

L'estratto che stai consultando  
fa parte del volume in vendita  
su **ShopWKI**,  
il negozio online di **Wolters Kluwer**

[Torna al libro](#)



CEDAM

IPSOA

**UTET**<sup>®</sup>  
GIURIDICA

il fisco

 ALTALEX

## TABLE OF CONTENTS

ALBERTO CAMON

THE PROJECT DEVICES AND DIGITAL EVIDENCE IN EUROPE	1
--	---

RAFFAELLA BRIGHI-MICHELE FERRAZZANO

### DIGITAL FORENSICS: BEST PRACTICES AND PERSPECTIVE

1. <i>Introduction, issues, and goals</i> .....	13
2. <i>Digital forensics</i> .....	16
3. <i>Standards and guidelines</i> .....	20
3.1. <i>International standards and guidelines</i> .....	20
3.2. <i>Overview of guidelines, best practices, and soft regulation of DEVICES' Partner</i> .....	24
3.3. <i>Guidelines on Digital Forensic Procedures for OLAF Staff</i> .....	26
4. <i>Digital forensics expert: roles and skills</i> .....	28
5. <i>Main steps in digital investigations</i> .....	33
6. <i>The digital forensics lab: tools, facilities, and requirements</i> .....	40
7. <i>The big amount of data: technical requirements versus privacy</i> .....	43
8. <i>Conclusions: recommendation and perspective</i> .....	47

SABINE GLESS-THOMAS WAHL

### THE HANDLING OF DIGITAL EVIDENCE IN GERMANY

1. <i>Digital Evidence in Germany – Virtually Unknown? ..</i>	49
2. <i>National Legal Framework on Digital Investigations</i> .....	53
2.1. <i>Using Technology and Constitutional Limits: Clandestine Access to Data by Law Enforcement</i> .....	54

2.2.	<i>Transfer of Rules from the Analogue to the Virtual</i>	56
2.3.	<i>Delineating Open and Covert Investigative Requirements – Seizure of Emails as a Case Example</i> .....	58
3.	<i>Ensuring Data Integrity – the Technical Side of Digital Evidence in Germany</i> .....	60
3.1.	<i>Procedure of Digital Investigation – Involved Persons</i> .....	61
3.2.	<i>Rules on “Digital Investigations”</i> .....	64
3.2.1.	<i>Guidelines</i> .....	64
3.2.2.	<i>Best Practices</i> .....	65
3.3.	<i>Practical Implications</i> .....	67
4.	<i>Defense Rights</i> .....	68
4.1.	<i>Right to Information</i> .....	68
4.2.	<i>Right of Access to Files</i> .....	70
4.2.1.	<i>Right to Access the File by Defense Counsel</i> .....	71
4.2.2.	<i>Right to Access the File by the Defendant without Defense Counsel</i> .....	73
4.3.	<i>Remedies against Investigative Measures in Relation to Digital Evidence</i> .....	73
4.3.1.	<i>Covert Investigative Measures</i> .....	74
4.3.2.	<i>Other Coercive Measures, e.g. Search and Seizures</i> .....	75
5.	<i>Admissibility of Digital Evidence at Trial</i> .....	76
5.1.	<i>Exclusion of Evidence Stipulated in the Law</i> .....	77
5.1.1.	<i>Ban from Using Evidence Concerning the Core Area of Privacy for Interception Measures</i> .....	77
5.1.2.	<i>Protection of Professional Secrets</i> .....	78
5.1.3.	<i>Use of Digital Evidence in Other Proceedings</i> .....	79
5.2.	<i>Exclusion of Evidence not Stipulated in the Law</i> .....	82
6.	<i>Conclusions</i> .....	85

## LAURA BARTOLI-GIULIA LASAGNI

## THE HANDLING OF DIGITAL EVIDENCE IN ITALY

1.	<i>The digital investigation: a regulatory overview</i> .....	87
1.1.	<i>Constitutional framework</i> .....	87
1.2.	<i>Regulatory framework: police investigation</i> .....	89
1.3.	<i>Regulatory framework: the expert consultant</i> .....	93
1.4.	<i>Technical standards</i> .....	95

1.5.	<i>Conundrums</i> .....	97
1.6.	<i>Privileged information</i> .....	101
1.7.	<i>Chain of custody</i> .....	102
2.	<i>Investigating authorities</i> .....	104
2.1.	<i>Law Enforcement</i> .....	104
2.2.	<i>Digital Forensics Consultants</i> .....	107
2.2.1.	<i>Digital Forensic Consultants Hired by the Prosecution Service</i> .....	110
2.2.2.	<i>Digital Forensic Consultants Hired by the Judge</i> .....	112
3.	<i>Defence Rights: Information and Right to be Heard</i> .....	113
3.1.	<i>Defensive Investigations</i> .....	115
3.2.	<i>Consent of the Accused</i> .....	116
3.3.	<i>Remedies</i> .....	117
3.4.	<i>Third-Party Rights</i> .....	118
4.	<i>Digital evidence at trial</i> .....	119
4.1.	<i>Admissibility</i> .....	119
4.2.	<i>Production of evidence in different proceedings</i> .....	120

KATALIN LIGETI-GAVIN ROBINSON

## THE HANDLING OF DIGITAL EVIDENCE IN LUXEMBOURG

1.	<i>The legal framework</i> .....	123
1.1.	<i>Constitutional framework</i> .....	125
1.2.	<i>Administrative punitive proceedings</i> .....	127
1.3.	<i>Seizure, copies and deletion</i> .....	129
1.4.	<i>Other investigative measures</i> .....	132
1.5.	<i>Flagrancy</i> .....	137
1.6.	<i>Quick freeze, urgent expertise and decryption</i> .....	137
1.7.	<i>Proportionality: rules, challenges and best procedure</i> .....	139
1.8.	<i>Privileged information</i> .....	143
1.9.	<i>Chain of custody and data protection</i> .....	146
1.10.	<i>Duties and prerogatives of the investigating judge</i> ..	148
1.11.	<i>Digital forensic laboratories and storage of seized data</i> .....	149
1.12.	<i>Cooperation with OLAF</i> .....	150
2.	<i>Investigating authorities</i> .....	151
2.1.	<i>Experts and training</i> .....	152
3.	<i>Defence and third-party rights</i> .....	154
4.	<i>Admissibility at trial</i> .....	157

4.1. <i>Burden of proof</i> .....	160
4.2. <i>Administrative-criminal crossover</i> .....	161
5. <i>Concluding remarks</i> .....	162

## LORENA BACHMAIER WINTER

## THE HANDLING OF DIGITAL EVIDENCE IN SPAIN

1. <i>Introduction</i> .....	165
2. <i>Some preliminary notions on the applicable legal framework and standards on digital forensics</i> .....	166
3. <i>Digital Investigations: the national framework</i> .....	169
3.1. <i>The applicable standards in digital forensic procedures</i> .....	169
3.2. <i>The proportionality principle in digital investigations</i> .....	171
3.3. <i>Search and seizure of digital data: the legal framework</i> .....	175
3.4. <i>The protection of digital sensitive or privileged information</i> .....	178
3.5. <i>Procedures for specific phases of digital investigations</i>	181
a) <i>Procedures for Phase 1 and 2 (acquisitive and investigative stages)</i> .....	181
b) <i>The digital forensic laboratories</i> .....	184
c) <i>The synthesis of an explanation, within agreed limits, for the factual information about evidence (the interpretation of the analysis)</i> ....	185
d) <i>Obligation to record/document the procedures</i>	186
e) <i>Data retention</i> .....	187
3.6. <i>Cooperation with OLAF in digital investigations</i> .	188
4. <i>Investigating authorities (DEFR, DES)</i> .....	189
5. <i>Defence and third party rights</i> .....	191
5.1. <i>Main defence rights and procedural safeguards</i> .....	191
5.2. <i>Digital evidence ex parte</i> .....	194
5.3. <i>Protection of third parties</i> .....	195
5.4. <i>Liability in cases of an unlawful interference in the fundamental rights</i> .....	196
6. <i>Admissibility of digital evidence at trial</i> .....	198
6.1. <i>Admissibility and Reliability of the digital evidence</i>	198
6.2. <i>Challenging the authenticity of the evidence and the chain of custody</i> .....	201
6.3. <i>Accidental findings</i> .....	203

7. <i>Concluding remarks</i> .....	204
------------------------------------	-----

## LAURA BARTOLI-GIULIA LASAGNI

ANTIFRAUD INVESTIGATION AND DIGITAL FORENSICS: A  
COMPARATIVE PERSPECTIVE

1. <i>Introductory remarks</i> .....	207
2. <i>Constitutional and regulatory framework</i> .....	208
3. <i>Copyright issues</i> .....	216
4. <i>Specialization of Investigative Bodies</i> .....	217
4.1. <i>“Basic” vs “Complex” Digital Forensics         Operations</i> .....	219
4.2. <i>Training</i> .....	221
4.3. <i>Challenging Police Expertise: The Problem of First         Responders</i> .....	222
5. <i>Digital Forensics Consultants</i> .....	224
6. <i>Defence Rights</i> .....	225
6.1. <i>Right to Information and Access to File</i> .....	226
6.2. <i>Right to be Heard</i> .....	227
6.3. <i>Remedies</i> .....	228
7. <i>Third-Party Rights</i> .....	231
8. <i>Admissibility at trial</i> .....	232
9. <i>Production of digital evidence in different proceedings</i> .....	234

## MICHELE CAIANIELLO

## CONCLUSIVE REMARKS

ANTIFRAUD INVESTIGATIONS AND RESPECT FOR  
FUNDAMENTAL RIGHTS FACED WITH THE CHALLENGE OF  
E-EVIDENCE AND DIGITAL DEVICES

1. <i>Digital evidence and financial crimes: General     considerations</i> .....	237
2. <i>Results emerging from the research project</i> .....	241
2.1. <i>Common Solutions</i> .....	241
2.1.1. <i>Starting from searches and seizures</i> .....	241
2.1.2. <i>Technical neutrality in legislation</i> .....	243
2.1.3. <i>The proportionality principle</i> .....	243
2.1.4. <i>A comprehensive approach to digital             investigations</i> .....	244

2.1.5.	<i>The need for more uniformity in the European realm</i> .....	246
2.2.	<i>Diverging aspects</i> .....	247
2.2.1.	<i>National constitutional principles v. Supranational European principles</i> .....	247
2.2.2.	<i>Regulation in “crimministrative” proceedings</i> ....	248
2.2.3.	<i>Diverging features in the law of evidence</i> .....	249
2.2.4.	<i>Legal provisions concerning documentation of digital investigative operations</i> .....	250
2.2.5.	<i>The authority empowered to issue the intrusion in the private sphere of the individual</i> .....	252
3.	<i>Conclusions. The need for more uniform legal provisions to ensure effectivity both in law enforcement and fair trial rights</i> .....	252
	<i>Contributors</i> .....	257

L'estratto che stai consultando  
fa parte del volume in vendita  
su **ShopWKI**,  
il negozio online di **Wolters Kluwer**

[Torna al libro](#)



CEDAM

IPSOA

**UTET**<sup>®</sup>  
GIURIDICA

il fisco

 ALTALEX