

Table des matières

SOMMAIRE	V
INTRODUCTION	1
1.1 Le contexte technologique et économique des objets connectés	2
1.2 Un panorama juridique en mutation	2
1.3 Les implications spécifiques de l'intelligence artificielle dans les objets connectés	3
1.4 Les objectifs de l'ouvrage	3

Chapitre 1 Les aspects techniques des objets connectés

1. LES PRINCIPES DE FONCTIONNEMENT DES OBJETS CONNECTÉS	6
1.1 Les types de déploiement et les cas d'usage de l'IoT	7
1.1.1 Les usages domestiques	7
1.1.2 Les usages industriels	7
1.1.3 Les usages urbains	8
1.1.4 Les usages médicaux	8
1.2 L'environnement de développement des objets connectés	8
1.3 Les flux de données dans un système IoT	10
1.4 L'architecture de base des objets connectés	11
2. LES DIFFÉRENTES TECHNOLOGIES COMPOSANT LES OBJETS CONNECTÉS	15
2.1 Les capteurs embarqués	15
2.2 Les unités de traitements	16
2.3 Les dispositifs de connectivité	16
2.3.1 Les dispositifs en cas de connexions filaires	17
2.3.2 Les dispositifs en cas de connexions sans fil	19
2.4 Les dispositifs de stockage et de gestion de l'énergie	21
2.4.1 Les dispositifs de stockage de l'énergie	21
2.4.2 Les dispositifs de gestion de l'énergie	21
2.4.3 Bilan	22
2.4.4 Conclusion	22

3.	LES PROTOCOLES DE COMMUNICATION ET L'INTEROPÉRABILITÉ DES OBJETS CONNECTÉS	22
3.1	La distinction entre réseau local (LAN) et réseau étendu (WAN)	23
3.2	Les protocoles de communication.	24
3.2.1	Les protocoles sans fil	24
3.2.2	Les protocoles filaires	27
3.3	L'interopérabilité entre les objets connectés.	29
3.4	Les défis de l'intégration multiplateforme et multi-protocoles	30
4.	LA SÉCURITÉ ENCADRANT LES OBJETS CONNECTÉS	31
4.1	La sécurité des objets connectés	32
4.1.1	Une architecture conçue pour la sécurité	32
4.1.2	L'obsolescence, un risque silencieux mais réel	33
4.1.3	Les interfaces de communication.	33
4.1.4	L'authentification des objets connectés	33
4.2	La sécurité des données	34
4.3	La sécurité des systèmes d'IA inclus dans les objets connectés	35
4.3.1	Les attaques visant les données d'entraînement.	35
4.3.2	Les attaques visant les prédictions du système d'IA	36
4.3.3	Les attaques de vol de modèles d'IA	36
4.3.4	L'exemple des voitures autonomes.	37
4.4	Les normes et standards	38
4.4.1	Les organismes élaborateurs	38
4.4.2	Les normes et standards notables	41

Chapitre 2

Les enjeux en droit des communications électroniques

1.	LES RÉGULATEURS DE L'INTERNET DES OBJETS.	54
1.1	Les régulateurs publics internationaux	54
1.1.1	L'Union internationale des télécommunications (UIT).	54
1.1.2	Les instances européennes	56
1.1.3	L'Orece	60
1.2	Les régulateurs publics nationaux	61
1.2.1	L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse	62
1.2.2	Le ministre chargé des communications électroniques	65

1.2.3	L'Agence nationale des fréquences (ANFr)	65
1.2.4	L'Autorité de la concurrence	66
1.3	Les autres instances : Fratel.	66
2.	LES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES	67
2.1	Le cadre légal général applicable aux réseaux et aux services de communications électroniques.	67
2.2	Les réseaux et services issus de la directive 2018/1972.	72
2.3	La pratique de l'Arcep	72
2.4	La disparition des formalités.	73
3.	LE RÉGIME DES FRÉQUENCES RADIOÉLECTRIQUES	74
3.1	L'Arcep, autorité affectataire	75
3.2	Les conditions générales de la délivrance de l'autorisation	76
3.2.1	Le pouvoir d'attribution	76
3.2.2	l'encadrement des conditions d'utilisation	76
3.2.3	La procédure d'attribution	77
3.3	Le marché secondaire des fréquences	78
3.3.1	La sous-attribution des fréquences	78
3.3.2	Les modalités de cession des fréquences.	78
3.4	Fréquences et objets connectés.	79
3.4.1	La remise à plat de la gestion du spectre	79
3.4.2	Le partage dynamique des fréquences	81
3.4.3	Les fréquences à usage libre.	82
4.	LE RÉGIME DES RESSOURCES EN NUMÉROTATION.	83
4.1	Les textes européens	83
4.2	La réglementation française	84
4.2.1	Le CPCE	84
4.2.2	Un plan de numérotation adaptatif.	85
4.2.3	Un plan de numérotation intégrant la croissance des objets connectés.	88
4.2.4	Modification des conditions d'utilisation des numéros mobiles de longueur étendue	89
4.2.5	Conditions d'usage des numéros mobiles de longueur étendue.	90

Chapitre 3

La commercialisation des objets connectés

1. LE CADRE RÉGLEMENTAIRE ET NORMATIF APPLICABLE À LA MISE SUR LE MARCHÉ.	92
1.1 La directive RoHS	92
1.1.1 Principes.	92
1.1.2 Objectifs.	92
1.1.3 Portée	93
1.1.4 Application aux objets connectés.	93
1.2 Le règlement REACH.	93
1.2.1 Principes.	93
1.2.2 Portée	94
1.2.3 Champ d'application.	94
1.2.4 Mise en œuvre.	94
1.3 Le Code des Postes et des Communications Électroniques.	95
1.3.1 Principes.	95
1.3.2 Champ d'application.	95
1.3.3 Procédure.	95
1.3.4 Le rôle de l'ANFR.	96
2. LA CERTIFICATION ET LE MARQUAGE CE	96
2.1 Le cadre du marquage CE.	96
2.1.1 Principes.	96
2.1.2 Forme du marquage	97
2.2 Le marquage CE des dispositifs médicaux	97
2.2.1 Définitions	98
2.2.2 Conditions du marquage CE.	98
2.2.3 Débiteur de l'obligation de marquage CE	99
2.2.4 Sanctions	99
2.3 Le marquage CE des systèmes d'IA à haut risque	100
2.3.1 Principe	100
2.3.2 Portée	100
2.4 L'application au secteur de la santé.	101
2.4.1 Application aux dispositifs médicaux (connectés ou non).	101
2.4.2 Enoncé des exigences	102
3. LES OBLIGATIONS ET RESPONSABILITÉS DES ACTEURS DES SYSTÈMES D'IA À HAUT RISQUE INTÉGRÉ.	102
3.1 Fournisseurs de systèmes d'IA à haut risque.	103

3.2	Importateurs de systèmes d'IA à haut risque.	103
3.3	Distributeurs de systèmes d'IA à haut risque.	103

Chapitre 4

La protection des données à caractère personnel

1.	LE CYCLE DE VIE DES DONNÉES PERSONNELLES DANS UN ÉCOSYSTÈME IoT.	105
1.1	Principes généraux de la protection des données à caractère personnel	106
1.2	Définition et qualification des données à caractère personnel dans un environnement IoT.	107
1.3	Données personnelles <i>versus</i> données anonymisées : une frontière floue.	108
1.4	La qualification des données particulières dans l'IoT	110
2.	LES OBLIGATIONS DES ACTEURS QUI TRAITENT CES DONNÉES	111
2.1	La distinction entre responsables de traitement et sous-traitants.	112
2.2	L'encadrement des relations entre acteurs	114
2.2.1	l'encadrement des relations entre responsable du traitement et sous-traitant	114
2.2.2	l'encadrement des relations entre responsables du traitement conjoints	115
2.3	Le registre des activités de traitement : un document unique pour chaque acteur. ...	116
2.4	Les évaluations de risques liés aux données à caractère personnel : des documents nécessitant la collaboration de tous les acteurs	116
2.4.1	l'analyse d'impact sur la protection des données (AIPD).	117
2.4.2	l'analyse d'impact sur les transferts de données hors de l'espace économique européen (AITD)	119
2.4.2.3	L'AITD	121
3.	LES GARANTIES RELATIVES À LA PROTECTION DES DONNÉES PERSONNELLES COLLECTÉES PAR DES DISPOSITIFS IoT	122
3.1	La protection des données dès la conception et par défaut	122
3.1.1	Les principes	122
3.1.2	La protection des données dès la conception.	123
3.1.3	La protection des données par défaut.	123
3.1.4	Le CEPD	123
3.2	La gestion des violations de données à caractère personnel	124
3.3	La garantie des droits des personnes concernées dans un environnement IoT	125
3.3.1	Droit d'accès	126
3.3.2	Droit de rectification.	126

3.3.3	Droit à l'effacement.....	126
3.3.4	Droit à la limitation.....	127
3.3.5	Droit à la portabilité.....	127
3.3.6	Droit d'opposition.....	127
3.3.7	Prise de décision automatisée et profilage.....	127
3.3.8	Application des droits garantie en fonction de la base légale retenue pour le traitement.....	128
3.4	Quelques spécificités en matière de protection des données dans les secteurs sensibles utilisant des objets connectés.....	128
3.4.1	Les données de santé.....	128
3.4.2	Les données issues de systèmes domotiques.....	129
3.4.3	Les données issues des véhicules connectés.....	129
4.	LES RECOURS ET LES SANCTIONS.....	129
4.1	Les recours des personnes concernées.....	129
4.1.1	Le droit d'introduire une réclamation auprès d'une autorité de contrôle.....	130
4.1.2	Le droit à un recours juridictionnel effectif.....	130
4.2	Les actions de groupe.....	131
4.2.1	La définition de l'action de groupe.....	131
4.2.2	L'influence des actions de groupe en matière d'objets connectés et de protection des données.....	131
4.3	Les pouvoirs des autorités nationales de contrôle.....	133
4.3.1	Les pouvoirs d'enquête.....	133
4.3.2	Les pouvoirs d'adopter des mesures correctrices.....	134
4.4	Les typologies de sanctions.....	135
4.4.1	Les sanctions administratives des autorités nationales de contrôle.....	135
4.4.2	La responsabilité civile et l'indemnisation des victimes en cas de préjudice lié à une violation du RGPD.....	136

Chapitre 5

La responsabilité civile et pénale

1.	LA DIRECTIVE SUR LA RESPONSABILITÉ DU FAIT DES PRODUITS DÉFECTUEUX.....	140
1.1	L'obligation de garantir la sécurité des objets connectés.....	140
1.2	Le champ d'application de la responsabilité du producteur.....	140
1.3	La notion de produit défectueux.....	141
1.4	Une responsabilité objective du producteur.....	141

1.4.1	Charge de la preuve	141
1.4.2	Limitation de la responsabilité.....	142
1.4.3	l'exonération de responsabilité du producteur en cas de faute de la victime.....	143
2.	LA RESPONSABILITÉ DES FABRICANTS ET DISTRIBUTEURS.....	144
2.1	Les obligations du fabricant en cas de risque pour la santé ou la sécurité, ou pour les droits fondamentaux d'un système d'IA.....	144
2.2	Les obligations des fabricants de produits comportant des éléments numériques.....	145
2.3	Responsabilité du distributeur pour des systèmes d'IA à haut risque.....	146
3.	LES RESPONSABILITÉS CIVILE ET PÉNALE DES OBJETS CONNECTÉS.....	147
3.1	La responsabilité civile : responsabilité du fait des choses.....	147
3.1.1	La responsabilité du fait des choses.....	147
3.1.2	La nécessité d'un régime spécifique.....	147
3.2	La responsabilité pénale des objets connectés.....	148
3.2.1	La difficulté d'imputabilité.....	148
3.2.2	Les pistes d'adaptation du droit pénal.....	148
3.2.3	l'évolution du cadre légal.....	149
3.2.4	l'impact sur les assurances et la gestion des risques.....	149

Chapitre 6

Les enjeux de propriété intellectuelle

1.	LA PROTECTION DES INNOVATIONS TECHNOLOGIQUES : BREVETS, MARQUES, DROITS D'AUTEUR, DESSINS ET MODÈLES	152
1.1	Les régimes de protection	152
1.1.1	Droit d'auteur	152
1.1.2	Droit des marques.....	154
1.1.3	Dessins et modèles	155
1.1.4	Créations techniques.....	157
2.	LA PROPRIÉTÉ DES DONNÉES GÉNÉRÉES PAR LES OBJETS CONNECTÉS	159
2.1	Les enjeux de la propriété des données dans l'IoT	159
2.2	Cadre juridique et régulation : le Data Act.....	160
2.3	Enjeux éthiques et perspectives	161
	CONCLUSION : PERSPECTIVES ET RECOMMANDATIONS POUR L'AVENIR	163
	INDEX	167