

TABLE DES MATIÈRES

Introduction : tendances actuelles en matière de réglementation du numérique 7

Gabriela DE PIERPONT

maître de conférences à l'UCLouvain Saint-Louis,
chargée de cours à l'ICHEC Management School

Enguerrand MARIQUE

maître de conférences à l'Université Catholique de Lille (France),
chargé de cours à l'Université Radboud de Nimègue (Pays-Bas),
chargé de cours invité à l'UCLouvain

Introduction 7

Section 1

L'impulsion européenne en matière de numérisation, saison 2 8

A. Évolution et nouveaux instruments juridiques 8

B. Mise en œuvre des engagements dans les États membres, singulièrement en Belgique 9

Section 2

Le portefeuille des commissaires européens 10

A. Compétences des commissaires (2019-2024) 10

B. Compétences des commissaires (2024-2029) 13

C. Constats et analyse de l'évolution des priorités numériques 14

1. Comparaison des compétences numériques (2019-2024 vs 2024-2029) 14

2. Évolution des priorités et gouvernance numérique 15

Section 3

Enjeux de la numérisation et objectifs de l'ouvrage 17

A. « Justice numérique » – Réforme des procédures civiles et pénales 17

B. Défis et opportunités liés aux « services numériques » 18

C. Régulation des « actifs numériques » 18

Première partie

JUSTICE NUMÉRIQUE

1

De quelques nouveautés législatives en matière de digitalisation de la procédure civile 23

Eva GILLARD

assistante à l'UCLouvain et à l'UNamur, membre du CPRI et du CRIDS

Justin VANDERSCHUREN

chargé de recherches au FR.S.-FNRS, chargé de cours invité à l'UCLouvain

Résumé de la contribution 24

Introduction 24

Section 1

La loi du 15 mai 2024 portant dispositions en matière de digitalisation de la justice et dispositions diverses II 25

- A. Le développement de la signification électronique 26
- B. La dématérialisation des actes d'huissier 29
- C. La consultation des décisions sur le site internet du portail de la Justice 32
- D. La création du dossier de la procédure numérique et du Registre central des dossiers de la procédure 34
 - 1. Le dossier de la procédure numérique 35
 - 2. Le Registre central des dossiers de la procédure 39

Section 2

La loi du 25 avril 2024 portant organisation des audiences par vidéoconférence dans le cadre des procédures judiciaires ... 45

- A. L'enregistrement des audiences 46
- B. L'organisation des audiences par vidéoconférence 49

Section 3

La loi du 28 mars 2024 portant dispositions en matière de digitalisation de la justice et dispositions diverses Ibis 62

- A. La « communication » électronique dans le contexte judiciaire 63
- B. La digitalisation de la procédure d'omission d'une cause du rôle général 70

Section 4

La loi du 19 décembre 2023 portant dispositions en matière de digitalisation de la justice et dispositions diverses.....	75
A. L'aide juridique de deuxième ligne.....	75
B. Les modifications apportées à la loi du 16 octobre 2022 visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements [...].....	77

2

Les nouvelles technologies et la récolte de preuves lors des enquêtes pénales : le cas des données informatiques	85
---	-----------

Mona GIACOMETTI

avocate au barreau de Bruxelles, professeure à l'U.L.B.,
professeure invitée à l'UCLouvain

Résumé de la contribution	86
Introduction	86

Section 1

Actualité en matière de récolte de données au moyen d'une recherche dans un système informatique.....	88
A. Présentation générale des recherches dans un système informatique	88
1. La recherche informatique non secrète	88
2. La recherche informatique secrète	95
B. L'accès aux données au moyen d'une recherche informatique : la Cour de justice de l'Union européenne impose un contrôle préalable par un juge ou une autorité administrative indépendante.	95
1. Quelques préalables utiles à la compréhension de la décision de la Cour de justice ..	96
2. L'affaire ayant donné lieu aux questions préjudicielles posées à la Cour de justice..	98
3. Les enseignements de l'arrêt rendu par la Cour de justice le 4 octobre 2024	98
4. Les conséquences de l'arrêt rendu par la Cour de justice le 4 octobre 2018 en droit belge.....	102

Section 2

Actualité en matière de récolte de données au moyen de la coopération avec les fournisseurs de services de communications électroniques	107
A. Présentation générale des dispositions régissant la coopération avec les fournisseurs de services.....	107

B. L'amélioration de la coopération avec les fournisseurs de services grâce aux injonctions européennes de production et de conservation des données.	109
1. Le nouveau règlement européen relatif aux injonctions de production et de conservation des preuves électroniques	109
2. Champ d'application matériel : tout type de données.	111
3. Champ d'application personnel : les fournisseurs de certains services dans l'Union.	112
4. Champ d'application territorial : des instruments obligatoires en cas de récolte transfrontière de preuves électroniques par les États participants	114
5. L'émission d'une injonction : l'autorité compétente et les conditions prévues par le règlement e-Evidence	115
6. Le destinataire de l'injonction : le fournisseur de services et, le cas échéant, l'État où est établi le destinataire de l'injonction	117
7. L'exécution d'une injonction : le principe de l'exécution obligatoire, le respect de délais stricts et la possibilité d'exécution forcée de l'injonction	118
Conclusion	122

Deuxième partie

SERVICES NUMÉRIQUES

3

La mise en œuvre du règlement sur les services numériques en Belgique 125

Clément MAERTENS
chercheur-doctorant à l'UCLouvain

Résumé de la contribution 126

Introduction 126

Section 1

Les modifications apportées par le règlement sur les services numériques 127

- | | |
|--|-----|
| A. Les évolutions du cadre juridique des intermédiaires en ligne : de la directive e-commerce au règlement sur les services numériques ... | 127 |
| B. Bref aperçu des nouvelles obligations de <i>due diligence</i> applicables aux fournisseurs de services intermédiaires | 129 |

Section 2

La mise en œuvre du règlement sur les services numériques en droit européen	131
A. Les pouvoirs de mise en œuvre de la Commission européenne	132
B. Les compétences et les pouvoirs de mise en œuvre des États membres	133
1. La détermination de l'État membre compétent	134
2. La mise en œuvre institutionnelle et administrative	134
C. Les mécanismes de coopération prévus par le règlement sur les services numériques	137

Section 3

La mise en œuvre du règlement sur les services numériques en droit belge	139
A. La répartition des compétences de mise en œuvre dans le régime fédéral belge	139
B. La mise en œuvre du règlement sur les services numériques dans le droit fédéral belge	142
C. La mise en œuvre du règlement sur les services numériques dans le droit communautaire belge	144
1. La mise en œuvre du règlement sur les services numériques dans le droit de la Communauté française	144
2. La mise en œuvre du règlement sur les services numériques dans le droit de la Communauté flamande	147
3. La mise en œuvre du règlement sur les services numériques dans le droit de la Communauté germanophone	150
D. Les mécanismes de coopération intrabelge	151
Conclusion	154

4

Why Does Supply Chain Cybersecurity Matter? 155

Charles-Albert HELLEPUTTE

avocat au barreau de Bruxelles, maître de conférences invité à l'UCLouvain Saint-Louis

Andrea OTAOLA

avocate aux barreaux de Madrid et de Bruxelles

Florence STEENACKERS

director, head of Privacy & Data Governance at Approach Cyber

Jérôme DE MEEÛS

senior Privacy & Data Governance Expert at Approach Cyber

Executive Summary..... 156

Résumé de la contribution 156

Introduction 158

Section 1

EU Regulatory Landscape 160

- A. **Foundations of EU Cybersecurity Policy: GDPR, NIS and CSA..... 161**
- B. **Strengthening Cybersecurity Resilience: The Synergy Between NIS2 and DORA 162**
- C. **Advancing Cybersecurity in the Digital Era: The AI Act and the CRA 164**

Section 2

Key Transversal Measures to Enhance Supply Chain Cybersecurity..... 165

- A. **Measure 1 – Management Accountability: Management Body of the Company Is Responsible for Managing Supply Chain Cybersecurity Risks 165**
 - 1. A Top-Down Approach to Supply Chain Security 165
 - 2. Making Supply Chain Security a New Compliance Subdomain 166
 - 3. Elevating Supply Chain Security at Management Level 166
- B. **Measure 2 – Internal Policies: Companies Shall or Must Have Policies in Place Covering Third-Party Cybersecurity Risks (Stand-Alone or Umbrella Policies) 167**
 - 1. Internal Policies as the Foundation of Accountability 167
 - 2. Policies for Structuring the Internal Management of ICT Third-Party Contracting 167
 - 3. Policies for Governing “End-To-End” Relationships with ICT Third-Party Suppliers 168

C. Measure 3 – Information Sharing: Companies Shall Provide Adequate Cybersecurity Information on Their Systems, Products or Services Across the Supply Chain	169
1. Providing Full Transparency To Demonstrate Compliance	169
2. Facilitating Information Flow Across the Supply Chain for Market Access	169
3. Strengthening Security Through Software Bill of Materials	170
D. Measure 4 – Mapping and Record Keeping: Companies Shall Keep Accurate and Up-To-Date Records of Their Suppliers and Their Impacted Processes	170
1. Mapping the Actors in the Supply Chain	170
2. Keeping a Record of All Contractual Arrangements With Third-Party Suppliers	171
E. Measure 5 – Risk Assessment and Security-By-Design: Companies Shall Apply a Risk-Based Approach and Include Third-Party Suppliers in Their ICT Risk Strategies	173
1. Integrating Supply Chain Cybersecurity Into ICT Risk Management	173
2. Risk-Based Approach to Supply Chain Cybersecurity	173
3. Strengthening Risk Assessment and Security-By-Design with Threat Modeling	174
4. Risk Assessment and Oversight by Authorities	174
5. Simplified Regime for Small and Medium-Sized Companies	175
6. Requalification of Third-Party Roles and Responsibilities	175
F. Measure 6 – Due Diligence and Contracts: Companies Shall Select Third-Party Suppliers Against a Set of Security Criteria, Which Must Be Translated in the Contractual Documents (Also With Any Subcontractors)	175
1. Cybersecurity Due Diligence of Subcontractors	175
2. Cybersecurity Restrictions on the Freedom to Contract	176
3. Intragroup Subcontracting Should Not Be Treated Differently From Third-Party Subcontracting	177
4. Due Diligence and Contracting Obligations for AI Systems and Products With Digital Elements	178
G. Measure 7 – Monitoring, Testing and Audit: Companies Shall Monitor the Level of Security of Third-Party Suppliers During the Contract, Including Through Testing and Audits	179
1. Monitoring Changes in the Cybersecurity Practices of Suppliers	179
2. Managing Vulnerabilities Through Testing	179
3. Threat-Led Penetration Testing: A Critical Component	180
4. Monitoring the Risks Related to the Use of AI Systems	180
5. Post-Market Monitoring by AI Providers	180
H. Measure 8 – Reporting Obligations: Third-Party Suppliers Shall Report Incidents or Non-Conformity Within a Specific Timeframe	181
1. Upstream Transfer of Information Across the Supply Chain	181
2. Notification on Behalf of the Principal Company	182
3. Notification by DSPs Under NIS2	182

I. Measure 9 – Role of Standards, Certifications, Code of Conduct, BCR: Companies Can Rely on Official “Security Stamps” To Assess Third-Party Cybersecurity	183
1. Cybersecurity Certifications as Second-Level Accountability Documents	183
2. Towards an EU Cybersecurity Certification for ICT Products, ICT Services and ICT Processes	184
3. Adherence to a Code of Conduct Ensures Adequate and Proportionate Security Safeguards	184
4. Binding Corporate Rules as an Indication of Data Protection (and Security) Maturity	185
Conclusion	185
List of Annexes	187

Troisième partie

ACTIFS NUMÉRIQUES

5

Quand Est et Ouest se rencontrent : la difficile factorisation de la qualité de la protection de la vie privée au sein du contrôle des opérations de concentration	193
---	-----

Jérôme DE COOMAN

premier assistant au Département de Droit européen de la Faculté de Droit,
de Science Politique et de Criminologie de l’ULiège

Résumé de la contribution	194
Introduction	195
Section 1	
Saga jurisprudentielle	198
Section 2	
La protection des données personnelles en tant que facteur de droit de la concurrence	210
A. Concurrence sur la qualité de la protection des données personnelles ...	210
B. Diminution de la qualité de la protection des données personnelles en raison d’une opération de concentration	221
Conclusion	224

6

IP/IT/Data and Blockchain 227

Sarah COMPANI

avocate à la Cour (France),
solicitor (England and Wales)

Executive Summary 228

Résumé de la contribution 228

Introduction 229

Section 1

Legal Background 231

Section 2

Definitions 232

Section 3

Introduction to the Concept of Immutability of a Smart Contract 233

Section 4

Legal Lessons 235

Conclusion 239