DAUPHINE
UNIVERSITÉ PARIS

2017/2018 BUSINESS CONSULTING MASTER'S DEGREE

RESEARCH PAPER

TO WHAT EXTENT THE LEVEL OF GDPR-RELATED KNOWLEDGE AFFECTS THE TRUST INDIVIDUALS PLACE IN THEIR BANK?

Charlotte BENAÏCHA-TANQUEREL

Thesis director: Eric CAMPOY

Defence date: September 07th, 2018

TABLE OF CONTENTS

TABLES OF FIGURES & TABLES 4
ABSTRACT 5
ACKNOWLEDGEMENTS 6
INTRODUCTION 7
LITERATURE REVIEW 9
GDPR-driven reshaping of the regulation context 9
Change in data-related habits 9
Impetus for change 13
Global legal interdependence 15
Trust-influenced individuals behaviours 16
Concept of trust 17
Trustworthiness 18
Propensity to trust 19
METHODOLOGY 23
Methodology presentation 23
Literature review 23
Research model 23
Global research process 26
Exploratory talks 26
Internal documents 28
Measurement instruments 28
Data collection 29
Data analysis 33
Tests of hypotheses 33
Results 35
GENERAL DISCUSSION 39
Recommendations 39
Theoretical implications 39
Managerial contributions 40
Limitations 41
CONCLUSION 43
REFERENCES i
APPENDIX iv
A. List of abbreviations iv
B. Tables with constructs iv
C. Findings related to the multiple regression analysis vi
D. Interview guide for exploratory talks x
E. Exploratory talks transcripts xi

Female, 49yo.....xi
Male, 55 yo.....xiv
Female, 22 yo.....xvi
Male, 25 yo.....xix

TABLES OF FIGURES & TABLES

FIGURE 1. RESEARCH MODEL. 26
FIGURE 2. AGE REPARTITION 30
FIGURE 3. AGE REPARTITION 31
FIGURE 4. AGE REPARTITION ACCORDING TO GENDER 31
FIGURE 5. EDUCATIONAL LEVEL REPARTITION 32
FIGURE 6. TENURE WITHIN BANK AGENCY 32
FIGURE 7. THE FIRST PHASE OF TESTING 34
FIGURE 8. THE SECOND PHASE OF TESTING 35
FIGURE 9. RELATED-SAMPLES WILCOXON SIGNED RANK TEST RESULTS 37
FIGURE 10. PARTIAL REGRESSION PLOT BETWEEN 'DIMENSIONS OF TRUST' AND 'BANK INSTITUTIONS' CHARACTERISTICS' VII
FIGURE 11. PARTIAL REGRESSION PLOT BETWEEN 'DIMENSIONS OF TRUST' AND 'PROPENSITY-TO-TRUST' VII
FIGURE 12. LINEAR REGRESSION HISTOGRAM VIII
FIGURE 13. NORMAL P-PLOT OF REGRESSION STANDARDIZED RESIDUAL IX

TABLE 1. ARTICLES RELATED TO GDPR PRINCIPLES (CNIL, 2018) 12
TABLE 2. LITERATURE REVIEW. 23
TABLE 3. INTERVIEWEE EXPERTISE PROFILE 28
TABLE 4. RELIABILITY STATISTICS RELATED TO 'BANK INSTITUTIONS CHARACTERISTICS' VARIABLE 36
TABLE 5. RELIABILITY STATISTICS RELATED TO 'DIMENSIONS OF TRUST' VARIABLE 36
TABLE 6. SUMMARY OF MULTIPLE REGRESSION ANALYSIS 36
TABLE 7. MEDIAN REPORT 37
TABLE 8. RELATED-SAMPLES WILCOXON SIGNED RANK TEST RESULTS TABLE 37
TABLE 9. HYPOTHESIS CONCLUSIONS 38
TABLE 10. LIST OF ABBREVIATIONS IV
TABLE 11. TABLE WITH CONSTRUCTS VI
TABLE 12. TABLE WITH CONTEXTUAL VARIABLES VI
TABLE 13. MODEL SUMMARY OF MULTIPLE REGRESSION VII
TABLE 14. CASEWISE DIAGNOSTICS (A) VIII
TABLE 15. ANOVA (A) TABLE OF MULTIPLE REGRESSION IX
TABLE 16. COEFFICIENTS TABLES X
TABLE 17. EXPLORATORY INTERVIEWS GUIDE XI

EQUATION 1. MULTIPLE REGRESSION MODEL EQUATION 36
EQUATION 2. RESEARCH REGRESSION EQUATION IX

ABSTRACT

Trust, in general, is leading most of the social interaction any individual may have, involving doubt and dependency. The online, namely virtual, interactions are no exception, especially regarding the anonymity (or the lack of proved identity) and the opportunism that the Web shows. Therefore, individuals express an increasing misgiving with regard to perceived (numeric) risks related to behaviours without a face-to-face checking possibility. The bank corporation is the trustee, meaning the party in whom trust is placed and who has the opportunity to take advantage of the trustor's vulnerability[1]. This concern is then enhanced by the scandals that the media raises about data-based abuses.

Trust issues are recognized as retail banks major concerns since it encompasses every interaction and may have a strong impact on brand recognition and client loyalty. The increasingly day-to-day collection of client data lays stress on the paramount importance for retail banks to build a trustworthy, long-term relationship with individuals. This study proposes and empirically tests five hypotheses with a sample of 170 persons of full age to provide a model substantiating the impact that individuals' knowledge degree related to protection-based regulation may have on customers' trust considering retail banking industry.

Keywords: The General Data Protection Regulation; GPDR; Banking; Transformation; Regulation; Data Protection; trust; trustworthiness; propensity to trust; customer relationships; human issues in online interactions.

[1] The trustor refers here to the individual.

ACKNOWLEDGEMENTS

I express my gratitude to my thesis director *Eric CAMPOY* for guiding me during my researches (and studies at Paris-Dauphine University). He provides my insightful comments and assistance during my work.
I would also thank *Anouck ADROT*, who was my tutor during my apprenticeship at Paris-Dauphine University. She accompanied me while finding the right words to guide me.

I commend my parents, *Virginie TANQUEREL & Ismaël BENAÏCHA*, for their unconditional support and help, as well as the several and final proofreading of my two research papers.

I would finally like to thank *Maxime LEROUX-GAGNON,* one of my managers during my first-year apprenticeship, for his proofreading and support.

INTRODUCTION

The current easily-accessible-information-system society is confronted with a growing interest from citizens in their data – pieces of information related to their personal environment. The 2013 Edward Snowden scandal - among others - drove the EU-regulator to propose a legislation enabling to establish a clearer delineation of responsibilities between the different protagonists within European Union and in its interactions with others. This symbolizes a new momentum that reshapes the online and offline data-driven paradigm. The banking industry is known to deal intrinsically with an important volume of personal data since every banking information is classified as such. Therefore, the banks must consider all the risks surrounding the deal flow. Besides their brand image, the data accountability and transparency are required to run the business with consumers. These users tend to be fickler as systems give them more and more effortless-accessed information.

Furthermore, regulatory constraints increasingly impact the day-to-day operations and administration, while rising an ethical issue linked to data, tampering by third-parties. Since May 25, 2018, European Union members, organisations, and citizens need to follow some new data protection principles through the General Data Protection Regulation (i.e. GDPR)[2]. Since the regulatory context may appear as increasingly demanding, especially for the organisation, benefiting the customers, this study seeks to understand the correlation between trust of individuals in banks and GDPR implementation.

In today's hyper-connected market, trust seems to be a key to succeed in realizing profits, since the clients, prospects and employees are increasingly able to check all the news and information related to a business in no time. Moreover, every generation of individuals is likely to use the Internet to do so, even if the phenomenon is increasing in scale with the youngest people[3]. Organisations are increasingly concerned with their brand image, heightened by the network effects. This study may provide opportunities for innovation in the way banks tend to conduct business, which can change and enhance the banking industry and

[2] To make this study easier to read, appendix A lists all the abbreviations used throughout this study.
[3] However, this statement must be nuanced, since each new generation seems to have new disruptive characteristics, such as the X & Y generation as well as the millennials.

its ecosystem. Regarding the long-run interest, banks have to cultivate long-term, mutually beneficial relationship with its customers (Ritter, 1993).

This research paper aims to conceptualise trust individuals put in retail banking industry while exploring the influence of the individuals' knowledge degree related to data protection-based regulation.

Based on the existing literature material, this study will first define the regulatory context where digital changes and habits occur, considering the legal texts and researches driven by the regulatory changes. Then, I will specify the concept of trust, its dimensions and antecedents from Mayer, Davis and Schoorman (1995) to Oliveira, Alhinho, Rita & Dhillon (2017) approaches. After examining the two concepts, I will determine how they are correlated to study to what extent data-protection-based regulation can influence the trust individuals put in their banks.

Finally, it appears that trust concerns increasingly occur since hyper-connected habits and relationships with banks are almost inescapable in every individual's life, both professional and personal, on a daily basis.

LITERATURE REVIEW

GDPR-DRIVEN RESHAPING OF THE REGULATION CONTEXT

Following the change in Internet-related habits and thanks to its high impact on individuals' freedoms, the regulatory system decided to oversee the possibilities in terms of treatments and uses of individuals personal data. Here is the main reason for GDPR to be implemented.

CHANGE IN DATA-RELATED HABITS

The General Data Protection Regulation provides a data environment where rights and duties are explained. The legal content[4] can be divided into the following 11 principles:

National law: since the GDPR is a multi-country regulation, it overtakes the national law existing within each State Member. Nevertheless, despite all the dispositions already implemented, additional details must still be reviewed.

Transfers, namely transfers of personal data within EU or across borders: the regulation indeed diverges regarding the destination, offering cross-border processing and binding corporate rules (BCR).

Pseudonymisation: it is defined as "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". It always refers to a natural person. The GDPR indeed considers that any information on an identifiable natural person should be then respectful regarding the regulation. The legal context allows that the data protection should not apply to anonymous information, namely information not related to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable (for instance, statistical or research purposes).

Data portability: it refers to the right that any individual has to receive all the personal data concerning him/her in a machine-readable format.

[4] Table 1 lists the related articles of the GDPR is proposed on page 12.

Infringement: since the regulation offers a legal framework, it generates a risk of opportunism to break the law. Consequently, the GDPR must provide meaningful and effective penalties for offences.

Consent: it represents the main litigious point of this new regulation since now the organisations are no longer allowed to consider the tacit agreement. Therefore, The GDPR offers the following definition about consent: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Profiling: it is defined by the GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". This new regulation includes limits and guidelines with regard to such a practice.

Healthcare: this principle refers to data concerning health, meaning "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Safety: this notion refers to concerns that may be generated especially considering the digital habits.

Certification mechanisms: they are used to demonstrate the existence of appropriate safeguards implemented by the firm. Such an approach is promoted by the Regulation since the review must be realized by a certification body that is recognized to do so.

Privacy Impact Assessment (PIA): it is related to risks management and specifically discussed in the Article 35 of the GDPR. It allows a company to include measures, safeguards and mechanisms that the firm implemented for mitigating risks that the PIA identified, ensuring the protection of personal data and thus demonstrating compliance.

Data Protection Officer (DPO): it means that an individual within the organization[5] is in charge of informing about the data-based framework, monitoring compliance and being

[5] It seems relevant here to specify that such a nomination is mandatory only if one or more of the three following conditions are fulfilled. Indeed, the Article 37 oversees the designation of the data protection officer

a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

the main contact point for both authority and collaborator. The section 4 of the GDPR explains all the related items.

The following table lists the principles-related articles from the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing directive 95/46/EC (also called General Data Protection Regulation).

National law	(008), (025), (031), (045), (050), (052), (071), (073), (081), (093), (111), (112), (121), (129), (131), (142), (146), (154), (158), Article 6, Article 9, Article 28, Article 29, Article 32, Article 37, Article 49, Article 62, Article 89 and Article 90
Transfers	(006), (048), (101), (102), (103), (107), (110), (111), (112), (113), (115), (153), Article 4, Article 13, Article 14, Article 15, Article 23, Article 28, Article 30, Article 40, Article 42, Article 44, Article 45, Article 46, Article 47, Article 48, Article 49, Article 70, Article 83, Article 88, Article 96 and Article 97
Pseudonymisation	(026), (028), (029), (075), (078), (085), (156), Article 25, Article 32 and Article 89
Portability	(068), (073), (156), Article 13, Article 14 and Article 20
Infringement	(073), (085), (086), Article 33, Article 34, Article 58 and Article 70
Consent	(032), (033), (038), (040), (042), (043), (050), (051), (054), (065), (111), (112), (157), (161), (171), Article7, Article 8, Article 9, Article 13, Article 14, Article 17, Article 20, Article 22, Article 40, Article 49 and Article 83
Profiling	(024), (060), (063), (070), (071), (072), (073), (091), Article 13, Article 14, Article 15, Article 21, Article 22, Article 35, Article 47 and Article 70
Healthcare	(035), (045), (052), (053), (054), (063), (065), (071), (073), (075), (091), (112), (155), (159), Article 9, Article 17, Article 23, Article 36 and Article 88
Safety	(039), (049), (071), (081), (083), (094), Article 5, Article 30, Article 32, Article 34, Article 45 and Article 47
Certification	(077), (081), (100), (166), (168), Article 24, Article 25, Article 28, Article 32, Article 42, Article 43, Article 46, Article 57, Article 58,

b) The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

	Article 64, Article 70 and Article 83
Privacy Impact Assessment (PIA)	(084), (089), (090), (091), (092), (094), (095), Article 35, Article 36, Article 39, Article 57 and Article 64
Data Protection Officer (DPO)	(077), (097), Article 13, Article 14, Article 30, Article 33, Article 35, Article 36, Article 37, Article 38, Article 39, Article 47 and Article 57

Table 1. Articles related to GDPR principles (CNIL, 2018)

The population tends then to be more focused on the day-to-day safety rather than following the new or debated pieces of legislation. In this way, a database of secure electronic titles[6] was implemented on October 28, 2017. It allows the government to collect and store biometric information about individuals by merging two of the administrative databases. This system has no explained purpose but records personal information, such as face pictures, fingerprints, mailing addresses, first and last name. But the authentication and the recognition are two different processes with two distinct aims. At this stage, this file is not able to identify anyone thanks to its fingerprints, but such a functionality law easily be implemented (Pellegrini & Vitalis, 2018).

The new era is led by the primacy of security approach. Nevertheless, Gallouédec-Genuys & Lemoine's outcomes (1980) have shown that the regulator forgot that during the second world war, lots and a significant number of persons to escape Nazis persecution thanks to falsified documents. Solove and Hoofnagle (2006) have highlighted that a model regime of privacy protection is arising to offset the security-breaches scandals, while the database industry is increasingly powerful with a voracious appetite for data and especially personal data, thanks to data brokers' offerings. Details about customers' habits and desires and possessions are such a lucrative business. Large data brokers, which represent only a segment of the database industry, provide services to a range of companies, from marketing ones to the government. And, besides, as Solove and Hoofnagle remember (2006) the government increasingly has been contracting with data brokers, since it used to more and more focus on data mining to generate predictions about future individuals' behaviours. But to do so, a huge volume of data is required to create patterns. As recalled by Hildebrandt and Tielemans (p.511, 2013), "generally speaking, legislation is not mean to be neutral". Therefore, the GDPR will have a normative and organizational impact, since it offers protective dimensions in the

[6] Base des titres électroniques sécurisés (TES) in French

technological (meaning data-based) environment. The regulation now compels data controllers to ensure Data Protection by Design. But as Mireille Hildebrandt (2011) noticed, this new legal protection by design (LPbD) is now made of unwritten and written law, next to digital law. But eventually, the regulation refers more to rules than principles. It should then be easier to properly comply with it.

IMPETUS FOR CHANGE

Joergensen & Marzouki (2016) remind the two major milestones that lead to such an evolution of the data-driven paradigm, with new digital rights. Therefore, they identified two main events that push the online environment forward.

The World Summit on The Information Society (WSIS)[7] ensures the "right to communicate" vision, linked to both indivisibility and interdependence of all Human rights.

The Internet Governance Forum (IGF) was then designed as a new forum for multi-stakeholder policy dialogue. The aim was to strengthen the Human rights perspective in the Internet policy considering local and regional lobbying in the context of web 2.0 beginning.
These two landmarks point different connectivity issues in terms of rights. Since the worldwide population remains without sufficient Internet access infrastructure, the debate linked to the recognition of the Internet Access as a Right may seem useless. However, an increasing number of organisations[8] try to figure out how dealing with a deficient electric access to solve socioeconomic issues. Such a technological solution it is all the more important that a BBC 2010 survey[9] shows that four in five adults consider it as a basic right. But regardless many key figures of the Internet governance, such as Vincent Cerf[10], speak out against such a legal frame since the technology is more an enabler than a right in itself.

Our current Society is led by digital change. Almost every individual aims to be multitasking thanks to digital platforms, such as portable devices, apps and software. Such a phenomenon is called hyper-connectivity. People are indeed constantly connected to others thanks to mobile devices and Internet connection from almost everywhere. Therefore, they are readily

[7] This congress was held in two phases: the first one in 2003 in Geneva, Switzerland, and then in 2005 in Tunis, Tunisia.
[8] For instance, the Association for Progressive Communication, also called APAC, aims to create Internet-frame related rights through a Charter, initially proposed in 2009.
[9] See http://news.bbc.co.uk/2/hi/technology/8548190.stm
[10] Vincent Gray Cerf is an American Internet pioneer, who is recognized as one of "the fathers of the Internet", due to its TCP / IP invention with Bob Kahn.

accessible. It is relevant for information, but also for phishing, hacking and other data fraud. Individuals' values, lifestyles, and technology-oriented goals in day-to-day life influence their both online and non-face-to-face behaviours.

Besides expectations of customers, the outcome of the Pittsburgh summit underlines that it is necessary for the European Union to keep a leading role in the run-up for designing a framework that allows the global financial system to continue to exist and, consequently, for national economies to continue on their path. Economic growth is indeed related to customers consumption because the ultimate act of buying also relies on intention to buy, depending on perceptions of risks factors.

The French context during the last decade was influenced by the fear related to terrorist attacks and GAFA[11] scandals. Such responses are not only specific to the French population. Nevertheless, a new legal environment was implemented in France. The whole country was in lockdown since the 2015 attacks in Paris. It ended on President Macron's decision on November 1, 2017[12]. Applied to protect the citizens, the new legal framework also limits the individual freedoms. Indeed, under such circumstances, the Prefect or the Minister of Home Affairs may decide to prohibit traffic, meetings. The powers of the national services have concurrently greater powers to control, proceed to administrative searches or pronounce house arrest.

In France, the authority dedicated to Data Protection is called CNIL[13]. It is also the watchdog for this related topic. The legal frame was first defined by the Data Protection Act[14]. GDPR proposes then a common framework, assuming more harmonisation, while each Member State still preserves its own decision-making power.

[11] The acronym GAFA refers to influent, digital-driven organizations, namely Google, Amazon, Facebook and Apple.
[12] This status was decreed during a Ministerial Council meeting on the night of Friday 13 to Saturday 14 November 2015. Extended six times by the French Parliament, the state of emergency ended on November 1, 2017, while the law of October 31, 2017, which strengthens internal security and the fight against terrorism, came into force.
[13] The acronym CNIL means *Commission Nationale de l'Informatique et des Libertés* in French.
[14] Loi Informatique & Libertés

On 24 May 2018, the General Data Protection Regulation of the EU (GDPR) will apply directly to processing activities of personal data which have a link to the European Union's territory or market[15].

GDPR now regulates almost all the data-related issues. Such an oversight will probably offer more certainty and coherence within European territory, thanks to a situational awareness. Then most of the local-based (global) companies have decided to comply with the GDPR as soon as possible. The aim is above all to prove that management put it as one of the key management priorities.

GLOBAL LEGAL INTERDEPENDENCE

The current data ecosystem is worldwide. Thus, the legal framework may appear as disconnected if not harmonized. Not surprisingly, the United States (US) chose to be involved in the European debate on the GDPR. The sometimes-scorned lobbying from the United States to amend provisions or changes in the text has been important.

With the Charter on Fundamental Rights, the EU recognizes the importance of protecting personal data and the right to privacy (Safari, 2017). In a worldwide context, the EU had to consider the abroad situations and frames. With this in mind, the European decision committee tried to harmonize its approach with the Americans regulation by implementing the Safe Harbor Framework. In contrast with GDPR regulation, it is supposed to be a voluntary decision to enter into it. This text only provides seven principles, assuming adequacy between two of the most powerful Unions around the world. Therefore, these principles lay down that the following prescription should proceed before dealing with data:

1. ***Notice***: before using data related to someone, every company should inform the data users concerned about the purpose of such treatment;
2. ***Choice***: once noticed, the individual must have the possibility of explicitly accepting as well as refusing the treatment of its personal data;
3. ***Onward transfer***: the firm needs to ensure to respect the compliance requirements by acknowledging the disclosure of information to a third-party if needed;
4. ***Access***: everyone can be assured that it can have access to data and/or information about itself and the chance to change them if necessary;

[15] (Albrecht, 2016)

5. ***Security***: precautions are taken in order to protect personal information from loss, destruction, unpredicted change, misuse…
6. ***Data integrity***: the data needs to be reliable for its intended use, accurate, complete, and current.
7. ***Enforcement***: the organization is responsible to assure those mechanisms, allowing individuals to check the data concerned as well as procedures to take over commitments to Safe Harbor principles and solve problems, are in place.

This interdependence between the two Unions allowed the Bridge Project to come to fruition. (Abramatic, et al., 2015) define it as "a collaboration between MIT and the University of Amsterdam to enhance a sustainable model for protecting privacy in the global Internet environment". It began in May 2014 and aims to:

> *"Bridge the gap between the data privacy regimes in the United States and the European Union, thus strengthening the framework of the Safe Harbor."* [16]

The research group shared its outcomes in September 2015, offering ten recommendations. The non-governmental initiative can also be considered as soft lobbying from the Obama Administration. The current US administration does not appear, at this stage, to question these arrangements. The value of data-dependent systems is indeed so important, that a part of the US economy, e.g. the Silicon Valley, relies on it.

If, as it appears, our Society, and more specifically its individuals, is increasingly connected to devices and algorithms that need a growing proportion of data about customers, habits and behaviours. Such a new paradigm creates hence opportunisms. It may be also analysed regarding the external and internal factors that lead people to put their trust in others, and more particularly in bank organisations.

TRUST-INFLUENCED INDIVIDUALS BEHAVIOURS

Trust is one of the most condition to fulfil to build long-run and strong relationships, whether they are interpersonal or commercial. Trust seems thus to be a solution to reduce the perceived risk of the trustor, namely the individuals, who may dread the uncertainty and/or

[16] (Safari, 2017)

interdependence that any bank-based relationship may rise. These fears flourish in many settings but thrive in cash-related, socially distant relationships.

CONCEPT OF TRUST

Researches from Mayer et al. (1995) have demonstrated that "trust is the outcome of an individual's willingness to be vulnerable to others and confidence that both the trustor and the trustee will demonstrate trustworthiness in a reciprocal manner". Therefore, this study will consider this citation as a proper definition of trust among all those the literature may provide. Indeed, trust has been defined by researchers in many ways, which often are correlated to the academic ecosystem of the researcher or study. The types of research agreed on this definition related to e-commerce.

Nonetheless, trust is a cross-disciplinary concept, mixing notions from marketing, sociology, psychology, strategy or organizational behaviour. Mayer, Davis & Schoorman (1995) argue that the need for trust can be explained by the interdependence inherent in any relationship or interaction. Perceived risk is thus a key dimension of this research.

Ashleigh, Higgs & Dulewicz (2012) enlighten on the positive effects that trust may have on the individuals and attitudes of groups, and workplace behaviours. But considering the banking relationship, the importance of consensual interactions between a bank and its customers seems to be such a hot issue these days, as it may cultivate a long-run relationship. Williamson (1993) among others has demonstrated that institutions can create a frame which reduces or limits the uncertainty (and then the perceived risk) for the customer.

Mukherjee & Nath's research (2003) have demonstrated that issues of trust are "particularly true in the case of online banking, where the banks and the customers are physically separated [because] contingencies are difficult to predict and incorporate into terms and conditions, relationships are difficult to monitor, and cyber-laws are not well-defined. The heightened risk perceptions of customers affect the level of trust towards the online banks and their systems". They highlight then that trust in non-customer-facing (i.e. online) banking is a growing body of management research, as current literature is more focused on general issues.

Besides, lack of trust is one of the most frequent reasons why people choose not to buy or use online services (Einwiller et al., 2000; Grabner-Krauter and Kalusha, 2003). But, as Mayer et al. (p. 711, 1995) remember, "the *need* for trust only arises in a risky situation". The essence of a virtual interaction is not to be face-to-face. Therefore, the organizations tend to feed an image mostly by their online website/application. The sharing of information is hence system-dependent, while every online process is correlated to transaction-specific uncertainty (Grabner-Krauter and Kalusha, 2003).

TRUSTWORTHINESS

This notion could be confusing due to the polysemous nature of the word. Indeed, for instance, there is no proper and unique translation for this word in French. For the purpose of this study, I consider trustworthiness as the ability to trust that individuals may put in bank institutions. It refers then to trusting beliefs. Researches outcomes from Mayer et al. (1995) have conducted to define trusting belief subconstructs: competence (or ability), integrity and benevolence. These three characteristics of a trustee appear thus often in the literature. With each other, they seem to explain a large part of the trustworthiness, since each contributes to a unique perceptual perspective to better understand the trustee's perception.

Competence refers to the expertise relevant to fulfil a mission. Rosen & Jerdee (1977) seem to be one of the first to integrate this subconstruct within the notion of trust, considering "two dimensions of trust: (a) degree of confidence in employees' judgment or competence in the matter and (b) likelihood that the group would put organizational goals ahead of individuals goals" (Rosen B. and Jerdee T. H., p. 630, 1977). A few decades later, Mayer et al (1995) use the term *ability* to fulfil this notion, considering it as "that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain.". Most of the main types of research about this trust antecedent highlight that the higher the competence, the higher the trust.

These authors also provide the most recognized definition for *integrity*, based on the types of research's outcomes of McFall (1987) considering that "the relationship between integrity and trust involves the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable". Thus, integrity goes hand in hand with trustee personality more than about the trustor-trustee relationship.

Benevolence refers to the "extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive (Mayer et al., 1995). It reflects the specific relationship between trustor, namely the individual and trustee (i.e. the bank organisation), not trustee kindness to all.

PROPENSITY TO TRUST

The literature offers three main approaches depending on the preponderance of the studied dimensions. But beside the trustworthiness concept, trusts antecedents also include trust-propensity, as an internal element the individuals have to draw on. As Ashleigh, Higgs & Dulewicz (2012) argue, it seems then relevant to include such a variable in the study, since experimental studies tend to suggest that a predisposition measure would be meaningful to predict future behaviours. To follow Mayer et al. 1995 definition, this study considers propensity-to-trust as the "dispositional willingness to rely on others" that individuals have.

DISPOSITION TO TRUST

Knee & Knox (1970) developed that the probability that someone (P) trust someone (O) else is linked to the evaluation that P will make of O's possibility of betraying P's trust. Consequently, P faces a dilemma game while deciding to trust O. The authors argued thus that propensity to trust is – at least partially – based on personality. This approach is also defended by Rotter (1967) who is recognized in the literature, as one of the firsts authors to put forward a model whereby trust is defined according to a personality-based view. He highlighted that trust developed during childhood as an infant seeks and receives help from his benevolent caregivers, resulting in a general tendency to trust others. He considered it as the interpersonal trust, but others may denominate it propensity-to-trust (Mayer & al, 1995).

So, the ability of people to trust someone or something is partly due to past experiences. Individuals will learn from their missteps and gains. They will enhance their risk perceptions whilst redefine their trusting ecosystem. In interpersonal relationships between employees, McAllister (1995) associates trust with the notion of behaviour or voluntary action. He believes that a person is considered trustworthy from the moment that it "acts voluntarily based on the words, actions and decisions of another person". He found two forms of trust on affective (emotions, feelings) and cognitive aspects (competence). Consequently, trust differs

from one people to another depending on the trust propensity. This determinant of trust affects hence the perceptions people have of happenings.

Chin, Porter Felt, Sekar and Wagner's types of research (2012) have exhibited that individuals increasingly make it a practice to access their bank account without bricks-and-mortar-business philosophy. They indeed pick up their phones. Nevertheless, the study's outcomes reveal that the more people are concerned with security reasons (especially the fear of someone hacking their phone or fear of losing it), the more they tend to use their computer over their smartphone to deal with personal data, such as health or banking data. Users' willingness to perform different types of potentially sensitive activities differs depending on their risk beliefs. The authors also highlighted that individuals are more concerned about privacy whilst picking up their phones with a difference of about 10% less compared to laptop's use. But people's relative level of concern about security on their phone is about 20% higher compared to the laptop. Participants who were more concerned about privacy on their phone mentioned during the study that their phones carry more personal information (e.g. pictures, text messages). Their phones reveal hence their location, and phone numbers are tied to their identity. But they mostly considered stocking fewer personal information on their computer, explaining why they are less concerned about privacy on it.

SOCIALLY-ENVIRONMENT-BASED TRUST PROPENSITY

McKnight & Chervany (2002) have demonstrated that trust-related behaviours, is dependent upon both dispositional and interpersonal[17] trust, but also conditional on institutional trust, meaning the trust that an individual would place in the situation or structure. This sociological point of view should be then duly noted, since the banking industry used to fuel lots of misconceptions, especially regarding the banking scandals and financial crisis of the last decades. It may then be recalled the Crédit Lyonnais case[18], the Barings crisis[19], the Enron

[17] McKnight and Chervany have described dispositional trust as "trust in general others", whereas they consider interpersonal trust to refer to "trust in specific others".
[18] In 1993 Crédit Lyonnais is a French nationalized bank which lost 130 billion French francs due to a hit and miss system for managing the then financial risks.
[19] The Barings Crisis is related to one of Barings bank's trader: Nick Leeson, based in Singapore, who misjudges the Japanese economic recovery. The UK bank finally drop with 850 million pounds of loss.

scandal[20], the Kerviel fraud[21], the Madoff affair[22] or the subprime turmoil[23], just to name a few.

Hansen, Dunford, Alge and Jackson (2015) have besides shown the influence of an ethical climate on employees' propensity-to-trust. Indeed, it seems reasonable to think that if an individual is evolving in a trust-friendly environment, then people are more likely to effectively trust each other. The outcomes of their tests have proved that the trust propensity may be moderated by the degree of trustworthiness of the working environment (namely by the intensity of corporate social responsibilities policy).

In contrast, trust propensity may be even more considered as a relevant antecedent of trust if the trustor does not know the trustee (Colquitt et al., 2007). Considering the banking system, as every institution, trustor and trustee can really not know each other because of the intangible nature of an industry. People are less likely to consider it as trustworthy. Trusting an institution is related to balancing risks and benefits derived from the relationship. It appears that in France, where this study takes place, every adult has the right to have a bank account. Contrary to common beliefs, in France[24], it is officially not a duty but a right. Nevertheless, it may be complicated to live without one since salary above 1,500€ or welfare benefits cannot be received without a bank account. It skewed the relationship you may have with such an institution. Moreover, money concerns are usually one of the most sensitive topics in our current capitalist world. The 2008 subprime crisis and financial scandals intensify the risk perceptions from individuals. Jacobe (2008) has pointed out that in this year, "only 32% of Americans express confidence in the U.S. banking institutions" matching the lowest 1991 score. Kim and Prabhakar (2000) explained that trust towards the institutions, as banking may be perceived, relies on guarantees that the organisation can provide. It triggers the question what guarantee financial organisations are able to provide. Nowadays, alternative to banks are raising with a provocative approach for traditional bank organisations: "Because today's hyper-connected world deserves a financial partner just as progressive" ("About Us |

[20] The Enron scandal refers to corruption that lead to pension funds of million Americans collapsing.
[21] Jérôme Kerviel used to be trader for a French bank. His financial operations led to 4.9 billion euros loss, in the meantime with the subprime mortgage crisis.
[22] Bernard Madoff is known to conceive high-return financial arrangements. The fraud consists in compounding interests thanks to newcomers' financial contributions.
[23] The subprime turmoil is one of the worst financial crises for decades. It appeared in the United States of America and led to a severe real-economy recession.
[24] This study takes place in France. Therefore, France is here the main example cited.

Revolut", 2018). They are not banking institutions with certifications. But they provide services increasingly expected by customers. Well aware of risks that they may be raised, these new challengers seem to invest massively in protection. As N26, one of the Revolut's competitor, claims it, "N26 bank account is guaranteed by the Compensation Scheme of German Banks up to €100.000" ("Security at N26", 2018). The start-ups challenging traditional bank paradigm, also called FinTechs[25], are on the rise. Using technology to launch innovative banking and financial services while traditional banks are still facing with slow performance partly due to the infrastructures-and-regulatory-related constraints they may have. But at the end of the day, individuals may be confused with such different approaches.

[25] Fintech refers to *fin*ancial *tech*nology. Providing financial services, these companies include any technological innovation in the financial sector, including innovations in financial literacy and education, retail banking, investment and even crypto-currencies.

METHODOLOGY

METHODOLOGY PRESENTATION

LITERATURE REVIEW

The first step in conducting this quantitative analysis was to test my hypotheses thanks to the identification of relevant articles through the literature. Therefore, I performed a search using Google Scholar and the Paris-Dauphine University library and databases, mainly using *trust* and *GDPR* as the keywords. I also obtained relevant papers through Google Research to look for unpublished presentations and pieces of grey literature.

I then shortlisted the articles depending on the trust-relevant variables (whether trustworthiness, propensity to trust, trust or online relationship).

The following table offers a general census of the authors, thanks to who I was able to clearly identify questions that should be part of the final questionnaire.

AUTHOR	CONSTRUCTS						
	PTT	GDPR	CS	BR	C	I	B
Ashleigh, Higgs & Dulewicz (2012)	X						
Chin, Felt, Sekar & Wagner (2012)	X		X				
Colquitt, Scott & LePine (2007)	X				X	X	X
CNIL (2018)		X	X				
Einwiller, Geissler & Will (2000)	X		X	X			
European Parliament & Council		X	X				
Gatfaoui (2005)	X		X	X	X	X	X
Joergensen & Marzouki (2015)		X	X	X			
Lemoine & Cherif (2012)	X			X			
Nguyen & Leblanc (2001)				X			
Oliveira, Alhinho, Rita & Dhillon (2017)	X		X		X	X	X
Palvia (2009)			X		X	X	X
Safari (2017)		X		X			
Teo & Liu (2005)	X		X		X	X	X
Yang (2006)	X				X	X	X

Table 2. Literature review.

RESEARCH MODEL

The research model presented in Figure 1 considers a unique source for individuals' trust in the banking system, namely bank institution characteristics, composed of customer

satisfaction and brand recognition. The source of trust influences the dimensions of individuals' trust, which are: competence, benevolence and integrity. In turn, these dimensions hold sway over individuals' confidence in the bank system, depending on the regulation degree of expertise. In that respect, hypotheses were created for each source, dimensions and moderating variables.

BANK INSTITUTIONS' CHARACTERISTICS

In this section, I argued that banks are actually perceived or considered by individuals through two dimensions, namely the customer satisfaction and the brand recognition. Indeed, I considered that an individual would create his/her conceptions of the banking system through the satisfaction derived from his/her interactions with his/her bank agency.

The service quality an individual would receive from a specific relationship with bank workers will then generate and influence his/her assumptions about the banking system. In digital storefronts, virtual transactions involve trust in one-to-one relationships. Since the customer would no more have a face-to-face contact for its bank-related interactions considering the increasing dematerialized banking environment, trust is growing with the belief that the transaction partner will behave with goodwill and toward his/her interests.

Types of research on institution-based trust (eg. Kim and Prabhakar, 2000) show that trust towards institution primarily depends on guarantees that the organisation can provide. Impressions that can alleviate individuals concern about privacy, security - among others - can no more be fulfilled in dematerialized relationships. Thus, structural assurances, more than physical cues or face-to-face interactions, are important to build individuals' trust.
As customer satisfaction and brand recognition have the same way of affecting individuals' trust, I keep a unique hypothesis about bank institution characteristics, as an aggregate of the two constructs.

Hypothesis 1. There is a positive relationship between bank institution characteristics and individuals' trust.

THE MODERATING ROLE OF THE INDIVIDUAL'S CHARACTERISTICS

In this section, I will advance the model by considering the influence of two individual inherent bias that individuals may have, namely trust-propensity and data protection-based regulation degree of knowledge.

Trust-Propensity

The literature review has confirmed that everyone has a unique but particular disposition to trust, which has a significant impact on effective trust, especially in institutions. The propensity to trust others is considered as inherent to everyone. It has much more influence on behaviours and perceived risks as the exchange occurs without the first-hand knowledge of the other party. So, the hypothesis formulated to inquire about the influence of trust-propensity is:

Hypothesis 2. The higher individual's propensity to trust, the higher individual's trust towards his/her bank prior to the influence of expertise in data protection-based regulation.

Knowledge degree of Data Protection-based Regulation

This part used to be the more difficult to formalise since the academic body of research has not yet considered such a point of view when studying bias. I thus referred to grey literature, meaning the researches and studies that come from the professional ecosystem. Based on a research paper by Benaïcha-Tanquerel (2017), it appears that GDPR implementation has an impact on organizational and working day-to-day. Individuals would then assess risks incurred while trusting the bank. But assessing the risks entails a cost-benefit analysis. As deviant behaviours, especially considering money involved and current media coverage, tend to increase the perceived risks for individuals. Based on this, I formulate the following hypothesis:

Hypothesis 3. The higher individual's expertise in data protection-based regulation, the lowest individual's trust towards his/her bank.

DIMENSIONS OF TRUST

I further develop my research model by proposing that in addition to considering the bank characteristics, individuals used to also interpret their environment in view of the several dimensions of trust.

The three dimensions studied came from research material proposed above. Consequently, for research purpose, I considered *competence* to refer to individuals' belief that banks have the ability or power to do for one what one needs done. In the case of the distant (virtual) banking relationship, the individual would believe that the bank institution can provide financial services in a proper and convenient way while keeping private/personal information secure. So, I examined *integrity* considering that banks make good faith agreements, tell the truth, act ethically, and fulfil promises. Moreover, if *benevolence* is high, I considered that the individuals would believe that banks care about them and are leading to acting in the customer's interest. The individual would hence consider that her/her bank agency would not act opportunistically by taking advantage of him/her. In order to enquire whether competent, integrated and benevolent are more likely to be trusted by individuals, I hypothesized that:

Hypothesis 4. Trust individuals place in a bank will be based on banks' perceived competence, integrity and benevolence.

Figure 1 illustrates below the different variables tested by the study.

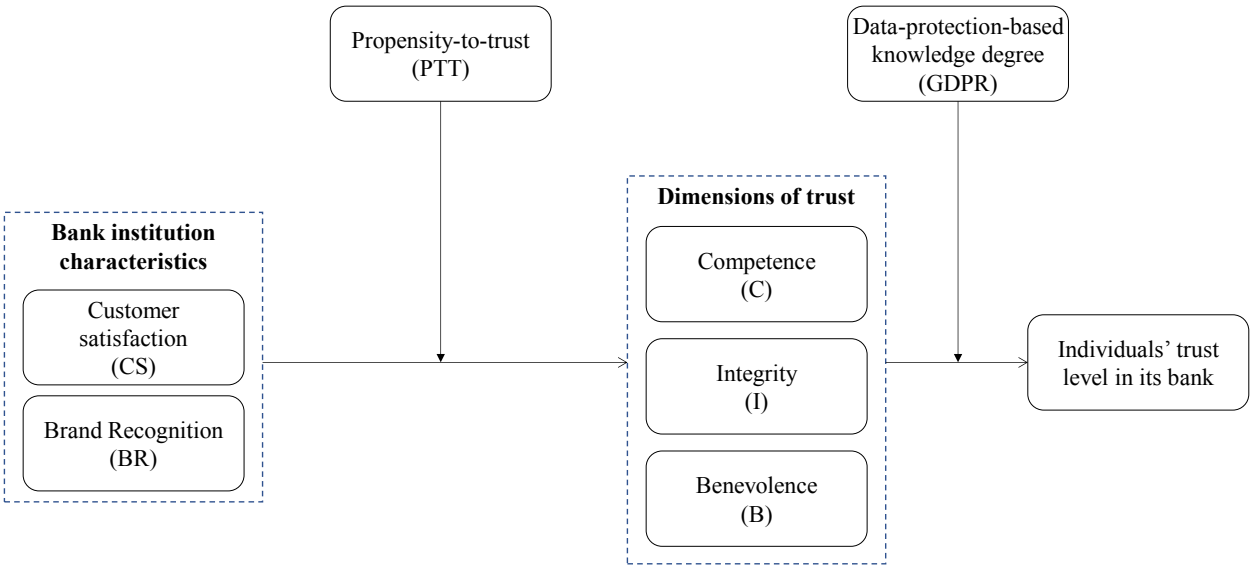

Figure 1. Research model.

GLOBAL RESEARCH PROCESS

EXPLORATORY TALKS

To establish the best criteria regarding this analysis, I chose to first conduct exploratory talks. I wished indeed to understand the vision people may have of the (retail) banking industry as well as their perceptions and knowledge degree of the legal context. Therefore, I selected the

half of the respondents among people who used to be the less aware of the two concepts I wanted to explore. By doing that, I wanted to be able to precise as much as possible the questionnaire I would conduct later. Conducting interviews with such individuals is here fundamental to create a questionnaire designed for any level of expertise in banking industry or regulation.

The interview guide is provided in Appendix D. It was created according to the first lectures I had about trust, especially trust toward the institutions. I prepared the interviewee guide by gathering all the notions I wanted to master for defining and narrowing the topic. Therefore, I gathered all key topics related to propensity-to-trust factors and regulation-change elements. The idea of such an approach was to understand how people would decide to actually trust an institution which can have such a significant impact in the case of data breach or leak of confidential information. Table 17 lists the theoretical background that justifies the elements I decided to investigate during the exploratory talks.

The transcripts of the exploratory talks are available in Appendix E. To identify the interviewees, I asked managers and friends. It allows me to know individuals who were novice and expert. Once I knew names, I directly contact them, explaining my approach and how I decided to study such an issue for my master's degree. Besides these contextual elements, I also justified my decision to pick them for my exploratory talks. Once they agreed, we chose an hour-long slot to meet and talk. I conducted semi-directive interviews, meaning that it was open-ended questions even if I kept in mind all the topics I wanted to be covered. All the interviewees allowed me to tape-record the conversation, enabling me to stay focus on the discussion and not on noting down key elements. I always tried to be as precise as possible, defining the notions and the acronyms I used, acting like the interviewee was not aware of none of the subjects.

Table 3 summarizes the expertise level[26] of each of the respondents.

EXPERTISE LEVEL ON GDPR	EXPERTISE LEVEL ON BANKING INDUSTRY	AGE	GENDER
1	2	49	Female

[26] The expertise level is rated according to a five-point Likert scale with 1 = low-level expertise and 5 = high-level of expertise.

EXPERTISE LEVEL ON GDPR	EXPERTISE LEVEL ON BANKING INDUSTRY	AGE	GENDER
0	1	55	Male
4	3	22	Female
2.5	4	25	Male

Table 3. Interviewee expertise profile

INTERNAL DOCUMENTS

I had the opportunity to be integrated within Management Consulting teams as part of my 2-year-apprenticeship. I was hired by consulting firms. Therefore, I had access to internal documents, which were truly relevant since the core business is to streamline and restructure organizations to get themselves leaner and meaner. Eventually, all the firms want to adapt the day-to-day process to fit as much as possible with their constraining ecosystem. Consulting firms gain a foothold with the GDPR implementation. Clients – so basically any business – need to comply with this new reference text. Thus, consulting firms have nowadays specialized in turnkey projects.

Being part of such firms allows me to access restricted and controlled documents. Some of them were available on the company's intranet. Hence, I needed additional information and feedbacks, so I looked for people able to do so. After naming them, I contacted and meet them. Besides the observation I can get, the team I met sent relevant files to me. The complementary documents are mainly presentations or commercial proposals. Internal documents are marked by a statement "confidential" with an increasing score depending on the inherent riskiness. Other documents were training material available on the intranet. These were generally more general informing collaborator about the regulation or wins of missions.

These documents help me in a first place to define and narrow the topic I wanted to cover. Regarding my first-year research paper on corporate challenges from GDPR implementation, I knew I want to study issues related to GDPR. Thanks to my academic tutor and my appetite for HR topics, I finally decided to mix these two concepts and figure out if they were correlated.

MEASUREMENT INSTRUMENTS

The items for all the constructs I used for this study are included in Appendix B. They have been chosen according to the literature. I identified seven variables: customer satisfaction (CS), competence (C), integrity (I) and benevolence (B) from Palvia (2009); brand

recognition (BR) from Nguyen and Leblanc (2001) cited in Oliveira & al (2017); propensity to trust (PTT) from Ashleigh, Higgs & Dulewicz (2012). All the items related to data protection were provided regarding the regulation from European Parliament & Council (2018). Thanks to the questionnaire they all offers in their research appendix, I was able to design my own questionnaire by being aware of the relevant questions depending on the notion studied. Table 11 in Appendix B lists all the constructs directly link to the trust and regulation notions, in addition, to provide numbers for each item for the purpose of later coding.

Chin, Porter Felt, Sekar and Wagner 2012 types of research' outcomes have emphasized the gap in worrying about privacy depending on age group. So, besides the questions directly related to the research topic, the questionnaire includes a measure of variables, such as gender, age, educational level, tenure within the bank agency where the respondents were clients. A more detailed description can be found in the Appendix. Table 12 in Appendix B stipulates the coding and the measure used for this study depending on the level. I choose to keep general scale – neither too larger nor too specific in order to be able to aggregate answers and make global deductions.

Based on the literature, the pre-test results and the exploratory talks, the final questionnaire was proposed both in English and French, since even if the research paper is in English, the sample mostly gathers French-speaking respondents. It was distributed online, using dauphinem1.eu.qualtrics.com, and requiring rating the questions on a five-point Likert scale, where 1 is "strongly disagree", and 5 is "strongly agree".

DATA COLLECTION

In May 2018, exploratory talks were finalized to be able to construct the adequate items for the survey.

In June 2018, a pilot survey was conducted with 17 answers in order to gauge the structure and the content before choosing the final items proposed in the questionnaire. It led to adding marginal modifications to the final questionnaire, such as adding the tenure variable and adjusting the French translations to better fit with the meaning.

From June to August 2018, the questionnaire was shared through emails and on social media, in order to reach as large an audience as possible, targeting any individuals of age, and a total of 268 answers were achieved. The final valid respondents' sample used to structure the analysis, consists of 170 peoples. A response is considerate as valid, once complete and non-subvert. Such characterised answer indeed provides an overall response rate of 63.34%.

The questionnaire was taken mostly by French-native speakers since 151 individuals (i.e. 88.82%) chose to play it in French (some answers - depicting 19 individuals or 11.17% of the respondents' sample - came from Canada, Belgium, and Switzerland and were in English).

The sample is made up of 170 individuals – 83 males (48.82%) and 87 females (51.18%) as illustrated in Figure 2. The statistics provided by the French Institute for official statistics (Insee) indicate that female represent 51.58% of the French population while men are only 48.42% of the population. It appears thus that the sample is sufficient to accurately represent the population.

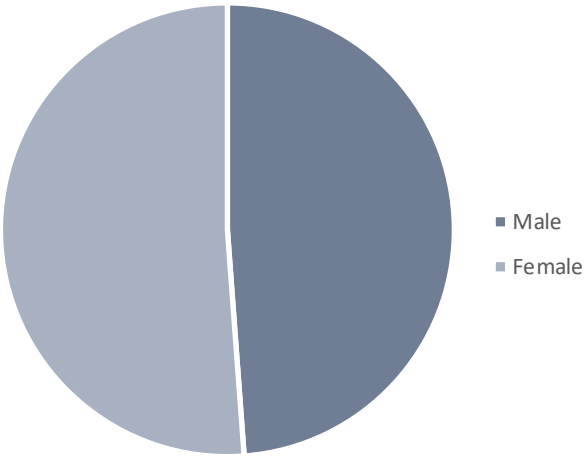

Figure 2. Age repartition

The average age of respondents is 37, the youngest respondent being 21, and the oldest 74 (see Figure 3). Once again, it appears concordant regarding the diffusion of the questionnaire. It was indeed shared among colleagues, managers, family and students.

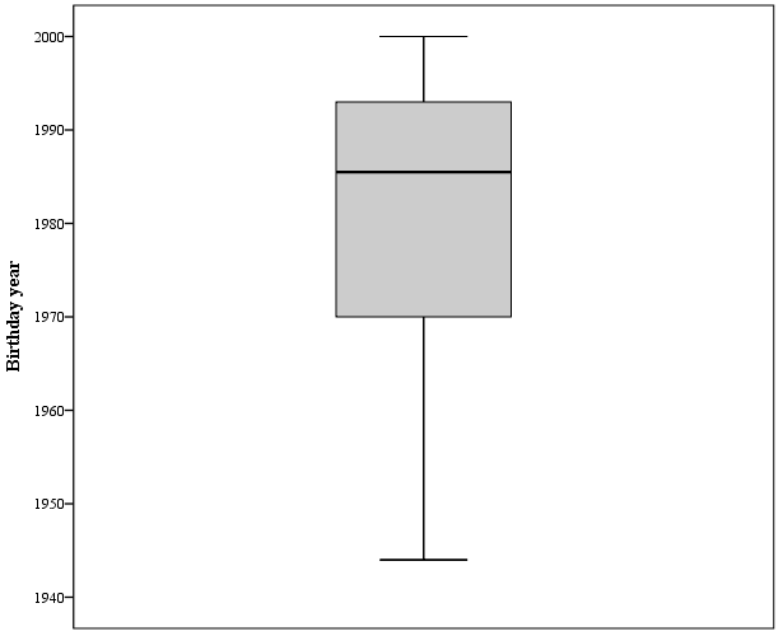

Figure 3. Age repartition

I may be relevant to notice that male respondents tend to be older than female (see Figure 4). Nevertheless, it may be a limit of my study since I did not investigate the gap in trusting others based on the gender repartition.

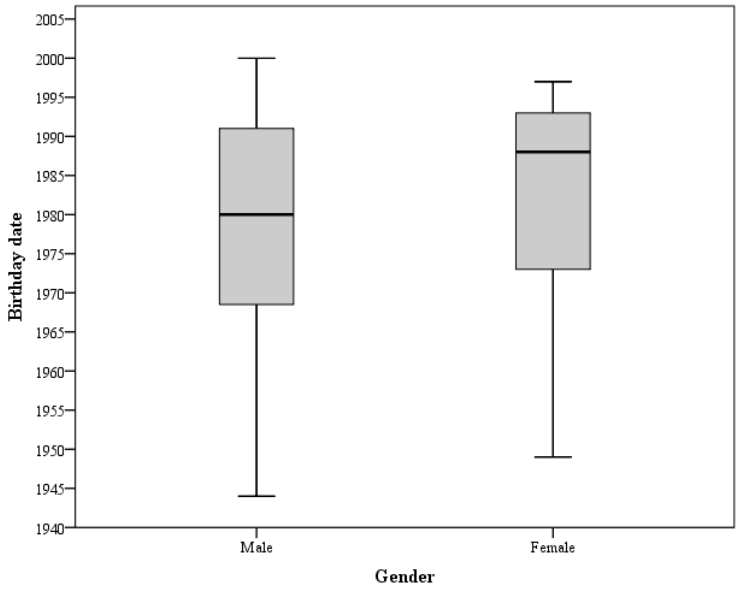

Figure 4. Age repartition according to gender

Regarding the education level, Figure 5 illustrates that most of the respondents (44.97%) have a master's degree (76 individuals), 11.83% an undergraduate degree (20 individuals), 8.28% a bachelor's degree or a thesis (14 individuals for both), 4.73% a high school degree (8 individuals) and 1.18% of the respondents have no diploma (2 individuals).

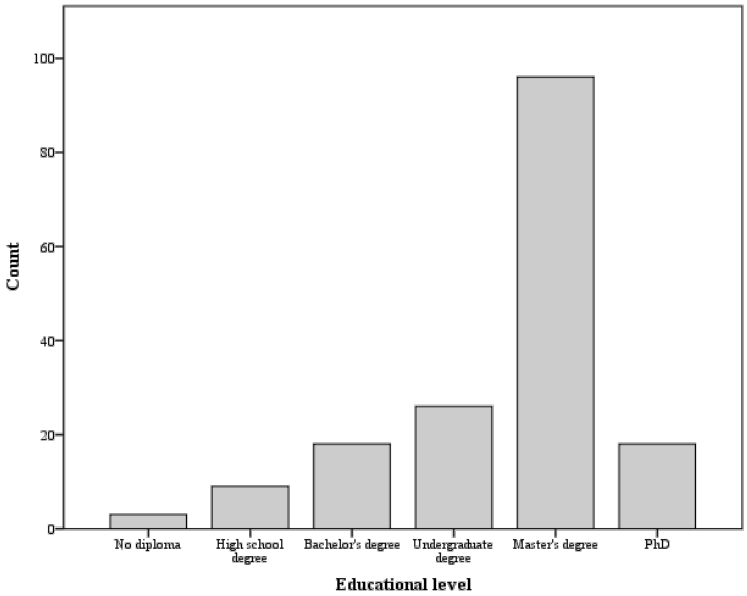

Figure 5. Educational level repartition

Finally, the Internet-mediated questionnaire exhibit that respondents tend to be longstanding customers of their current bank agency (see Figure 6). It may also affect the trust in banks depending on nature (conflicting or not) of the relationship with their bank advisor.

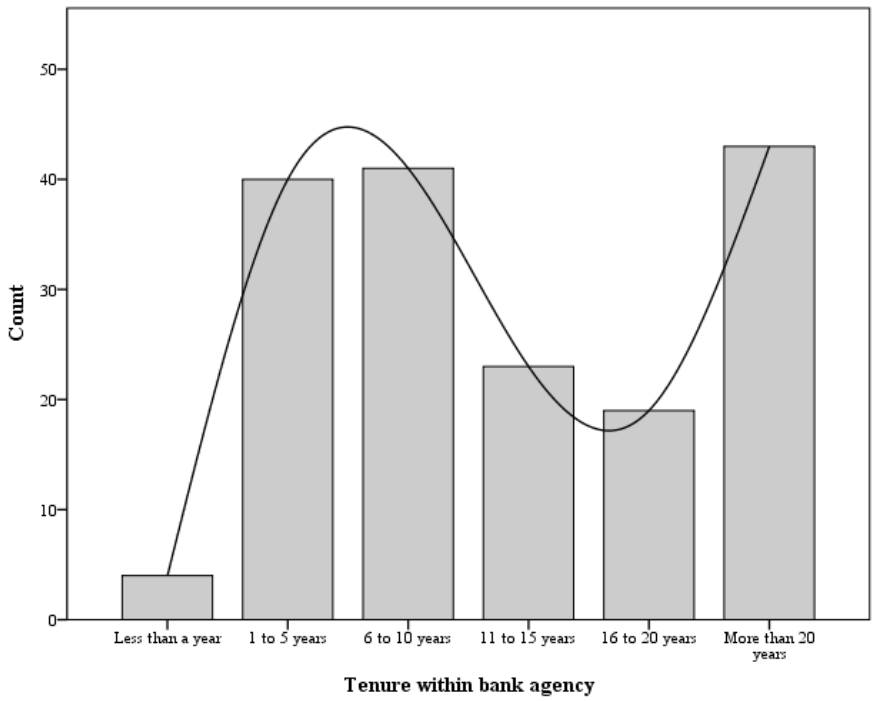

Figure 6. Tenure within bank agency

DATA ANALYSIS

TESTS OF HYPOTHESES

Testing my model involved a two-step approach since it seems that there is no direct test considering 4 variables, namely individuals' trust, propensity-to-trust, GDPR expertise and bank institutions' characteristics.

So, I first considered the correlation between individuals' trust, propensity-to-trust and bank institutions' characteristics (see Figure 7), before testing the influence of the GDPR expertise on this trust level (see Figure 8).

FIRST PHASE OF TESTING

The first phase of testing is about checking the reliability of the variables. Indeed, both *Bank Institutions characteristics* and *Dimensions of trust* are an aggregate construct of several dimensions. Therefore, the study has initially considered that 'Bank Institutions' characteristics' variable depends on 'Customer satisfaction' and 'Brand recognition', while 'Competence', 'Integrity' and 'Benevolence' constitute the 'Dimensions of trust' construct. To test this out, I calculated the Cronbach's Alpha. The coefficient helps to determine the consistency.

Once the internal coherence was checked, I tried to figure out how much trust can be explained by bank institutions characteristics and individuals' propensity-to-trust.

All the variables tested used at this stage to be ordinal. Then, based on the statistical requirements, I applied a multiple regression test.

Figure 7 illustrates below the different variables tested first in the two-step approach.

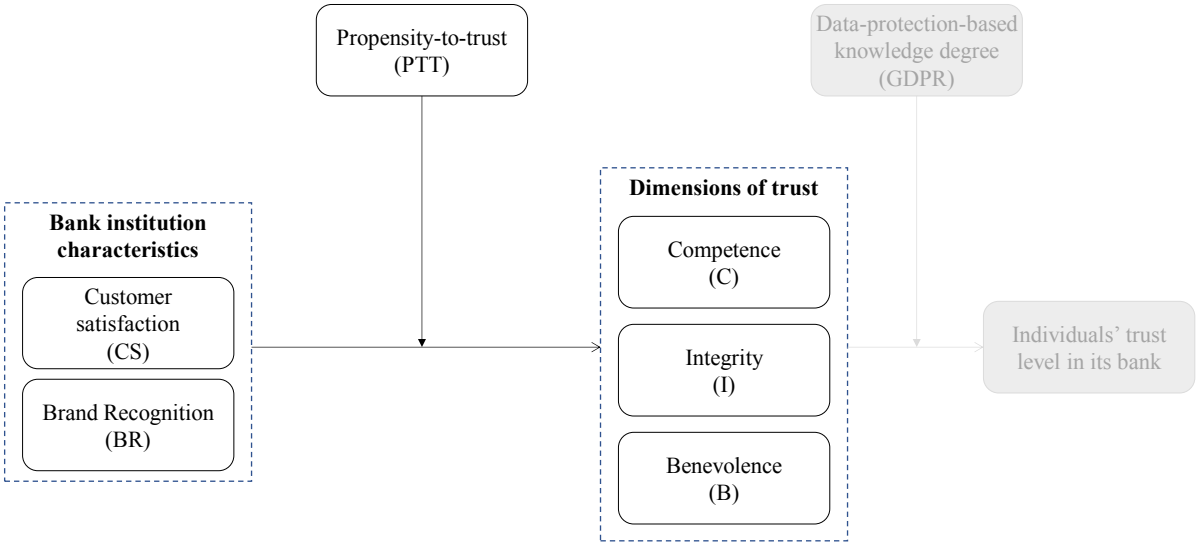

Figure 7. The first phase of testing

SECOND PHASE OF TESTING

According to Saunders, Lewis and Thornhill's guidelines (2008), this study relies then on ordinal data, because on one hand individuals' trusts (namely initial and final trust) are measured through a Likert scale, while on the other hand, GDPR expertise is rated according to a score from 0 to 12, depending on the level of knowledge.

To test the influence that data-protection-based regulation may have on trust level, I applied a Wilcoxon signed-rank test. Strictly speaking, it is designed for continuous data, but it is frequently run with ordinal data (Sheskin, 2011). The test involves the three following assumptions that need to be fulfilled for a significant conclusion:

1. The model includes one dependent variable. Here is the final trust variable.
2. The model includes one independent variable. Here are the two categorial, related groups, meaning before and after an explanation about GDPR.
3. Distribution of the differences between the two related groups must be symmetrical in shape. The assumption is also fulfilled since the groups are the same one at two periods of time (before and after explanations about GDPR).

Such a test induces to state null hypothesis, according to which there is no difference in individuals' trust in the bank system, depending on their GDPR expertise. The test will

determine whether the median difference between the two related groups is statistically significant.

Figure 8 illustrates below the different variables finally tested in the two-step approach.

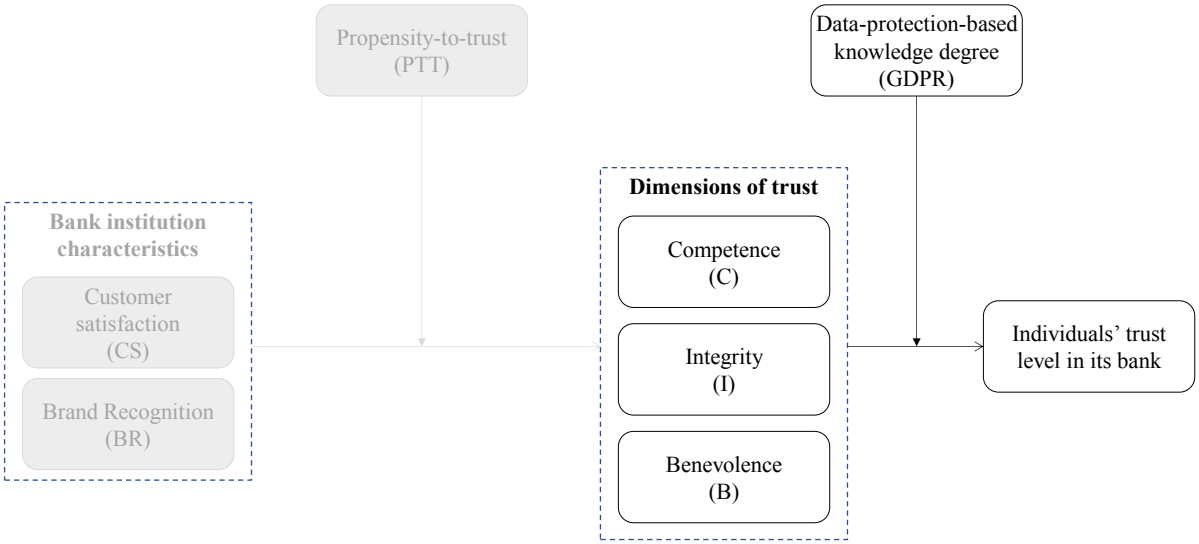

Figure 8. The second phase of testing

RESULTS

To make the results easier to read, the detailed charts, graphs and tables are available in Appendix C with all the extensive findings. Moreover, Table 9 summarizes the conclusion of all the findings generated by the statistical tests.

FIRST PHASE OF TESTING

As previously explained, I first checked the Cronbach's alpha related the Bank Institutions' characteristics in order to enquire whether or not the 'Customer Satisfaction' (CS) and 'Brand Recognition' (BR) variables were concordant with the 'Bank institutions' characteristics' constructs.

A questionnaire was employed to measure different, underlying constructs. One of them, 'Bank Institutions' characteristics', consisted of five questions. The related scale indicates a high level of internal consistency (DeVellis, 2003; Kline, 2005) between CS and BR because determined by a Cronbach's Alpha of 0.877 (see Table 4). To be considered as such, it must be above 0.7. So, it was relevant to aggregate BR and CS in the 'Bank institutions' characteristics' constructs.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.877	.875	5

Table 4. Reliability Statistics related to 'Bank Institutions characteristics' variable

Considering the construct related to trust (i.e. 'Dimensions of trust'), the ten questions are determined by a Cronbach's alpha of 0.777, so the construct reflects well the different dimensions of trust.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,777	,814	10

Table 5. Reliability Statistics related to 'Dimensions of trust' variable

A multiple regression was run to predict trust from propensity-to-trust and bank institutions characteristics. There was linearity as assessed by partial regression plots and a plot of studentized residual against the predicted values. There was the independence of residuals, as assessed by a Durbin-Watson statistic of 1.968 (see Table 13 available in Appendix C). There was homoscedasticity, as assessed by visual inspection of a plot of studentized residuals versus unstandardized predicted values. (see Figure 10 and Figure 11 in Appendix C) There was no evidence of multicollinearity, as assessed by tolerance values greater than 0.1 (see Table 14 in Appendix C). There is only one studentized deleted residual greater than ± 3 standard deviation (see Table 6), no leverage values greater than 0.2, and values for Cook's distance above 1. The assumption of normality was met, as assessed by a Q-Q Plot (see Figure 11 in Appendix C). The multiple regression model statistically significantly predicted as following:

$$Trust, F(2,167) = 66.481, p < 0.005, adj.R^2 = 0.437$$

Equation 1. Multiple Regression Model Equation

VARIABLE	B	SE_B	β
(Constant)	1.704	.288	
Bank Institutions Characteristics	.463	.040	.670*
Propensity-to-Trust	.048	.067	.042*

Note. *p < 0.05; B = unstandardized regression coefficient; SE_B = Standard error of the coefficient; β = standardized coefficient

Table 6. Summary of Multiple Regression Analysis

SECOND PHASE OF TESTING

Of the 170 Internet-mediated questionnaire's participants, the explanations and details elicited a declining trust in 107 participants compared to the participants without any GDPR expertise, whereas 27 individuals saw no difference and 36 consider that it helps to trust more their bank (see Figure 9).

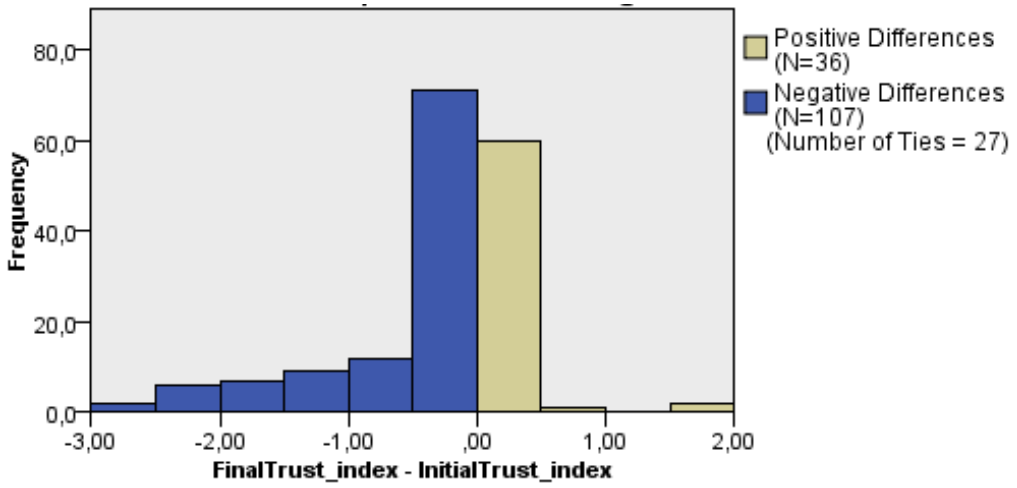

Figure 9. Related-samples Wilcoxon Signed Rank Test Results

As illustrated by Table 7, the Wilcoxon signed-rank test determined that there is a statistically significant median decrease in individuals trust towards bank institutions (Mdn = -0.20). By calculating the difference between the two stages (prior to and after explanation), it appears that the more people are aware of the knowledge level related to data protection, the lower the trust.

FinalTrust_index	InitialTrust_index	difference
3,30	3,55	-,20

Table 7. Median report

The results also lead to conclude that subjects learned with the questionnaire about data-protection-based regulation, and specifically about GDPR, regarding the trust level prior to explanations (Mdn = 3.55), compared to final one (Mdn = 3.30), $z = -6.993$, $p < 0.001$ (see Table 8).

Total N	170
Test Statistic	1 689,500
Standard Error	494,569
Standardized Test Statistic	-6,993
Asymptotic Sig. (2-sided test)	,000

Table 8. Related-samples Wilcoxon Signed Rank Test Results Table

RESULTS SUMMARY

Table 9 summarizes below the results demonstrated above in this section, with a hypotheses conclusion analysis.

HYP.	INDEPENDENT VARIABLES	DEPENDENT VARIABLES	FINDINGS	CONCLUSION
H1	Customer satisfaction Brand recognition	Dimensions of trust	The regression coefficient is 0.463 (> 0) with a Cronbach's Alpha of 0.877 (0.7)	Supported
H2	Propensity-to-trust	Dimensions of trust	The regression coefficient is 0.463 > 0	Supported
H3	Data-protection-based knowledge expertise	Dimensions of trust	The trust level decreases after explanations about GDPR (dif = -0.2)	Supported
H4		Competence Integrity Benevolence	The Cronbach's Alpha is 0.777 (> 0.7)	Supported

Table 9. Hypothesis conclusions.

GENERAL DISCUSSION

RECOMMENDATIONS

Although there is at this time only a limited body of research studying the correlation between compliance degree and trust, I have no doubt that the compliance upturn would generate more and more researches on related issues.

THEORETICAL IMPLICATIONS

My study offers three theoretical contributions to the trust literature.

First, by setting up a relationship between trust and compliance expertise, the results contribute to exhibit that knowledge-based trust is meaningful to well establish a long-run, virtual relationship. Indeed, most of the earlier studies only include customers-related factors, including propensity-to-trust. As Lemoine & Chérif (2012) show, the risks that a customer will perceive from the money-based settings have a significant impact on the final decision to continue further the relationship. It is therefore not only about the pricing (external factor) but also about the psychological barriers inherent to everyone. But besides these contextual factors defined by the cited authors, the earlier literature does not consider the degree of expertise on regulation as part of the consumer-related factors, on the same basis as familiarity with the website, the Internet or the new technologies area.

Second, my research shows that in a dematerialized context, individuals tend to be more suspicious especially about the sharing of personal data. Indeed, people are increasingly connected. So, the technology itself may be considered as an object of trust since it supposed to be predictable. The risks related to online transactions may be affected because technology helps to reduce system-dependent uncertainty. Grabner-Kräuter & Kalusha (2003) argue that both growing third parties in the online industry and increasing sophistication in technology would help to convey trust to clients.

Finally, as Benaïcha-Tanquerel (2017) already explained, regulation, and especially GDPR, should not be perceived - only - like constraints. They should indeed be considered as the catalyst for change. Creating a new business model means being proactive instead of a never-ending adaptation to follow new regulations, including costly changes. To do so, banks should

proceed to their current status assessment to be then able to identify development levers. It appears that GDPR is an impressive trigger to rethink human resources procedures, IT processes as well as strategic vision.

MANAGERIAL CONTRIBUTIONS

In addition to the three previous theoretical contributions, my study offers three managerial inputs.

Practically, banking organizations find advantages, if they more consider that virtual, social interactions are increasing with the dependence of the population on smartphones and others connected devices. Therefore, transactions processes tend to be more and more dematerialised. In the context of this study, no bank may afford to expose individuals' sensitive information and financial data. This may appear as a paradox since the individuals are willing to more and more easy-accessed individual banking monitoring with the background but also fitting information. The individuals, especially working people, want to be able to chat with their bank advisor without meeting at their local bank agency - often closing at 6 PM or sooner. This raising requirement may explain the spate of online banks creation. But banks should pay attention to their marketing message especially with the current conflict among all the myriad of similar offerings. Moreover, it may be relevant to really think about the user interface about sensitive information required by banking transactions as privacy by design refers to. Such an improvement would help customers to feel comfortable, appeased but mindful while using their devices.

Based on my study's outcomes, I may find relevant for bank institutions to be more concerned about user education to avoid misconceptions about security and privacy. Concordantly with Chin, Porter Felt, Sekar and Wagner (2012) types of research, a long way in helping clear false assumptions could be valuable in security, banking contexts. To do so, frequent interactions with the bank counsellor would help the clients to enhance their trust in the banking institutions because they would feel as important, well-known customers. It would also intensify the degree of relationship. The banking experience would hence be easier and personalized. Moreover, further explanations about constraints and requirements that banks are facing could help to improve their brand image. Indeed, one of the interviewees told me that "I think it is crazy that my so-called traditional bank requires two days to execute a bank

transfer, while the amount had been debited to my account in less a second. But the money is transferred only two days later to the beneficiary account. For a long time, I thought there is a reason for such a delay like a need for infrastructure, but now all these raising fintechs tend to prove that it is not so." Such a comment is no exception.

Third, the regulation is increasingly present within the banking industry[27], implementing a demanding, costly framework. It appears that data minimization may be a promising idea since the GDPR involves a defined purpose for each use of personal data. Banks tend nowadays to keep all the data they collect "just in case". Regarding the cost generated by the data solution providers, rightfully choosing the archived data may be efficient to generate cost savings. To do so, thinking about a meaningful data management policy, as well as implementing a "privacy by design[28] and by default[29]" seems to be a good start. Nevertheless, it seems that GDPR involves costly transformations, since the data portability and transfers to mention just a few, generate a technical evolution to subsequently comply with this new regulation. Vanberg & Ünver (2017) have investigated the limitations generating by the data portability requirements. They confirm that complying may incur disproportionate costs and efforts.

LIMITATIONS

Although the outcomes of my research were consistent with theories and expectations, this study comes with its limitations.

First, when exploring issue related to GDPR, a first major challenge I faced is related to prior literature. It is, in fact, a regulation implemented since May 25, 2018. Therefore, not many research papers address this topic so far. In papers I considered for this research, authors observe the regulation in terms of change of paradigm and habits with no consideration of

[27] Here are some of the current regulations. The Foreign Account Tax Compliance Act (**FATCA**) aims to reduce the level of tax avoidance by U.S citizens and entities through non-U.S financial institutions and offshore accounts. The markets in financial instruments directive (**MiFID**) aims to increase the transparency across the European Union's financial markets by standardizing the regulatory disclosures required for particular markets.
[28] "Principle based on this insight that building in privacy features from the beginning of the design is preferable over the attempts to adapt a product or service at a larger stage" (Danezis et al., 2015)
[29] "[Principle based on the fact that] in the default setting the user is already protected against privacy risks" (Danezis et al., 2015)

trust. This cognitive bias may be explained by the short time since the regulation is known and studied.

Second, even if all the study variables were fulfilled via the questionnaire I administered, this study's results may have been affected to some degree by same-source bias. I was indeed able to submit my survey mostly to my professional, social and familial circles.

Third, as is the case with most research papers for the master's degree, results may not be generalized beyond my sample organization. As far as I know, there is no such paper at this present time, studying the bias generated by compliance-based expertise degree on trust in organizations. Therefore, the sample may not be representative of the global population in terms of gender repartition, in terms of age, in terms of habitus.

CONCLUSION

In this study, I presented a theoretical model arguing that data-protection-based expertise impacts the trust level of individuals towards retail banking institutions. I also studied links between banks' characteristics, propensity to trust and dimensions of trust. It appears that the more they are aware of regulation, the more suspicious individuals tend to be about banks and data breaches.

The study's outcomes aim at clearing up the influence of the regulation expertise on the individuals' behaviours, as other customers' factors (propensity to trust, brand image perceptions and so on). In prior literature, no proper link has been set between trust and regulation expertise. Hence it appears that individuals tend to be more and more eager to know what firms and institutions may do with their personal data and the inherent risks.

To perform this research, internal documents presenting GDPR transformation plans as well as internal communication about this new regulation were examined in order to acquire an understanding of banks' issues and context. Then, exploratory talks were performed to be in touch with reality related to bank perceptions individuals may have, regardless of their degree of expertise in the banking system or regulation. Finally, an Internet-mediated questionnaire was administered to better understand the reliability and influence of variables.

The research highlights first some antecedents of trust. It appears that individuals tend to take into consideration banks' characteristics to actually put their trust in. In addition to these external factors, individuals are biased by their propensity to trust depending on their aversion to risks, the trust in others and their perceptions about others' reliability and integrity. Yet, the questionnaire conducted to demonstrate that individuals have good knowledge about the risks related to a data breach.
It also appears valuable to educate web users to balance out the data-protection risks while they tend to be increasingly hyper-connected with multiple devices both personal and professional. Banks should also adapt their data-oriented strategy with a posteriori

anonymisation and pseudonymisation at the earliest convenience. Moreover, storage privacy[30] may be enhanced. Nevertheless, it may be costly for organisations to apply such changes to comply with all the guidelines proposed by the new regulation. To offset negative beliefs about regulations requirements, this study advocates considering such as an impressive opportunity to proactively change the business model of traditional banking institutions to better fit with customers' desires and expectations.

[30] Storage privacy refers to the ability to store data without anyone being able to read or change them, except the party that stored them in the first place or someone approved.

REFERENCES

About Us | Revolut. (2018). Retrieved from https://www.revolut.com/about

Abramatic, J.-F., Bellamy, B., Callahan, M. E., Cate, F., van Eecke, P., van Eijk, N., … Hijmans, H. (2015). Privacy Bridges: EU and US Privacy Experts In Search of Transatlantic Privacy Solutions.

Accenture. (2017). GDPR & Accenture. Retrieved December 2017

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review*, *2*(3), 287–289.

Ashleigh, M. J., Higgs, M., & Dulewicz, V. (2012). A new propensity to trust scale and its relationship with individual well-being: implications for HRM policies and practices. *Human Resource Management Journal*, *22*(4), 360–376.

Benaïcha-Tanquerel, C. (2017). *Les données personnelles en entreprise*. Université Paris-Dauphine, Paris.

Butler Jr, J. K. (1991). Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. Journal of Management, 17(3), 643–663.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (p. 1). Washington, D.C.: ACM Press.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*(4), 909.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering.

DeVellis, R. F. (2016). *Scale development: Theory and applications* (Vol. 26). Sage publications.

Diker Vanberg, A., & Ünver, M. B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*, *8*(1).

Duane Hansen, S., Dunford, B. B., Alge, B. J., & Jackson, C. L. (2016). Corporate Social Responsibility, Ethical Leadership, and Trust Propensity: A Multi-Experience Model of Perceived Ethical Climate. *Journal of Business Ethics*, *137*(4), 649–662.

Einwiller, S., Geissler, U., & Will, M. (2000). Engendering Trust in Internet Business using Elements of Corporate Branding (p. 54). Presented at the AMCIS 2000 Proceedings.

European Parliament & Council. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2018).

Gallouédec-Genuys, F., & Lemoine, P. (1980). Les enjeux culturels de l'informatisation. *Documentation Français*, *9*.

Gatfaoui, S. (2005). Une analyse dynamique de la construction de la confiance dans la relation client-particulier/banque : une approche par les études de cas rétrospectives (PhD Thesis). Université Paris XII Val De Marne UFR de Sciences Economiques et de Gestion IRG–Pôle marketing et logistique.

Gazagne, D. (2016, January). Enquête numérique: les systèmes d'information ont de la mémoire. Sécurité & Stratégie, 21, pp. 36 - 43. Retrieved January 2018

Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, *58*(6), 783–812.

Hansen, S. D., Dunford, B. B., Alge, B. J., & Jackson, C. L. (2016). Corporate Social Responsibility, Ethical Leadership, and Trust Propensity: A Multi-Experienced Model of Perceived Ethical Climate. *Journal of Business Ethics*, *137*(4), 649–662.

Hildebrandt, M. (2015). Legal Protection by Design: Objections and Refutations. *Legisprudence*, *5*(2), 223–248.

Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509–521.

Hoxmeier, J. A., Nie, W., & Purvis, G. T. (2000). The impact of gender and experience on user confidence in electronic mail. *Journal of Organizational and End User Computing (JOEUC)*, *12*(4), 11–20.

Institut national de la statistique et des études économiques. (2018). Population par sexe en 2018. Retrieved 15 August 2018, from https://www.insee.fr/fr/statistiques/2381466#tableau-Donnes

Internet access 'a human right'. (2010, March 8). *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/technology/8548190.stm

Jacobe, D. (2008). Confidence in U.S. Banks Down Sharply. *Gallup Poll Briefing, 1*.

Joergensen, R. F., & Marzouki, M. (2015). Reshaping The Human Rights Legacy In The Online Environment. *L'Observateur Des Nations Unies*, *38*, 17–33.

Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Journal of Conflict Resolution*, *14*(3), 357–366.

Kim, G., Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, *19*(3), 283–311.

Kim, K., & Prabhakar, B. (2000). Initial trust, perceived risk, and the adoption of internet banking. In *Proceedings of the twenty-first international conference on Information systems* (pp. 537–543). Association for Information Systems.

Kline, R. B. (2015). *Principles and Practice of Structural Equation Modeling, Fourth Edition*. Guilford Publications.

Laerd Statistics (2015). Wilcoxon signed-rank test using SPSS Statistics. *Statistical tutorials and software guides*. Retrieved from https://statistics.laerd.com/

Lemoine, J.-F., & Cherif, E. (2012). Comment générer de la confiance envers un agent virtuel à l'aide de ses caractéristiques ? Une étude exploratoire. *Management & Avenir*, (8), 169–188.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709.

McAffe, A., & Brynjolfsson, E. (2012, October). Big Data: The Management Revolution. Harvard Business Review, pp. 61 - 68. Retrieved September 2017

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. Academy of Management Journal, 38(1), 24–59.

McFall, L. (1987). Integrity. *Ethics*, *98*(1), 5–20.

McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, *6*(2), 35–59.

Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, *21*(1), 5–15.

Nguyen, N., & Leblanc, G. (2001). Corporate image and corporate reputation in customers' retention decisions in services. Journal of Retailing and Consumer Services, 8(4), 227–236.

Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior*, *71*, 153–164.

Palvia, P. (2009). The role of trust in e-commerce relational exchange: A unified model. *Information & Management*, *46*(4), 213–220.

Pelligrini, F., & Vitalis, A. (2018). L'ère du fichage généralisé. *Le Monde Diplomatique*, 3–6.

PricewaterHouse Coopers (PwC) & Association Management des Risques et des Assurances de l'Entreprise (AMRAE). (2015). Le Baromètre du Risk Manager. AMRAE. Retrieved March 2016.

PricewaterHouse Coopers (PwC). (2017). 8 tendances techno : comment s'y préoparer. Paris. Retrieved April 2017.

Ritter, D. S. (1993). *Relationship banking: cross-selling the bank's products & services to meet your customer's every financial need*.

Rosen, B., & Jerdee, T. H. (1977). Influence of subordinate characteristics on trust and use of participative decision strategies in a management simulation. *Journal of Applied Psychology*, *62*(5), 628.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*(4), 651–665.

Safari, B. A. (n.d.). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, *47*, 40.

Saunders, M., Lewis, P., & Thornhill, A. (n.d.). *Research Methods for Business Students* (5th ed.). Pearson Education.

Security at N26. (2018). Retrieved from https://n26.com/en-fr/security

Sheskin, D. J. (2011). *Handbook of parametric and nonparametric statistical procedures*.

Teo, T. S., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore and China. Omega, 35(1), 22–38.

Yang, K. (2006). Trust and citizen involvement decisions: Trust in citizens, trust in institutions, and propensity to trust. *Administration & Society*, *38*(5), 573–595.

Williamson, O. E. (1993). Calculativeness, trust, and economic organization. The journal of law and economics, 36(1, Part 2), 453-486.

APPENDIX

A. LIST OF ABBREVIATIONS

The following table offers a list of all the abbreviations used in this study.

A	» A: Age
B	» B: Benevolence » BCR: Binding Corporate Rules » BR: Brand recognition
C	» C: Competence » CJEU: Court of Justice of the European Union » CNIL: Commission Nationale de l'Informatique et des Libertés - *in French* » CS: Customer satisfaction
D	» DPO: Data Protection Officer
E	» EL: Educational level » EU: European Union
G	» G: Gender » GDPR: General Data Protection Regulation » GAFA: Google-Amazon-Facebook-Apple
I	» I: Integrity IGF: Internet Governance Forum
J	» JNC: JustNet Coalition
L	» LPbD: legal protection by design
M	» MIT: Massachusetts Institute of Technology
O	» OR: Others' reliability and integrity
P	» PIA: Privacy Impact Assessment » PTT: Propensity to trust
R	» RA: Risk aversion
T	» T: Tenure within their banking agency » TO: Trusting others
U	» US: United States
W	» WSIS: World Summit on the Information Society

Table 10. List of abbreviations

B. TABLES WITH CONSTRUCTS

The section below refers to the constructs used to create the final questionnaire with depending on the construct, its description and its short form.

CONSTRUCTS	DESCRIPTION	ITEMS
Propensity-to-trust	**Factor 1 – trusting others**	
	» Other people are out to get as much as they can for themselves	PTT-TO1
	» I have little faith in other people's promises	PTT-TO2
	» Other people are primarily interested in their own welfare despite what they say	PTT-TO3
	» In these competitive times, I have to be alert; otherwise, others will take advantage of me	PTT-TO4
	» Other people who act in a friendly way towards me	PTT-TO5

CONSTRUCTS	DESCRIPTION	ITEMS
	are disloyal behind my back » Other people lie to get ahead » Other people let you down **Factor 2 – others' reliability and integrity** » Other people can be relied upon to do what they say they will do » Those in authority are likely to say what they really believe » Experts can be relied upon, to tell the truth about the limits of their knowledge » Other people live by the idea that honesty is the best policy **Factor 3 – risk aversion** » It is important to 'save for a rainy day' » I prefer a modest but safe return on my savings rather than a higher return that is uncertain » "It is better to be safe than sorry"	 PTT-TO6 PTT-TO7 PTT-ORI1 PTT-ORI2 PTT-ORI3 PTT-ORI4 PTT-RA1 PTT-RA2 PTT-RA3
Data protection regulation knowledge degree	» I already heard about the GDPR. » I am able to harness data protection principles. » I am aware of the principle related to domestic law. » I am aware of the principle related to transfers. » I am aware of the principle related to pseudonymisation. » I am aware of the principle related to portability. » I am aware of the principle related to infringement. » I am aware of the principle related to consent. » I am aware of the principle related to profiling. » I am aware of the principle related to healthcare. » I am aware of the principle related to safety. » I am aware of the principle related to certification. » I am aware of the principle related to privacy impact assessment. » I am aware of the principle related to data protection officer.	GDPR1 GDPR2 GDPR3 GDPR4 GDPR5 GDPR6 GDPR7 GDPR8 GDPR9 GDPR10 GDPR11 GDPR12 GDPR13 GDPR14
Customer satisfaction towards bank agency	» Overall, I am satisfied with my bank agency. » I did the right thing when I decided to choose my bank agency.	CS1 CS2
Brand recognition of a specific bank	» In my opinion, my bank has a good image in the minds of consumers. » In general, I believe that my bank always fulfils the promises that it makes to its customers. » I would encourage friends and relatives to do business with my bank.	BR1 BR2 BR3
Competence	» I believe my bank has the ability to handle sales transactions on the Internet.	T-C1

CONSTRUCTS	DESCRIPTION	ITEMS
	» I believe my bank has sufficient expertise to do business on the Internet.	T-C2
Integrity	» I believe my bank is honest with its customers. » I believe banks are truthful in their dealings with its clients. » My bank has a good reputation in the market. » My bank has a good reputation for being consumer-oriented. » I believe my bank meets its commitments.	T-I1 T-I2 T-I3 T-I4 T-I5
Benevolence	» I believe my bank would act in its customers' best interest. » If a customer required help, I believe that my bank would do its best to help him/her. » In situations of conflict of interest, I believe that my bank would put its interest over the customers' ones.	T-B1 T-B2 T-B3

Table 11. Table with constructs

Here is the coding used for the contextual variables.

VARIABLES	MEASURE	ITEMS
Educational level	1 = no diploma; 2 = high school degree; 3 = bachelor's degree; 7 = undergraduate degree; 8 = master's degree; 9 = PhD	EL
Tenure within their banking agency	1 = less than a year; 2 = 1–5 years; 3 = 6–10 years; 4 = 11–15 years; 5 = 16–20 years; 6 = More than 20 years	T
Age		A
Gender	0 = male 1 = female	G

Table 12. Table with contextual variables

C. FINDINGS RELATED TO THE MULTIPLE REGRESSION ANALYSIS

This study aims to establish if a linear relationship exists between the dependent variable and "each" of the independent variables. To do so, I used a partial regression plot.

As described by the table below, there was the independence of residuals, as assessed by a Durbin-Watson statistic of 1.968. R^2 for the overall model was 44.3% with an adjusted R^2 of 43.7%.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.666[a]	.443	.437	.439	1.968

a. Predictors: (Constant), PTT_index, BankInstitutionsCharacteristics_index

b. Dependent Variable: InitialTrust_index

Table 13. Model Summary of Multiple Regression.

There was a homoscedasticity, as assessed by visual inspection of a plot (see Figure 10 and Figure 11) of studentized residuals versus unstandardized predicted values.

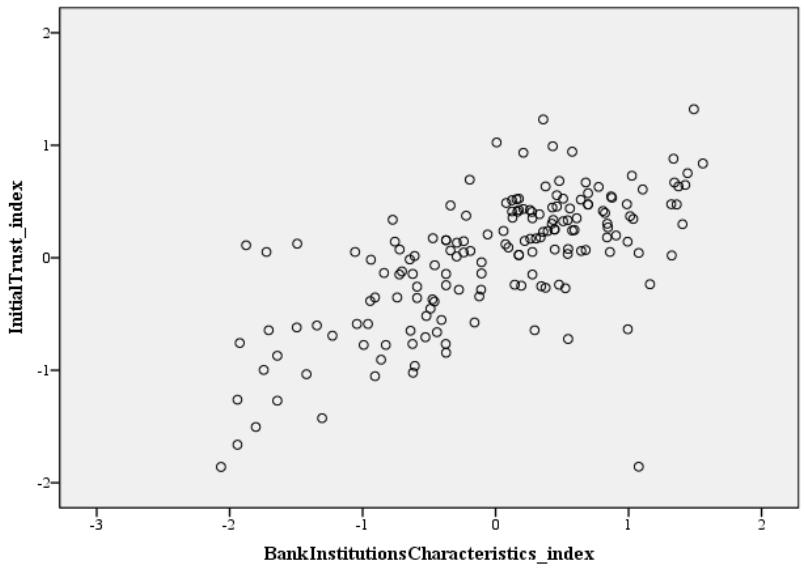

Figure 10. Partial Regression Plot between 'Dimensions of trust' and 'Bank Institutions' characteristics'

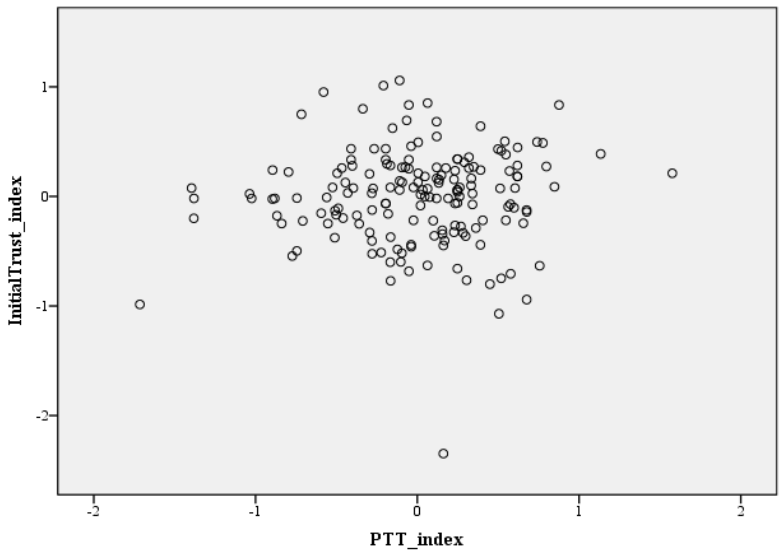

Figure 11. Partial Regression Plot between 'Dimensions of trust' and 'Propensity-to-Trust'

Moreover, it appears that one respondent answer does not follow the usual pattern of points. This is highlight within the Table 14 were the Casewise Diagnostics table shows any case where the standardized residual is greater than ±3 standard deviations. Since only one outlier appears, I keep considering all the measures together[31].

Case Number	Std. Residual	InitialTrust_index	Predicted Value	Residual
117	-5,363	2	3,96	-2,355

a. Dependent Variable: InitialTrust_index

Table 14. Casewise Diagnostics (a)

As the final assumptions' requirement, I checked for normality. It appears that the distribution is approximatively normally distributed (see Figure 10 and Figure 11).

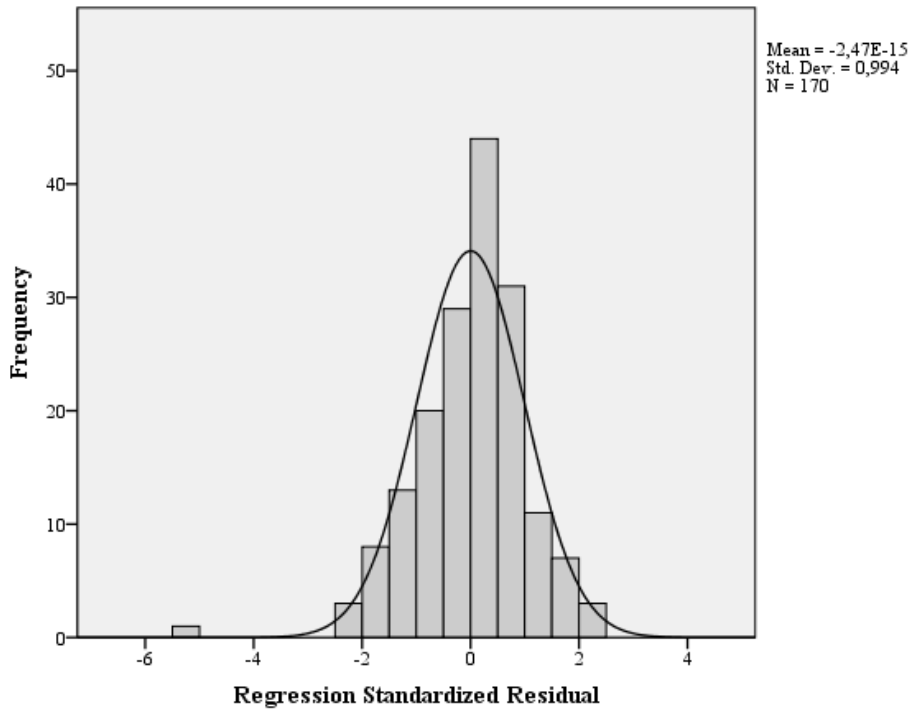

Figure 12. Linear Regression Histogram

[31] The Cook's Distance values are all above 1 (Cook and Weisberg, 1982) with no leverage value above the "safe" value of 0.2.

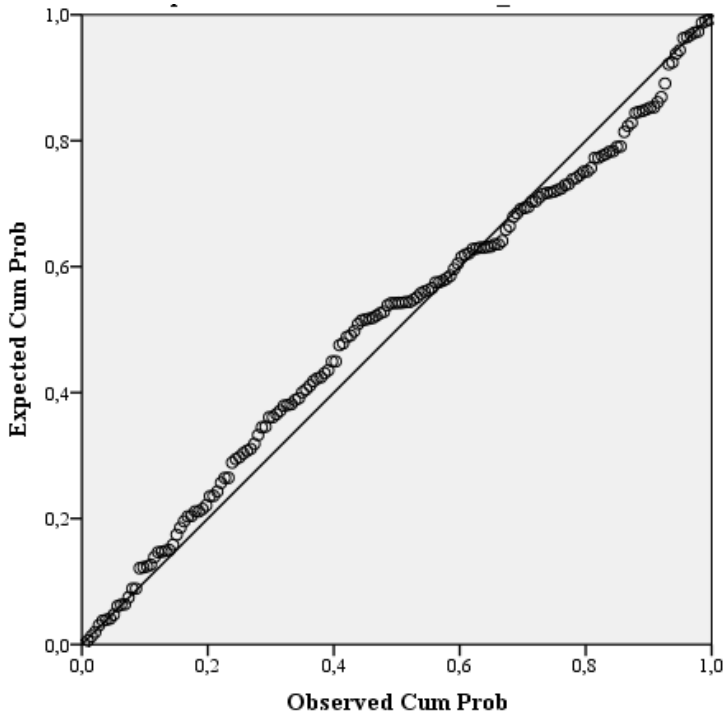

Figure 13. Normal P-Plot of Regression Standardized Residual

Table 15 shows that Propensity-to-trust (PPT) and Bank Institutions Characteristics (CS and BR) statistically predicted Trust (Initial Trust prior GDPR expertise), $F(2, 167) = 66.481$, $p < 0.001$[32].

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	25,648	2	12,824	66,481	,000[b]
	Residual	32,214	167	,193		
	Total	57,861	169			

a. Dependent Variable: InitialTrust_index

b. Predictors: (Constant), PTT_index, BankInstitutionsCharacteristics_index

Table 15. ANOVA (a) Table of Multiple Regression

Table 16 highlights that there is no linear relationship in the population regarding the PPT variable ($p > 0.05$, i.e. Sig = 0.476). But it appears that:

$$Trust\ prior\ GDPR\ expertise = 1.704 + 0.463 * Bank\ Institutions\ Characteristics + 0.48 * Trust\ Propensity$$

Equation 2. Research regression equation

[32] This report may be deducted according to the ANOVA table (Table 8), where 'F' indicates that a F-test was used, 'df' means degrees of freedom and 'p' related to the probability of obtaining the observed F-value if the null hypothesis is true.

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
	B	Std. Error	β			Lower Bound	Upper Bound
(Constant)	1.704	.288		5.920	.000	1.136	2.272
BankInstitutions Characteristics_index	.463	.040	.670	11.493	.000	.383	.542
PTT_index	.048	.067	.042	.714	.476	-.085	.181

	Correlations			Collinearity Statistics	
	Zero-order	Partial	Part	Tolerance	VIF
(Constant)					
BankInstitutionsCharacteristics_index	.665	.665	.664	.980	1.021
PTT_index	-.054	.055	.041	.980	1.021

Table 16. Coefficients tables

D. INTERVIEW GUIDE FOR EXPLORATORY TALKS

In order to best fit with the population to whom I wish to submit my questionnaire, I talked to equal numbers of men and women, considering only one individual who used to work within a bank institution and therefore more aware about the reality of such an environment. Here is proposed the working material and references used to imagine the framework of the exploratory talks.

QUESTION		
	RESEARCHED ELEMENTS	THEORETICAL BACKGROUND
In a dematerialized context, without human contact, to which risk factors do you pay attention to?		
	Online trust antecedents (as opposed to trusting someone in physics)	5 determining factors of trust regarding a website (Lemoine and Cherif, 2012): 1. Website-related 2. Consumer-related 3. Third-party-related 4. Brand-related 5. Context-related
What characteristics do you attribute to a trustworthy-considered institution?		
	Types of trust Characteristics of the definition of trust	Partners' individual expectations that help define a relationship of trust (Gatfaoui, 2005) bi or three or four-dimensional trust (McAllister, D. J., 1995; Butler Jr, J. K., 1991)

QUESTION		
	RESEARCHED ELEMENTS	THEORETICAL BACKGROUND
According to a Likert scale - 1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = indifferent, 5 = somewhat agree, 6 = agree, 7 = strongly agree - would you say you trust: • ***To your family?*** • ***In general?*** • ***To strangers?*** • ***In knowledge?*** • ***In honesty?*** • ***In integrity?***		
	Propensity to trust Degree of trust (distrust / mistrust / trust / faith) (Servet, 1997)	Natural predisposition to the degree to which an individual is willing to trust others in a global way (Rotter, 1967 and 1971)
According to you, what role the reputation of a firm has in the development of a trusted-base relationship?		
	Mechanisms and processes through which trust and confidence emerge as part of a customer/bank relationship (business relationship)	Asymmetric information between customer and bank ➔ stakeholder opportunism Trust as a way to maintain a reputation
Which principles proposed by the new regulation concerning the GDPR have you been able to remember?		
	The scale of sensitivity to risk according to the category of principles	GDPR principles
How would you describe your trust in the banking industry? Why?		
	Evaluation of the system's reputation	Organizational trust The propensity to trust towards institutions
Do you consider that you have different data-protection awareness, depending on your professional or personal environment? Why?		

Table 17. Exploratory interviews guide

E. EXPLORATORY TALKS TRANSCRIPTS

Here are the transcripts of the four interviews I had to be able to submit the questionnaire the most appropriate, regarding presuppositions and expertise degree about both the banking system and data-based regulation. The transcripts are formalized in French since the interviewee were all French native speakers.

FEMALE, 49 YO

Charlotte Benaïcha-Tanquerel (CBT) : Merci de prendre le temps de répondre à ces quelques questions pour mon mémoire !

Interviewee (I) : Je t'en prie. Dis-moi, en quoi je peux t'aider.

CBT : Comme tu le sais, dans le cadre de mon master, je rédige un mémoire de recherche pour essayer de comprendre en quoi le degré de connaissance du RGPD

influence la confiance que les particuliers placent dans l'industrie bancaire.
I : D'accord.

CBT : En guise de mémo, le RGPD signifie règlement général sur la protection des données personnelles. Il est entré en vigueur depuis le 25 mai dernier. N'hésite pas à m'arrêter si tu ne comprends pas un acronyme.
I : D'accord.

CBT : Pour cette recherche, j'ai choisi d'opter pour une approche quantitative, à travers un questionnaire soumis à un échantillon de population. Je voudrais donc te poser une dizaine de questions pour délimiter au mieux mon sujet. Dans un contexte dématérialisé, c'est-à-dire sans contact humain, quels sont, selon toi, les facteurs de risque ?
I : Hum, lorsque je suis sur Internet, j'ai conscience que je suis exposée à un piratage de mes données d'une part, mais aussi à l'absence de confidentialité possible. C'est vrai, dès lors qu'il n'y a plus de contact humain, dès qu'il y a un traitement informatique.

CBT : Je vois. Du coup, qu'est-ce qui te permet d'avoir confiance en une institution (comme l'industrie bancaire ou l'état) ? Que peut faire un organisme pour limiter ta crainte vis-à-vis de ses risques.
I : Le fait que cette institution soit responsable en cas de défaillance du système, et qu'une réparation des dommages causés soit effectuée sans difficulté.

CBT : Sur une échelle de Likert
I : Qu'est-ce que c'est ?

CBT : J'allais te l'expliquer : il s'agit d'une échelle où 1 = fortement en désaccord et, disons 7 fortement d'accord, que tu utilises pour quantifier une mesure.
I : Ah oui, je vois.

CBT : Très bien, alors à combien évalues-tu ta confiance en ta famille ? Tu n'as pas besoin de te justifier.
I : 6

CBT : D'accord. As-tu confiance en général ?
I : Je dirai 5

CBT : et qu'en est-il des étrangers ? Fais-tu confiance aux gens que tu ne connais pas ?
I : Assez peu, je dirai 3.

CBT : Très bien et en termes de concepts, en utilisant l'échelle, as-tu confiance en la connaissance ?
I : Oui plutôt, je dirai que sur 7, j'y crois à hauteur de 5

CBT : Et l'honnêteté ?
I : Seulement 3 pour l'honnêteté.

CBT : Et enfin, qu'en est-il par rapport à l'intégrité ?
I : Je n'y crois pas vraiment, disons aussi 3.

CBT : D'accord, merci ! Je voudrais aussi investiguer la relation de confiance. Aussi penses-tu tenir compte de la réputation d'une entreprise pour juger de la confiance à lui accorder et pourquoi ?)
I : Oui j'en tiens compte ... malgré moi

CBT : Comment ça malgré toi ?
I : Je tiens compte de la réputation parce que je n'ai pas la connaissance de la réalité. Une réputation peut être fausse, j'en suis consciente

CBT : Pourquoi penses-tu tenir compte de la réputation ? d'autant plus si tu as conscience d'un biais que tu pourrais avoir ?
I : J'aimerais pouvoir faire autrement... C'est la raison pour laquelle je dis « malgré moi »

CBT : En ce qui concerne la réputation d'une industrie, quel rôle penses-tu qu'elle a dans le développement d'une relation de confiance ?
I : Comment ça ?

CBT : Tiens-tu compte des scandales pour attribuer ta confiance ? Ca t'influence beaucoup ?
I : Oui j'en tiens compte

CBT : à quelle hauteur tu penses ?
I : Vu la pluralité d'offres sur le marché, j'irai plutôt chez le concurrent si j'apprends une mauvaise nouvelle, un scandale, sur une entreprise, surtout ma banque. Je réfléchirai à en partir peut-être

CBT : D'accord. En ce qui concerne la régulation, on en entend beaucoup parler depuis le 25 mai. Quels principes proposés par la nouvelle régulation en matière de protection des données personnelles as-tu en tête ?
I : Peu ou pas grand-chose.

CBT : Mais encore ?
I : La nouveauté pour moi a été la possibilité de paramétrer à minima les cookies. Mais c'est surtout que j'ai maintenant la confirmation que mes données sont vendues.

CBT : Et ça te choque ?
I : Oui, ça me choque parce que je communique des infos dans un but et non pas pour autre chose, d'autant moins si l'entreprise en question monnaye mes données

CBT : Penses-tu que ta banque vende tes données ?
I : Je le crains.

CBT : Comment tu qualifierais ta confiance dans l'industrie bancaire ? Pourquoi ?
I : J'ai assez peu de confiance mais le système nous contraint à devoir y avoir recours. Donc je fais appel à leurs services.

CBT : Pour revenir sur ton comportement en ligne, comment te comportes-tu sur Internet ?
I : Comme une utilisatrice moyenne.

CBT : C'est-à-dire ?
I : J'utilise le terme d' « utilisatrice moyenne », car je ne suis pas informaticienne, je ne maîtrise pas le domaine, je suis donc méfiante.

CBT : Pourquoi avoir cette attitude en ligne ?
I : J'essaie d'être vigilante sur les données transmises.

CBT : Comment ?
I : Je n'ai pas de compte Facebook par exemple ni autre réseau social. Je n'inscris aucune donnée sur les blogs...

CBT : Penses-tu adopter une attitude différente dans un environnement de travail vs environnement personnel ?
I : Non, j'ai la même vigilance, vu que j'évolue dans un milieu professionnel classé « confidentiel ».

CBT : C'est noté. Encore merci pour toutes tes réponses. Ça m'éclaire sur l'orientation à adopter pour mon mémoire.
I : De rien,

CBT : Une dernière question, vu que les entretiens sont anonymisés, peux-tu me dire ton âge, ton niveau d'étude (bac + combien ?), le nombre de banques que tu as eu et la durée depuis laquelle tu es cliente de ta banque actuelle stp ?
I : Bien sûr. J'ai 49 ans et j'ai un bac + 5.

CBT : et concernant ta banque ?
I : Je suis dans ma banque depuis 3 ans et j'ai été cliente de 5 banques en comptant mon organisme actuel.

MALE, 55 YO

Charlotte Benaïcha-Tanquerel (CBT) : Bonjour, merci d'échanger avec moi. Notre échange constituera un de mes entretiens préliminaires me permettant à terme d'orienter mon analyse pour mon mémoire de recherche de master 2. Comme je te l'expliquais en te proposant ce rendez-vous, je suis étudiante à l'Université Paris-Dauphine en master 2 en Business Consulting. Une des exigences pédagogiques pour l'obtention de mon diplôme est la rédaction d'un mémoire de recherche. J'ai choisi, pour compléter celui écrit l'an passé, de m'intéresser à la confiance des particuliers en l'industrie bancaire, au regard de leur degré de connaissance du RGPD. Le RGPD c'est l'acronyme pour règlement général sur la protection des données personnelles. Il rentrera en vigueur le 25 mai prochain.
Pour cette recherche, j'ai choisi d'opter pour une approche quantitative, à travers un questionnaire soumis à un échantillon de population.
Interviewee (I) : D'accord, j'ai saisi le contexte. Je t'écoute.

CBT : A quoi es-tu particulièrement attentif, considérant cela comme potentiellement dangereux, lors que tu évolues en ligne, que tu surfes sur Internet ?
I : Sur Internet, je me soucie de la capture de mes données durant l'échange, par une tierce personne dont je ne connais rien du fait du contexte dématérialisé, mais aussi de la retranscription erronée des informations communiquées ou d'une erreur de compréhension de l'utilisateur

CBT : De l'utilisateur ?
I : Oui, par exemple, dans le cadre d'une déclaration d'impôt en ligne. Je réfléchis bien à ce que je renseigne, sachant que l'utilisateur des données, c'est le FISC et que je ne voudrais pas qu'il ait une mauvaise compréhension.

CBT : D'accord, je comprends mieux. Merci ! Désolée, je t'ai coupé, tu m'expliquais donc être vigilant sur la compréhension - ou retranscription pour utiliser ton terme – des données que tu fournissais sur Internet.
I : Oui exactement. Je me méfie notamment de la différence entre la retranscription officielle accessible et visible des données et la retranscription officieuse, accessible à un petit nombre de décisionnaires/acteurs et dont la conservation desdites données dans le temps ne dépend pas de moi. Je n'ai donc aucune maîtrise de l'utilisation qui en est faite, alors même que je suis le plus concerné. Je pense notamment à une inscription sur un réseau social quelconque disons à l'âge de 18 ans, quand majeur on se croit invincible, et dont les données vont être conservées et consultées disons 30 ans. Ça peut alors nuire à la personne même autant de temps après.

CBT : Je comprends. Internet a une mémoire (précise de surcroit) bien plus conséquente que la plupart d'entre nous, avec un arrière-plan si je puis dire, que l'on maitrise rarement.
I : c'est ça et je tente aussi d'éviter le piratage informatique.

CBT : Très bien. Pour résumer, tu considères les facteurs de risque comme toute utilisation frauduleuse ou non précisée des données qu'un internaute pour fournir sciemment ou non sur la toile.
I : C'est ça.

CBT : Cela, à mon sens, rejoint une idée de confiance. Dis-moi si je me trompe, mais si tu avais confiance dans les acteurs qui évoluent au sein de l'écosystème d'Internet, tes craintes seraient probablement différentes non ?
I : Oui, sûrement.

CBT : Du coup, que doit selon toi avoir une institution ou un groupe d'acteurs pour que tu les considères dignes de confiance ?
I : La confiance s'établit dans une relation duelle, en se construisant dans le temps. Je ne serai donc jamais en mesure de directement faire confiance à une institution, comme la banque pour rester dans ton sujet. La relation de confiance qui va se construire au fil du temps sera impactée forcément par des ajustements et réajustements. C'est d'ailleurs, à mon sens, le travail du conseiller clientèle qui va faire évoluer l'offre proposée par la banque.
L'aptitude d'empathie de l'interlocuteur est aussi fondamentale.

CBT : Certes. En évoquant l'empathie, c'est une caractéristique dont chacun à sa propre définition et perception, a l'instar de la propension à faire confiance. Toutes ces notions n'ont pas de valeur normée établie… J'aimerai si tu le permets te poser quelques questions pour être en mesure d'affiner ma compréhension de ta perception.
I : Je t'en prie. Je ne suis pas sûr d'être de ceux qui attribue facilement leur confiance, je te préviens !

CBT : Ne t'en fais pas, il n'y a pas de bonnes ou de mauvaises réponses. Alors, je vais t'énoncer diverses valeurs ou groupes de gens et j'aimerai que tu situes la confiance que tu leur attribues instinctivement, sur une échelle de 1 à 7.
I : Avec 1 pour Pas du tout confiance ?

CBT : Exactement ! Et 7 pour tout à fait confiance.
I : Vas-y.

CBT : Ta confiance en général ?
I : 4

CBT : Et vis-à-vis d'étrangers ?
I : 4 aussi. Je ne fais pas de distinction avec le général. Autrui est un étranger.

CBT : à ta famille ?
I : 7

CBT : Passons aux valeurs. Dans quelle mesure as-tu confiance en la connaissance ?
I : 7

CBT : En l'honnêteté ?
I : 4 à nouveau

CBT : En l'intégrité ?
I : l'intégrité ? Hum… Oui 4.

CBT : Je rebondis sur la notion d'intégrité. Tu sembles de prime abord y accorder peu de confiance. Du coup, est-ce que tu dirais que tu tiens compte de la réputation d'une banque par exemple pour juger de la confiance à lui accorder ?
I : Oui j'en tiens compte puisqu'une réputation entachée renvoie aux risques d'être à son tour victime de la société en question. Dans le cas d'une banque, on parle de mon argent, de mes économies, donc clairement oui. Je ne veux pas prendre plus de risques que nécessaire, alors que je dois déjà tout lui fournir.

CBT : Pourtant les banques sont soumises à une forte régulation. L'Etat impose beaucoup de règles et limites pour éviter tout risque, notamment aux particuliers. D'ailleurs, que sais-tu du règlement relatif à la protection des données personnelles, le fameux RGPD ?
I : Rien.

CBT : D'accord. En revenant sur la confiance en ta banque, plus généralement, as-tu un peu plus (ou moins d'ailleurs) confiance en l'industrie bancaire ?
I : Je n'ai pas du tout confiance en l'industrie bancaire. Je reste persuadé qu'aucune banque ne travaille pas pour mes intérêts ou dans mon intérêt si tu préfères. Il suffit de se souvenir du scandale du crédit lyonnais, depuis rebaptisé LCL…
D'ailleurs, je trouve ça dingue que ma banque dite traditionnelle mette deux jours

à procéder à un transfert d'argent, alors que c'est bel et bien débité de mon compte dans la seconde. Mais ça met deux jours à être crédité sur le compte bénéficiaire. J'ai longtemps pensé à une nécessité d'infrastructure, mais on le voit maintenant avec toutes ces fintechs, il n'en est rien.

CBT : Hum hum. En parlant de scandale, d'un autre type puisqu'il ne s'agit pas de détournements et autres malversations monétaires, mais … scandale tout de même si cela arrivait. Je voudrais que tu me décrives ton attitude par rapport à la divulgation de tes données personnelles selon qu'il s'agisse d'un environnement de travail ou personnel ?
I : Oh, il y a tant de scandales qui n'ont pas encore été repris par les médias… Mais pour répondre à ta question, je ne fais aucune différence entre le boulot et le perso. Je suis conscient que les données numériques ne peuvent été sécurisées, regarde Facebook. Donc je limite autant que possible.

CBT : Cohérent jusqu'au bout. Je crois que c'est le mot de la fin. Merci beaucoup. Il me reste jusque quelques précisions sur ta relation à ta ou tes agences bancaires.
I : Je t'écoute

CBT : Combien en as-tu eu et depuis quand es-tu client de la dernière ?
I : J'ai eu 5 banques et ça fait… 5 ans que je suis client de la dernière.

CBT : Super, voilà j'ai fini ! Encore merci pour ton temps !

FEMALE, 22 YO

Charlotte Benaïcha-Tanquerel (CBT): Bon commençons, si c'est ok pour toi ?
Interviewee (I): Allons-y, je t'écoute !
Je t'en prie. Dis-moi, en quoi je peux t'aider.

CBT : Laisse-moi tout d'abord te remettre un peu dans le contexte. Comme je te l'expliquais, dans le cadre de mon master 2, je suis tenue de rédiger un mémoire de recherche. J'ai donc décider de tenter de comprendre en quoi le degré de connaissances du RGPD a (ou pas) un impact sur la confiance que les particuliers ont dans leur banque.
I : D'accord. Parfait, ma connaissance du milieu bancaire, bien que mince, pourra peut-être t'aiguiller un peu, je l'espère.

CBT : N'hésite pas à m'arrêter si je parle chinois, surtout au vu des acronymes ! Mais sinon, en guise de mémo, RGPD fait référence au règlement général sur la protection des données personnelles. Il est entré en vigueur depuis le 25 mai dernier.
I : Ok, oui j'en ai entendu parler.

CBT : Donc, du coup, pour mon mémoire, histoire d'avoir un peu plus de challenge encore que l'an passé, j'ai choisi d'opter pour une approche quantitative. En gros, tu testes tes hypothèses avec une démarche statistique. J'ai donc prévu de créer un questionnaire. Notre échange vise à ce qu'il soit le plus pertinent possible, grâce à nos échanges. Je le ferai ensuite aussi tester : ce sera la phase de pré-test, pour m'assurer qu'il est prêt à être diffuser à une échelle plus large. Tu es évidemment la bienvenue si tu souhaites aussi répondre à ce pré-test !
I : Oui pas de souci, tu me l'enverras.

CBT : Ahah, merci ! Avec plaisir, je te le ferai parvenir dès qu'il est prêt. Concernant notre échange, je voudrais te poser une petite dizaine de questions pour délimiter au mieux mon sujet. Prête ?
I : Je t'écoute.

CBT : Dans un contexte dématérialisé, j'entends par là sans contact humain, quels sont, à ton avis, les facteurs de risque ?

I : Euh, tu veux dire par exemple si je vais sur mes comptes en ligne. Ca marche ça comme situation pour répondre.

CBT : Oui c'est une situation même idéale. Dans le cas où tu te connecterais en ligne sur tes comptes, à quoi es-tu attentive parce que tu considères le risque comme élevé ?
I : Bah je fais attention au site, tu sais que la page soit bien sécurisée avec le hppts. Après je fais comme avec les mails au boulot et les risques de fishing. S'il y a des fautes, je quitte le site. Donc je dirai que le site doit sembler fiable et « pro ». Mais s'il s'agit d'une banque connue par exemple, je serais moins méfiante, parce que je sais qu'il y a des moyens mis derrière pour limiter le risque pour les utilisateurs.

CBT : Je vois. Donc le site et ses caractéristiques et l'institution ou l'organisation du site, c'est ça.
I : Ouais. En gros, je dirai que c'est tout parce que je ne reste pas non plus 3h devant ma page à tout regarder.

CBT : je comprends : quelques points que tu vérifies pour te rassure et ton expérience en ligne continue.
I : Exactement.

CBT : Du coup, qu'est-ce qui te permet d'avoir confiance en une institution. Par institution, j'entends une organisation reconnue, comme l'industrie bancaire ou l'état.
I : Bah du coup, je te disais son nom, enfin sa renommée. Par exemple, pour une banque, si c'est N26 ou BNPP, ma confiance varie. Pas forcément dans le sens que l'on pense d'ailleurs si tu vois ce que je veux dire.

CBT : Ahah oui je saisis l'allusion.

I : Et puis je dirais que ça c'est le RETEX[33] des autres que je recherche avec la renommée. Mais mon expérience en propre ou celle de mon cercle proche va aussi compte, peut-être même plus.

CBT : D'accord, donc la satisfaction que tu tires de ta relation avec l'institution mais aussi l'image de marque qu'elle va avoir compte pour toi, c'est ça ?
I : Exactement.

CBT : Pour essayer de comprendre la façon dont tu attribues ta confiance, ce que j'appellerai plus ou moins ta propension à faire confiance, j'aimerai que tu notes de 1 à 7 où 1 vaut pour fortement en désaccord et 7 pour fortement d'accord la confiance que tu mets dans les éléments/notions que je te citerai. Prête ?
I : Vas-y !

CBT : Très bien, alors à combien évalues-tu ta confiance en ta famille ? Sans réfléchir, comme ça.
I : 6 voire 6,5. J'ai peu d'esprit critique si ça vient de mon entourage.

CBT : D'accord. Et en général ?
I : Ah là, plus euh 4

CBT : et envers des étrangers ? Fais-tu confiance aux gens que tu ne connais pas du tout, jamais rencontrés ?
I : Hum, 3 ou 3,5.

CBT : 3/3,5, ok. Et dans quelle mesure as-tu confiance en la connaissance ?
I : La connaissance… Bah chaque époque à sa connaissance, regarde Galilée, on lui expliquait qu'il avait tort. Bref, je dirai 3. Non, allez, sur 7, plutôt 4.

CBT : Et l'honnêteté ?
I : Seulement 2 pour l'honnêteté. Les gens ne sont pas fiables dès qu'ils ont des

[33] Retour d'expérience

intérêts en jeu. Or tout le monde a ses intérêts à protéger et tu ne les connais pas, ou pas souvent, disons.

CBT : Certes. Ton point de vue au regard de l'intégrité ?
I : Je n'y crois pas vraiment, donc 2.

CBT : Tu me disais tout à l'heure, dis-moi si j'extrapole trop, que plus une banque, par exemple, était connue et reconnue, plus tu lui ferais facilement confiance. Right ?
I : C'est ça !

CBT : En ce qui concerne la réputation d'une industrie, donc pas un établissement comme la BNPP, mais toute l'industrie bancaire,
I : Ouais je vois

CBT : Quel rôle penses-tu donc que la réputation d'une industrie au global ait dans le développement d'une relation de confiance ?
I : Comment ça ?

CBT : Hum… Je vais essayer de reformuler. Euh. Penses-tu que les scandales qui vont entachés la réputation d'un secteur vont t'influencer ?
I : Bah oui, j'en tiens compte.

CBT : Vraiment ? Tu peux développer un peu ?
I : Bah avec les médias maintenant, les scandales sortent pas mal. Du coup, si une banque, genre comme la SG, subit un scandale, bah je partirai peut-être.

CBT : Mais du coup, tu quitterais la SG, pas la banque… Tu vois ce que je veux dire. Tu garderais des comptes bancaires.
I : Ah mais oui tu as raison, j'ai mal réagi… Tu m'as bien dit pas une banque. Bah alors non, si ce n'est pour critiquer. Parce qu'au final, je serai toujours obligée d'avoir un compte bancaire… Du coup, l'émergence de scandales ne m'influencerait pas tant que ça…

CBT : D'accord. Je change un peu de sujet, pour parler de régulation.
I : Joie. En banque, on a l'habitude d'entendre parler du régulateur. Vas-y.

CBT : C'est vrai. Les exigences réglementaires sont particulièrement fortes. Tous les individus ne le perçoivent toutefois pas, je te l'assure. Mais je digresse. Je voulais te parler du RGPD.
I : Ouais. On en entend pas mal parler depuis mai, c'est même sans cesse passer aux infos lorsque ça a été lancé.

CBT : Et du coup, tu penses que tu maîtrises cette nouvelle norme ?
I : Non, je sais juste que les entreprises vont devoir faire attention à ce qu'elles font avec nos données personnelles, mais à titre perso, j'en sais pas beaucoup plus.

CBT : Tu connais les grands principes ?
I : Ouais vite fais : il y a la portabilité, le consentement, euh… bah ils prévoient aussi les punitions et les trucs de sécurité genre PIA et tout. Ah et puis, maintenant, dans les grosses boites, il faut un gars référent.

CBT : Bah tu vois, tu t'y connais pas mal.
I : Léger, léger. J'ai assez peu de confiance mais le système nous contraint à devoir y avoir recours. Donc je fais appel à leurs services.

CBT : Pour revenir sur ton comportement en ligne, comment te comportes-tu sur Internet ?
I : Je suis prudente.

CBT : Pourquoi avoir cette attitude en ligne ?
I : J'essaie d'être vigilante sur les données transmises. Mais c'est aussi valable dans la vie, genre avec ma CB etc.

CBT : Penses-tu adopter une attitude différente dans un environnement de travail ? Je veux dire par rapport au perso
I : Non, franchement c'est pareil vu qu'au boulot je dois faire gaffe déjà.

CBT : Alright. Merci pour ton temps.
I : Bah pas de souci. N'hésite pas à m'envoyer ton questionnaire si ça peut t'aider ;

CBT : Une dernière question, ne t'en fais pas, notre échange sera anonymisé. Mais t'as quel âge ?

I : 22 ans et toutes mes dents.

CBT : Ahah et ton niveau d'étude ?
I : bah l'an prochain, normalement master hein.

CBT : t'as été cliente de combien de banques ?
I : Euh… Attends. 4 je crois.

CBT : et concernant ta banque actuelle, ça fait combien de temps ?
I : Je suis dans ma banque depuis 3 ans.

MALE, 25 YO

Charlotte BENAÏCHA-TANQUEREL (*CBT*) : Bonsoir, merci de m'accorder ce point.
***I*nterviewee (*I*)** : Allez, je t'écoute.

CBT : Alors, pour te remettre dans le contexte. Dans le cadre de mon master 2 en Business Consulting au sein de l'Université Paris-Dauphine, je dois rédiger un mémoire de recherche portant sur la confiance des particuliers en l'industrie bancaire, au regard de leur degré de connaissance du RGPD. RGPD ou GDPR ça veut dire règlement général sur la protection des données personnelles. Il est actif depuis le 25 mai dernier. Pour cette recherche, j'ai choisi d'opter pour une approche quantitative, à travers un questionnaire soumis à un échantillon de population.
I : Ok.
CBT : J'aimerai d'abord comprendre à quels facteurs de risque tu penses dans le cadre d'une expérience en ligne. Bref, quand tu vas sur un site, à quoi fais-tu particulièrement attention ?
I : N'importe quel site ?
CBT : Oui
I : Le site : je regarde s'il est en français ou en anglais, s'il y a des fautes d'orthographe ou de grammaire. Je parle d'un site sur lequel je peux faire des opérations (achats ou transferts d'argent ou même partager de n'importe quelle donnée personnelle). Donc, si de l'argent transite je fais attention au https avec le petit cadenas. Je fais attention à si j'ai un espace personnel.

CBT : Pourquoi ?
I : Parce qu'en général j'essaie de ne pas partager d'infos personnelles si je n'ai pas de compte. C'est comme ma carte d'identité que j'accepte de partager avec l'entreprise.
CBT : D'accord, merci.

I : Et si je dois faire une transaction sur ce site, je vais vérifier s'ils comptent partager mes données ou pas. J'essaie d'éviter autant que possible le partage de mes infos perso. Un facteur que je prends en considération mais que je ne peux connaitre qu'à la fin, ça va être s'il y a bien 2 facteurs d'identification ou le coté facture.
CBT : D'accord.

I : Ah et dernier point : voir si je peux modifier, supprimer ou rétracter mes données. Ce qui ne veut pas dire que je ferai la démarche
CBT : Mais tu veux savoir s'ils ont pensé au processus ?
I : C'est ça.

CBT : Et dans le cadre d'une institution comme la banque, qu'en est-il ?
I : Pour être une institution, ou reconnue comme telle, comme une banque, elles ont dû passer des certifications. Contrairement à une start-up par exemple, qui sont plus des organismes financiers. Si ce sont de grands noms comme BNPP, qui a des certifications alors j'ai tendance à faire plus confiance, surtout que je bosse en banque.
CBT : hum.
I : Ah et j'oubliais dans le point précédent le bouche à oreille importe beaucoup dans la confiance que je vais accorder. Et je regarde le site au format mobile et desktop ou j'attends plus d'infos de la version desktop que mobile.

CBT : Pourquoi ?
I : Parce que la version mobile on la veut ergonomique alors que la version bureau est faite pour le gars devant son ordinateur posé. Donc ça me choquera moins de trouver moins d'informations sur la version mobile.

CBT : D'accord, je comprends ton point. En parlant de confiance qui peut varier selon ton interlocuteur et son aptitude à te mettre en confiance, j'aimerai te poser quelques questions pour tenter d'évaluer ta propension à faire confiance. En 6 questions, j'aimerai que tu donnes une note allant de 1 à 5 sur la confiance que tu accordes, 5 étant le max.
I : Vas-y.

CBT : A combien évalues-tu ta confiance en ta famille ?
I : 4

CBT : En général ?
I : 2,5

CBT : Et face à des étrangers ?
I : Des gens que je ne connais pas du tout, alors 2.

CBT : Maintenant, discutons de concept. Même exercice, avec la connaissance.
I : 3

CBT : L'honnêteté ?
I : Ah c'est pas facile. J'ai dit combien pour le en général ?
CBT : 3
I : Bah je dirai 3 pour l'honnêteté.

CBT : Et enfin, l'intégrité ?
I : N/A. Elle est super dure cette question. C'est trop large. Mais si je devais mettre une note, je dirais 1,5.

CBT : D'accord, merci. Quel rôle, selon toi, a la réputation d'une entreprise dans le développement d'une relation de confiance ?
I : Ça veut dire que si bonne réputation, on fait plus confiance ?

CBT : Qu'en penses-tu oui ?
I : Tout dépend de ce que tu appelles réputation : c'est la notoriété ?

CBT : Oui, entre autres.
I : Ça peut jouer pour que j'aille vers eux. Par contre, je vais me baser sur l'échange que je vais avoir avec au début. Dans le cas d'une banque, s'il y a écoute de mes besoins ou fausse écoute pour juste me vendre un produit financier, bah c'est différent. Mais je vais plus facilement aller vers eux au premier abord si la réputation est bonne.

CBT : Du coup, considères-tu des scandales qui ont pu ternir la réputation d'un secteur pour juger de la confiance à lui accorder et pourquoi ?
I : Non car à ma connaissance, il n'y a eu aucun scandale, lié à des fuites de données personnelles. En gros, que les banques fassent du business avec des pays soumis à embargo comme cuba ou l'affaire avec Kerviel ou autre, ça ne me choque pas car d'autres industries le font. Mais si une banque fait fuiter des informations pour s'enrichir ou faire des trucs illégaux alors

là non. Voilà, s'il y a un équivalent de Lafarge, où ma banque fait du business avec du terrorisme comme Daech alors là ouais il y a moyen que je m'en aille.

CBT : D'accord, je comprends. Que sais-tu du règlement relatif à la protection des données personnelles ?
I : ahah du GDPR ? ahah c'est pas juste de me demander ça, je n'ai rien retenu.
CBT : Je suis sûre que tu exagères.

I : Ouais bon, alors, il y a informer le citoyen d'une utilisation externe de ses données et notamment en dehors de l'UE.
CBT : C'est le cas oui.
I : C'est le plus gros truc que j'ai retenu. C'est triste…
CBT : Non d'autant que c'est le hot point. Et puis, la médiatisation de cette nouvelle réglementation a été particulière.
I : Oui parce que maintenant je sais qu'il y a une meilleure protection des données personnelles mais je ne sais pas dans quelle mesure ou comment. Je crois que ça va dans la prolongation de la loi informatique.
CBT : Tout à fait. C'est son prolongement. Mais en tant que texte supra national, il permet aussi d'harmoniser la norme au sein de tout l'union. Pour revenir à la confiance, as-tu confiance en l'industrie bancaire et pourquoi ?
I : Une institution bancaire, j'ai confiance en elle sur la protection des données, pas forcément sur l'utilisation qu'ils font de mon argent mais ça m'importe peu parce que c'est leur business. En revanche, avec un start up, je vais être plus suspicieux quant à mes données et mon argent, pacque que s'ils se font hacker, ça peut faire très mal. J'ai du mal à avoir confiance en leur capacité à te rembourser intégralement en cas de problème. Avec des institutions présentes depuis plusieurs décennies voire siècles, j'ai moins de crainte.

CBT : Ok c'est clair. Penses-tu adopter une attitude différente par rapport à la divulgation de données personnelles selon qu'il s'agisse d'un environnement de travail ou personnel ?
I : Je suis très très très prudent quand je suis au boulot : je check plusieurs fois les destinataires de mes mais, ce que j'écris, ce que j'envoie, je ne me suis jamais connecté à mes mails perso ou mon Facebook.

CBT : Et sinon, comment qualifies-tu ton comportement en ligne et pourquoi ?
I : J'utilise énormément internet notamment avec les réseaux sociaux mais je suis très prudent quand je fais un achat ou quand je poste. Je regarde les avis avant de faire un achat. Je vais jamais enregistrer ma CB sauf sur quelques sites où j'ai vraiment confiance, genre Amazon. J'évite d'avoir des sessions ouvertes sur mes appareils outre les app de réseaux sociaux et les mails où c'est trop chiant d'avoir à me reconnecter à chaque fois.
CBT : Alright.
I : Donc je suis internetovre mais prudent quand même.
CBT : Belle tournure, ce sera notre mot de la fin.
I : Ahah. Parfait.

CBT : Juste quelques questions de fin te concernant ? 25 ans n'est-ce pas ?
I : Oui.
CBT : Ton niveau d'étude ?
I : Bac+5.

CBT : Depuis combien de temps es-tu client de ta banque ? et combien de banques en 25 ans ?
I : Oula, euh je suis client de ma banque depuis genre 20 ans. Et j'ai 2 banques.