

Table des matières

Avant-propos	1
Remerciements	3
Introduction	7
Chapitre 1. De la philosophie de la trace aux traces numériques . .	15
1.1. La trace comme <i>vestigium</i> et empreinte	15
1.2. La trace comme empreinte à valeur d'indice et de signe	19
1.3. La trace chez Heidegger, Levinas et Derrida	25
1.4. Analyse critique du concept de trace numérique	29
Chapitre 2. Formalisme associé aux projections algorithmiques . .	37
2.1. Introduction au formalisme	37
2.2. Formalisme projectif	38
2.2.1. Algorithme	39
2.2.2. Système	40
2.2.3. Projection algorithmique	41
2.2.4. Définition d'une projection algorithmique	41
2.2.5. Projection algorithmique instantanée	42
2.2.6. Partition d'accessibilité	42
2.2.7. Partition de libre arbitre	43

2.2.8. S-projection algorithmique d'un opérateur	45
2.2.9. S-projection instantanée	45
2.2.10. Projection algorithmique globale d'un individu	46
2.2.11. Données massives et bases de projections algorithmiques	48
2.2.12. Quelques exemples de projections algorithmiques.	49
2.2.12.1. Algorithmes <i>print</i>	49
2.2.12.2. Algorithmes <i>mail</i>	49
2.2.12.3. Algorithmes <i>bid</i>	50
2.2.12.4. Autres familles d'algorithmes	50
2.2.13. Volumes d'une projection algorithmique	51
2.2.13.1. Volume brut d'une projection.	51
2.2.13.2. K-volume d'une projection	51
2.2.13.3. Volume compressé moyen d'une projection	52
2.3. E-réputation et projections algorithmiques	52
2.3.1. Réputation numérique	52
2.3.2. Bref historique de l'e-réputation	52
2.3.3. Approche systémique de l'e-réputation d'un opérateur.	54
2.4. Concurrences, duels et projections algorithmiques.	55
2.5. Les enjeux d'une approche projective des données : structurer les données massives par le formalisme projectif	57

Chapitre 3. Objets connectés, niveau d'ubiquité d'un lieu et consentement algorithmique de l'utilisateur 61

3.1. Introduction.	61
3.2. L'évolution exponentielle des objets connectés à l'horizon 2020	62
3.3. Formalisme projectif appliqué aux objets connectés.	65
3.4. Niveau d'ubiquité d'un lieu	67
3.5. Consentement algorithmique d'un individu	68
3.5.1. Définition du consentement algorithmique	69
3.5.2. Prospérité et développement d'une ville intelligente	69
3.6. La ville ubiquitaire, génératrice de projections algorithmiques	70
3.6.1. Définitions	70
3.6.2. L'exemple de U-Songdo, première ville ubiquitaire	72
3.6.3. U-Songdo, ville ubiquitaire, ville du futur ?	73
3.7. Algorithmes prédictifs et boucles rétroactives	74
3.8. La boucle systémique data-prédictif-action	75
3.9. Les limites des algorithmes prédictifs face au hasard sauvage	76

Chapitre 4. Sur la valeur d'une donnée et d'une projection algorithmique	79
4.1. Le problème complexe du relèvement d'une donnée	79
4.2. Comment définir la valeur d'une donnée ?	80
4.2.1. Un déluge de données à valoriser	80
4.2.2. Valeur instantanée d'interprétation d'une donnée, valeur d'impact, valeur de vente	81
4.2.2.1. Un tweet à 136 milliards de dollars	81
4.2.2.2. La vente légale de données clients par Microsoft au FBI	83
4.2.3. Approche systémique de la valeur d'une donnée	83
4.2.3.1. Donnée et mot binaire	84
4.2.3.2. Notations.	84
4.2.3.3. Contexte, sous-contexte et système	84
4.2.3.4. Valeur instantanée d'une donnée selon un algorithme	85
4.2.3.5. Valeur initiale d'une donnée selon un contexte	86
4.2.3.6. L'exemple du faux tweet SEA	87
4.2.3.7. Un exemple de vente de données groupées	89
4.2.3.8. Raffinage d'une donnée	89
4.2.3.9. Valeur instantanée et sous-contexte	90
4.2.3.10. Origine et nature de la donnée	90
4.2.3.11. Diffusion de la donnée	90
4.3. Valeur d'un corpus de données massives	91
4.3.1. Les qualités d'un corpus de données massives en 6V	92
4.3.2. Valeur d'un corpus de données	93
4.3.2.1. Ligne de contrainte.	93
4.3.2.2. Définition de la valeur d'un corpus de données	93
4.3.2.3. Le cas des éoliennes Vestas.	94
4.3.2.4. Le cas du zoo de Cincinnati	95
Chapitre 5. Fausses données et projections algorithmiques fictives	97
5.1. La prolifération des données fictives et des faux profils	97
5.1.1. Déluge de fausses données et majorité de robots-visiteurs	97
5.1.2. De la fausse donnée pour protéger son anonymat	99
5.1.3. Vers une prolifération des profils fictifs sur les réseaux sociaux.	99
5.1.4. L'achat de faux abonnés pour construire sa popularité	101
5.1.5. Le cas spécifique de Twitter.	103
5.1.6. Opérations d'influence, faux profils et <i>socialbots</i>	105

5.1.6.1. Détection des faux profils sur Twitter	106
5.1.6.2. L'influence des <i>socialbots</i>	108
5.1.7. L'application de réseautage Tinder et ses dérivés	108
5.1.8. L'expérience Robin Sage	110
5.2. Représentation projective des données fictives	111
5.2.1. Contexte d'usurpation d'identité et d'imitation d'un individu réel	112
5.2.1.1. Cas d'usurpation d'identité après récupération des identifiants d'un utilisateur réel sur un système S	112
5.2.1.2. Cas d'usurpation d'identité d'un utilisateur réel par imitation sans identification sur un système S	112
5.2.1.3. Cas d'usurpation d'identité d'un utilisateur réel depuis un autre système	113
5.2.2. Contexte de création de profils fictifs	113
5.2.3. Complexité de maintenance en cohérence d'un groupe de profils fictifs	114
5.2.4. La confiance en une donnée	114
5.2.5. Antifragilité des systèmes	115
5.3. Projections algorithmiques fictives et cybersécurité	116
5.3.1. L'ingérence économique réalisée à partir de faux profils	116
5.3.2. Une cyberattaque ciblant un grand cabinet de conseil à partir d'un profil fictif	117
5.3.3. Les profils fictifs attractifs (PFA) en période de guerre	118
5.3.4. Conflit syrien et PFA	119
5.3.5. Une opération d'influence par PFA contre des soldats américains attribuée à la Russie	120
5.3.6. La Chine, Sun Tzu et les PFA	121

Chapitre 6. Cyberopérations à fort impact construites sur des projections algorithmiques fictives 123

6.1. L'opération de cyberespionnage Newscaster-Newsonair	123
6.1.1. Une opération sophistiquée	123
6.1.2. <i>Modus operandi</i>	124
6.1.3. Une confiance qui s'inscrit dans la durée et la cohérence	127
6.2. Attaques par <i>hoaxcrash</i> et FOVI : la puissance du leurre cognitif	128
6.2.1. Facteur humain et leurre cognitif : les clés des attaques par <i>hoaxcrash</i> et FOVI	128
6.2.2. Les attaques par <i>hoaxcrash</i>	129
6.2.2.1. Le cas du <i>hoaxcrash</i> Vinci	129

6.2.2.2. Les mécanismes du <i>hoaxcrash</i>	134
6.2.2.3. Efficacité et puissance d'un <i>hoaxcrash</i>	139
6.2.3. Les attaques par FOVI et arnaques au Président	140
6.2.3.1. FOVI, arnaques au Président, des attaques ciblées et lucratives	140
6.2.3.2. Des statistiques concernant les arnaques au Président	141
6.2.4. Détection automatisée des attaques par <i>hoaxcrash</i> et FOVI	147
6.2.4.1. Les approches possibles dans la lutte contre les <i>hoaxcrash</i> et FOVI	147
6.2.4.2. Perspectives	149
Chapitre 7. Épilogue prospectif : projection algorithmique globale et convergence NBIC	151
7.1. Introduction.	151
7.1.1. Un mot sur l'entropie.	151
7.1.2. Les convergences technologiques et la DIADEH	152
7.2. Convergence NBIC	152
7.3. Convergence CKTS	154
7.4. Convergence M-I	155
7.5. DIADEH	156
7.6. Projection algorithmique globale et convergences technologiques	158
Bibliographie	161
Index	171