
Table des matières

Préface	15
Mathieu JEANDRON	
Chapitre 1. Les identités numériques	19
Maryline LAURENT, Julie DENOUEL, Claire LEVALLOIS-BARTH et Patrick WAELBROECK	
1.1. Introduction	19
1.2. Dimension juridique.	21
1.2.1. Les sanctions relatives à l'usurpation d'identité	23
1.2.1.1. Les sanctions relatives aux conséquences de l'usurpation d'identité numérique d'une personne physique	24
1.2.1.2. Le délit spécial d'usurpation d'identité	28
1.2.2. La sécurisation des supports de l'identité numérique	31
1.2.2.1. La difficile mise en place d'une carte nationale d'identité électronique.	31
1.2.2.2. L'interopérabilité de l'identité numérique à l'échelle européenne.	36
1.3. Dimension sociale sous l'angle de la représentation de soi en ligne.	47
1.3.1. L'identité numérique : au carrefour de la configuration des plates-formes et des tactiques des internautes.	47
1.3.1.1. L'identité personnelle par le prisme de la sociologie des usages	47
1.3.1.2. Identité et Web 2.0	48
1.3.2. Différentes logiques	49
1.3.2.1. Une logique expressive	49
1.3.2.2. Une logique de mise en visibilité	50
1.3.2.3. Une logique rationaliste	50

1.3.2.4. Une logique de la déprivatisation du soi	51
1.3.2.5. Une logique relationnelle	51
1.3.2.6. Une logique risquophile à des fins de reconnaissance	51
1.4. Dimension socio-économique	53
1.4.1. Introduction	53
1.4.1.1. Pourquoi s'intéresser à l'économie des identités numériques ? A-t-elle un impact sur l'économie réelle ?	53
1.4.1.2. Pas d'interactions directes entre agents économiques dans le modèle de référence (équilibre général).	55
1.4.1.3. Organisation de la discussion.	55
1.4.2. Les identités numériques : deux approches sociologiques	56
1.4.2.1. Le laboratoire d'identités	57
1.4.2.2. Gestion active d'identités multiples, manifestations et projection de soi	58
1.4.2.3. Boucle interactive entre la construction et la projection de soi	60
1.4.3. Approches économiques	61
1.4.3.1. Littérature économique sur l'identité	62
1.4.3.2. Economie de la protection de la vie privée.	65
1.4.3.3. Les marchés à plusieurs versants, la valorisation des données et le gratuit.	67
1.4.3.4. Asymétrie d'information et réputation	68
1.4.4. Conclusion	69
1.5. Dimension technologique	70
1.5.1. Les notions importantes	73
1.5.2. Les différents identifiants numériques.	74
1.5.3. La gestion des identités numériques	75
1.5.3.1. Schéma isolé ou en silos	76
1.5.3.2. Schéma centralisé	77
1.5.3.3. Schéma fédéré	77
1.5.3.4. Schéma centré sur l'utilisateur	78
1.5.4. Les normes	79
1.5.5. Les risques liés à l'identité numérique.	80
1.6. Conclusion	81
1.7. Bibliographie	81

Chapitre 2. La gestion d'identités par la fédération 91

Augustin DE MISCAULT

2.1. Les fondamentaux de la fédération d'identités	91
2.1.1. L'identité : un ensemble d'attributs à caractère personnel	92

2.1.2. La fédération d'identités : propager l'identité	92
2.1.3. Les concepts de la fédération d'identités	95
2.1.4. La confiance : un prérequis à la fédération d'identités	96
2.1.5. Les acteurs de la fédération d'identités	98
2.2. Les limites techniques des solutions avant la fédération d'identités	99
2.2.1. Faire du WebSSO au-delà d'un domaine DNS	99
2.2.1.1. Les gains du WebSSO : ergonomie, sécurité et administration	99
2.2.1.2. La limite du WebSSO : le domaine DNS	102
2.2.1.3. Les solutions de contournement avant la découverte de la fédération d'identités	103
2.2.1.4. La fédération d'identités : le WebSSO au-delà d'un domaine DNS	105
2.2.2. Propager l'identité de l'utilisateur dans des appels Web-services	106
2.2.2.1. La limite des Web-services : l'appel pour le compte d'un utilisateur	106
2.2.2.2. Les solutions de contournement avant la découverte de la fédération d'identités	108
2.2.2.3. La fédération d'identités : la propagation de l'identité dans des appels Web-services	110
2.3. La valeur d'usage de la fédération d'identités	111
2.3.1. Les catalyseurs de la fédération d'identités	111
2.3.2. Les cas d'utilisation de la fédération d'identités	112
2.3.3. Accéder à des applications en mode SaaS	113
2.3.3.1. Accéder à des applications en mode SaaS sans fédération d'identités	113
2.3.3.2. Les pré-requis à l'utilisation de la fédération d'identités	114
2.3.3.3. Accéder à des applications en mode SaaS avec la fédération d'identités	116
2.3.4. Echanger entre partenaires commerciaux et filiales	118
2.3.4.1. Donner accès à ses partenaires sans fédération d'identités	118
2.3.4.2. Donner accès à ses partenaires <i>via</i> la fédération d'identités	120
2.3.5. Sphère grand public : s'inscrire et accéder à une application en trois étapes	121
2.3.5.1. En moyenne, les internautes en France ont douze comptes	121
2.3.5.2. Les navigateurs Internet comme solution de mémorisation de l'identité ?	122

2.3.5.3. S’inscrire à une application <i>via</i> la fédération d’identités	122
2.3.5.4. Accéder à l’application <i>via</i> la fédération d’identités	124
2.4. SAML2.0 et OAuth2.0 : standards de fait de la fédération d’identités	125
2.4.1. SAML2.0	126
2.4.1.1. Principaux composants	126
2.4.1.2. Aperçu des spécifications	126
2.4.1.3. Des exemples du profil Web Browser SSO	127
2.4.2. OAuth2.0 : accéder à une ressource au nom d’un utilisateur	130
2.4.2.1. Anti-pattern de mot de passe	130
2.4.2.2. OAuth2.0	132
2.4.2.3. OAuth2.0 et les applications Web	133
2.4.2.4. OAuth2.0 et les applications basées sur un <i>user-agent</i>	134
2.4.2.5. OAuth2.0 et les applications natives (smartphone)	135
2.5. Conclusion	137
2.6. Bibliographie	138

Chapitre 3. Systèmes d’authentification 139

Christophe KIENNERT, Samia BOUZEFRANE et Pascal THONIEL

3.1. Introduction	139
3.1.1. Définition et enjeux de l’authentification	140
3.1.1.1. Identification, authentification, autorisation	140
3.1.1.2. Authentification simple et authentification mutuelle	141
3.1.1.3. Les enjeux de l’authentification	141
3.1.2. Les facteurs d’authentification des individus	142
3.1.3. Les fondamentaux sécuritaires des protocoles réseau	142
3.1.3.1. Les services de sécurité	142
3.1.3.2. Typologie des attaques réseau	143
3.1.4. Les principes de la cryptographie	145
3.1.4.1. La cryptographie symétrique	146
3.1.4.2. La cryptographie asymétrique	147
3.1.4.3. Les fonctions de hachage	148
3.2. Les principaux systèmes d’authentification	150
3.2.1. Les systèmes d’authentification à mot de passe statique	150
3.2.1.1. Mot de passe en clair	150
3.2.1.2. Mot de passe chiffré	151
3.2.1.3. Mot de passe haché	152
3.2.2. Les systèmes d’authentification de type défi-réponse	152
3.2.2.1. Principe du défi-réponse	152

3.2.2.2. Avec des fonctions de hachage	153
3.2.2.3. Avec des fonctions de chiffrement	154
3.2.2.4. Conclusion sur les systèmes de type défi-réponse	155
3.2.3. Les systèmes d'authentification à OTP	156
3.2.3.1. Le protocole S/KEY	157
3.2.3.2. Les OTP <i>hardware</i>	158
3.2.3.3. Les tables de codage	158
3.2.3.4. La vulnérabilité des OTP au <i>Man-in-the-Middle</i>	160
3.2.4. Les systèmes d'authentification biométrique	161
3.2.4.1. Définition et principes de la biométrie	161
3.2.4.2. Limitations des systèmes d'authentification biométriques	162
3.2.5. Le protocole TLS	163
3.2.5.1. Définition et principes du protocole TLS	163
3.2.5.2. L'identité numérique dans le protocole TLS	164
3.2.5.3. Limitations du protocole TLS	166
3.2.6. Le rôle des cartes à puce	167
3.3. L'authentification dans les systèmes de gestion d'identité	168
3.3.1. Les composants des systèmes de gestion d'identité	169
3.3.1.1. Description abstraite des composants	169
3.3.1.2. Sélecteurs d'identité et authentifieurs	170
3.3.1.3. Les protocoles de sécurisation des accès aux services Web	171
3.3.2. Les acteurs de la gestion d'identité	171
3.3.2.1. Liberty Alliance	171
3.3.2.2. Shibboleth	172
3.3.2.3. Higgins	173
3.3.2.4. OpenID	173
3.3.3. Les tendances du Web pour la gestion d'identité	174
3.4. Conclusion	174
3.5. Bibliographie	175

Chapitre 4. Gestion de la vie privée et protection des données à caractère personnel

Maryline LAURENT et Claire LEVALLOIS-BARTH

4.1. Introduction	179
4.2. Usage à risques des technologies de l'information	180
4.2.1. Intelligence ambiante	180
4.2.2. Communications et services	181
4.2.3. Réseaux sociaux	183

4.3. Aspects juridiques relatifs à la création, la collecte, l'utilisation et le partage des données à caractère personnel	184
4.3.1. Champ d'application	186
4.3.1.1. Notions clés	186
4.3.1.2. Critère d'application territoriale	191
4.3.1.3. Exclusion des copies temporaires	191
4.3.2. Principes clés	192
4.3.2.1. Principe de finalité(s) et de qualité des données personnelles	192
4.3.2.2. Principe de légitimation	193
4.3.2.3. Principe concernant les données personnelles sensibles	196
4.3.2.4. Principe de sécurité et de confidentialité	197
4.3.2.5. Principe de niveau de protection adéquat	198
4.3.2.6. Principe d'information préalable (ou principe de transparence)	200
4.3.2.7. Principe du droit d'interrogation et du droit de suite	201
4.3.2.8. Principe d'opposition	202
4.3.2.9. Principe de déclaration auprès de la CNIL	203
4.3.3. Sanctions et atteinte à l'image de marque	204
4.4. Solutions techniques de protection de la vie privée et des données personnelles	206
4.4.1. Plus de contrôle dans l'intelligence ambiante	206
4.4.2. Solutions d'anonymisation des communications	210
4.4.2.1. Eléments fondamentaux des réseaux IP	210
4.4.2.2. Techniques d'anonymisation du trafic	211
4.4.2.3. Solutions logicielles	213
4.4.3. Outils de protection des données personnelles lors de transactions	215
4.4.3.1. Langages d'expression de la vie privée	215
4.4.3.2. Traitement des données personnelles pendant une transaction	217
4.4.3.3. Traitement des données personnelles après une transaction	221
4.5. Pistes de recherche	222
4.5.1. Vers la fourniture d'outils atomiques, évolutifs et simples	223
4.5.1.1. Insuffisances des langages P3P et APPEL et besoin d'ontologies	223
4.5.1.2. Vers une administration et un contrôle facilités	225
4.5.1.3. Une certification comme gage de bonne conduite	227
4.5.1.4. Un service d'anonymat « sous contrôle »	227
4.5.2. Gestion des attributs personnels	228

4.5.3. Négociation des termes contractuels liés au respect de la vie privée	230
4.5.4. La réforme des règles européennes de protection des données personnelles	232
4.6. Conclusion	237
4.7. Bibliographie	237

Chapitre 5. L'identité numérique dans le Cloud computing 243

Christophe KIENNERT, Samia BOUZEFRANE

et Amira Faiza BENKARA MOSTEFA

5.1. Introduction	243
5.2. Les concepts du Cloud computing	243
5.2.1. Définition du Cloud computing	243
5.2.2. Le principe du Cloud computing	244
5.2.3. Les modèles de déploiement du Cloud computing	244
5.2.4. Les propriétés du Cloud computing	246
5.2.5. Les avantages du Cloud computing	247
5.3. Autres caractéristiques fondamentales du Cloud Computing	248
5.3.1. Les services du Cloud computing	248
5.3.2. Les acteurs du Cloud computing	250
5.3.3. Principales préoccupations	252
5.3.4. Les interactions inter-Clouds	253
5.3.5. Cloud computing et identité numérique	253
5.3.6. Au-delà de l'identité numérique dans le Cloud	254
5.4. Les solutions classiques de gestion de l'identité numérique dans le Cloud	255
5.4.1. Interactions client-Cloud	256
5.4.1.1. Cas d'un Cloud privé	256
5.4.1.2. Cas d'un Cloud public	257
5.4.2. Interactions inter-Clouds	260
5.4.2.1. Cas de Clouds de même niveau	260
5.4.2.2. Cas de Clouds imbriqués	261
5.4.3. Limites des solutions classiques de gestion d'identité dans le Cloud	262
5.5. Solutions alternatives pour la gestion de l'identité numérique dans le Cloud	263
5.5.1. <i>Identity as a Service</i>	263
5.5.2. <i>Authentication as a Service</i>	266
5.6. Gestion de la vie privée et des données personnelles dans le Cloud computing	269

5.6.1. Fédération d'identités et gestion des données personnelles	269
5.6.1.1. L'approche OpenID	270
5.6.1.2. L'approche SAML	271
5.6.1.3. Solutions existantes	271
5.6.2. Solutions pour la protection de la vie privée dans le Cloud	272
5.7. Conclusion	275
5.8. Bibliographie	276
Index	279