

Milad DOUEIHI et Jacopo DOMENICUCCI (dir.)
(2018), *La confiance à l'ère numérique*

Paris, Éditions rue d'Ulm

Bertrand Mocquet



Édition électronique

URL : <http://journals.openedition.org/communication/11856>

ISBN : 978-2-921383-92-9

ISSN : 1920-7344

Éditeur

Université Laval

Référence électronique

Bertrand Mocquet, « Milad DOUEIHI et Jacopo DOMENICUCCI (dir.) (2018), *La confiance à l'ère numérique* », *Communication* [En ligne], vol. 37/1 | 2020, mis en ligne le 11 mai 2020, consulté le 20 juillet 2020. URL : <http://journals.openedition.org/communication/11856>

Ce document a été généré automatiquement le 20 juillet 2020.



Les contenus de la revue *Communication* sont mis à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International.

Milad DOUEIHI et Jacopo DOMENICUCCI (dir.) (2018), *La confiance à l'ère numérique*

Paris, Éditions rue d'Ulm

Bertrand Mocquet

RÉFÉRENCE

Milad DOUEIHI et Jacopo DOMENICUCCI (dir.) (2018), *La confiance à l'ère numérique*, Paris, Éditions rue d'Ulm

- 1 L'ouvrage collectif¹ propose des perspectives riches sur les enjeux de la confiance dans nos sociétés numériques.
- 2 Des philosophes et des spécialistes du numérique contribuent à ce volume par des articles scientifiques écrits, en français ou en anglais traduits pour cet ouvrage, entre 2015 et aujourd'hui mêlant les réflexions sur l'éthique, la philosophie de la technique, la philosophie sociale et les études sur le numérique.
- 3 Dès l'introduction générale, les auteurs nous précisent que nous sommes bien dans une démarche pluridisciplinaire, où « le numérique n'est pas un objet technique » (p. 14), mais « un ensemble de structures symboliques et matérielles, culturelles et sociales » (p. 14). Ils rappellent à plusieurs reprises l'influence de la cybernétique de Norbert Wiener. Le numérique est aussi considéré comme une civilisation pour les auteurs dont l'adhésion « est plutôt à comprendre sur le modèle d'une conversion religieuse » (p. 14). Une des questions centrales de cet ouvrage pourrait être la suivante : quelles formes de confiance existent dans le numérique, comment se créent-elles et dans quel intérêt, comment évoluent-elles ? Et cela, sous l'angle des questions classiques en philosophie, au travers d'une complémentarité entre le témoignage — « la possibilité d'acquérir des connaissances de seconde main, par opposition à la connaissance par expérience » (p. 16) — et la coopération — « l'interrogation à propos des actions qui

dépassent l'individu seul et des conditions de vivre-ensemble » (p. 16). Les auteurs nous rappellent que nous sommes dans une relation complexe où « le numérique est révélateur de confiance et la confiance comme analyseur du numérique » (p. 18), que cela se nourrit l'un de l'autre, évolue et se métamorphose dans des négociations quasi quotidiennes. Ils tiennent aussi à insister sur le fait que l'on ne peut réduire la confiance numérique à la sécurité informatique : « [...] concrètement on peut mettre en place des systèmes d'authentications et d'identifications très sophistiqués contre les attaques [...] mais il faut aussi travailler les usagers et leur crédulité pour contrer la menace du social engineering » (p. 24).

- 4 La sécurité numérique serait une condition nécessaire à la confiance numérique, mais pas une condition suffisante selon eux.
- 5 L'ouvrage est structuré en trois parties contenant chacune des publications d'auteurs internationaux différents : « La confiance en ligne – Toiles, interfaces et téléprésences », « La confiance dans les dispositifs numériques – Dispositifs, algorithmes, blockchain », puis « La confiance en devenir – Mutations de la confiance et de la privacy dans une société connectée ». Ces trois parties sont complétées par une introduction générale, des introductions par parties et une ouverture intitulée « In code we trust », rédigées par les deux directeurs de cette édition. Il en ressort de ce fait une forte cohésion des propos durant tout l'ouvrage, les articles se répondant les uns les autres.

La confiance en ligne – toiles, interfaces et téléprésence

- 6 L'introduction de cette partie est confiée aux deux auteurs principaux, Milad Doueïhi et Jacopo Domenicucci. Afin de nous préparer aux deux chapitres suivants, ils focalisent notre attention sur « La confiance connectée ». Ils nous invitent, entre autres, à constater qu'Internet permet de formidables échanges avec des individus, tout en développant des incertitudes contextuelles, suivant le type d'applications utilisées, et des incertitudes structurelles, la proximité virtuelle par rapport à l'éloignement physique, au point que l'on se fie aux inconnus avec qui l'on communique. Dans cette partie, le numérique est essentiellement traité comme un milieu, un environnement, un média.
- 7 Le texte de Laurent Jaffro, « Interactions en ligne et concept de confiance », ouvre cette partie de l'ouvrage en introduisant des considérations théoriques. Il rappelle qu'en philosophie, la confiance est

une conduite par laquelle un agent se place dans la dépendance d'une conduite d'un autre agent afin de réaliser une certaine fin, qu'il lui serait difficile d'atteindre sans cela, en escomptant plus ou moins sciemment que le signalement de cette dépendance incite l'autre agent à adopter cette conduite (p. 34).
- 8 En s'appuyant sur les travaux de Thomas W. Simpson, ce chercheur nous alerte sur l'existence de la pluralité des formes de confiance dans les interactions en ligne. Il distingue ainsi la confiance « cognitive [...], conative [...], affective et prédictive » (p. 37). À cela, il propose d'ajouter deux échelles de la confiance, celle qu'il nomme la « petite échelle (absences de suspicions [...] → assurance → confiance décidée) » (p. 38) et l'autre, la « grande échelle (défiance complète → prudence → coopération → confiance) » (p. 39). Au-delà de ces considérations théoriques, dans le cadre de

l'interaction en ligne, Jaffro propose de qualifier cette confiance de systémique, « qui concerne les environnements mêmes des interactions et pas seulement les interactions » (p. 42). Il l'illustre d'ailleurs fort justement par le cas du logiciel GnuPG, qui permet la transmission de messages électroniques signés et chiffrés, ce qui garantit leurs authenticité, intégrité et confidentialité. Cette confiance systémique est étroitement liée à un concept de confiance pratique, dans le cadre d'un achat sur Internet par exemple, où l'on « pense qu'on est peut-être [...] en train de se faire arnaquer » (p. 46), qui ne se confond pas avec la confiance épistémique, « ce qui touche à l'information en ligne » (p. 47). L'auteur rappelle par là même que la confiance ne peut se résumer à la sécurité, mais qu'« en même temps un certain degré de sécurité de l'environnement est indispensable » (p. 49). La troisième partie aborde les obstacles à la confiance en ligne et quelques problèmes à la fois théoriques et pratiques : l'identité sur Internet, la désincarnation, le contrôle d'accès, le traçage et la surveillance. L'auteur nous rappelle que « la communication sur Internet ne mobilise pas le langage corporel mais s'appuie sur la langue écrite » (p. 53).

- 9 L'article de Thomas W. Simpson, traduit de l'anglais et intitulé « Téléprésence et confiance : une théorie des actes de langage appliquée à la communication médiée », pose la question suivante : « Comment la communication par des représentants de personnes peut-elle soutenir la confiance limitée par des preuves ? » (p. 60). L'auteur place de ce fait la confiance au centre de notre vie sociale, tant du point de vue épistémique que pratique. Il s'appuie sur les usages numériques contemporains à succès, notamment les réseaux socionumériques, pour constater que « nous sommes présents auprès des autres, mais à distance » (p. 64). Cette téléprésence est ainsi un terrain où peut se traiter la question de confiance. L'auteur développe une théorie parole-acte de la communication par voie numérique, en s'inspirant de l'identification de l'acte illocutoire par Austin : le message convoyé par un énoncé au-delà de son sens immédiat. Ainsi « la confiance, pour une part importante, va au-delà des éléments de preuves apparents » (p. 70). Le chercheur développe l'idée que la confiance se bâtit sur le choix d'une technologie de communication particulière. Il considère que cela fait partie non seulement de ce qui est communiqué, mais aussi des indices pour gagner la confiance. Pour reprendre un des exemples qui illustrent cette partie, l'usage d'une communication au moyen de la webcam n'a pas le même sens sur un site de rencontre, du type Chatroulette, que sur un site de conversations comme Skype. En conclusion, l'auteur affirme à nouveau que « la téléprésence peut être un bon moyen d'entretenir certaines formes de confiance. Elle est moins propice à la créer » (p. 86).

La confiance dans les dispositifs numériques – dispositifs, algorithmes, *blockchain*

- 10 L'introduction de ce chapitre élaboré par Doueichi et Domenicucci se nomme « Se fier aux artefacts numériques ». Ils s'intéressent dorénavant davantage aux dispositifs qu'à l'espace social numériquement augmenté. Il s'agit ici des systèmes informatiques embarqués qui développent des actions en suivant des algorithmes, pour lesquels les auteurs reconnaissent « le pouvoir d'action croissant » (p. 89) et qui nous invite à une autre forme de confiance, « une confiance algorithmique » (p. 90). Ainsi, pour évaluer cette confiance, il faut placer son analyse aussi bien d'un point de vue expérience-utilisateur (« niveau phénoménologique ») que d'un point de vue technique (« fiabilité

technique »). De ce fait, la conception des dispositifs, ou artéfacts selon les auteurs, peut se faire selon deux niveaux : « à un niveau [qui] vise une adaptation pragmatique aux besoins de l'utilisateur et à ses dynamiques psychologiques » (p. 91) et « à un autre niveau [celui] de la réflexion sur la possibilité d'inscrire des critères éthiques, voire de véritables vertus » (p. 90). Pour illustrer ces propos, les artéfacts tels que le *cloud computing*, la *blockchain* et le *big data* sont utilisés.

- 11 Le premier texte de Christopher Thomson, « Faire confiance aux artéfacts — faire confiance à distance », rappelle le concept d'artéfact et nous invite à considérer la confiance non plus d'un point de vue systémique, ou anthropomorphique ou heuristique, mais bien d'un point de vue de l'objet technologique fabriqué par un ou des individus possédant une intention : il s'agit ici de la « confiance envers les artéfacts ». Pour illustrer son propos, l'auteur s'appuie sur le cas de la voiture à laquelle on fait confiance tous les matins pour démarrer, mais, par relation, aussi aux salariés qui l'ont conçue et fabriquée : il s'agit ici de la notion de *reliance*, de *to rely*, signifiant « s'appuyer sur, faire confiance ». Il définit ainsi l'état de toutes choses qui sont connectées, liées entre elles, dans une relation interpersonnelle : une forme de causalité de la conception vers l'usage. Thomson nous démontre ainsi que la confiance dans l'intention du concepteur est primordiale dans la constitution de la confiance en un artéfact.
- 12 Le chapitre 2 est intitulé « Les paradoxes de la confiance distribuée : l'architecture pair à pair et la confiance des utilisateurs dans le système bitcoin ». Il est rédigé par Alexandre Mallard, Cécile Méadel et Francesca Musiani. L'artéfact observé est le système de monnaie électronique décentralisé Bitcoin, une technologie récente hautement médiatisée. L'article décrit le principe de cette monnaie, et notamment le fait de faire appel à des tiers chargés de légitimer la valeur monétaire concernée : c'est ici que repose la problématique de la confiance. Dans l'état actuel du développement, les discours qui se déroulent au sein d'espaces d'information et de discussion liés à Bitcoin peuvent être analysés à la lumière de leur capacité à produire à la fois les représentations de la valeur, les pratiques selon lesquelles il est transformé et évolue, et les dispositifs permettant sa mise en œuvre. La littérature sur le système montre comment les débats sur les Bitcoins ne se propagent pas simplement, communiquent et diffusent la représentation de cette monnaie, mais qu'ils sont étroitement liés à la pratique de la monnaie elle-même. En focalisant son attention sur un corpus spécifique, celui du discours d'experts, l'article montre comment, en présentant et en discutant un dispositif, une dynamique ou une opération spécifique comme étant en quelque sorte lié à la confiance, cette expertise contribue à la définition et à la confiance au sein du système Bitcoin — ce qui contribue finalement à réaliser la définition partagée de sa valeur en tant que devise.
- 13 Le *cloud computing*, ou « informatique dématérialisée », gagne rapidement du terrain dans la société et offre aux entreprises des services en ligne à la demande (tels que Gmail, iCloud et Salesforce). L'article intitulé « Le cloud : éthique du nuage informatique » et rédigé par Boudewijn de Bruin et Luciano Floridi propose d'examiner les *clouders*, les professionnels et particuliers utilisant ces services. Le regard est porté sur l'éthique des professionnels fonctionnant avec cette nouvelle technologie en analysant les obligations d'information des entreprises d'accueil qui possèdent et exploitent des centres de données d'informatique en nuage (par exemple Amazon). La première partie du document indique que les sociétés d'hébergement, les fournisseurs

de services et les *clouders* ont des obligations d'information mutuelles (épistémiques) consistant à fournir et à rechercher des informations sur des questions pertinentes telles que la confidentialité, la fiabilité des services, l'exploration et la propriété des données. Le concept d'*interlucency* est développé comme une vertu épistémique régissant une communication efficace sur le plan éthique. La deuxième partie examine les formes potentielles de restrictions ou d'interdictions gouvernementales contre le développement et l'utilisation de la technologie de l'informatique en nuage. Faisant référence au concept de neutralité technologique, les auteurs font valoir que l'*interlucency* avec les sociétés d'hébergement et les fournisseurs de services en nuage n'est guère nécessaire ni justifiée. Toutefois, il est également avancé que les entreprises utilisant des services de *cloud* (banques, cabinets d'avocats, hôpitaux, etc., stockant des données clients dans le *cloud*) devront se conformer à des réglementations plus strictes.

La confiance en devenir – mutations de la confiance et de la *privacy* dans une société connectée

- 14 La troisième partie, toujours introduite par les auteurs, s'intitule « La confiance dans une société numérique » et s'intéresse ici à l'évolution du devenir de la confiance. Il s'agit bien d'impact du numérique sur le vivre-ensemble et de la façon dont la confiance permet une évolution, abordée dans ce chapitre dans le contexte de la *privacy*, de la surveillance de masse ou en fonction du défi de la défiance numérique imaginée comme post-vérité.
- 15 Le premier chapitre de cette partie est rédigé par Tobias Matzner et intitulé « La *privacy* dans les médias numériques : une approche arendtienne ». L'auteur commence par justifier son appui sur la pensée d'Hannah Arendt, d'abord en raison de « la peur d'être fondamentalement déterminé par des attributions externes et par des théories hétéronomes de subjectivation » (p. 174), puis en réaction à cette menace non pas contre le sujet de l'individu autonome qui est d'ailleurs remis en cause ici, mais bien contre « un sujet politique pris dans une situation sociale déterminée » (p. 174). L'article montre que la pensée d'Arendt, « plutôt que d'opposer le pouvoir d'un acteur individuel au pouvoir d'un sujet hétéronome, [...] pluralise le pouvoir de subjectivation » (p. 174). Cela amène l'auteur à définir de nouvelles bases pour la *privacy*, compatible avec la communication numérique.
- 16 En commençant le texte intitulé « Confiance et testaments : questions de vie privée et d'écoute éthique à l'ère de la surveillance de masse ex-ante » par la citation d'un militant turc et membre du Parti Pirate — « Je pense que tout dépend du sujet sur lequel on fait confiance à quelqu'un. Je ne leur confierais pas mon téléphone portable. Je leur confierais ma vie » —, Jessica Feldman nous amène dans le contexte de ceux qui contestent les répressions. Elle considère qu'en abandonnant nos données personnelles sur les réseaux socionumériques, nous nous sommes habitués à une forme de régulation et de surveillance. Elle insiste d'ailleurs sur la menace contre la démocratie que représente l'analyse de ses traces numériques, par exemple. En conclusion, elle invite les sujets des systèmes numériques à en « inventer, qui réunissent les conditions nécessaires à l'amitié et à la confiance, et qui hébergent des formes de communication nous permettant d'accéder aux faits et à l'expérience et de changer d'avis » (p. 214).

- 17 Le dernier texte, intitulé « Post-vérité : le défi de la défiance » et rédigé par Maurizio Ferraris, se propose de comprendre la post-vérité qui sévit sur les réseaux sociaux numériques directement comme un accomplissement du postmodernisme philosophique.

Conclusion

- 18 La rédaction de ce livre est de grande qualité. Pour plusieurs raisons, il nous paraît essentiel à tous ceux qui s'intéressent dans leurs travaux de recherche à la confiance dans un environnement numérique pour plusieurs motifs : usages, conceptions, éthique ou philosophique. La première raison repose sur sa capacité à décrire les objets technologiques sur lesquels le discours se pose de façon simple et précise : cette lecture permettra aux moins aguerris d'entre nous de se faire une idée du *cloud* ou de la *blockchain*, par exemple. La deuxième raison est qu'à proximité de cette description technologique est développé un discours social et humain sur l'impact de la technologie. Enfin, la troisième raison est liée au fait que le discours est structuré, qu'il propose des éléments académiques précis dans la description des artefacts, variés dans les contextes et complets dans le questionnement sur la confiance associée. Sur le plan philosophique, son point de vue peut contribuer à amener cette question de confiance numérique auprès de ceux qui tiennent la gouverne des organisations publiques par exemple.
-

NOTES

1. Milad Doueïhi est philosophe, historien des religions et titulaire de la chaire d'humanisme numérique à l'Université de Paris-Sorbonne (Paris 4). Jacopo Domenicucci est agrégé de philosophie, normalien, en thèse à l'Université Paris 1 Panthéon-Sorbonne.

AUTEURS

BERTRAND MOCQUET

Bertrand Mocquet est un expert numérique à l'Agence de mutualisation des universités et établissements d'enseignement supérieur ou de recherche (AMUE) et chercheur au laboratoire Médiations, informations, communication, arts (MICA) de l'Université de Bordeaux Montaigne. Il est aussi chercheur associé au Centre de recherche sur les sociétés et les environnements méditerranéens (CRESEM) de l'Université de Perpignan. Courriel : bertrand.mocquet@amue.fr
