

Le devoir d'informer lors d'une violation de la sécurité des données

Avec un regard particulier
sur les données bancaires

Célian Hirsch

TABLE DES MATIÈRES

REMERCIEMENTS	VII
SOMMAIRE	IX
INTRODUCTION	1
L'intérêt du thème	1
I. L'évolution de la protection des données	1
II. Un « nouveau » devoir: le devoir d'informer lors d'une violation de la sécurité	3
III. L'augmentation des violations de la sécurité des données	5
Le plan, quelques problématiques et la délimitation du thème	7
PREMIÈRE PARTIE: LES NOTIONS	13
§ 1. Les données personnelles	13
I. Un cas introductif: la transmission de données bancaires pseudonymisées aux États-Unis	13
II. La notion de données personnelles	14
A. La définition légale	14
B. L'information	15
C. Concernant une personne physique	16
1. Une référence...	16
2. ... à une personne physique	18
D. Les données des personnes morales	18
1. La protection des personnes morales sous l'empire de l'aLPD	18
2. L'exclusion des personnes morales lors de la révision de l'aLPD	19
3. La protection des données des personnes morales hors LPD	21
a) La protection contre l'État	21
i) Le droit à l'autodétermination informationnelle	21
ii) L'exigence d'une base légale	23
iii) Les obligations positives	25
b) La protection contre les particuliers	26
i) Le droit de la personnalité des personnes morales (art. 53 cum 28 CC)	27
ii) Un droit à l'autodétermination informationnelle fondé sur l'art. 28 CC?	29
E. Personne identifiée ou identifiable	32

III.	La pseudonymisation, l'anonymisation et la réidentification des données personnelles	33
A.	La pseudonymisation	33
1.	Pour l'auteur de la pseudonymisation	34
2.	Pour les autres personnes	35
a)	L'approche absolue	35
b)	L'approche subjective	36
c)	La solution retenue par la jurisprudence	37
d)	Notre approche	38
B.	L'anonymisation	39
C.	La réidentification	40
1.	La sécurité de la clé	40
2.	L'identité retrouvée	41
a)	Les efforts raisonnables	41
b)	L'intérêt concret	44
c)	La temporalité	45
d)	Une brève synthèse	45
D.	Le fardeau de la preuve	46
1.	Les faits dirimants	47
2.	La distinction entre le recoupement intrinsèque et le recoupement extrinsèque	47
3.	Le fardeau de la preuve du recoupement extrinsèque	48
4.	Notre conclusion	49
IV.	Une synthèse	50
§ 2.	La notion de données bancaires	51
I.	Un cas introductif: l'affaire SWIFT	52
II.	Les données bancaires protégées par la LPD	53
A.	La notion de « responsable du traitement »	54
B.	La responsabilité conjointe	56
C.	La notion de « sous-traitant »	56
D.	La banque comme « responsable du traitement »	57
III.	Les données protégées par le secret bancaire	59
A.	La portée et le fondement du secret bancaire	59
B.	Le critère de l'identification	60
IV.	Les données critiques	62
V.	Une synthèse	64
§ 3.	La notion de violation de la sécurité	65
I.	Un cas introductif: la violation de la sécurité au sein d'un groupe de sociétés	65
II.	Une notion large	66
A.	La définition légale	66

B.	Les deux approches	67
1.	L'approche de la mise en danger	68
2.	L'approche de la prise de connaissance effective	70
3.	La violation de la sécurité comme une approche mixte	71
C.	L'absence d'exigence de faute ou d'illicéité	74
1.	L'absence d'exigence de faute	74
2.	L'absence d'exigence d'illicéité	75
D.	La distinction avec le principe de sécurité des données	77
1.	Le principe de sécurité des données	77
a)	Le principe de sécurité selon l'art. 8 LPD et l'art. 32 RGPD	77
b)	L'évaluation du risque	79
c)	Les mesures de sécurité	81
2.	La distinction entre le principe de sécurité et la violation de la sécurité des données	81
III.	Les cas de violation de la sécurité	84
A.	La perte	85
B.	L'altération	86
C.	La divulgation non autorisée	87
D.	L'accès non autorisé	88
1.	Un accès... ..	88
2.	...concret... ..	89
3.	...non autorisé	91
a)	En général	91
b)	L'accès non autorisé par des employés	93
IV.	Une synthèse	94
§ 4.	Une synthèse des notions	95

DEUXIÈME PARTIE: LES FONCTIONS, LES SOURCES ET LES CONDITIONS DU DEVOIR D'INFORMER LORS D'UNE VIOLATION DE LA SÉCURITÉ 99

§ 5.	Les fonctions et la limite du devoir d'informer lors d'une violation de la sécurité	99
I.	L'information en faveur de l'autorité	100
A.	La surveillance de la sécurité des données	100
B.	L'aide aux administrés	102
C.	L'effet préventif	106
II.	L'information en faveur des personnes concernées	110
A.	La protection de la personnalité et des droits fondamentaux	111
B.	L'effet préventif	112
C.	La confiance entre le responsable du traitement et les personnes concernées	113

D.	La possibilité d'invoquer ses droits	114
E.	La validité du consentement?	116
F.	Une sanction?	117
III.	La limite de l'information: la surcharge informationnelle	118
IV.	Une synthèse	121
§ 6.	Les sources et les conditions du devoir d'informer	
	lors d'une violation de la sécurité	122
I.	Un cas introductif: la violation de la sécurité subie par Swisscom	124
II.	La protection des données	126
A.	Le contexte et l'évolution réglementaire	126
1.	L'influence du droit européen dans la révision totale de la loi sur la protection des données de 1992	126
2.	L'influence du droit européen dans l'interprétation de la LPD	130
B.	Le devoir d'informer l'autorité compétente en matière de protection des données	134
1.	Ancienne LPD	134
2.	Convention 108 modernisée	135
3.	L'art. 33 par. 1 RGPD	136
a)	Le principe du devoir d'information	137
b)	L'évaluation du risque	137
i)	La notion de risque	137
ii)	Les éléments déterminants	138
iii)	Une approche concrète	141
iv)	La réévaluation	143
c)	L'information à l'autorité de contrôle	143
4.	L'art. 24 al. 1 LPD	144
5.	Les droits cantonaux	151
a)	Zurich	151
b)	Genève	152
C.	Le devoir d'informer les personnes concernées	153
1.	Ancienne LPD	153
2.	Convention 108 modernisée	154
3.	Le droit à l'autodétermination informationnelle (art. 13 al. 2 Cst.)	154
4.	L'art. 34 par. 1 RGPD	157
5.	L'art. 24 al. 4 LPD	159
a)	L'existence d'un risque (élevé)?	160
b)	Lorsque cela est nécessaire à sa protection	162
c)	Lorsque le Préposé l'exige	164
6.	Les droits cantonaux	165
a)	Zurich	165
b)	Genève	166

D.	Le devoir du sous-traitant d'informer le responsable du traitement (art. 24 al. 3 LPD et art. 33 par. 2 RGPD)	167
1.	Les normes légales: l'art. 24 al. 3 LPD et l'art. 33 par. 2 RGPD	167
2.	Le but de ce devoir	167
3.	La nature légale ou contractuelle de ce devoir	168
4.	Le devoir du sous-traitant ultérieur	170
E.	Une brève synthèse	173
III.	Le droit civil	174
A.	Les règles de la bonne foi	175
1.	La bonne foi dans la LPD (art. 6 al. 2 LPD)	175
a)	Le texte légal: l'art. 6 al. 2 LPD (art. 4 al. 2 aLPD)	175
b)	La bonne foi dans l'aLPD (art. 4 al. 2 aLPD)	175
c)	Pas davantage d'information aux personnes concernées	177
d)	Mais un devoir d'informer les tiers en faveur des personnes concernées	177
2.	La bonne foi hors LPD (art. 2 al. 1 CC)	179
B.	La protection de la personnalité (art. 28 CC)	183
1.	La violation de la sécurité comme atteinte à la personnalité?	183
2.	Le devoir d'informer découlant de l'atteinte à la personnalité?	186
C.	L'incombance de réduire le dommage (art. 44 al. 1 CO)	187
D.	L'interdiction de créer un état de fait dangereux	189
E.	Des contrats	191
1.	Le mandat (art. 398 al. 2 CO)	191
a)	Le devoir de discrétion	192
b)	Le devoir d'information	193
i)	Quelques généralités	193
ii)	L'existence d'un devoir d'information lors d'une violation de la sécurité	193
iii)	La prise en compte du risque pour la personnalité du mandant	194
iv)	La prise en compte de la violation du devoir de discrétion	195
2.	Le contrat de travail	196
a)	L'obligation de l'employeur d'informer l'employé d'une violation de la sécurité (art. 328 CO)	196
i)	L'obligation de protéger la personnalité de l'employé	196
ii)	La distinction avec le devoir d'informer prévu par l'art. 24 al. 4 LPD	196
aa)	L'application concurrente de la LPD	196
bb)	Les buts communs de l'art. 328 CO et de la LPD	197
cc)	L'absence de la surcharge informationnelle en droit du travail	197
iii)	Le critère du risque, et son seuil, pour déterminer l'existence d'un devoir d'informer à la charge de l'employeur	198

b) L'obligation de l'employé d'informer l'employeur d'une violation de la sécurité (art. 321a al. 1 CO)	199
3. Les contrats entre responsables du traitement et les contrats de sous-traitance	201
a) Une disposition contractuelle spécifique: la liberté contractuelle	201
b) Une disposition contractuelle type: les clauses contractuelles types	202
F. Une brève synthèse	205
IV. Le droit bancaire et financier	206
A. L'obligation d'informer la FINMA (art. 29 al. 2 LFINMA)	206
1. Les personnes visées par l'obligation d'informer la FINMA	207
a) Les assujettis	207
b) Les sociétés d'audits	210
i) L'obligation générale de l'art. 29 al. 2 LFINMA	210
ii) L'obligation spécifique de l'art. 27 LFINMA	210
iii) L'obligation spécifique de l'art. 30 LSA	212
c) Les sous-traitants de banques, d'assurances et d'établissements financiers	212
i) Les dispositions légales pertinentes: l'art. 23 ^{bis} al. 1 LB, l'art. 47 al. 2 LSA et l'art. 64 al. 1 LFin	212
ii) Une critique de cette obligation d'information directe à l'autorité	213
2. La portée générale de l'art. 29 al. 2 LFINMA	215
3. Le devoir d'annoncer les cyberattaques (Communication sur la surveillance 05/2020)	217
a) La distinction entre cyberattaque et violation de la sécurité des données	218
b) Les actifs d'importance critique	219
c) La mise en danger des objectifs de protection	219
d) Le constat de ce devoir d'annonce: des défaillances à corriger	220
4. Le devoir d'annoncer les incidents importants relatifs aux données critiques (Circulaire 2023/1)	221
5. Une appréciation	222
B. L'obligation d'informer l'organisme de surveillance	223
C. L'obligation d'informer les clients	224
1. Une importante violation de la sécurité de CID	224
2. La garantie de l'activité irréprochable (art. 3 al. 2 let. c LB et art. 11 LFin)	226
V. Le droit étranger	227
A. L'obligation d'informer des prestataires de services de paiement	227
1. L'art. 96 de la Directive concernant les services de paiement (DSP2)	227

2. Application indirecte en Suisse	228
3. L'incident majeur	229
B. Le <i>SHIELD Act</i> de l'État de New York	230
1. Les données personnelles et privées	231
2. La notion de breach of the security of the system	231
3. L'application extraterritoriale	232
4. Le principe de l'information	232
§ 7. Une synthèse	233

TROISIÈME PARTIE : L'ÉTENDUE, LES RESTRICTIONS ET LES MODALITÉS DU DEVOIR D'INFORMER LORS D'UNE VIOLATION DE LA SÉCURITÉ 239

§ 8. L'étendue du devoir d'information	239
I. Un cas introductif: les données d'un prestataire informatique sur le dark web	239
II. L'information aux autorités administratives	240
A. L'information à l'autorité de contrôle européenne (art. 33 par. 3 RGPD)	240
1. La nature de la violation de la sécurité (art. 33 par. 3 let. a RGPD)	242
2. Les conséquences de la violation de la sécurité (art. 33 par. 3 let. c RGPD)	243
3. Les mesures prises ou proposées pour remédier à la situation (art. 33 par. 3 let. d RGPD)	244
B. L'information au PFPDT (art. 24 al. 2 LPD et art. 15 al. 1 OPDo)	247
C. L'information à la FINMA (art. 29 al. 2 LFINMA)	249
III. L'information aux personnes concernées	250
A. Au regard du RGPD (art. 33 par. 2 RGPD)	250
1. En général	250
2. Les mesures prises ou à prendre	251
3. Des recommandations?	252
B. Au regard de la LPD (art. 15 al. 3 OPDo)	254
C. Au regard du droit civil	255
IV. L'information du sous-traitant au responsable du traitement	257
§ 9. Les restrictions du devoir d'information	258
I. Un cas introductif: la violation de la sécurité qui met en lumière une infraction pénale	258
II. Les restrictions pour l'information aux autorités: le principe <i>nemo tenetur se ipsum accusare</i>	259
A. Un rappel du principe <i>nemo tenetur</i> sous l'angle de l'art. 6 CEDH	260
1. L'accusation en matière pénale	260

a) La nature des sanctions	260
b) L'application temporelle	262
2. La contrainte abusive	264
3. Les conséquences de l'application du principe <i>nemo tenetur</i>	265
4. Les restrictions au principe <i>nemo tenetur</i>	266
a) Les pre-existing documents	266
b) La distinction entre les personnes physiques et morales	268
c) Les questions purement factuelles	269
d) L'existence d'un intérêt public	270
5. Des limites peu prévisibles	270
B. Son application vis-à-vis des autorités de contrôle européennes	271
1. L'application du principe <i>nemo tenetur</i> lors de l'obligation d'informer d'une violation de la sécurité	272
a) Le caractère pénal des sanctions prévues par le RGPD	272
b) L'application du principe <i>nemo tenetur</i> avant l'existence de soupçons	273
2. La contrainte abusive	274
3. Les conséquences de l'application du principe <i>nemo tenetur</i>	276
4. Les restrictions au principe <i>nemo tenetur</i>	276
a) Les pre-existing documents	276
b) La distinction entre les personnes physiques et morales	279
5. La solution allemande	280
C. Son application vis-à-vis du Préposé fédéral à la protection des données et à la transparence	282
1. Un bref rappel des pouvoirs du Préposé fédéral	282
2. Les conséquences de l'absence de sanctions pénales	283
3. La décision du Préposé avec menace de sanction pénale	284
D. Son application vis-à-vis de la FINMA	285
1. La « contrainte abusive » de la FINMA	286
a) Les mesures de la FINMA comme « accusation en matière pénale »	286
b) La sanction pénale	288
i) La sanction pénale d'office	288
ii) La décision avec menace pénale	289
E. Une brève synthèse	291
III. Les restrictions pour l'information aux personnes concernées	292
A. Le régime en protection des données	292
1. Les restrictions en droit européen (art. 34 par. 3 RGPD)	292
a) Les mesures de protection techniques et organisationnelles appropriées	293
b) Les mesures postérieures	294
i) Selon le genre de l'atteinte	295
ii) Des mesures immédiates?	296

iii) Une diminution ou suppression du risque?	297
c) Les efforts disproportionnés (art. 34 par. 3 let. c RGPD)	297
i) La condition des efforts disproportionnés	298
aa) Le nombre important de personnes concernées?	298
bb) Le temps nécessaire pour communiquer directement?	299
cc) Une application restrictive?	300
ii) La communication publique	301
d) Les autres restrictions possibles	302
i) L'article 23 RGPD	302
ii) L'article 29 BDSG	303
iii) Des restrictions possibles en Suisse?	304
2. Les restrictions en droit suisse (art. 24 al. 5 LPD)	305
a) Les intérêts prépondérants d'un tiers ou l'intérêt public l'exigent	306
i) Les intérêts prépondérants d'un tiers l'exigent (art. 24 al. 5 let. a cum art. 26 al. 1 let. b LPD)	306
aa) Son application comme restriction au droit d'accès (art. 26 al. 1 let. b LPD)	306
bb) Son application comme restriction au devoir d'informer lors d'une violation de la sécurité des données	307
ii) L'intérêt public prépondérant ou la confidentialité l'exigent (art. 24 al. 5 let. a cum art. 26 al. 2 let. b LPD)	308
aa) Son application comme restriction au droit d'accès (art. 26 al. 2 let. b LPD)	309
bb) Son application comme restriction au devoir d'informer lors d'une violation de la sécurité des données	310
b) Un devoir légal de garder le secret l'interdit (art. 24 al. 5 let. a in fine LPD)	311
i) L'interprétation systématique	312
aa) La délégation du traitement et l'obligation légale de garder le secret (art. 9 al. 1 let. b LPD)	312
bb) Le devoir d'information général et l'obligation légale de garder le secret (art. 20 al. 1 let. c LPD) ...	313
cc) Le devoir d'informer lors d'une violation de la sécurité des données et l'obligation légale de garder le secret (art. 24 al. 5 let. a in fine LPD)	313
c) L'information impossible ou disproportionnée (art. 24 al. 5 let. b LPD)	315
i) L'information impossible	315
ii) Les efforts disproportionnés	316
d) La communication publique (art. 24 al. 5 let. c LPD)	317
e) Les mesures postérieures?	319
f) La renonciation par la personne concernée?	319

B.	Le régime en droit civil	321
1.	La bonne foi	321
2.	Le mandat	322
3.	Le contrat de travail	323
§ 10.	Les modalités du devoir d'information	324
I.	La forme	324
A.	La forme de l'annonce aux autorités	325
1.	Les autorités européennes	325
2.	Les autorités suisses	326
B.	La forme de l'annonce aux personnes concernées	327
1.	En droit européen (art. 34 par. 2 RGPD)	327
a)	Une communication « en des termes clairs et simples »	327
b)	Une communication propre	329
c)	La langue de la communication	329
d)	Le moyen de communication	330
2.	En droit suisse	331
II.	Le délai	334
A.	Le début du délai	334
1.	Le droit européen: la prise de connaissance de la violation	334
a)	La brève enquête	334
b)	L'analogie avec le Règlement n° 611/2013	336
c)	La connaissance effective ou également imputable?	337
d)	La marge d'appréciation importante	339
2.	Le droit suisse	340
a)	En protection des données	340
b)	En droit bancaire et financier	341
B.	La durée du délai pour les autorités administratives	343
1.	La durée du délai pour les autorités européennes (art. 33 par. 1 RGPD)	343
2.	La durée du délai pour le PFPDT	345
3.	La durée du délai pour la FINMA	346
C.	La notification échelonnée	348
1.	En droit européen	348
2.	En droit suisse	350
a)	La notification échelonnée au PFPDT	350
b)	La notification échelonnée à la FINMA	352
D.	Le délai pour les personnes concernées	352
1.	Le délai en droit européen	352
2.	Le délai en droit suisse	355
III.	Le devoir de documenter	358
A.	En droit européen	358

B. En droit suisse	361
1. Une obligation légale invalide... ..	361
2. ... mais une documentation recommandée	362
§ 11. Une synthèse	363

QUATRIÈME PARTIE: LA TRANSMISSION AUX AUTORITÉS PÉNALES ET LE DROIT D'ACCÈS AU RAPPORT DE VIOLATION DE LA SÉCURITÉ

367

§ 12. La transmission du rapport aux autorités pénales et son exploitabilité	367
I. L'information de la FINMA aux autorités pénales	368
A. Le devoir d'informer de la FINMA en faveur des autorités pénales	368
1. Le principe: l'information spontanée (art. 38 al. 3 LFINMA)	368
2. L'exception: la restriction du transfert d'informations	369
a) La collaboration pourrait nuire à la surveillance des marchés financiers (art. 40 let. b LFINMA)	369
b) Pas de restriction selon le principe <i>nemo tenetur</i>	370
B. Le droit de la FINMA d'informer spontanément les autorités pénales	372
C. L'exploitabilité par les autorités pénales	374
1. Le principe <i>nemo tenetur</i> en faveur de l'assujetti ne s'applique pas	374
2. Le principe <i>nemo tenetur</i> en faveur de l'assujetti s'applique	375
a) La conséquence: l'inexploitabilité	375
b) La portée personnelle de l'inexploitabilité	376
i) Pour l'assujetti	377
aa) Le principe	377
bb) L'assujetti comme personne morale	377
ii) Pour les organes de l'assujetti	379
iii) Pour les employés non-organes	380
II. L'information de l'autorité européenne à l'autorité pénale – l'exemple allemand	381
III. L'information du Préposé fédéral aux autorités pénales	382
A. Le droit du Préposé d'informer les autorités pénales	382
1. La proposition de l'avant-projet: une obligation de dénoncer	382
2. La solution proposée et adoptée: un droit de dénoncer	383
B. La violation du principe <i>nemo tenetur</i> dans l'AP-LPD	383
C. La solution législative: l'art. 24 al. 6 LPD	384
1. La solution du Conseil fédéral... ..	384
2. ... adoptée par le Parlement	385
3. La portée personnelle de l'art. 24 al. 6 LPD	386
D. Excursus: une comparaison avec la solution proposée lors du devoir d'annoncer les cyberattaques	388

1. L'avant-projet: la même solution pour les annonces des cyberattaques (art. 73c AP-LSI)	388
2. Le projet: le principe <i>nemo tenetur</i> déjà applicable lors de l'annonce (art. 74e al. 4 P-LSI)	388
IV. Une brève synthèse	389
§ 13. Le droit au rapport de violation de la sécurité	390
I. Le rapport de violation de la sécurité peut-il être protégé par le secret de l'avocat?	392
II. Le droit matériel d'obtenir le rapport de violation de la sécurité	395
A. Le droit à l'encontre du responsable du traitement	396
1. Le droit à la reddition de compte (art. 400 CO)	396
a) Le but du droit à la reddition de compte	397
b) La portée du droit à la reddition de compte	398
c) Les limites du droit à la reddition de compte	398
i) La distinction entre les documents internes et ceux purement internes	399
ii) Les intérêts du mandataire	400
aa) Les intérêts du mandataire au maintien du secret (Geheimhaltungsinteressen des Beauftragten)	400
bb) La recherche disproportionnée	402
cc) Les documents déjà remis	402
iii) Les intérêts des tiers	403
aa) Le substitut (art. 399 al. 3 CO)	404
bb) L'employé du mandataire (art. 328 CO)	404
cc) Le tiers contre lequel le mandant pourrait avoir des droits (art. 401 CO)	407
dd) Tout autre tiers	407
d) Le droit à la reddition de compte et le rapport de violation de la sécurité	407
i) Le rapport permet de vérifier l'activité du mandant	408
ii) Les restrictions de l'accès au rapport de violation de la sécurité	409
aa) Le rapport n'est pas un document purement interne	409
bb) Les intérêts du mandataire au maintien du secret (Geheimhaltungsinteressen)	409
cc) Les intérêts des tiers	413
2. Le droit d'accès (art. 25 LPD)	413
a) Le rapport de violation de la sécurité contient des données personnelles	414
b) Le rapport de violation de la sécurité ne contient pas des données personnelles « en tant que telles »	415
c) Une requête abusive	416
3. Le droit à la remise de documents (art. 72 LSFin)	417

4. Une brève synthèse	419
B. Le droit à l'encontre des autorités fédérales	420
1. L'accès au rapport grâce au principe de la transparence (art. 6 LTrans)	420
a) Pas de transparence pour la FINMA?	420
i) La FINMA n'est pas soumise à la LTrans (art. 2 al. 2 LTrans)... ..	420
ii) ... mais la FINMA est soumise à l'art. 10 CEHD	421
aa) Le droit d'accès à l'information grâce à l'art. 10 CEHD	421
bb) L'application de la jurisprudence de la CourEDH au rapport de violation de la sécurité	424
1(a) Le but de la demande d'information	424
1(b) La nature des informations recherchées	425
1(c) Le rôle de la requérante	426
1(d) La disponibilité des informations	426
1(e) L'ingérence « nécessaire dans une société démocratique »?	426
b) La transparence à l'encontre du Préposé fédéral à la protection des données et à la transparence	427
i) Le rapport de violation de la sécurité constitue un document officiel	428
ii) Les exceptions à l'accès au rapport de violation de la sécurité	429
aa) Libre formation de l'opinion et de la volonté du Préposé (art. 7 al. 1 let. a LTrans)	430
bb) L'entrave à l'exécution de mesures concrètes du Préposé (art. 7 al. 1 let. b LTrans)	431
cc) La révélation des secrets par le PFPDT	432
dd) La garantie de confidentialité du Préposé (art. 7 al. 1 let. h LTrans)	434
iii) La protection de la sphère privée (art. 7 al. 2 LTrans) et des données (art. 9 LTrans)	436
aa) La protection de la sphère privée (art. 7 al. 2 LTrans)	437
bb) La protection des données (art. 9 LTrans)	438
cc) La pesée des intérêts (art. 7 et art. 9 LTrans)	439
2. L'accès aux données (art. 25 LPD) envers les autorités	440
3. Une brève synthèse	441
III. Le droit procédural d'obtenir le rapport de violation de la sécurité	442
A. Les moyens de preuve (art. 168 CPC), l'objet de la preuve (art. 150 CPC) et le droit à la preuve (art. 152 CPC)	442
B. En amont de la procédure au fond: la preuve à futur (art. 158 CPC)	443
1. La preuve à futur (art. 158 CPC)	443

2. L'accès au rapport de violation de la sécurité grâce à la preuve à futur	445
C. Dans la procédure au fond : l'obligation de collaborer (art. 160 CPC)	446
1. Le principe de l'obligation de collaborer (art. 160 CPC)	446
2. Les restrictions à l'obligation de collaborer	446
a) Les restrictions légales (art. 163 ss CPC)	446
b) Les restrictions extra-légales à l'obligation de collaborer	447
c) Les modalités de protection des intérêts (art. 156 CPC)	448
i) La restriction de l'accès à la preuve par la partie adverse	448
ii) L'interdiction de divulgation sous la menace pénale	449
D. Une brève synthèse	450
IV. Une brève synthèse	450

CINQUIÈME PARTIE : LES CONSÉQUENCES DU MANQUEMENT AU DEVOIR D'INFORMER LORS D'UNE VIOLATION DE LA SÉCURITÉ 453

§ 14. Les conséquences civiles	454
I. La responsabilité du débiteur de l'information	454
A. La violation du devoir d'informer	455
1. La violation du devoir d'informer comme violation du contrat ...	455
2. La violation du devoir d'informer comme acte illicite	455
a) Selon la théorie classique : l'illicéité de comportement	456
b) Selon la conception de WERRO : le manque de diligence	457
c) Une brève appréciation	457
B. Le préjudice et la causalité	458
1. Le préjudice et la causalité hypothétiques	458
a) En général	458
b) Lors d'une violation du devoir d'informer	459
i) Le vol des données de cartes de crédit	459
ii) Le vol de données bancaires et l'amnistie fiscale	460
iii) Le vol de données bancaires et les articles de presse dénigrants	461
c) Une brève appréciation	462
2. Un tort moral ?	463
a) Le tort moral lors d'une atteinte illicite à la personnalité	463
b) Une atteinte à la personnalité ?	464
c) Une gravité suffisante ?	467
i) La violation de la LPD	467
ii) La violation du devoir d'informer	469
d) Une autre satisfaction	471
e) En droit de l'Union européenne	472
f) Une brève appréciation	474
C. La faute	476

D.	Le fardeau de la preuve	479
1.	La preuve de la violation fautive du devoir d'informer	479
2.	La preuve de la causalité et du dommage	480
a)	En général	480
b)	Lors d'une violation du devoir d'informer	481
i)	Le vol des données de cartes de crédit	481
ii)	Le vol de données bancaires et l'amnistie fiscale	481
iii)	Le vol de données bancaires et les articles de presse dénigrants	482
E.	La prescription	483
1.	Le <i>dies a quo</i> en matière extracontractuelle	483
2.	Le <i>dies a quo</i> en matière contractuelle	487
F.	La violation du devoir d'informer de l'employé	488
G.	Une brève synthèse	489
II.	La résiliation immédiate du contrat	491
A.	La résiliation du contrat de travail	491
1.	La résiliation par l'employeur	491
2.	La résiliation par l'employé	492
B.	La résiliation du contrat de mandat	493
C.	La résiliation du contrat de sous-traitance	495
III.	L'invalidité du consentement	497
IV.	Une brève synthèse	497
§ 15.	Les conséquences administratives	499
I.	Les mesures pouvant être prises par le PFPDT	500
A.	L'investigation préalable	500
B.	L'enquête (art. 49 al. 1 LPD)	501
C.	La renonciation à l'enquête (art. 49 al. 2 LPD)	502
D.	L'obligation de collaborer (art. 49 al. 3 LPD)	504
E.	L'obligation d'informer le PFPDT ou d'informer les personnes concernées (art. 51 al. 3 let. f LPD)	505
F.	Les autres mesures (art. 51 al. 1 LPD)	506
II.	Les mesures pouvant être prises par la FINMA	507
III.	La coordination des procédures et l'assistance administrative	510
A.	La consultation préalable du PFPDT (art. 53 al. 1 LPD)	510
B.	La coordination des procédures (art. 53 al. 2 LPD)	512
C.	L'assistance administrative (art. 36 et 55 LPD)	513
IV.	Les sanctions prévues par le RGPD	515
A.	La fixation de l'amende en cinq étapes	516
1.	Identifier les traitements de données	517
2.	Déterminer le point de départ pour le calcul de l'amende	518
3.	Évaluer les facteurs aggravants ou atténuants	520

4. Déterminer le plafond de l'amende	521
5. Vérifier le montant final	521
B. L'application des sanctions contre un responsable du traitement ou sous-traitant suisse	522
1. L'amende contre le représentant (art. 27 RGPD) ?	522
2. La compétence de l'autorité d'un État membre à l'encontre d'une entreprise suisse	523
3. La notification de l'amende par une autorité étrangère à une entreprise suisse	524
a) La notification directe	524
b) La notification via le représentant	526
c) La notification par l'entraide judiciaire ou assistance internationale	527
§ 16. Les conséquences pénales	528
I. La violation du Code pénal	528
II. La violation de la LPD	530
A. L'avant-projet LPD	530
B. Le projet LPD	530
C. LPD	531
III. La violation des normes pénales des lois sur les marchés financiers	532
A. Les fausses informations (art. 45 LFINMA)	532
B. L'omission d'effectuer les annonces prescrites	534
1. Les textes légaux	534
2. L'interprétation doctrinale de l'art. 49 al. 1 let. b LB	534
3. Notre interprétation	536
§ 17. Une synthèse	541
 SYNTHÈSE GÉNÉRALE	545
CONCLUSIONS	555
1. Le passé: la mise en œuvre récente du devoir d'informer lors d'une violation de la sécurité	556
2. Le présent: le devoir d'informer atteint ses objectifs principaux	559
3. L'avenir: quel respect du devoir d'informer?	561
a) L'augmentation de cas entraînant un devoir d'annonce	561
b) La surveillance FINMA comparée à celle du PFPDT	562
c) Les faibles conséquences lors d'un manquement au devoir d'informer	563
d) Les conséquences en cas de respect du devoir d'informer	565
e) Le respect du devoir d'informer devra être vérifié	568

GENERAL SUMMARY	571
CONCLUSIONS	579
1. The Past: The Recent Implementation of the Duty to Inform in the Event of a Data Breach	580
2. The Present: The Duty to Inform Achieves its Main Objectives	582
3. The Future: How Will the Duty to Inform Be Respected?	584
a) Increase in Cases Requiring Notification	584
b) FINMA Oversight Compared to that of the FDPIC	585
c) Weak Consequences of Failing to Comply with the Duty to Inform ...	586
d) Consequences of Complying with the Duty to Inform	588
e) The Duty of Notification Needs Verification	590
ALLGEMEINE ZUSAMMENFASSUNG	593
FAZIT	603
1. Die Vergangenheit: Die jüngste Umsetzung der Informationspflicht bei einer Verletzung der Datensicherheit	604
2. Die Gegenwart: Die Informationspflicht erreicht ihre Hauptziele	607
3. Die Zukunft: Wie wird die Informationspflicht erfüllt?	609
a) Zunahme der Fälle, die eine Meldepflicht auslösen	609
b) Die FINMA-Aufsicht im Vergleich zur EDÖB-Aufsicht	610
c) Die geringen Folgen von Verletzungen der Informationspflicht	612
d) Die Folgen bei Einhaltung der Informationspflicht	614
e) Die Einhaltung der Informationspflicht muss überprüft werden.	617
ANNEXE	619
TABLEAU RÉCAPITULATIF	621
Tableau récapitulatif de la jurisprudence de la CourEDH relative au principe <i>nemo tenetur</i> entre 1993 et 2022	621
Situation 1: un suspect qui, menacé de subir des sanctions s'il ne témoigne pas, soit témoigne soit est puni pour avoir refusé de le faire	622
Situation 2: des pressions physiques ou psychologiques, souvent sous la forme de traitements contraires à l'art. 3 CEHD, sont exercées pour obtenir des aveux ou des éléments matériels	630
Situation 3: le recours par les autorités à un subterfuge pour extorquer des informations qu'elles n'ont pu obtenir par un interrogatoire	631
Situation 4: le suspect n'a pas été informé de son droit de garder le silence et/ou de son droit d'être assisté d'un avocat et il s'est auto-incriminé ou son silence a été interprété à sa charge	633

BIBLIOGRAPHIE	639
LISTE DES ABRÉVIATIONS	699
TABLE DES MATIÈRES	709