

Roger Blanpain and Marc Van Gestel

# Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work

*Law and Practice*



KLUWER LAW  
INTERNATIONAL

**Studies in Employment and Social Policy**

# **Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work**

**Law and Practice**

**Roger Blanpain**

Professor at the Catholic University of Leuven, Limburg (Belgium)  
and the University of Tilburg (The Netherlands)

President of the International Society for Labour Law and  
Social Security, Member of the Royal Flemish Academy of Belgium

**Marc Van Gestel**

Technical Director, eMailMasters.com nv

Translated by Rita Inston



**KLUWER LAW INTERNATIONAL**

THE HAGUE / LONDON / NEW YORK

*Published by:*

Kluwer Law International

P.O. Box 85889, 2508 CN The Hague, The Netherlands

[sales@kluwerlaw.com](mailto:sales@kluwerlaw.com)

<http://www.kluwerlaw.com>

*Sold and Distributed in North, Central and South America by:*

Aspen Publishers, Inc.

7201 McKinney Circle, Frederick, MD 21704, USA

*Sold and Distributed in all other countries by:*

Extenza-Turpin Distribution Services

Stratton Business Park, Pegasus Drive, Biggleswade,

Bedfordshire, SG18 8QB, United Kingdom

**A C.I.P. Catalogue record for this book is available from the Library of Congress.**

*Printed on acid-free paper.*

ISBN 90-411-22664

All rights reserved

© 2004 Kluwer Law International

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording, or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

Printed in The Netherlands.

# **Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work**

**Law and Practice**

---

## **Studies in Employment and Social Policy**

---

In the series Studies in Employment and Social Policy this book *Use and Monitoring of E-Mail, Intranet and Internet Facilities at Work* is the twenty-seventh title.

*The titles published in this series are listed at the end of this volume.*

## List of Abbreviations

ABVV	<i>Algemeen Belgisch Vakverbond</i> [Belgian General Federation of Labour]
ACLBV	<i>Algemeen Centrale der Liberale Vakbonden</i> [Federation of Liberal Trade Unions of Belgium]
ACV	<i>Algemeen Christelijk Vakverbond</i> [Confederation of Christian Trade Unions]
BBTK	<i>Belgische Bond van Bedienden, Technici en Kaderpersoneel</i> [national white-collar union affiliated to the Belgian General Federation of Labour]
B.S.	Belgisch Staatsblad [Belgian Official Gazette]
BVBA	Ltd (company with limited liability)
BW	Burgerlijk Wetboek [Civil Code]
CCTV	closed-circuit television
CEO	chief executive officer
CNE	<i>Centrale Nationale des Employés</i> [French-speaking white-collar section within the Confederation of Christian Trade Unions]
HR	human resources
ICT	information and communications technology
ILO	International Labour Organization
IT	information technology
J.T.T.	Journal des Tribunaux de Travail
LBC	<i>Landelijke Bedienden Centrale</i> [Dutch-speaking white-collar section within the Confederation of Christian Trade Unions]
No.	number
NV	plc (public limited company)
NVK	<i>Nationaal Verbond Kaderpersoneel</i> [union for professional and managerial staff]
OJ	Official Journal of the European Communities
PC	personal computer
R.W.	Rechtskundig Weekblad
Sw.	Strafwetboek [Criminal Code]
tu	trade union
UNI	Union Network International
VBO	<i>Verbond van Belgische Ondernemingen</i> [Federation of Belgian Enterprises]
VDU	visual display unit
WAP	Wireless Applications Protocol

# Code of Practice

## USE AND MONITORING OF E-MAIL, INTRANET AND INTERNET FACILITIES AT WORK

The company encourages the use of on-line communications and has drawn up a Code of Practice.

As an employee/user, you have been informed and consulted about the content of this Code.

The complete text of the Code is available on the company's Web site. The following rules incorporate its essential provisions.

1. The communications facilities provided by the company are intended only for work-related use. And all such use should be in a manner that promotes the company's image and the quality of the work of those concerned.
2. Private use of these communications facilities is permitted provided it does not jeopardize the efficient operation of the service. In cases of private use, indicate the fact in the communication concerned. Store incoming private e-mail in a clearly marked folder.
3. In the interests of keeping the network secure, protecting data confidentiality, socially acceptable standards of use, preventing overloading of the network and ensuring continuity of the service supplied by the company, permanent monitoring of use is carried out.
4. This monitoring takes place only in so far as is necessary and with due respect for the right to personal privacy.
5. The company has the right to oversee the work-related use of communications facilities and to examine the content of the communications concerned. It intercepts one out of every 100 e-mails and can examine their content.
6. In the case of private communications, where there are serious grounds for suspecting failure to observe the Code of Practice they can be examined as to their number and/or content in the presence of the employee concerned, possibly with the assistance of an accompanying trade union representative.
7. You have a right of access to all data stored regarding your on-line communications and can request their rectification.
8. The disciplinary sanctions for failure to observe the Code of Practice are decided by the company in accordance with the works rules as laid down in the company's staff handbook.

# Table of Contents

<b>List of Abbreviations</b>	xvii
<b>Code of Practice</b>	xix
<b>Preface</b>	1
<b>Privacy and the Specific Nature of Labour Law</b>	1
<i>A National Collective Agreement</i>	1
<i>Commission for the Protection of Personal Privacy</i>	1
<i>Monitoring by the Employer: a Highly Restrictive Interpretation</i>	1
<i>No Monitoring of the Content of On-Line Messages</i>	3
<i>Indecisive Legal Doctrine</i>	3
<i>Employers: a Normal Policy</i>	5
<i>Room for Negotiation</i>	5
<b>Introductory Remarks</b>	9
<b>The Digital Society: Opportunities and Challenges</b>	9
<i>Companies</i>	9
<i>Employees and Other Workers</i>	10
<i>Employee Representatives</i>	10
<i>Reasons for Regulation and Scanning</i>	11
<i>Codes of Practice</i>	12
<i>Privacy</i>	13
<i>Normal Policy – Subsidiarity</i>	13
<b>Design and Outline of the Study</b>	15
<i>Company Communications Policies</i>	15
<i>Representative Overview</i>	15
<i>Content</i>	15
<b>Part I. De Facto: An Examination of Practice</b>	17
Introduction	19
Chapter I. Use of On-Line Communications at Work	21
§1. Form in Which Codes of Practice Exist: Written, Digital or Oral/Tacit	21
§2. Legal Commitment	22
I. Special Document	22
II. Schedule Appended to the Individual Contract of Employment	23
III. Works Rules	23
IV. Multiple-Channelled Commitment	23
V. Circular – Procedural Guide	24



## *Table of Contents*

VI. Corporate Culture	24
VII. Alteration	24
§3. Scope of Application	24
I. Territorial Coverage	24
II. Personnel Coverage	25
A. Employees	25
B. Other users	26
III. Substantive Coverage	27
A. On-line communications	27
B. Broader coverage	27
C. Changes	28
§4. General Principles and Objectives and Policy Statements	28
I. Résumé	28
A. Justification and authority	29
B. Objectives	29
1. Transparency	29
2. Interests – Risks	29
a. Company	29
b. Employees	29
c. Customers, shareholders and third parties	29
3. Encouraging the use of on-line communications	30
4. Promoting communication	30
5. Security of networks and computer systems	30
6. Professional manner of use	30
7. Protection of confidential information	30
C. Values	30
D. Privacy	30
E. Monitoring	31
F. Responsibility. Sanctions	31
II. Numbered List	31
III. Passages Quoted from Codes of Practice	34
§5. Access to On-Line Communications Facilities	41
I. Grant of Access	41
II. Refusal of Access or Withdrawal of Authorization	42
III. Continuity of Service	43
§6. Use of On-Line Communications Facilities	43
I. Work-Related Purposes	43
II. Personal Use	47
A. Ban on personal use	47
B. Limited personal use	48
C. Identification and responsibility	50
D. Withdrawal of personal use	51
E. Categorization	52

III. Banned Use	52
A. Banned access	53
B. Copyright	53
C. Chat rooms and chat files, newsgroups, mailing lists, chain letters, mail to all	54
D. Junk mail, mail of unknown origin	55
E. Entertainment, gambling or other games	55
F. Commercial advertising and other advertising	56
G. Concealment of identity	56
H. Large files	56
I. References	56
J. Viruses	57
K. Disruptive and unlawful conduct	57
L. Vandalism and destruction of computer files	57
M. Credit cards	57
N. Pornography	58
O. Making complaints against the company	58
P. The company's good name	58
Q. Dignified conduct	58
R. Confidential data	63
S. Follow-up	65
IV. Organization of Use	66
A. Access to information systems	66
B. Passwords	67
C. Security	69
D. Antivirus protection	70
E. Use	70
F. Back-up	71
G. Undesirable contacts	71
H. Internal audits and controls	71
I. Recording of telephone conversations	72
Chapter II. Responsibility and Liability – Monitoring and Sanctions	73
§1. Responsibility and Liability	73
I. Responsibility	73
II. Liability	74
A. Damage	74
B. Criminal offences	74
C. Liability disclaimers	75
§2. Monitoring	75
I. Employee Consent	75
II. Objective	76

## Table of Contents

III. Reasons – Legitimate Purpose	77
IV. Subject of Monitoring. Proportionality	81
A. Subject of monitoring	82
B. Proportionality	85
V. Individualization of Monitoring – Transparency	86
VI. Mediator and Contact Person	88
VII. Confidentiality	89
VIII. Access to Personal Data	90
§3. Sanctions	90
Chapter III. Use of On-Line Communications Facilities at Work by Employee Representatives	94
Chapter IV. A Random Sample of Practice: Four Company Codes	100
§1. First Code of Practice: Mail and Internet Policy	100
I. Objective	100
II. E-Mail	101
A. Use	101
B. Out of office	101
C. Prohibited activities	101
D. Volume restrictions	102
E. Archiving and ‘housekeeping’	102
F. Precautions	102
III. Internet	103
A. Use	103
IV. Monitoring and Sanctions Regarding E-Mail and Internet Use	103
A. Monitoring	103
B. Purposes of monitoring	104
C. Monitoring measures and individualization	104
D. Employee rights with respect to the monitoring of electronic on-line communications data	105
E. Miscellaneous	105
F. Sanctions	106
§2. Second Code of Practice: Charter on Information System Security in the Group’s Companies in Belgium	107
I. Introduction	108
II. Policy on the Security of the Information System	108
A. Why protect information?	108
B. What information?	109
III. Categories of Information	109
A. Public	109
B. Restricted	109

1. Internal information	109
2. Confidential information	109
3. Strategic information	110
IV. It Concerns Us All	110
A. The owner of information	110
B. The information user	110
C. Managers	111
D. Person responsible for information system security	111
E. The systems administrator	111
F. Person responsible for development	111
G. Internal Audit	111
V. What Principles must we Observe?	112
VI. Standards for Users: What Must We Do?	112
A. Classified information	113
1. For information that has been classified as confidential or strategic	113
2. For classified information (internal, confidential or strategic)	113
B. Access to information systems (programs, applications and computer files)	113
C. Workstations (desktop, portables, home workstations, PCs)	114
1. Access security	114
2. Software protection	114
3. Antivirus protection	114
4. Back-up	114
5. Special protection of portables and home workstations	115
D. Protection of data during transmission	115
1. Transmission of information	115
2. E-mail and faxes	115
3. Access to the internet	116
VII. Monitoring and Possible Sanctions	
Declaration regarding the security of the company IT system	118
§3. Third code of practice: Rules of Practice for the Use of Company IT and Communications Facilities	119
I. Basic Assumptions and Definitions	120
A. The facilities covered	120
B. Ownership of the facilities	120
C. General principle	121
D. Scope of application	121
E. Relation to other forms of regulation within the Group	121
II. Specific Rules of Practice with Respect to Information and Communication	121

## *Table of Contents*

A. Liability for content	121
B. Dealing with messages	122
C. Security and confidentiality	122
D. Moral and ethical rules	122
E. Employee delegations	123
1. Definition	123
2. Type of communication	123
3. Publication of information	123
III. Monitoring	124
A. Objectives	124
B. Individualization procedures for data collected during monitoring	125
1. Use of general quantitative data	125
2. Use of individual quantitative data	125
3. Use of individual qualitative data	125
IV. Sanctions	127
§4. Fourth Code of Practice	127
Worldwide Electronic Messaging, Telephone and Networking and Computing Resources Acceptable Use Policy	127
Minimum Implementation Standards	127
Acceptable Use	127
Privacy Considerations	127
Worldwide Internet Acceptable Use Policy	127
Minimum Implementation Standards	127
Acceptable Use	127
Download of Copyrighted Software	130
Privacy Considerations	130
<b>Part II. The Attitude of the Social Partners</b>	<b>131</b>
Chapter I. The Attitude of the Trade Unions	133
§1. Rights and Obligations of Individual Employees	133
I. Viewpoint of the Belgian General Federation of Labour	133
II. Viewpoint of the Confederation of Christian Trade Unions	135
III. Viewpoint of Union Network International	136
§2. Rights of Employee Representatives	137
I. Viewpoint of the Belgian General Federation of Labour	137
II. Viewpoint of the Confederation of Christian Trade Unions	138
III. Viewpoint of Union Network International	139
Chapter II. The Attitude of the Federation of Belgian Enterprises	140

<b>Part III. <i>De Jure</i></b>	143
Chapter I. Sources of Law	145
§1. Labour Law in General: the Employer/Employee Relationship	145
I. Rights and Obligations of the Employer and the Employee	145
A. Employee	145
B. Employer	146
II. Rights and Obligations of Employee representatives	148
§2. Legislation on Privacy, Telecommunications and the Protection of Personal Data	150
I. Principles	150
A. Rules on privacy	150
B. Secrecy of private communications	151
C. Processing of personal data	153
II. Applicability to the Employer/Employee Relationship	155
A. Rules on privacy	155
B. Secrecy of private telecommunications	155
C. Processing of personal data	156
§3. The Role of the National Labour Council: National Collective Agreements	157
I. The Role of the National Labour Council	157
II. CCTV Surveillance in the Workplace: National Collective Agreement No. 68	159
III. Monitoring of On-Line Communications: National Collective Agreement No. 81	160
IV. Analysis of National Collective Agreement No. 81	162
A. Scope	162
B. Definition	162
C. Commitments undertaken	162
D. Rules on the monitoring of electronic on-line communications data	163
1. General provisions	163
2. Principles	163
a. Legitimate-purpose principle: objective of monitoring	163
b. Proportionality	164
c. Informing employees – transparency	165
1) Advance information	165
a) There is a works council	165
b) No works council exists	165
2) Information when the monitoring system is being installed	165

## Table of Contents

a) Nature of the information	165
b) Quality of the information	166
c) Good faith	166
d. Consultation	166
e. Individualization of on-line communications data	166
1) Definition	167
2) Principles	167
a) Legitimate-purpose principle	167
b) Proportionality principle	167
c) Procedural conditions	168
(1) Direct individualization	168
(2) Indirect individualization	168
(a) Notification phase	168
(b) Interview	169
f. Assistance	169
g. Final provisions	169
V. Critical Assessment of National Collective Agreement No. 81	170
A. Validity	170
1. Only in the case of work-related use by employees	170
2. Other users	171
B. Contrary to mandatory law	171
C. A clear conception of privacy	172
D. Individualization: overlapping objectives	173
Chapter II. Access, Use and Ensuring the Security and Efficient Operation of Company E-Mail, Intranet and Internet Systems	174
§1. Access	174
I. Personnel Coverage	174
A. Employees	174
1. Principle: the employer's prerogative	174
2. Concept: employee	175
B. Self-employed workers and contractors	175
II. Substantive Coverage: Electronic On-Line Communications	175
§2. Use	176
I. Principle: the Employer's Prerogative	176
II. Work-Related and/or Private Use	176
III. Liability Disclaimers	178
IV. Manner of Use	178
V. Banned Use	178
VI. Continuity of Service	179
VII. Recording of Telephone Conversations	179

§3. Provision of Information, and Form and Legal Commitment	179
I. Informing Employees	179
II. Form and Legal Commitment	180
§4. Helpline, Complaints and Reporting Abnormal Use	180
§5. Ensuring Security and Efficient Operation	181
Chapter III. Monitoring of E-Mail, Intranet and Internet Use	182
§1. Monitoring of Work-Related Use	182
I. Validity	182
II. Subject of Monitoring	183
III. Objective of Monitoring – Legitimate Purpose	183
IV. Provision of Information – Transparency	185
A. Informing employees	185
1. Advance information	185
a. There is a works council	185
b. No works council exists	185
2. Information when the monitoring system is being installed	185
a. Nature of the information	185
b. Quality of the information	186
c. Good faith	186
B. Informing other users	186
V. Consultation of Employees (Representatives)	186
VI. Monitoring Methods – Proportionality	187
A. General data	187
B. Individual data	188
1. Monitoring of employees and similar workers	188
a. Monitoring and the employer's managerial authority	188
b. National Collective Agreement No. 81	189
1) Unclear and unsound	189
2) Individualization	190
a) General provisions	190
b) Principles	190
(1) Legitimate-purpose principle	190
(2) Proportionality principle	191
(3) Procedural conditions	191
(a) Direct individualization	191
(b) Indirect individualization including a prior notification phase	192
* Notification phase	192
* Interview	192
2. Monitoring of other users	193



*Table of Contents*

§2. Monitoring of Private Use	194
I. Coverage	194
A. Private use	194
B. Personnel coverage	194
II. Legal Principles	195
§3. Storage, Accessibility and Rectification of Data	195
Chapter IV. Liability for Use – Sanctions – Assistance	197
§1. Liability	197
I. User Liability	197
A. Liability for work-related use	197
1. Employee liability	197
2. Liability of other users	198
B. Liability for private use	198
II. Company Liability	198
A. Liability for work-related use	198
1. Liability for damage caused by an employee	198
2. Liability for damage caused by other users	198
B. Liability for damage caused in the context of private use	199
§2. Sanctions	199
I. Work-Related Use	199
A. Employees	199
B. Other users	199
II. Private Use	199
§3. Assistance	200
Chapter V. Rights and Obligations of Employee Representatives	201
§1. Information and Consultation	201
I. Organization of Work	201
II. Introduction of New Technologies	202
III. Use and Monitoring of On-Line Electronic Communications	203
A. Advance information	203
B. Information when the monitoring system is being installed	203
1. Nature of the information	203
2. Quality of the information	204
3. Good faith	204
4. Consultation	204
§2. Information Announcements to the Workforce – Meetings	205
§3. Assistance	205
Chapter VI. Model Codes of Practice	207
§1. Code of Practice for Individual Users	207