmiques, dans la mesure où l'algorithme *constate* que ce ciblage excluant augmente les recettes publicitaires.

Mais nous pouvons aller un peu plus loin : et si nous pouvions développer un méta-algorithme qui impose des contraintes à ce type d'algorithmes, garantissant qu'ils seront nécessairement équitables. Et si nous pouvions développer un *algorithme éthique*, basé sur la formalisation d'un concept spécifique d'équité ? Bien qu'il s'agisse d'un moyen merveilleux d'atteindre un type spécifique d'équité, cela réduira ou transformera l'espace de l'action éthique. Peut-être, dans ce cas, l'espace d'action éthique est-il limité à ceux qui comprennent le code et/ou à ceux qui peuvent décider de l'emploi et du développement du code.

La réduction de l'espace de choix éthique se traduira nécessairement par une perte d'espace pour exercer son sens moral. Comme l'a fait remarquer Roger Brownsword, il en va de même pour la loi. Si nous développons des algorithmes qui sont *légaux par conception* ou *éthiques par conception*, nous réduisons l'espace du droit ou de l'éthique en faveur de la *gestion technologique*. Cela peut finalement avoir un impact sur notre compréhension de l'éthique et du droit, notamment lorsque certains affirment que la gestion technologique de nos architectures de choix est un meilleur moyen de parvenir à une *bonne* société que le droit ou l'éthique.

11.3 L'interaction entre le droit, le code et l'éthique

En explorant les distinctions entre le droit, le code et l'éthique, ainsi que leur relation, nous avons préparé le terrain pour une étude de leur interaction. À un niveau conceptuel, nous le ferons en discutant des approches *dès la conception (by design)* du droit et de l'éthique et, à un niveau plus concret, nous le ferons en déterminant comment le droit et l'éthique interagissent avec le code dans le contexte de l'équité algorithmique.

11.3.1 Approches dès la conception en droit et en éthique

On a vu plus haut que la certitude juridique, l'une des valeurs fondamentales du droit, ne consiste pas à fixer une fois pour toutes le sens des normes juridiques. La certitude juridique vise plutôt l'équilibre délicat entre des attentes stables et la capacité de les reconfigurer ou de les contester.

Cela implique que la certitude juridique résiste à la formalisation, car cela figerait le sens des normes juridiques, réduirait leur nature adaptative et diminuerait leur contestabilité (seuls ceux qui comprennent le code peuvent le contester). Il en va de même pour l'éthique, qui peut être encore plus adaptative, car elle n'est pas contrainte par l'exigence de certitude et de fermeté juridiques. Le code, cependant, implique une formalisation, il ne peut exister sans un acte de traduction qui lève l'ambiguïté et définit en termes précis et de plus en plus machinaux le problème qui est résolu (du code source au langage de programmation ou au code objet en passant par le compilateur). La formalisation supprime l'élasticité et l'adaptabilité qui sont inhérentes au langage humain.

Rappelons la définition pragmatiste de la signification (Section 11.1.4) :

Considérez quels effets, qui pourraient avoir des implications pratiques, nous concevons que l'objet de notre conception ait. Ensuite, notre conception de ces effets est la totalité de notre conception de l'objet.

Cette définition est particulièrement adaptée à la compréhension de ce que *fait* le langage, car elle souligne la nature anticipative de l'usage du langage et du sens qu'il génère. Dans la Section 2.1.2, nous avons brièvement évoqué la théorie de l'acte de langage pour expliquer le caractère performatif de la loi ; si des conditions juridiques spécifiques sont remplies, la loi attribue des effets juridiques spécifiques. Par exemple, la signification du terme *meurtre* est définie par une combinaison de conditions juridiques qui génèrent l'effet juridique d'une action *comptant* comme un meurtre. Cela signifie que quiconque a accompli cette action devient punissable.

Le code informatique est capable d'opérations similaires, bien qu'il ne s'agisse pas ici d'*effets*, qui *pourraient avoir des conséquences pratiques*, mais d'un ensemble préconçu et déterminé d'effets (même si la complexité est telle que nous ne pouvons pas tous les prévoir en raison de notre rationalité limitée).

Le code ne produit pas de sens mais de *simples* effets, au niveau de ses circuits intégrés, de ses opérations logiques, de son débit et de ses résultats décisionnels (y compris les effets dans le monde réel, par exemple dans un internet des objets (IoT), ou lors de l'utilisation de la fintech, des moteurs de recherche ou des réseaux sociaux). Nombre de ces effets peuvent être non seulement imprévus, mais aussi involontaires, en particulier lorsque les résultats sont diffusés dans le monde réel. C'est là que les approches dès la conception en droit et en éthique deviennent intéressantes, en partie parce que ces limitations peuvent également s'appliquer aux approches dès la conception qui reposent sur l'adaptation du code comme solution.

Le respect de la vie privée dès la conception est depuis longtemps un exemple d'approche dès la conception en éthique, car il n'y avait aucune obligation légale d'intégrer le respect de la vie privée au niveau de la conception. La protection des données dès la conception (DPbD) est un exemple d'approche dès la conception en droit, du moins dans le cadre du règlement général sur la protection des données (RGPD), car depuis 2018, il s'agit d'une obligation légale.

Cela a des implications à la fois pour la vie privée et pour d'autres droits fondamentaux, par exemple le droit à la non-discrimination :

1. Premièrement, on peut vouloir contrer les problèmes de vie privée existants en les définissant d'une manière qui se prête à la formalisation, puis en trouvant un moyen de résoudre les problèmes tels qu'ils sont définis. Par exemple, le k-anonymat et la confidentialité différentielle (*differential privacy*) définissent la confidentialité en termes de dissimulation des données et/ou de non-identification des données dans les données globales ou dans les modèles qui en sont déduits. Sur la base de cette définition, on peut développer des mesures qui permettent de prouver mathématiquement dans quelle mesure la vie privée est protégée. On pourrait, par exemple, affirmer que la confidentialité différentielle protège mieux la vie privée que le k-anonymat, tout en conservant les données agrégées et les informations déduites qui servent son objectif.
2. Des tentatives similaires pour contrer les implications indésirables des systèmes de décision algorithmiques sont faites en ce qui concerne l'équité. Le problème est défini d'une manière qui permet sa formalisation et est ensuite résolu - à ce niveau - par rapport à cette définition spécifiée de l'(in)équité. Dans la mesure où le traitement inéquitable est illégal, l'exigence légale du DPbD peut nécessiter que les systèmes de décision algorithmiques soient conçus de manière à atténuer l'iniquité, car le DPbD ne se limite pas à la vie privée. Comme nous l'avons vu à la Section 5.5.2 ¶9, l'Article 25 du RGPD définit la DPbD en fonction des *risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques*. Le droit fondamental à la non-discrimination (par exemple, l'Article 21 de la Charte des droits fondamentaux de l'Union européenne (CDFEU)) exige donc une approche dès la conception en droit concernant un manque d'équité qui viole le droit à la non-discrimination.

Toutefois, ce droit est limité à la discrimination fondée sur un type spécifique de motifs (l'Article 21 du CFREU parle de tout motif tel que *le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, le handicap, l'âge ou l'orientation sexuelle*), et peut être justifié si des conditions spécifiques s'appliquent (par exemple, réserver le paiement d'une pension aux personnes ayant dépassé un certain âge, réserver le congé de maternité aux femmes et réserver la discrimination positive à une minorité défavorisée).

Dans la mesure où les systèmes de prise de décision algorithmique entraînent des violations de l'équité qui ne sont pas illégales au sens de la DPbD, l'obligation ne s'applique pas. Dans ce cas, une approche de conception pourrait être basée sur des considérations éthiques. Dans la sous-section suivante, j'aborderai l'informatique équitable en tant qu'exemple d'équité par la conception qui peut en partie être justifiée par l'obligation légale de DPbD et en partie être basée sur une approche dès la conception des questions éthiques liées à l'équité dans l'informatique.

11.3.2 Équité dès la conception et paradigmes de l'*informatique équitable*

Avant d'aborder le thème de *l'équité dès la conception*, je dois aborder deux questions préliminaires.

1. Tout d'abord, il est crucial de reconnaître que la formalisation d'un problème peut - involontairement - aboutir à une mauvaise représentation du problème. Il se peut que certaines formes d'injustice puissent être détectées, alors que d'autres restent insaisissables. La tentation peut être de s'attaquer à ce qui peut être défini et résolu, **alors que le problème qui dérange vraiment les gens résiste au type de généralisation qu'implique la formalisation**. Il s'agit d'une question à laquelle il faut faire face sans détour, sous peine de perdre du temps, de l'argent et des efforts dans une sorte de solutionnisme technologique qui ne s'appuie pas sur les problèmes du monde réel. Notre connaissance tacite de ce qui est injuste peut être difficile à retrouver dans des expressions plus explicites qui peuvent être à la fois trop et pas assez inclusives ; la connaissance tacite peut être trop complexe pour être rendue en termes propositionnels sans perdre plusieurs dimensions qui font la différence. Cela peut même être dû au fait que nous n'avons peut-être pas de mots pour décrire notre perception de l'injustice, ce qui donne lieu à ce que Miranda Fricker a appelé *l'injustice herméneutique*.³ Ceci est lié au fait que les problèmes d'équité nécessitent un cadrage, et que des positions éthiques différentes donneront lieu à des cadrages différents. Ainsi, alors que certains peuvent trouver la discrimination par les prix injuste pour ceux qui paient un prix plus élevé, d'autres soutiendront qu'elle est en fait bénéfique pour ceux qui ont moins à dépenser car elle peut faire baisser leur prix. En réalité, le prix plus élevé peut toutefois être payé par ceux qui ont moins de moyens. Par exemple, l'assurance maladie peut être plus chère dans les quartiers où les résidents à faibles revenus sont plus nombreux, car statistiquement ils ont plus de problèmes de santé. Certains trouveront cela justifié, du point de vue de la compagnie d'assurance, d'autres trouveront cela injustifiable, sur la base d'un voile d'ignorance rawlsien.
2. La deuxième question à laquelle il faut faire face est que les solutions techniques peuvent être utilisées pour légitimer des systèmes de décision algorithmiques qui sont justes d'une manière particulière, mais qui sont par ailleurs massivement invasifs et peut-être injustes

3. *L'injustice herméneutique désigne l'impossibilité pour un groupe social de bénéficier des ressources intermédiaires nécessaires à l'acquisition de privilèges considérés comme normaux.* nous informe Wikipédia.

de nombreuses autres manières. Comme l'ont fait valoir Powles et Nissenbaum, l'apport de ce type de solution peut détourner l'attention de la question préliminaire de savoir si nous voulons réellement remplacer le jugement humain par une prise de décision informatique, dans des domaines tels que la médecine, la comptabilité, le droit ou l'éducation. Ces questions ne doivent pas être posées à un haut niveau d'abstraction, mais abordées dans des situations concrètes, en tenant compte de l'impact que l'introduction de la prise de décision algorithmique peut avoir sur notre écosystème d'information, sur la répartition des risques et sur les capacités des êtres humains qui en subiront ou en apprécieront les conséquences.

Après avoir attiré l'attention sur ces questions préliminaires, je pense qu'il est néanmoins essentiel d'investir dans la recherche et l'exploration de *l'équité dès la conception*. La Section 11.1.2 a fourni une analyse de la discrimination dans les décisions de libération conditionnelle basées sur des logiciels propriétaires, démontrant que différentes personnes et organisations formulent différemment la question de l'équité, aboutissant à une impasse entre ceux qui revendiquent l'objectivité statistique et ceux qui soutiennent que les personnes individuelles sont en fait injustement discriminées, en raison de profils agrégés qui ne s'appliquent pas à elles (le fait que 87% des personnes noires récidivent ne signifie pas que chaque personne noire a 87% de chances de récidiver). Nous voyons ici la différence cruciale entre (1) les notions éthiques d'injustice qui sont par définition contestables; (2) les notions juridiques d'injustice qui sont raisonnablement circonscrites mais restent contestables sur le plan juridique; et (3) les notions computationnelles d'injustice qui sont nécessairement désambiguïsées pour répondre au besoin de formalisation.

Ce que je veux dire, c'est aussi que :

1. les notions éthiques d'injustice doivent être contestables, car les notions incontestables d'injustice appartiennent au domaine de l'idéologie;
2. les notions juridiques d'injustice doivent être suffisamment délimitées pour permettre à la fois la prévisibilité et la contestabilité; et
3. les notions informatiques d'injustice doivent être formalisables, car on ne peut pas former un algorithme sans lui fournir une tâche lisible par la machine et une mesure de performance.

Notez que je suis passé de la question de l'équité à celle de l'injustice, car dans un contexte de conception, il peut être un peu prétentieux de prétendre que l'on peut concevoir *l'équité*, alors qu'un effort soutenu et systématique de conception contre l'injustice nous permettra également de rester attentifs aux nouveaux types d'injustice. La logique binaire nous fait défaut ici; le fait qu'une chose ne soit pas injuste (dans un certain sens du terme) n'implique pas qu'elle soit juste (dans tous les sens du terme). L'équité est ce que Gallie appellerait un concept essentiellement contesté qui requiert vigilance et acuité plutôt que fermeture.

Le but de cet exercice est de développer un respect mutuel pour la différence entre les notions éthiques, juridiques et informatiques d'équité et d'iniquité. Pour démontrer ce que j'entends par ce respect mutuel, je vais esquisser trois approches dès la conception de l'utilisation du logiciel COMPAS : une approche éthique, une approche juridique et une approche informatique. Avant cela, j'explique le contexte des décisions soutenues par le COMPAS.

L'affaire COMPAS

Lorsqu'ils décident de la détention ou de la libération d'un accusé ou d'un délinquant criminel, les tribunaux des États-Unis évaluent la probabilité de récidive. Cela peut concerner les décisions avant le procès (probation), les décisions lors du procès (condamnation) et les décisions après le procès concernant la libération anticipée (libération conditionnelle). Ces décisions sont dans une certaine mesure discrétionnaires, ce qui signifie que le tribunal n'est pas lié par des conditions légales strictes (cela peut varier d'un État à l'autre, et des règles plus strictes peuvent s'appliquer

à la détermination de la peine). Une forte probabilité de récidive est l'un des facteurs qui pèsent dans la décision de détenir ou de libérer l'accusé (qui attend son procès), ou le délinquant (qui a été condamné et attend sa sentence ou a été détenu mais peut bénéficier d'une libération anticipée). L'idée est que la détention empêche la commission d'autres infractions, de sorte que l'objectif de cette évaluation particulière est de protéger les victimes potentielles (ce qui est souvent identifié comme la protection du *public* ou de la *communauté*).

Les tribunaux évaluent le risque de récidive sur la base de l'audition du défendeur ou du délinquant, ainsi toute une série d'informations supplémentaires sont prises en compte et pas seulement la probabilité de récidive. Cela semble se perdre dans la discussion mais il faut bien préciser qu'il est crucial de se rappeler que la récidive ne devrait pas être le seul critère pour décider de la détention ou de la libération.

L'évaluation de la probabilité de récidive est effectuée par la personne compétente pour décider de la détention ou de la libération. Les personnes compétentes (souvent les tribunaux, soutenus par les commissions de libération conditionnelle, les agents de probation, etc) peuvent faire appel à leur bon sens et à leur intuition ainsi qu'aux rapports empiriques de conseillers expérimentés ou d'experts pour parvenir à une conclusion. Dans la lignée des appels à des décisions de condamnation *fondées sur des preuves* (*evidence based*), divers types d'outils logiciels basés sur des données ont été développés, qui sont généralement censés évaluer le risque pertinent de manière plus précise ou plus rapide. Certains de ces logiciels ont été développés par des tribunaux fédéraux ou d'État, mais d'autres s'appuient sur des logiciels propriétaires de fournisseurs commerciaux. L'un de ces fournisseurs, qui détient une part de marché importante, est Northpointe (aujourd'hui Equivant), qui a mis au point le système COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*). Le score de risque de COMPAS est basé sur six caractéristiques, après que son algorithme d'apprentissage ait été entraîné sur des ensembles de données disponibles avec un espace de 137 caractéristiques. L'algorithme d'apprentissage a trouvé ces six caractéristiques hautement indicatives de la récidive. Le score de risque est basé sur un entretien et/ou un questionnaire rempli par le défendeur ou le délinquant, et sur son dossier pénal.

En raison de l'impact majeur de l'utilisation de logiciels propriétaires sur les décisions de détention, Julia Angwin (une journaliste d'investigation travaillant pour Propublica), a décidé de tester l'exactitude des prédictions et est arrivée aux conclusions suivantes (basées sur ses propres recherches scientifiques fondées sur des données).

On prédisait souvent aux accusés noirs un risque de récidive plus élevé que celui qu'ils couraient en réalité. Notre analyse a révélé que les prévenus noirs qui n'ont pas récidivé sur une période de deux ans étaient presque deux fois plus susceptibles d'être classés à tort comme présentant un risque plus élevé que leurs homologues blancs.

Tandis que les prévenus blancs étaient souvent considérés comme présentant moins de risques qu'ils ne l'étaient.

Cela a donné lieu à un débat houleux, où Northpointe a accusé Angwin d'incompétence méthodologique, affirmant que ses propres prédictions étaient le résultat d'une application objective des statistiques. Cela a donné lieu à une série d'articles scientifiques des deux côtés du débat et à un certain nombre d'initiatives du côté du droit, des sciences sociales et de l'informatique pour contrer ce que l'on a appelé *les préjugés dans l'apprentissage automatique*, ce qui a finalement donné lieu à une nouvelle conférence ACM consacrée à l'informatique *équitable, responsable et transparente* (FAccT).⁴

4. <https://facctconference.org/index.html>

Une approche computationnelle de l'équité dès la conception pour les décisions des tribunaux en matière de détention et de libération

Trois questions se posent ici :

- la question de savoir si l'algorithme de sortie du COMPAS est effectivement précis, et ce que cela signifie d'un point de vue computationnel ;
- la question de savoir si l'algorithme est injuste, et si oui, ce que cela signifie en termes de formalisation computationnelle ;
- la question de savoir si les réponses aux questions précédentes sont objectives, et si oui dans quel sens.

L'argument principal de Julia Angwin est que, bien que la précision soit la même pour les accusés noirs et blancs, l'erreur dans le cas des accusés noirs concerne les **faux positifs** (on leur attribue un score de risque plus élevé par rapport à leur récidive réelle), alors que dans le cas des accusés blancs l'erreur concerne les **faux négatifs** (on leur attribue un score de risque plus faible par rapport à leur récidive réelle). Northpointe/Equivant a fait valoir que cette situation est inévitable car les noirs (dans leur ensemble) récidivent plus souvent. L'utilisation correcte des statistiques - selon Northpointe/Equivant - aboutit à un résultat disparate indésirable mais inévitable.

On pourrait rétorquer que cela dépend de la façon dont vous formez votre algorithme d'apprentissage. Si la tâche lisible par la machine consiste à s'assurer que tous les accusés qui ne récidivent pas auront le même taux d'erreur pour les faux positifs et les faux négatifs dans le cas des accusés noirs et blancs, alors l'algorithme d'apprentissage apprendra exactement cela.

La question sous-jacente est de savoir s'il est injuste de juger une personne noire en se basant sur le fait que d'autres personnes noires (d'après les données) récidivent plus souvent que les personnes blanches, ou s'il est injuste qu'une personne blanche qui va récidiver bénéficie du fait qu'en général (d'après les données) les personnes blanches récidivent moins souvent que les personnes noires. Dans ce cas, on ne peut pas avoir le beurre et l'argent du beurre, il faudra faire un choix entre ces deux types d'injustice.

Du point de vue de l'informatique, les deux peuvent être formalisés et rendus opérationnels. Étant donné qu'en tant que société, nous pouvons ne pas être d'accord sur le choix à faire ici, il est difficile d'exiger une *fermeture* des informaticiens.

Ce qu'ils peuvent faire, c'est

1. expliquer les implications des choix de conception et leurs compromis ; et
2. développer encore d'autres moyens d'entraîner un algorithme d'apprentissage de manière à réduire des types similaires d'injustice.

À l'heure actuelle, les informaticiens ont imaginé des dizaines de manières différentes de formaliser l'équité. Cela démontre que l'utilisation de ce type de logiciel peut sembler rapide et efficace, alors qu'en fait, elle peut créer plus de problèmes qu'elle n'en résout.

Une approche éthique de l'équité dès la conception dans les décisions judiciaires de détention/libération

À la lecture des travaux de recherche présentés par Julia Angwin, Northpointe/Equivant et d'un certain nombre d'autres auteurs, on ne peut que conclure que la simple *correction* des algorithmes COMPAS ne suffira pas. Lors de tutoriels à différentes conférences en informatique, le professeur Narayanan a présenté plus de vingt définitions formalisables différentes de l'équité, et dans la bibliographie ci-dessous, je fais référence à la version préliminaire d'un livre qu'il co-écrit avec Barocas et Hardt sur *Équité et apprentissage automatique. Limites et opportunités*. Il est

clair que plus les arguments des informaticiens en faveur de divers types d'équité sont sophistiqués, plus nous devons nous asseoir et déterminer quel type d'équité nous devons appliquer dans quelles circonstances. Cela ne concerne pas seulement le logiciel COMPAS, mais l'emploi de nombreux autres types de systèmes d'aide à la décision, tels que la police prédictive, la détection des fraudes fiscales et sociales, l'éligibilité aux soins (pensez aux enfants potentiellement maltraités ou aux personnes âgées), l'accès à l'éducation, au marché du travail et aux assurances.

Le cas de COMPAS illustre donc bien la complexité des décisions que doit prendre le tribunal et l'interaction entre les différents facteurs qui entrent en jeu du côté du défendeur ou du délinquant. Dans l'affaire Loomis (condamné à 6 ans de prison suite aux recommandations de COMPAS), le défendeur avait accepté un *plea bargain*, ce qui signifie que - même s'il n'a pas avoué - il était prêt à accepter une peine. Il s'agit d'une pratique courante aux États-Unis qui offre au système judiciaire un certain allègement des exigences procédurales, en échange d'une réduction de la peine ou de l'amende pour le défendeur. L'accord est conclu entre le procureur et le défendeur, ce qui signifie que le tribunal n'est pas lié par cet accord, bien qu'il en tienne le plus souvent compte (certains l'appellent *commercer avec la justice* (*trading with justice*)). Il se peut qu'une grande partie de l'injustice commence ici, et même beaucoup plus tôt, lorsque les Noirs américains ont beaucoup plus de chances d'être désavantagés à de nombreux égards et d'être traités d'une manière qui ne reflète pas l'idée qu'un gouvernement devrait traiter chaque citoyen avec *la même attention et le même respect*.

Définir l'injustice d'une manière qui tienne compte à la fois des préjugés, du résultat d'un traitement injuste antérieur et d'autres causes profondes de récidive n'est pas une tâche facile, que l'évaluation de la probabilité de récidive soit effectuée par un humain ou un système informatique. Dans les deux cas, le problème réside dans le passage d'une évaluation au niveau global à une évaluation au niveau individuel (en psychologie, on parle de stéréotype), et la recherche médicale nous apprend que ce qui est raisonnable au niveau épidémiologique peut ne pas l'être au niveau individuel.

Rappelons-nous que nous prenons chaque jour des décisions de ce type, fondées sur divers types de généralisation. Nous ne pouvons échapper au dilemme que posent ces décisions.

C'est ici, je crois, que la contribution de l'éthique peut être déterminante. Cela ne fonctionnera que si nous nous écartons des analyses coûts-avantages utilitaristes non informées qui mettent en balance, par exemple, des biens publics tels que la vie privée comme s'il s'agissait de simples intérêts privés, avec les intérêts privés de l'État sous le titre de sécurité publique, en restant souvent bloqués dans un acte-utilitarisme simpliste. De même, nous ne devons pas tomber dans le piège qui consiste à romancer la singularité des défendeurs individuels, en prétendant qu'ils ne devraient jamais être comparés aux autres. Comme j'ai essayé de l'expliquer dans la Section 11.1, l'éthique est profondément préoccupée par la nécessité d'articuler des règles qui ne sont pas informées par des intérêts particuliers, tant dans le cadre de l'utilitarisme des règles que dans celui du raisonnement déontologique. Une interprétation naïve de la règle qui maximise l'utilité (globale ou moyenne) pourrait s'aligner sur la position adoptée par Northpointe/Equivant, dans la mesure où le coût des faux positifs des accusés noirs qui ne récidiveraient pas devrait être inférieur au coût des faux négatifs des accusés noirs qui récidivent. Cette position est naïve car la répartition du coût n'est pas prise en compte (quels coûts sont pondérés par rapport à quels bénéfices ?), et aussi parce que cette approche renforce les préjugés existants et peut entraîner un coût énorme à terme, lorsque les communautés noires sont confrontées à une spirale descendante d'irrespect. Nous pourrions plutôt examiner si le principe de maximin de Rawls pourrait être appliqué ici, en suggérant que les algorithmes équitables devraient au moins empêcher la perte d'utilité pour les moins favorisés, ou développer un seuil dans l'algorithme d'apprentissage qui exclut de s'en prendre à ceux qui souffrent déjà d'un désavantage systémique.

Mais peut-être que le rôle de l'éthique n'est pas seulement de réaliser quelque chose comme

une *contre-optimisation*. Peut-être que l'éthique de la vertu et l'éthique pragmatiste peuvent souligner la nécessité du jugement humain, en montrant qu'en fin de compte, cela peut être moins compliqué et moins dépendant de calculs invisibles, tout en pouvant être signalé de manière plus transparente.

Une approche juridique de *l'équité dès la conception* pour les décisions judiciaires de détention/libération

Comme indiqué plus haut, l'auteur pense que l'obligation légale d'intégrer le DPbD à la lumière des risques pour les droits et libertés des personnes physiques n'est pas limitée à la protection de la vie privée dès la conception (et n'est même pas limitée aux personnes concernées). Au contraire, l'articulation dans le RGPD souligne la nécessité de prévoir les implications pour d'autres droits fondamentaux, comme l'exige le DPIA. Cela signifie que nous avons déjà une obligation légale d'au moins remédier à *l'injustice dès la conception*.

La décision d'un tribunal de détenir ou de libérer un défendeur ou un délinquant est le plus souvent discrétionnaire ; elle repose sur une marge d'appréciation plus large que d'autres décisions, notamment la condamnation elle-même (en raison de la présomption d'innocence, un tribunal ne peut pas condamner une personne s'il existe un doute raisonnable quant à la culpabilité du défendeur). Dans le cadre de l'État de droit, cependant, le pouvoir discrétionnaire n'est pas synonyme de décision arbitraire. Un tribunal doit prendre en compte un certain nombre de facteurs avant de prendre une décision, et cette prise en compte ne peut être confiée à une machine. La raison en est qu'une telle externalisation peut, d'une part, permettre l'échelonnement et la rationalisation des décisions, mais, d'autre part, elle peut déqualifier le juge dans la mesure où il n'est plus tenu d'examiner lui-même ces facteurs, face à face avec le défendeur ou le délinquant. Cela peut diminuer la sagesse pratique du tribunal, ce qui augmente le risque que les tribunaux se fient sans critique aux calculs d'un logiciel qu'ils ne peuvent pas évaluer.

Cela signifie qu'une approche de *l'équité par la conception* en droit nécessite deux mises en garde :

- Affirmer qu'un algorithme peut *rendre* les décisions équitables revient à exagérer ce que les algorithmes peuvent faire dans ce domaine ; pour cette raison, il est préférable de développer une approche de *lutte contre l'injustice par la conception*.
- Ces outils ne devraient pas être utilisés pour remplacer le jugement juridique mais pour le remettre en question, renforçant ainsi la sagesse pratique du tribunal au lieu de la diminuer ; pour cette raison, les avocats et les informaticiens devraient s'asseoir ensemble pour écrire un code qui permette aux tribunaux de rester agiles et précis.

11.4 Fermeture : la force de la technologie et la force du droit

Dans ce chapitre, nous avons fait valoir que si l'éthique s'aligne sur la force de la technologie, l'État de droit est confronté à un dangereux concurrent dans notre espace normatif. Le fait que l'éthique ne dispose pas des freins et contrepoids de la règle de droit signifie que nous ne devrions pas être surdéterminés par les *technologies éthiques* (quoi que cela puisse signifier).

Cependant, nous pouvons également imaginer l'utilisation de moyens technologiques pour limiter l'injustice de la prise de décision algorithmique, soutenant ainsi l'égalité de préoccupation et de respect qu'un gouvernement doit à chacun de ses citoyens. Cela ne fonctionnera que si les systèmes algorithmiques d'aide à la décision remettent en question l'acuité du jugement humain au lieu de le remplacer.