

TABLE DES MATIÈRES

Sommaire 5

Avant-propos 7

Introduction : Le droit pénal à l'ère numérique 9

PREMIÈRE PARTIE :
Défis politiques et pratiques

DÉFIS DE LA SOCIÉTÉ NUMÉRIQUE : PERSPECTIVES POLITIQUES. 21

 I. Loi du 25 décembre 2016 21

 II. Autres projets et évolutions futures 26

 III. Dimension internationale. 30

 Conclusion. 33

SECONDE PARTIE :
Le droit pénal face aux défis de la société numérique

COMPÉTENCE DES JURIDICTIONS PÉNALES FRANÇAISES FACE AUX INFRACTIONS
COMMISES VIA INTERNET 37

 Introduction. 37

 I. État du droit avant la loi du 3 juin 2016 38

 II. Questions sur le droit depuis la loi nouvelle du 3 juin 2016. 42

 Conclusion. 45

PROTECTION DES MINEURS EN LIGNE EN DROIT PÉNAL BELGE 47

 Introduction. 47

 I. Protection pénale des mineurs en ligne contre le cyberharcèlement,
 la cyberintimidation, la cybercalomnie 49

 Section 1. – Répression du cyberharcèlement (ou cyberbullying)
 par l'article 442bis du Code pénal 49

Section 2. – Répression du cyberharcèlement par l'article 145, § 3bis, de la loi du 13 juin 2005 relative aux communications électroniques	51
Section 3. – Répression du cyberharcèlement fatal par les articles 418-419 du Code pénal	52
Section 4. – Répression de la cyberintimidation et de la cybercalomnie par les articles 443 à 450 du Code pénal .	53
II. <i>Protection pénale des mineurs en ligne contre la violation de leur vie privée réalisée par la diffusion non autorisée d'enregistrements intimes</i> .	58
III. <i>Protection pénale des mineurs en ligne contre la réception d'images, de vidéos ou de messages non désirés ou problématiques</i>	61
Section 1. – Dans le domaine sexuel	62
Section 2. – Dans le domaine des violences exemptes de connotation sexuelle.	64
Section 3. – Dans le domaine terroriste	64
Section 4. – Dans le domaine des téléchargements illicites	66
IV. <i>Protection pénale des mineurs en ligne contre le grooming et la cyberprédation</i>	67
Section 1. – Utilisation d'une technologie de l'information par un majeur pour entrer en communication avec un mineur en vue de faciliter la commission d'une infraction à son détriment (<i>grooming</i>)	68
Section 2. – Cyberprédation	71
HACKING « ÉTHIQUE » EN DROIT PÉNAL BELGE	73
<i>Introduction</i>	73
Section 1. – Notions	74
Section 2. – Application du droit pénal belge.	75
I. <i>Intrusion dans un système informatique</i>	76
Section 1. – Intrusion externe.	76
1. – Éléments constitutifs matériels.	76
1.1. Accès ou maintien dans un système informatique .	76
a) Système informatique	76
b) Accès ou maintien.	77
c) Protection du système informatique.	78
d) Dommage causé au système informatique.	79
1.2. Absence totale d'autorisation.	80
a) Autorisation expresse	80
b) Autorisation tacite.	81

2. – Élément moral : volonté d'accès au système et connaissance de l'absence d'autorisation	82
Section 2. – Intrusion interne	83
1. – <i>Éléments constitutifs matériels</i>	83
1.1. Existence d'une autorisation partielle	83
1.2. Dépassement de l'autorisation	85
2. – Élément moral	85
2.1. Volonté d'outrepasser son autorisation	85
2.2. Intention spéciale : frauduleuse ou dessein de nuire	85
Section 3. – Circonstances aggravantes de l'intrusion	86
1. – Reprise des données	86
2. – Utilisation du système visité	87
3. – Dommage au système informatique ou aux données	88
Section 4. – Hacking éthique et intrusion	88
II. <i>Infractions connexes à l'intrusion</i>	90
Section 1. – Tentative d'intrusion	90
Section 2. – Mise à disposition de moyens pour faciliter une intrusion	91
1. – Éléments constitutifs matériels	91
2. – Élément moral	92
Section 3. – Ordre ou incitation	92
1. – Éléments constitutifs matériels	93
2. – Élément moral	93
Section 4. – Recel de données informatiques obtenues suite à une intrusion	93
1. – Éléments constitutifs matériels	94
1.1. Détention, révélation, divulgation ou encore usage quelconque	94
1.2. ... de données stockées, traitées ou transmises par un système informatique préalablement obtenues par la commission d'une intrusion informatique	94
2. – Élément moral	95
Section 5. – Hacking éthique et infractions connexes à l'intrusion	95
III. <i>Violation de données informatiques</i>	96
Section 1. – Éléments constitutifs matériels	97
1. – Introduction, modification ou suppression de données informatiques par tout moyen technologique	97

2. – Absence d'autorisation	98
Section 2. – Élément moral.	98
Section 3. – Circonstances aggravantes	98
1. – Intention frauduleuse ou but de nuire.	98
2. – Dommage aux données	98
3. – Entrave au fonctionnement du système.	98
Section 4. – Mise à disposition de moyens pour faciliter la violation de données	99
1. – Éléments constitutifs matériels.	99
2. – Élément moral	100
Section 5. – Tentative	100
Section 6. – Hacking éthique et violation de données informatiques	100
IV. <i>Infractions relatives au secret des communications</i>	101
Section 1. – Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique	101
1. – Élément matériel	102
1.1. Interception, prise de connaissance ou enregistrement, à l'aide d'un appareil	102
1.2. Communications non accessibles au public, auxquelles on ne prend pas part.	103
1.3. Absence de consentement des participants	104
2. – Élément moral	104
Section 2. – Actes préparatoires	105
1. – Installation d'un appareil	105
1.1. Élément matériel.	105
1.2. Élément moral	105
2. – Partage d'un dispositif	105
2.1. Éléments constitutifs matériels	105
2.2. Élément moral	105
Section 3. – Recel de communications illicitement obtenues	106
1. – Élément matériel	106
1.1. Contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont on a pris connaissance illégalement	106
1.2. Détention, révélation, divulgation à une autre personne ou utilisation d'une manière quelconque	106
2. – Élément moral	106

TABLE DES MATIÈRES	371
Section 4. – Tentative	107
Section 5. – Secret des communications électroniques	107
1. – Éléments constitutifs matériels	107
1.1. Autorisation des personnes directement ou indirectement concernées	107
1.2. Prise de connaissance intentionnelle de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement	108
a) Information transmise par voie de communication électronique	108
b) Information de toute nature qui ne lui est pas destinée personnellement	109
1.3. Identification intentionnelle des personnes concernées par la transmission de l'information et son contenu	109
1.4. Prise de connaissance de données en matière de communications électroniques et relatives à une autre personne	109
1.5. Modification, suppression, révélation, stockage ou usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non	110
2. – Élément moral	110
3. – Exceptions prévues par l'article 125 de la loi	110
Section 6. – Hacking éthique et secret des communications	111
<i>Conclusions</i>	113
PROTECTION DES BANQUES ET DE LEURS CLIENTS CONTRE LES CYBERCRIMINELS PAR LE DROIT PÉNAL FRANÇAIS	115
<i>Introduction</i>	115
I. <i>Cybercriminalité en matière bancaire</i>	116
Section 1. – À l'égard des clients de la banque	117
Section 2. – À l'égard de la banque elle-même	118
II. <i>Réponse pénale à la cybercriminalité en matière bancaire</i>	121
Section 1. – Incriminations utiles figurant dans le Code pénal	121
Section 2. – Dispositions du Code monétaire et financier	124
III. <i>Réponse pénale efficace ?</i>	125
Section 1. – Difficultés des poursuites	125

Section 2. – Réponse technique préférable.	127
Section 3. – Réponse civile utile.	128
<i>Conclusion.</i>	130

TROISIÈME PARTIE :

La procédure pénale face aux défis de la société numérique

RECHERCHE POLICIÈRE ET JUDICIAIRE SUR INTERNET : ANALYSE CRITIQUE DU NOUVEAU CADRE LÉGISLATIF BELGE.	133
<i>Introduction.</i>	133
I. <i>Recherche non secrète et recherche secrète dans un système informatique</i>	135
Section 1. – Recherche non secrète dans un système informatique qui a été saisi et qui est non verrouillé (art. 39bis, § 2, al. 1 ^{er} , C.i.cr.)	139
Section 2. – Recherche informatique non secrète dans un système informatique qui n'a pas été saisi mais était susceptible de l'être (art. 39bis, § 2, al. 2, C.i.cr.)	148
Section 3. – Recherche informatique non secrète dans un système informatique qui a été saisi mais nécessitant le recours à des dispositifs techniques (art. 39bis, § 2, al. 2 et § 5, al. 1 ^{er} , C.i.cr.)	149
Section 4. – Recherche non secrète dans un système informatique saisi avec extension de la recherche (art. 39bis, § 3 et § 5, al. 1 ^{er} , C.i.cr.)	151
Section 5. – Recherche non secrète dans un système informatique avec extension de la recherche et moyennant le recours à des dispositifs techniques (art. 39bis, §§ 3-4 et 5, al. 2, C.i.cr.)	158
Section 6. – Recherche secrète dans un système informatique (art. 90ter C.i.cr.)	161
II. <i>Conservation rapide de données informatiques</i>	165
Section 1. – Niveau national (art. 39ter C.i.cr.)	167
Section 2. – Niveau international (art. 39quater C.i.cr.)	173
1. – Demande de conservation rapide émise par les autorités belges (art. 39quater, § 1 ^{er} , C.i.cr.)	173
2. – Demande de conservation rapide adressée aux autorités belges (art. 39quater, § 2, C.i.cr.)	176
III. <i>Contrôle visuel discret</i>	179
IV. <i>Infiltration sur internet</i>	184

<i>V. Obligations de collaboration des fournisseurs de services : Yahoo-isation et quelques autres modifications pertinentes.</i>	196
Section 1. – Champ d'application personnel des obligations de collaboration	197
Section 2. – Champ d'application territorial des obligations de collaboration	202
Section 3. – Quelques autres modifications pertinentes	205
<i>VI. Création d'une banque de données d'empreintes vocales</i>	209
<i>Conclusion.</i>	213
<i>Postface.</i>	214
MESURES D'INVESTIGATION FACE AU DÉFI NUMÉRIQUE EN DROIT FRANÇAIS	217
<i>Introduction.</i>	217
I. Adaptation des mesures d'investigation existantes.	220
Section 1. – Adaptation des perquisitions et saisies	220
1. – Perquisition des systèmes informatiques	221
2. – Saisies de données informatiques	224
Section 2. – Adaptation des réquisitions.	227
1. – Réquisitions aux fins de communication des données informatiques	227
2. – Réquisitions aux fins de déchiffrement des données cryptées	230
II. Adoption de mesures d'investigation innovantes.	232
Section 1. – Adoption de mesures d'investigation plus clandestines	232
1. – Recours à une fausse identité	232
2. – Respect de la loyauté de la preuve	235
Section 2. – Adoption de mesures d'investigation plus intrusives.	237
1. – Captations massives de données personnelles	238
2. – Respect au droit à la vie privée et de famille	240
<i>Conclusion.</i>	244
CONSERVATION DES DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES EN BELGIQUE : UN JUSTE ÉQUILIBRE ?	245
<i>Introduction.</i>	245
I. De la loi de 2005 sur les communications électroniques à la loi de 2016 sur la rétention des données de communication	246
II. Loi du 29 mai 2016 : une question de proportionnalité ?	248

Section 1. – Enjeux.	248
Section 2. – Garanties.	249
1. – Accès aux données modulé en fonction de la finalité, de la nature des données et de la gravité de l'infraction.	249
2. – Autres garanties procédurales.	252
3. – Obligations relatives à la sécurisation des données . . .	253
Section 3. – Équilibre bouleversé : l'arrêt Tele2 du 21 décembre 2016 et l'avis 1/15	254
1. – Arrêt Tele2 : une lecture stricte du principe de proportionnalité	254
2. – Quel avenir pour l'obligation de conservation généralisée des données de communication ?	258
3. – Impact sur le système belge de conservation des données de communication	263
<i>Conclusion.</i>	265

QUATRIÈME PARTIE : La coopération internationale face aux défis de la société numérique

CROSS-BORDER GATHERING OF ELECTRONIC EVIDENCE: MUTUAL LEGAL ASSISTANCE, ITS SHORTCOMINGS AND REMEDIES	269
I. <i>Shortcomings of mutual legal assistance</i>	271
II. <i>Existing alternatives</i>	273
Section 1. – Voluntary (direct) cooperation	274
Section 2. – Unilateral access.	275
Section 3. – European Investigation Order	277
III. <i>The Commission's e-evidence initiative</i>	277
Section 1. – The draft Regulation	279
Section 2. – The draft Directive	281
IV. <i>The CLOUD Act</i>	283
<i>Conclusions</i>	284
COLLECTE TRANSFRONTALIÈRE DE PREUVES NUMÉRIQUES SELON LE POINT DE VUE BELGE. LA DÉCISION D'ENQUÊTE EUROPÉENNE, UN MOYEN APPROPRIÉ ?	287
<i>Introduction.</i>	287
I. <i>Preuves numériques – définition</i>	288

II. <i>Récolte de preuves numériques au moyen de la décision d'enquête européenne</i>	291
Section 1. – Émission d'une décision d'enquête européenne portant sur la collecte de preuves numériques	291
1. – Autorités nationales compétentes	291
2. – Champ d'application procédural et personnel.	294
3. – Mesures d'enquête pouvant être sollicitées via une décision d'enquête européenne	296
3.1. Dispositions générales : toute mesure d'enquête ..	296
3.2. Exception : les équipes communes d'enquête	296
3.3. Spécificités de certaines mesures d'enquête	297
a) Exécution d'une mesure d'enquête requérant l'obtention de preuves en temps réel.	298
b) Interception de télécommunications visée à l'article 90 ^{ter} du Code d'instruction criminelle	299
3.4. Assistance des autorités étrangères par des autorités belges	300
4. – Procédure d'émission d'une décision d'enquête européenne.	301
5. – Utilisation en Belgique des éléments de preuve recueillis irrégulièrement à l'étranger – La clause Antigoon.	302
Section 2. – Exécution d'une décision d'enquête européenne portant sur la collecte de preuves numériques	304
1. – Autorités nationales belges compétentes	304
1.1. En vue de la réception de la décision d'enquête européenne.	305
1.2. En vue de l'exécution de la décision d'enquête européenne.	305
2. – Procédure d'exécution d'une décision d'enquête européenne en droit belge	306
2.1. Délais	306
2.2. Causes de refus d'exécution	307
2.3. Décision relative à l'exécution de la mesure d'enquête sollicitée	311
2.4. Droit applicable.	312
2.5. Intervention d'autorités de l'État d'émission	313
3. – Sort des preuves recueillies à l'issue de l'exécution de la décision d'enquête européenne	313

III. <i>Collaboration directe avec les fournisseurs de services d'information : une méthode plus efficace pour assurer la collecte transfrontière des preuves numériques ?</i>	316
Section 1. – Obligation de coopération relativement large	317
Section 2. – Destinataires de l'obligation : les opérateurs de réseaux et les fournisseurs de services au sens large	318
Section 3. – Collaboration « en temps réel » ou au moment déterminé dans la réquisition	321
Section 4. – Appréciation souple du principe de territorialité ?	322
<i>Conclusion.</i>	323
PROTECTION DES DONNÉES DANS LE SECTEUR DE LA « POLICE » ET DE LA « JUSTICE »	327
<i>Introduction.</i>	327
I. <i>Instruments de protection des données dans le secteur de la police et de la justice</i>	329
II. <i>Titre 2 de la loi du 30 juillet 2018</i>	333
Section 1. – Champ d'application matériel	333
Section 2. – Principes relatifs aux traitements de données à caractère personnel	337
1. – Principes de licéité et de loyauté	337
2. – Principe de finalité	339
3. – Principe d'exactitude	340
4. – Durée de conservation des données	341
Section 3. – Catégories de personnes concernées	343
Section 4. – Catégories particulières de données	346
Section 5. – Droits des personnes concernées	349
Section 6. – Prise de décision individuelle automatisée et profilage	354
Section 7. – Principe de sécurité des données	355
Section 8. – L'autorité de contrôle indépendante	359
Section 9. – Transferts internationaux de données	362
<i>Conclusion.</i>	365
Table matières	367