MASTER IN BUSINESS ENGINEERING PROFESSIONAL FOCUS IN DATA SCIENCE

The impact of decision-making explanation on user privacy calculus

Wuyts, Nicolas

Award date:
2021

Awarding institution:
University of Namur

The impact of decision-making explanation on user privacy calculus

Nicolas Wuyts

Director: Prof. Wafa HAMMEDI

Thesis presented
in order to obtain the title of
Master 120 in management engineering, specialising in
in data science

ACADEMIC YEAR 2020-2021

Université de Namur, ASBL Faculté des Sciences économiques, sociales et de gestion – Département des Sciences de gestion

Rempart de la Vierge 8, B-5000 Namur, Belgique, Tel. +32 [0]81 72 48 41/49 58, Fax +32 [0]81 72 48 40

Abstract:

Consumer data has become a goldmine for companies. This data is valuable because AIs (artificial intelligence) can extract highly accurate predictions from it and enable companies to offer personalised services to their consumers. The operation of these AIs is not easily understood and this raises privacy issues for consumers. To solve this problem, techniques to explain how AIs work have been developed. These are called explainable AI (XAI). This thesis will investigate the impact of these explanations on the privacy calculus. The privacy calculus is a process in which the consumer will estimate his intention to disclose his data by evaluating the risks and benefits of a situation. In this thesis, I will analyse the impact of explanations through the effect of overall transparency on users' overall trust in AIs and the effect of this trust on the perceived risks of privacy calculus. To carry out this analysis, I performed a quantitative analysis on 138 responses. The results show that while overall transparency in AI does have an effect on overall trust in AI, overall trust in AI has no impact on perceived risks. I have, however, highlighted the significant influence of perceived data sensitivity on overall trust in AI and perceived risks. I also highlighted the influence of AI knowledge and AI self-efficacy on overall trust in AI and confirmed the independence of the variables overall trust in AI and privacy concerns.

Preface:

This thesis is by far the most important test and the most complete work I have done during my studies. It is the culmination of 5 years of study as a management engineering student ending at the University of Namur. Of course, I did not get there alone. That is why I would like to thank the people who helped me get there.

First of all, I would like to thank the promoter of my thesis, Professor Wafa Hammedi, for her patience and kindness towards me.

I would like to thank my friend Thomas Keiser for the support he gave me during the writing of my thesis. He was a great help to me during my periods of confusion.

I would also like to thank my sister Julie Wuyts for her help with the data collection and my father Patrick Wuyts for proofreading.

Finally, I would like to thank all those who have helped me in one way or another in my studies.

Summary Table:

1 INTRODUCTION

1.1 CONTEXT

Nowadays, data is everywhere. It is used in many fields and intervenes in every moment of our lives. It has become so important that we have given a name to this gigantic data flow: Big Data. This term characterizes data flows according to 3 criteria: the volume of data, its velocity and its variety (Chintagunta, Hanssens and Hausser, 2016).

These data are a source of information for companies, allowing them to better understand the behaviours and opinions of their consumers. The characteristics of Big Data provides them the most accurate information for their own purposes: the *volume* allows to increase the precision of the analysis, the *velocity* allows to adapt the analysis in real time and the *variety* allows to combine different sources of information carrying in them complementary information (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). All this information allows, through AI, to predict consumer preferences or to determine how to interact with them. This is a practice called *personalization*. The companies are able to personalize their offer depending on the customer they face.

A concrete example is Netflix's AI that it uses to suggest to its subscribers which movies, series to watch. It is impossible for Netflix' subscribers to efficiently choose the movies they want to watch from the catalogue without help. This is not possible because for people to be able to make an informed choice, they would have to watch the entire catalogue and it is way too big. To solve this problem, Netflix provides them with *recommendations*. These are based on their past choices, the choices of people with similar characteristics to them (age, country, etc.) as well as notable preferences in the user-generated data. This will result in making each Netflix account unique, *personalized* (Huang M., Rust R., 2020).

In this context, AIs are used by the vast majority of people and in many situations to improve their user experience. AIs are by definition techniques that simulate human intelligence and make our daily lives much easier. This goes from object recognition, to natural language processing, to voice assistants (Bauer K. and al., 2021). Amongst this enormous number of techniques, some of these techniques are called *machine learning*. Machine learning techniques consist in training models in order to solve specific tasks. These models are created from the data that have been used to train them. The problem with these techniques is that they are difficult to explain. Indeed, models created as a result of machine learning techniques work with their own reasoning. This is the result of mapping techniques that make it possible to establish links between information using statistics (Huang M., Rust R., 2020). It is therefore almost impossible, even for an AI designer, to determine with precision how a model resulting from machine learning techniques reasons to propose a solution. This problem has led the world to consider these models as "black boxes" (Rai A.,

2020). By definition, “black boxes” are systems where only inputs and outputs are observable (Bunge M., 1963) or, in the context of AI, systems where the relation between the two cannot be understood (Vinson N., Molyneaux H., Lapointe J., 2018).

Particularly complex techniques are those of *deep learning*. These techniques are based on the training of complex artificial neural networks. Artificial neural networks are techniques inspired by the functioning of neural networks in the human brain. The structure, links and other characteristics of the network are established during the training phase. Then the network is able to classify complex things like images according to what they represent or groups of people according to their musical habits. The problem is that the way the final decision is made is impossible to explain. Each parameter of the system has its impact on the final decision: the number of neurons involved, which neurons are involved, the connections within the network, etc. Obviously, the more demanding the task, the more the complexity of the network and its number of neurons increases.

This situation is highly problematic because AIs are making more and more decisions for their users. Some of these decisions have a direct and important impact on their lives. This is why a lack of comprehensible explanation of the AI's decision making for the user is problematic. For example: how could a banker justify refusing a loan to customers if the AI that made the decision does not provide any explanation? This also raises questions about the responsibility of the parties involved in such decisions. If an AI is free to make choices for the user and makes a problematic choice, makes a mistake, then who is responsible? We can also take autonomous cars as an example. Some of these autonomous cars put on the road by Tesla had accidents in 2016 and a driverless Uber car hit a woman in 2018 (Huang, Rust, 2020). In these cases, who is responsible? The AI designer? The company that produced the car? The owner of the car? The responsibility is not easy to establish. This is a point that will undoubtedly need to be addressed.

It is natural, then, that users are beginning to develop a certain distrust of AI. This distrust of technology has long been present in the culture of our societies. This is evidenced by the numerous anticipation movies depicting AIs as problems if they continue to take a more and more important part in our lives (Matrix, Terminator, etc.). A number of artists and thinkers have also portrayed the development of new technologies as a serious problem for our freedom. For example, Isaac Asimov (creator of the "three laws of robotics") wrote: "The advance of civilization is nothing but an exercise in the limiting of privacy.” (Huang, Rust, 2020). It is developing as a result of scandals revealing the increasing impact that AIs have on people's lives, too (expl. Facebook and Cambridge Analytica case).

Other issues such as *AI bias* related to AI negatively influence users’ trust. A good example was given by the New York Times in 2019. An article titled "Are we more likely to be criminals because we look like criminals?" called out readers on some more than questionable uses of an AI by the U.S. Immigration and Customs Enforcement. This agency was using a facial

recognition algorithm on driver's license photos. The purpose of this component was to detect potential criminals based on the emotions expressed on people's faces. The use of AI in this component led to an increased risk of using non-emotional features of people's faces to predict whether they were potential criminals (Huang, Rust, 2020). This example illustrates that AIs can be subject to bias and error just like any other technique or tool. The difference with AIs is the "black box" nature of AIs (especially machine learning techniques) that prevents us from detecting and solving these problems easily.

This type of realization causes users to worry about the lack of control over their personal data and their use. In the remainder of this thesis, I will use the notion of *privacy* defined as the *access to individually identifiable personal data* (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021).

On their side, companies try to offer a personalized service to their customers. For that purpose, they develop databases containing customer information and are even interested in purchasing customer data. These data, and more specifically personal data, have become so important that it has taken on the evocative name of "New Oil" (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). The New Oil also refers to the fact that data has become a commodity like any other. The growing demand and commodification of data is translated into a booming data market and companies that specialize in the purchase, aggregation and resale of personal data. These companies are called *data brokers*. These brokers are problematic from the customer's perspective because, while customers benefit from data aggregation, they also suffer from the lack of control over the flow of their personal data. The companies they interact with know everything about them which can lead to uses of their personal data that they disapprove.

A good example of a use that can lead to distrust is an AI that would allow data brokers to create a "Good Meat Fan" category of consumers. This is not problematic in itself, but it can become problematic when that same information is gets exploited by insurance companies. They could indeed mark this category of customers as "at risk" for health or life insurance. This would lead to disastrous effects for the people involved: increased insurance costs or even denial of insurance, etc (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). These manipulations of their data and the consequences that follow are not known to consumers and they have no control over them.

This has already proven to be problematic for the U.S. Federal Trade Commission, which has investigated some brokers because of these practices. The Commission investigated nine data brokers and concluded that they performed data aggregation behind consumers' backs (Federal Trade Commission, 2014). A European data regulation, the General Data Protection Regulation (G.D.P.R.) has also emerged to protect consumers from similar abuses. State interventions in the data markets are all the more interesting as the size of this industry

is colossal. We are talking about 5,000 data points per person for about 700 million individuals that are owned by data brokers right now around the world (Wolfie C., 2017).

1.2 RESEARCH MOTIVATION

Trust is an important factor if AIs are to achieve their goals. This is reflected in the following reflexion on AI: "Machines are beneficial to the extent that their actions can be expected to achieve our objectives." (Russell S., 2019). If we can no longer expect their actions to achieve our objectives, we can no longer trust them. We no longer benefit from them.

This trust is challenged by the inability of AIs to provide transparent and interpretable predictions. Techniques that try to solve this problem are called *explainable AI* (XAI). XAI techniques are not yet able to explain the reasoning of complex models in a way that is clear and understandable to the user. Global explanations are still limited but local explanations (for specific instances) are already well advanced (Ribeiro M., Singh S, Guestrin C., 2016). This creates different problems such as a lack of immediate *responsibility* for the consequences of the AI predictions, a problem in the *interaction* between human and AI because the solutions are not understandable and a problem of *acceptance* from the users, especially if the decision turns out to be important for the user (Bauer K. et al., 2021). These problems create a climate of mistrust among users towards AIs and their uses of personal data.

Users are increasingly torn between two positions regarding the disclosure of their personal data. On one hand, accepting the disclosure of their data allows the consumer to access personalized, potentially cheaper, more efficient services. On the other hand, the problem with accepting this disclosure is an increase in the risk of unauthorized access to this data (unauthorized sharing, data theft, etc.) which can lead to even more serious problems like identity theft (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). **This dilemma is called the *user privacy calculus* which corresponds to the cost-benefit evaluation of this situation.**

This privacy calculus is a worrying problem for managers because it can lead to negative consumer behaviours. The lack of trust of the customer can indeed decrease its willingness to even continue interactions with the company (Hollebeek L. and al., 2021). This also poses a problem for companies related to their expectations of optimization and user experience personalization (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). These expectations can be crucial for them in a competitive landscape.

It is interesting to note that binding laws related to data and the use of AI have come into force. For example, the General Data Protection Regulation (G.D.P.R.) requires companies to adapt their procedures in order to respect privacy laws. Among other things, this regulation obliges companies to provide their customers with explanations about the data they collect, use and analyse. They must also provide the customer with some control over the disclosure

of this data. The stated goal is to allow consumers to make informed choices about their privacy. It also requires anonymization of consumer personal data (Wieringa J., Kannan P.K., Ma X., Reutterer T., Risselada H., Skiera B., 2021). It identifies personal data as "any information relating to an identified or identifiable natural person". These regulations are incentives for managers to invest in making AI explainable. XAI allows them to explain the impact of the data provided by the customer on the decisions made by the AI and to respect the legislation. But to anticipate the effects of the explanations of XAI to their activities, it is interesting for them to have more information on these effects in a general way.

1.3 EXAMPLES OF XAI VISUALS FOR USERS

It is very important for the end user of an XAI to be able to effectively understand the explanation provided by the XAI. I will therefore give two concrete examples of visual ways to make it easier to understand how AI predictions were made.

To do this I will use examples of output from the LIME (Local Interpretable Model-agnostic Explanations) method. Note that this method offers accurate explanations for specific instances but poor explanations for the underlying AI model used. The outputs of this method are therefore explanations of instances that cannot be generalized to the model but that may nevertheless show problems in the starting dataset (Ribeiro M., Singh S, Guestrin C., 2016).

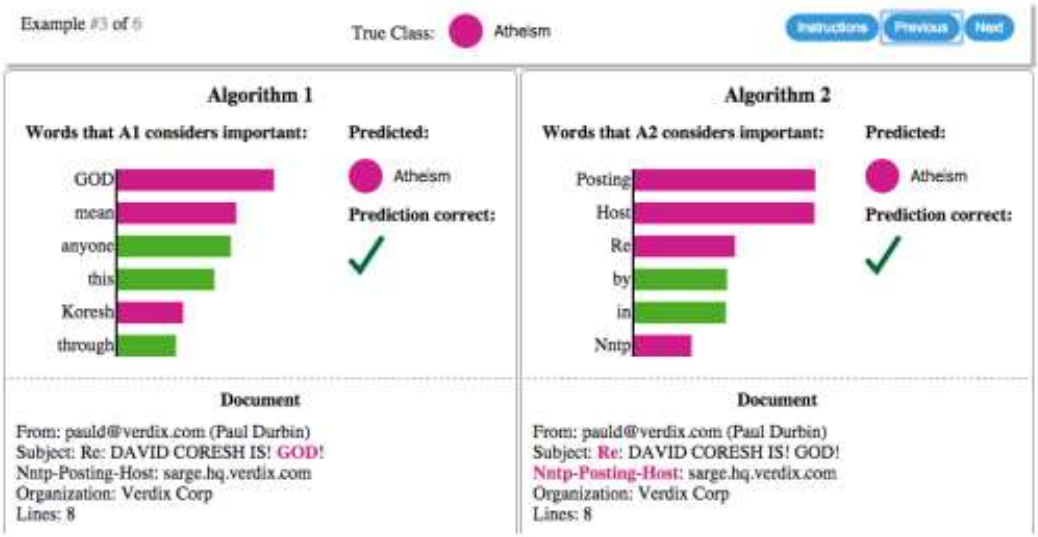


Figure 1 Explaining individual predictions of competing classifiers trying to determine if a document is about "Christianity" or "Atheism". The bar chart represents the importance given to the most relevant words, also highlighted in the text. Color indicates which class the word contributes to (green for "Christianity", magenta for "Atheism").

Algorithm 1 and Algorithm 2 are two different algorithms that try to predict whether a piece of text is rather about "Christianity" or about "Atheism". Figure 1 indicates which words led each algorithm to make their prediction i.e. which words had the biggest impact in the

decision-making process, ranked according to their importance. The colour indicates which decision they tipped the balance towards: green for "Christianism" and purple for "Atheism". It can be seen that the algorithm on the right (although specified by the article as more accurate in its decision) does not work properly. It uses words that are meaningless in making its decision: "Posting", "Host", "Re". This allows for objective criticism by non-expert users of the algorithm (Ribeiro M., Singh S, Guestrin C., 2016).

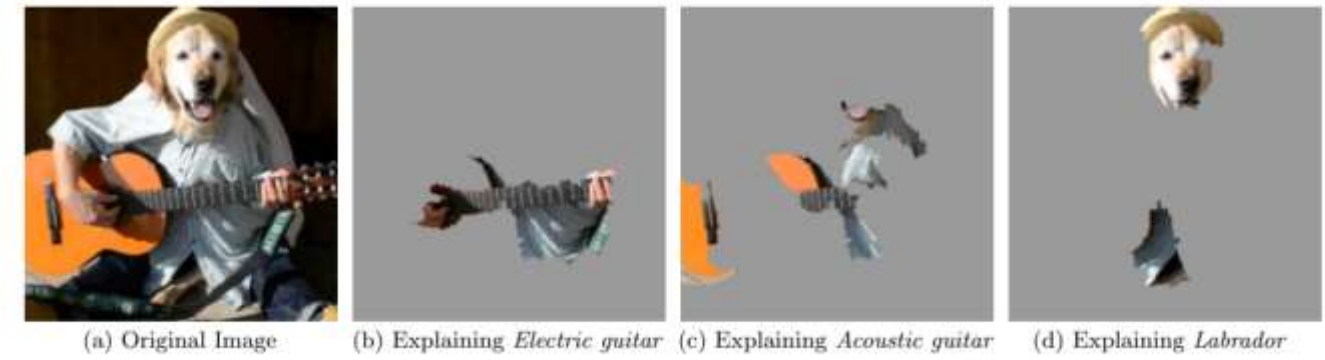


Figure 2 Explaining an image classification prediction made by Google's Inception neural network. The top 3 classes predicted are "Electric Guitar" (p = 0.32), "Acoustic guitar" (p = 0.24) and "Labrador" (p = 0.21)

Figure 2 shows the explanation of the classification of an image by an AI into several categories that are not mutually exclusive. The XAI shows the main pixels used for classification in each category. It can be seen that the AI has classified the image into both "acoustic guitar" and "electric guitar". It can also be seen that this confusion is due to the fretboard of the guitar. The explanation allows the user to enter the AI's trade-off decision process and thus understand more precisely how it works (Ribeiro M., Singh S, Guestrin C., 2016).

1.4 ACADEMIC MOTIVATION

The problem of the trade-off between benefits and loss of privacy is still a very active research topic. It regularly revolves around the user's trust in the AI and in the firm that uses it. For example: "Customers must balance privacy concerns against the benefits of personalized recommendations and offers. Important questions relate to how customers determine the optimal trade-off, including which individual difference variables and state variables might moderate their choices. Does the trade-off depend on the product category or the level of the customer's trust in the firm, for example? Also, how would this trade-off shift over time?" (Davenport T., 2020). Part of the research is therefore focused on the link between trust in AI and consumer privacy.

The research field associated with trust issues in AI is in full development. Explainable AI techniques are becoming more and more developed in order to be able to explain increasingly complex AIs such as, for example, deep learning. It has become crucial for

marketing researchers to be able to explain the decisions of different types of AI techniques, to be able to make well-considered decisions about the dilemma between explainability and accuracy, and to be able to market profitable AIs in which one can be trusted (Rai A., 2020). The influence of XAI on the computation of user privacy is a derivative of these research issues.

The current literature has not yet sufficiently delved into the influence of explainable AI techniques on consumer behaviour. There is also a lack of research on the influence of the use of explainable AI techniques on consumer trust in machine learning models (Bauer K. and al., 2021). This area of research is however popular among researchers: "how explanations on the use of personal information by algorithms can redefine the privacy calculus of consumers" (Rai A., 2020). This also applies to the broader implications of this research, such as the impact of this research on customer engagement research: "However, further research questions for ML-based service interactions include: How can these interactions be improved to optimize CE [Customer Engagement, NDLR]?" (Hollebeek L. and al., 2021)

To close the gap on these topics, I will analyse how an explainable AI technique impacts the user privacy calculation. My thesis will analyse the influence that explainable AI techniques have on different factors involved in privacy computation such as individual user privacy concern or user trust in the technology. I will adapt a model to highlight the factors that will be influenced by the XAI.

2 LITERATURE REVIEW

2.1 CONTEXT OF THE RESEARCH

This thesis focuses on some specific topics that will be developed in the literature review. These topics such as explainable AI, trust or privacy calculus are broad topics and can be applied in various contexts. Some of them, such as the privacy calculus, are even dependent on the situation in which they are applied. I will therefore set a general context to reduce this situation dependency problem.

I will analyse the situation of a consumer interacting with an AI or with any other interventions only through a computer. This means that no human contact will be considered, whether via the computer, via telephone or live. I made this decision because of the large number of possible situations to analyse in the context of consumer interaction with an AI and the analysis of privacy calculus. Moreover, user interactions with AIs in the computer environment take place most of the time under these conditions.

2.2 PROBLEMS OF TRUST IN AI

Machine learning techniques bring with them technological advances. The use of these techniques implies questioning the trust that users have in these tools. The fundamental problem with these tools is that they are not easy to understand. This problem of understanding generates 3 types of higher-level problems:

- The use of AI for predictions generates a lack of *direct accountability*. When an AI makes decisions that cannot be explained, it relieves users of responsibility for its behaviour.
- It limits the *contribution of AI to learning*. The lack of understanding of what the AI uses to make a decision and how it factors into the decision prevents the user from learning something from the AI.
- It hinders *acceptance* of their use. The lack of understanding of the machine's decision by the user can lead to resistance and hinder collaboration between the human and the machine (Bauer K. and al., 2021).

In this thesis, I will explore the third issue further. Indeed, the trust that users can place in these black boxes and their decisions depends directly on their understanding of the AI behaviour. To meet this need to understand the behaviour of the system, explanation techniques have been developed to clarify how these black boxes work (Ribeiro M., Singh S, Guestrin C., 2016).

2.3 EXPLAINABLE AI

These techniques are called *explainable AI (XAI)*. XAIs aim to describe how AI reasons to make predictions or decisions. They give the user a glimpse of how the AI will behave in the future by exposing the strengths and weaknesses of its reasoning. These techniques address the current trade-off between *accuracy* and *explainability* of AI. They fall into two different categories: *inherently interpretable AIs* and *post-hoc techniques* that are added to the AI (Rai A., 2020).

2.3.1 Inherently interpretable techniques

The first category of XAIs is composed of AIs that generate models that are directly interpretable by the user. These models include simple linear regressions, Bayesian classifiers or even decision trees. As long as one of these models is correctly implemented, it will be simple enough in its structure to provide the user with a traceable and transparent overview of the decision-making process. The weakness of these techniques is that they generate less accurate predictions (Rai A., 2020).

2.3.2 Post-hoc techniques

The second category of techniques is directly related to the problems raised by machine learning AIs and more particularly deep neural networks. The deep neural networks have "sacrificed transparency and traceability for predictive accuracy." (Rai A., 2020). To respond to this lack of transparency and traceability, post-hoc techniques approximate black box models with simpler models that explain the original one. They allow to explain the functioning of the model or the prediction related to a *specific instance*.

Post-hoc techniques must be interpretable by humans. They must therefore use input of explanations from the original AI that can be understood by a human. An input is a data that is used by the original data in this case. For example, an input of “word embeddings” is useful to the AI in a text classification logic but is not interpretable by a human. Instead, explainable AI will use a representation of the presence or absence of a word as a substitute. Furthermore, these explanations must be adapted to the target user. The same explanations will not be given to an AI expert as to a non-expert. The same applies to an expert in the field in which the AI is applied and a non-expert in that field (Rai A., 2020).

The main difference between the two categories of techniques is the trade-off between explainability and prediction accuracy. Inherently interpretable models generally offer better explanations but produce less accurate predictions. Post-hoc techniques give the opposite results for this trade-off (Bauer K. and al., 2021).

2.3.2.1 Kinds of post-hoc techniques

Post-hoc techniques can be further classified along 2 different axes. One axis corresponds to whether the XAI is related to a particular model (model-specific) or whether it does not take into account the model it explains (model-agnostic). The other axis corresponds to the level of explanation provided by the technique. The technique provides a *global explanation* of the model or a *local explanation* i.e., for a specific instance (Rai A., 2020).

Model-specific XAIs introduce constraints into the original AI models to improve the interpretability of the models. Model-agnostics XAIs only use model inputs and outputs to produce explanations. The level of explanation of the technique depends on the level of trust it wishes to achieve. A global level of explanation explains how the model works to make a prediction. This improves the user's trust in the model. A local level of explanation explains how a specific prediction was made. This improves the user's level of trust in the prediction and thus enables him to make further decisions based on it (Rai A., 2020).

Table 1 Classification of XAI Techniques

	Model-specific	Model-agnostic
Global	Enforce interpretability constraints into the structure and learning mechanisms of deep learning models	Develop interpretable global surrogate models based on input-output associations predicted by a black-box model Apply diagnostic techniques to understand the importance of specific features in a black-box model's predictions
Local	Use attention mechanisms to show how the model selectively focuses on features in high-dimensional input for an instance	Develop interpretable surrogate models with local fidelity in the vicinity of an instance

Figure 3: Classification of XAIs according to the two axes: model-agnostic/model-specific, global/local (Rai A., 2020, p.139).

For this thesis, I will focus more particularly on *local model-agnostic XAI*. This corresponds more to the needs of an individual facing a privacy calculus situation. The individual has to decide whether he is willing to share personal information and, if so, how far he is willing to share it. It is therefore a decision based on what they know about the use of their data and AI. He doesn't necessarily need to trust the model but he does need to trust at least the decision. A local XAI is therefore very suitable for this situation The choice of model-

agnostic XAI is more related to the ease of use. A model-agnostic technique allows to ignore the model on which it is applied.

2.3.3 SHAP method

In this thesis, I will use the SHAP (SHapley Additive exPlanations) explainable AI technique. This technique uses Shapley values to help explain an AI prediction for a specific instance. Shapley values come from coalitional game theory. They allow to determine the distribution of outputs among the players. In our case, this corresponds to the share of responsibility of each feature in the prediction. A player can be a single feature (e.g. a single pixel in an image) or a set of features (e.g. a group of pixels in an image or *super pixel*). We can interpret them more precisely like: "Given the current set of feature values, the contribution of a feature value to the difference between the actual prediction and the mean prediction is the estimated Shapley value." (Molnar C., 2021).

2.3.3.1 Advantages

The SHAP technique is actually a linear regression where the constants associated with the features are Shapley values. This ensures a fair distribution of the effects of the features on the forecast. Other methods such as LIME do not allow this fair distribution. This makes this method most appropriate to meet the explainability requirements of regulations like G.D.P.R. It also allows contrasting explanations at different levels of abstraction or precision. This kind of advantage is missing in other local techniques (Molnar C., 2021).

These advantages make the SHAP technique interesting but the most interesting advantage over other techniques like LIME is its ability to support more types of variables. This difference is what limits the practical uses that can be made of these other XAI techniques (Molnar C., 2021).

2.3.3.2 Disadvantages

However, the model has some disadvantages. Depending on the way it is implemented (KernelSHAP, TreeSHAP), it can lead to giving too much weight to certain variables (KernalSHAP feature dependence) or to use features that are not easily understood by the user (TreeSHAP unintuitive feature attribution).

However, its biggest disadvantage is its slowness. The way Shapley values are theoretically constructed creates enormous computational demands. This becomes problematic when you want to use the SHAP method for a large number of instances. This increases the amount of computation to be performed and makes the operation very slow (Molnar C., 2021).

2.3.3.3 Conclusion on the SHAP method

This method gives a good indication of where we stand today with AI-related explanatory techniques. These techniques are able to provide all users with explanations that are accessible for them and accurate for their needs. For the remainder of this thesis, we will consider that XAIs are capable of providing convincing explanations.

2.4 EXPLANATIONS

2.4.1 Features for a local model

For the local models, the creators of the LIME (Local Interpretable Model-agnostic Explanations) method put forward 4 characteristics that the explanations must have.

Explanations must provide the AI target audience with an interpretable explanation between the input variables and the AI response. This implies that the type of explanation must be adapted to the audience and that the explanation must be adapted to be easy to understand. It is not necessary to seek precision at all costs or to stick absolutely to reality.

Explanations must be locally faithful to the functioning of the model. This implies that locally faithful explanations are not necessarily faithful to the whole model. These explanations must explain how the model proceeded at that point to achieve its output.

Explanations must be model-agnostic. This makes it possible to consider the models we are trying to explain as black boxes. This is the case for many commonly used models. It also allows for more flexibility and the ability to anticipate future models.

Explanations should give a global perspective. The aim here is to provide trust in the model by explaining different instances. This allows the user to be shown different explanations of instances and to be reassured that the model is able to produce outputs in which he/she can have trust. This reassures the user that he or she will not be misled into falling for a particular case of the model (Ribeiro M., Singh S, Guestrin C., 2016).

2.4.2 Other features

Other explanatory features have been put forward by researchers. They emphasise the form that explanations of black box systems should take in general. In their view it is important that the explanations address the problems of fairness, contestability and competence that they may pose. To this end, they have identified certain features that these explanations must meet in order to improve the acceptance of these models (Vinson N., Molyneaux H., Lapointe J., 2018).

- “The explanation should refer to the personal characteristics of the person about whom the decision is made.

- The explanation should provide the inputs that influenced the decision (including trade-offs).
- The explanation should describe the procedure by which inputs led to the decision, though this may not be possible for black boxes.
  […]
- That identifiable groups of people are not intentionally or accidentally disadvantaged.
- An acceptable level of performance." (Vinson N., Molyneaux H., Lapointe J., 2018)

However, the last two features have the disadvantage that they are not suitable for local explanation. Indeed, to be able to satisfy these features, a more complete explanation of the general functioning of the model would be required. I will therefore concentrate on the first 3 features that the explanations should have.

In addition, when making a decision leading to a refusal, a way of providing an explanation has been proposed. This is to present the explanations in a counterfactual form that represents the explanation of the conditions that would have led to the opposite decision. For example, you would have been granted the loan if you had a 10% higher income. It is interesting to note that if the system is biased, this kind of explanation would bring up the latent discrimination in the system by comparison (Vinson N., Molyneaux H., Lapointe J., 2018).

Users also tend to prefer complex explanations. These complex explanations are mostly requested by users in order to be able to detect internal trades-off in the model (Vinson N., Molyneaux H., Lapointe J., 2018).

2.4.2.1 SHAP example

The SHAP method provides many of these required features by representing the main inputs that influenced the decision.

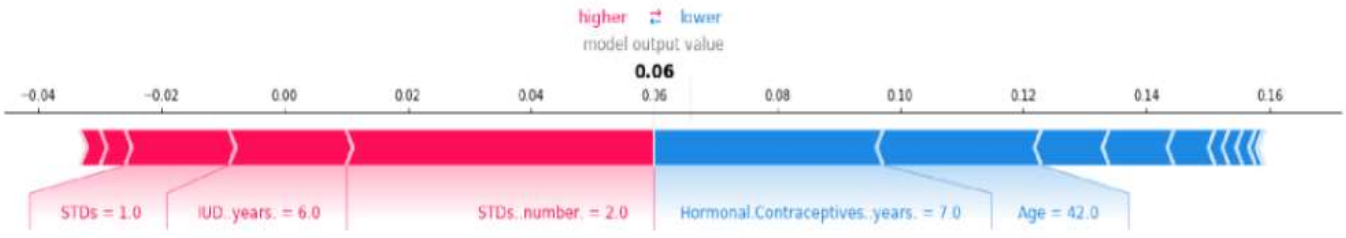


Figure 4: Explanation of the main factors influencing the decision in the predicted cancer probability of a woman (Molnar C., 2021).

Figure 4 is an example that shows the main elements that led to the prediction of the cancer probability: STDs (whether the person has ever had a sexually transmitted disease), IUD years (the number of years with an intrauterine device), STDs number (the number of

sexually transmitted diseases the person has contracted), Hormonal contraceptives years (the number of years the person has been taking contraceptive hormones) and the age of the person.

By indicating which inputs were decisive and in what sense they influenced the decision, part of the AI's reasoning is revealed to the user. By extrapolation, one can also identify the main changes that would need to be made to modify the decision.

As can be seen in Figure 4, the other features of a good explanation developed earlier in this thesis are provided by the SHAP method. This allows us to support the fact that the current XAIs are able to meet the requirements of the explanations to be believed.

However, Figure 4 is not easy to understand for non-expert users. It would therefore need to be clearer, for instance by adding explanatory text, modifying abbreviations, adding a legend, etc. It can be understood by an informed public though (data experts familiar with the domain, domain experts experienced in the use of AI, etc.). An important factor in analysing reactions to an XAI is therefore the *user's knowledge*.

2.4.3 Link between explanation and trust

XAIs provide explanations to the user, which improves their trust in the model's predictions (Bauer K. and al., 2021). The relationship between these explanations and the renewed trust in the model still needs to be clarified. In order to examine the impact of explanations on trust, it is necessary to do so in the context of the situation we are analysing. Our situation is completely online, so we need to analyse this impact through the prism of an interaction with a computer. We need to look at the impact on trust of an explanation without human interaction.

Empirical studies on user's trust provide an interesting basis. They conclude that user's trust depends on the granularity of the explanation and the transparency of the system. They also conclude that, for a recommendation system, *organisation-based explanations* do a better job than simple *computational explanations*. "In organisation-based approaches, recommendations are categorised according to common features." (Pieters W. 2010) A recommendation system in an organisation-based approach offers users recommendations based on common characteristics between several things. An example would be to offer him a beach holiday in an all-inclusive since he has already looked at such a holiday proposal on the internet, prefers the beach and has put a positive review of an all-inclusive on a travel advice site. The explanation of this recommendation will therefore be based on the common characteristics of the data with the recommendation. The computational recommendation will highlight the percentage of involvement of the data in the prediction. We could therefore have parasitic information such as 5% involvement of the data relating to the viewing of a video on dolphins.

2.4.3.1 Kind of explanations

The definition of explanation itself may offer some food for thought. Explanations can have 3 different purposes: giving *instructions*, giving *justifications* (offering reasons) and improving *transparency* (describing in detail).

For some expert systems, researchers have developed 5 different types of explanations: "*justification* (explain why the answer is a good answer), *transparency* (explain how the system reached the answer), *relevance* (explain why a question asked is relevant), *conceptualisation* (clarify the meaning of concepts) and *learning* (teach the user about the domain)." (Pieters W. 2010)

With regard to these 2 groups of explanation types, I will focus in this thesis on *justification* and *transparency*. This comes from the fact that:

- no instructions will be given,
- we will try to answer questions and not explain why they are relevant,
- the primary goal is not to teach the user something and
- we will not clarify the meaning of concepts.

So, our meaning of explanation is to give to the user's justifications of the decisions made by the model and improving the transparency of the model by describing the decision in detail.

2.4.3.2 Explanations meet trust

Trust must also be defined in order to understand it. "Trust is a form of self-assurance. It entails reliance upon something else, and the belief that this other will not fail in meeting certain expectations." (Pieters W. 2010). There is a fundamental difference that has been defined in other works between *confidence* and *trust*. "Confidence means self-assurance of the safety or security of a system without knowing the risks or considering alternatives. Trust means self-assurance by assessment of risks and alternatives." (Pieters W. 2010). This difference shows part of what the explanations will have to provide to the user: a visualisation of *risks* and *alternatives*. Explanations to improve trust will therefore need to explain how the system works by revealing details of the inner workings. This means opening up the black boxes to explain their internal workings if we want to improve the user's trust in them (Pieters W. 2010).

For AIs in particular, the main type of explanation expected is a *justification*: "*why* was such a decision made by the AI?". This justification is usually accompanied by a sub-question of *transparency* if one wishes to gain the user's trust and not simply stop at his confidence: "*how* was such decision made by the AI?".

Justification is important but it is not the most important factor when it comes to creating trust. Justification alone does not mean that the explanation solves the black box nature of the AI (Pieters W. 2010). To achieve trust, transparency is essential.

The type of XAI we have chosen (local, model-agnostic) therefore allows these questions to be answered. Indeed, the local XAI seeks to increase the user's trust in the AI's decision. To do this, it explains which inputs are taken into account to arrive at the outputs given by the basic model (justification). It can also approach an overall explanation (transparency) by looking at the distribution of influence of variables across a sample of instances. This is exactly what the SHAP method is capable of (Molnar C., 2021).

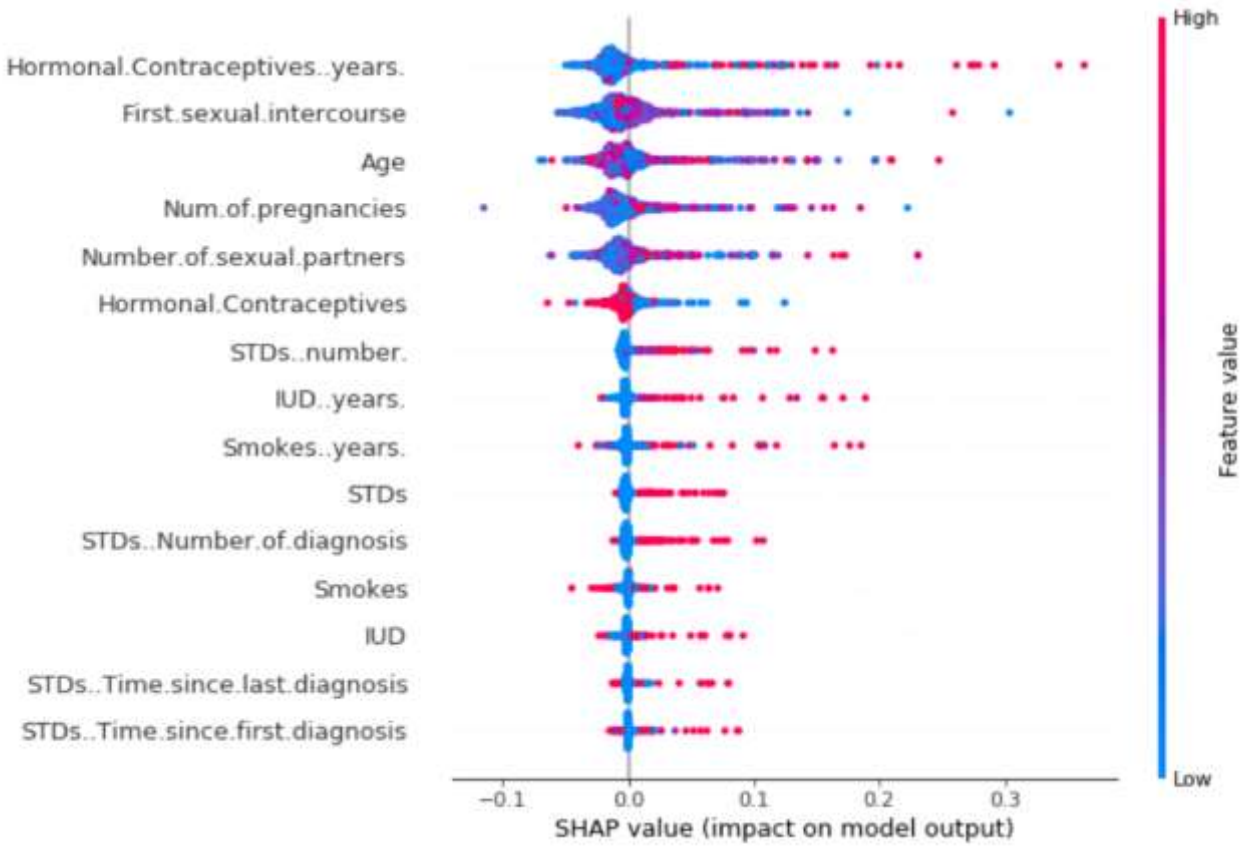


Figure 5: SHAP summary plot. Representation of the functionality of the inputs of several instances according to their values and their influence on the output. Your regular reminder: all effects describe the behaviour of the model and are not necessarily causal in the real world (Molnar C., 2021).

Figure 5 shows an approximation of a global explanation by aggregating instance explanations. On the graph, you can see the different SHAP values that the different features can take. The colours also show the relative values (high/low) of the features when they have been assigned a certain SHAP value. This allows us to estimate how the feature is considered by the AI. For example, the feature "Hormonal Contraceptives years" generally has a low SHAP value when its value is low while the feature "Hormonal Contraceptives" generally has a low SHAP value when its value is high. This allows us to estimate for each variable the general influence it has on the AI's decisions. This allows us to determine that the current XAIs are able

to bring a certain transparency to the functioning of the AIs and thus to positively influence the trust of the user in the AI.

The link between transparency and trust is based on several different explanatory factors. One of these factors is the *psychological distance* theory. The idea is that improving the transparency of decision making will decrease the psychological distance of the customer from the company they are interacting with. This distance is influenced by 4 different factors: geographical distance, temporal distance, distance between a social target and the individual and uncertainty. Social distance is the most important factor. It is generated by the consumer's perceived power asymmetry with the organisation he interacts with. A high social distance is directly related to a low level of trust in the company with which the consumer interacts. This is easily explained by the fact that a consumer who does not have information will fill this gap with stereotypes. The transparency of the decision-making process allows him to avoid this and to focus on the way the decision was made (Grimmelikhuijsen S., Herkes F., Leistikow I., Verkroost J., de Vries F., G. Zijlstra W., 2019).

Trust is very important for businesses as it can positively influence word of mouth and consumer purchase intentions. It has been shown that trust is influenced by consumers' perception of the effort to be transparent and socially responsible. The effect of transparency on consumer trust is greater the more the consumer wants to make a 'correct' choice (Dexe, J., Franke, U. & Rad, A., 2021).

This leads to the first hypothesis of my thesis:

H1: The overall transparency in AI positively influences the overall trust in AI.

In an online consumer context, the beliefs of trust are divided between the online seller and the technology used in the transaction. The consumer needs to trust both the seller (retention of personal information, execution of the transaction, etc.) and the technology used in the transaction for the security, reliability, etc (Tang T., Tsai C., Wu W., 2005).

2.5 PRIVACY CALCULUS

2.5.1 General consideration

The notion of the privacy calculus stems from previous research on behavioural intentions showing that:

- different influencing factors come into play when making decisions: "institutional norms of appropriate behaviour, expected benefits, and unpredictable consequences." (Laufer and Wolfe, 1977, p.37).
- individuals' beliefs are paramount in understanding their behaviour. In the particular context of purchasing products and services, a transaction that requires

the transmission of information to be completed involves a privacy calculus (Dinev T., Hart P., 2006).

Privacy calculus is a process that takes place during decision making. It has already been analysed in many studies and contexts like for mobile applications or health care. The implication of this process is that the individuals involved in it perform a **trade-off between the risks and benefits perceived of disclosing private information**. The process is seen as relatively stable in the literature. When the risks and returns are comparatively the same in different situations, the final decision of the process are the same. It should also be noted that the *context* has an important impact on the process. Privacy is context-dependent, which directly affects the privacy calculus (Hassandoust F., Akhlaghpour S., Johnston A., 2021).

2.5.1.1 Expectancy theory

An interesting parallel has been drawn with expectancy theory. Expectancy theory explains that individuals behave in a way that maximizes positive outputs and minimizes negative outputs. The privacy calculus theory is relatively identical but takes into account the situation where the individual must consider the impact of the disclosure of personal information. This explains the idea in the privacy calculus theory that an individual has an incentive to share information if the benefits outweigh the risks (Dinev T., Hart P., 2006).

2.5.1.2 Dilemma of believes

In the theory of privacy calculus, the dilemma of the process of revealing personal information is made between the perceived risks and benefits of this situation. This dilemma takes into account all the beliefs of the individual in either direction. The result of this dilemma will be a behavioural intention. This implies that the individual's decision will be the most likely behaviour taking into account all their beliefs. Each belief influences the probability of the behaviour and none of them can deny another (Dinev T., Hart P., 2006).

2.5.1.3 Psychological limitation

Some of the literature rightly argues that there are psychological limits to the proposition of rational consumer thinking in the privacy calculus process. Limitations such as the inability of consumers to process all the information in the cost-benefit trade-off, the difficulty of estimating the effect of time on the elements of the process or the irrationality of immediate gratification (Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015).

2.5.2 Perceived benefits

The perceived benefits can be diverse and not necessarily directly concerned with the individual. The common good can be taken into account in the benefits perceived, for example. The perceived personal benefits can also be called personal interest and it’s an incentive to pass on personal information during transaction. Personal interest depends on

what an individual expects as an outcome of a transaction with a third party. It positively influences the intention to disclose personal information (Dinev T., Hart P., 2006).

H2: The perceived benefits positively influence the intention to disclose.

2.5.3 Perceived risks

The perceived risks aspect of the process is related to the loss of control and misuse of the information an individual shares. In an internet environment, the perceived risks are related to the sometimes-opportunistic behaviours of the seller which results in losses for the customer. The privacy risk is increased by the use of information technology during a transaction with an obligation to share information (Dinev T., Hart P., 2006). Certain methods can reduce this perceived risk such as a privacy notice especially when the party requesting personal information is unfamiliar (Milne and Culnan, 2004).

H3: The perceived risks negatively influence the intention to disclose.

2.5.4 Link between perceived risks and benefits

Much of the literature argues that perceived benefits and risks are independent. But some research has shown that this is not the case and that in some situations perceived risks influence perceived benefits negatively. This is because significant risks tend to undermine perceived benefits whether or not they are significant due to risk aversion. An example is nuclear energy. It is perceived as a risky energy and its benefits are perceived as less important because of these same risks (Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015).

H4: The perceived risks influence negatively the perceived benefits.

2.5.5 Perceived data-sensitivity

The perceived sensitivity of the data is an important contextual element in the privacy calculus. It highlights the perceived importance of the data to the consumer's privacy. This factor is recognised as a crucial aspect of the privacy calculus. It influences perceived risk, perceived benefit (Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015) and trust (Malhotra, Naresh K.; Kim, Sung S.; Agarwal, James, 2004).

Perceived data sensitivity can influence the overall trust of individuals as it indicates a version of privacy sensitivity. The way in which data sensitivity is generally addressed gives an indication of the trust individuals have in the third party they generally have to disclose data (Malhotra, Naresh K.; Kim, Sung S.; Agarwal, James, 2004).

H5: A higher perceived data-sensitivity positively impact perceived risks.

H6: A higher perceived data-sensitivity negatively impact perceived benefits.

H7: A higher perceived data-sensitivity negatively influence overall trust in AI.

2.5.6 Trust in privacy calculus

Trust in the privacy calculus has not been consistently conceptualised in the scientific literature. Its relationship to the other elements involved in the process is variable depending on the study. It should also be noted that the institutional trust used in several studies represents very different things depending on the study: general trust in the Internet, the data collection website, etc (Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015). I have based myself on the trust of the individual in the third party of the transaction whether it is a company or not. In the situation I develop in this thesis, the third party is represented by the AI that asks them for the data.

The trust aspect of the process is related to the individual's trust in the retention of his personal information. If he does not trust the party asking him to share his information, he will be less likely to share it. Trust is a belief that is a multi-dimensional construct. Trust is a set of beliefs that positively influences the intention of individuals to engage in transactions. It encompasses the belief that the third party of the transaction will not engage in opportunistic behaviour towards the user. The structure of beliefs included in trust varies widely in studies analysing the influence between trust and intention to disclose personal information in a transaction (Dinev T., Hart P., 2006).

However, an aggregation around 3 factors has been retained for perceived trust: *competence or ability*, *benevolence*, *integrity*. These factors are deliberately broad enough to allow for the inclusion of all of their constituent sub-factors (McKight and al., 2002).

These factors are relatively consistent in recent studies but tend to be slightly modified depending on the subject under study. But in general, they correspond to relatively similar concepts. For example, a version analysing online transactions requiring disclosure of personal information by a consumer uses the following three characteristics of trust: *competence*, *reliability* and *safety*. Competence refers to the ability of the seller (trusted one) to perform the behaviour expected by the consumer (trustor). Reliability is considered to be the consistency between words and actions. Safety refers to the belief that the information disclosed will be kept secure and confidential (Dinev T., Hart P., 2006). Institutional trust is a general view of these factors in relation to the third parties involved in such transactions (type of company, etc.).

2.5.6.1 Link between trust and risk

The link between trust and risk is not obvious because there is a gap between trust and trusting behaviour. "Trust is the willingness to assume risk; behavioural trust is the assuming of risk." (Mayer et al. 1995, p. 724) The AI perceived trust is however related to a perceived level of risk (Dinev T., Hart P., 2006). A greater trust in the third party of a transaction that

requires the sharing of personal information leads the user to perceive less risk in their disclosure. (Dan and al. 2008).

H8: The overall trust in AI negatively influences the perceived risks.

2.5.6.2 Other factors influencing trust

2.5.6.2.1 AI knowledge

Scientific knowledge in general of individuals influences their behaviour through direct and indirect channels. This is scientific reasoning skills. These skills enable them to better understand situations that require complex specific knowledge (direct channel). It also allows them to improve their reasoned confidence in the associated scientific technology which in turn influences their reasoning.

In other words, general scientific knowledge allows for a better understanding of complex technologies. This influences their behaviour through the reasoned confidence that can be developed in the technology and through a better understanding of the technology (Sailer M. and al., 2021).

As AI technology is rather specific, it would be interesting to know the level of knowledge of individuals in this field. This would make it possible to examine the influence that the level of knowledge of individuals may have on the construction of trust.

2.5.6.2.2 AI self-efficacy

We can define self-efficacy as: “people's beliefs in their capabilities to produce desired effects by their own actions” (van Esch P., Cui Y., Jain S.P., 2021). Self-efficacy gives individuals the psychological capacity to respond to challenges and to learn. In this context, the self-efficacy felt by individuals when interacting with an AI will necessarily affect their reaction and trust. An individual with good AI self-efficacy will feel able to deal with the potential problems that an AI may generate. This will influence their trust in the AI.

2.5.7 Privacy concerns

Privacy concerns impact trust and perceived risk The perceived risks subsequently impact on the decision-making process. The privacy concern is the internalization of a possible loss. In the context of purchasing a product or service online, privacy concerns are an assessment of what happens if individuals disclose personal information on the internet. This concern is largely based on the technical possibilities for companies to achieve their goals on the internet. Data mining is one of the most impactful relevant technologies in this context. It allows to extract the patterns of individuals from their data and to profile and target them. This highlights the consequences of sharing personal data with a third party. The more unclear the final use of the data by the third party of the transaction is, the more the privacy concerns are exacerbated. The more unclear it is to the consumer when and how his data will be used, the more extensive the privacy concerns of the individual will be (Dinev T., Hart P., 2006).

H9: The privacy concerns negatively influence the overall trust in AI.

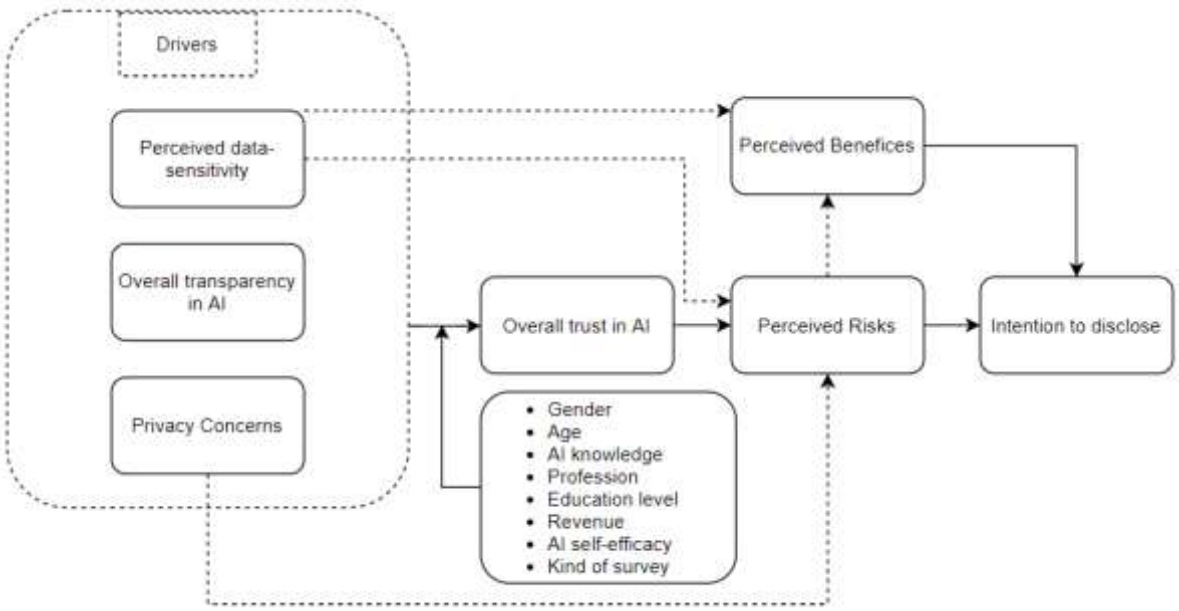
H10: The privacy concerns positively influence the perceived risks.

In the context of the privacy calculus process, the privacy context is seen as the pre-existing attitudes towards privacy. Privacy concerns is therefore opposed in the literature to situation-based privacy constructs. This opposition is reflected in the situational decision of consumers. A consumer who is generally opposed to the disclosure of his or her information may be willing to disclose it in exchange for gains in time, money, pleasure, or the like (Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015).

2.5.7.1 Privacy paradox

"The privacy paradox exists when individuals express concerns over the privacy of their personal information's but act contrary to these concerns and readily surrender their personal information's to use an information system." (Smith et al., 2011). This paradox has had many explanations over time. Either it is trust or it is a rational cost-benefit calculation (privacy calculus) that explains it (Awad and Krishnan, 2006; Dinev and Hart, 2006). It can also be explained by psychology: affect, cognitive biases, etc (Acquisti, 2005; Li et al., 2011). The answer is surely multifactorial but, in this work, I will verify the existence of a relationship between privacy concern and intention to disclose as well as the relationship between privacy calculus (risks, benefits) and intention to disclose. This will at least confirm the privacy paradox and the privacy calculus factor.

2.6 MODEL



The model created for this thesis is based in part on the model of. Hassandoust F., Akhlaghpour S. and Johnston A. Specifically, the relationship between overall trust in AI, privacy concerns and perceived risks (Hassandoust F., Akhlaghpour S., Johnston A., 2021).

3 RESEARCH DESIGN

3.1 METHODOLOGY

In this section, I will detail the methodology I used in order to verify the assumptions of our model. We will therefore discuss our data collection material and the collection of the data itself.

3.1.1 Data collection material

Our data collection was done through a quantitative questionnaire aiming at testing the hypotheses we posed in the literature review section (see Appendix 8.1 Surveys). The questionnaire we used is broken down into several stages.

The first stage is an information stage. It allows us to provide the survey participants with information such as the objective of the questionnaire or inform them about the guaranteed anonymity of their answers.

The second stage is a verification stage. It allows us to verify that the participants have at least once used an AI, to identify at least one with which they have interacted and to inform us about their frequency of interaction. If they have never interacted with an AI, the survey will be considered invalid.

The third stage is a stage that allows us to determine the participant's relationship with “AI and privacy” through their AI knowledge, privacy concerns, opinion on AI transparency and overall trust in AI.

The fourth stage is an experimentation stage. The aim is to put the participant in front of a situation in order to identify the influence of situational variables. The variables we try to determine are the perceived sensitivity of the data involved, the perceived benefits and risks and also the intention to disclose the data.

The fifth stage is a socio-demographic positioning stage. This stage allows the participant to be positioned socio-demographically in the population.

3.1.2 Data collection

We shared this questionnaire via social networks (Facebook) and via e-mail. We managed to collect 149 responses of which 138 were valid. The non-valid ones are those that declared they did not interact with AIs or did not finish the survey. They were detected and set aside in the second stage of the questionnaire.

3.2 MEASURES

Here we present the measures we used for the different variables. We will also talk about the experimentation we set up, our sample and the reliability of our scales.

3.2.1 Kind of scales

We used two different types of scales in this thesis: a 7-point Likert scale and a 7-point semantic differential scale. The 7-point Likert scales are all ranging from "strongly disagree" to "strongly agree" and the 7 points semantic differential scales from “X” to “Y” in the propositions X/Y. Depending on the variables, different scales were used:

Variables	Scale	Adapted from
AI knowledge	7-point Likert	Çoklar & Ferhan Odabaşi (2009)
Overall transparency in AI	7-point Likert	*Bertot et al. (2010)*
Perceived data-sensitivity	7-point semantic differential	Xie et al. (2006)
Privacy concerns	7-point Likert	Malhotra et al. (2004)
Overall trust in AI	7-point Likert	Chattaraman et al. (2019)
Perceived Benefit	7-point Likert	Dinev et al. (2012)
Perceived Risks	7-point Likert	Dinev et al. (2012)
Intention to disclose	7-point semantic differential	Anderson and Agarwal (2011)
AI self-efficacy	7-point Likert	Yim et al., 2012

3.2.2 Construct/Items

3.2.2.1 Dependant variables

3.2.2.1.1 Intention to disclose

Please specify the extent to which you would reveal your personal information to use the AI service:
ITD1: Willing/unwilling
ITD2: Unlikely/likely
ITD3: Not probable/probable

3.2.2.1.2 Perceived risks

RIS1: It would be risky to give personal information to the AI service.
RIS2: There would be high potential for privacy loss associated with giving personal information to the AI service.
RIS3: Personal information could be inappropriately used by using the AI service.
RIS4: Providing the AI service with my personal information could involve many unexpected problems.

3.2.2.1.3 Overall trust in AI

TRU1: AI Products/Services competently and effectively interact with me.
TRU2: AI Products/Services perform all their roles very well.
TRU3: Overall, AI Products/Services are capable and proficient.
TRU4: AI Products/Services are truthful to me.
TRU5: I would characterize AI Products/Services as being honest.
TRU6: AI Products/Services are sincere and genuine.

3.2.2.2 *Independent variables*

3.2.2.2.1 Perceived benefits

BEN1: Providing my personal information to the AI service will entail benefits.
BEN2: Revealing my personal information to the AI service will help me obtain the services I want.
BEN3: I believe that as a result of my personal information disclosure, I will benefit from a better, more customized service.

3.2.2.2.2 Perceived data-sensitivity

How sensitive do you perceive the information requested by the AI to be?
SENS1: Localisation (Not sensitive at all/very sensitive)
SENS2: Speed (Not sensitive at all/very sensitive)
SENS3: Travel time (Not sensitive at all/very sensitive)
SENS4: Age (Not sensitive at all/very sensitive)
SENS5: Residence (Not sensitive at all/very sensitive)
SENS6: Year of manufacture (Not sensitive at all/very sensitive)
SENS7: Car type (Not sensitive at all/very sensitive)
SENS8: Distance travelled (Not sensitive at all/very sensitive)

3.2.2.2.3 Privacy concerns

PCO1: Compared with others, I am more sensitive about the way AI services/products handle my personal information.

PCO2: To me, it is the most important thing to keep my privacy intact from AI services/products.
PCO3: In general, I am very concerned about threats to my personal privacy.

3.2.2.2.4 Overall transparency in AI

TRA1: The AI Product/Service allows me to track my activities.
TRA2: The AI Product/Service provides information about his decisions and actions.
TRA3: The AI Product/Service provides information on his rules and regulations
TRA4: The AI Product/Service disseminates information on his own performance.
TRA5: Overall, AI Product/Service has an enhanced transparency on what it does.

3.2.2.3 Moderator variables

3.2.2.3.1 AI knowledge

AIK1: I can explain how AI Products/Services operate.
AIK2: I can use AI Products/Services in different ways.
AIK3: I can do basic things regarding AI technology.
AIK4: I can explain general concepts related to AI technology.
AIK5: I can use AI Products/Services effectively.

3.2.2.3.2 AI self-efficacy

ASE1: I have confidence in my ability to use AI effectively.
ASE2: I do not doubt my ability to use with AI effectively.
ASE3: I have excellent skills and ability in the field of AI.
ASE4: I am proud of my skills and ability in the field of AI.

3.2.2.3.3 Age, Gender, Profession, Education, Revenue

For Age, Education, Profession and Revenue, categorisation is provided in the socio-demographic section. There are 10 categories for Age, 7 for Education, 6 for Revenue and 7 for Profession. A binary choice is proposed for Gender (Male/Female).

3.2.3 Experimentation

The experimentation that we propose to the participants during the survey is an experimentation developed within the framework of a study similar to ours (Kehr and al., 2015). The material used in this similar study was a mobile application that allowed questions to be asked on both the visual and the background of the application in order to see the effects on the participants' privacy (perceived benefits, perceived risks, intention to disclose).

In our survey, we do not ask questions about the visual and the background of a mobile application but we need to confront the participants with a concrete situation. We choose the following situation: an AI that serves to "record and track driving behaviour and to provide customized feedback on the own driving style in order to promote better and safer driving." (Kehr and al., 2015).

The reuse of a similar experimentation allows us to rely on data that have already been classified by the researchers into two categories: sensitive and non-sensitive. These groups of data types will then allow us to determine the perceived data sensitivity. Respondents were given a choice between a survey containing the sensitive data and a survey containing the non-sensitive data. They did not know which of the two surveys they were responding to. With this material, we will be able to form two different samples which will be confronted with different data demands in terms of sensitivity. This will allow us to determine the importance of this variable in the model according to the data requested.

3.2.4 Presentation of the sample

My sample is composed of 149 answers. I excluded 11 responses from the survey because the participants said they did not interact with AIs or did not complete the survey. Amongst the valid surveys, 55,79% of the participants answered to the first survey (the sensitive-data one) and 44,21% of them answered to the second survey (non-sensitive data). 62,32% of the respondents are women and 37,68% are men. 41.3% of the respondents are between 19 and 25 years old and 24.63% are between 26 and 30 years old. 69.565% of the respondents are under 30 years old. 57.971% of the respondents have a university degree. The second largest category is represented by 27.536% of the respondents who have a non-university degree. 44.928% of the respondents are employees and another 31.159% are students. As for income, it is distributed in a constant manner below to 3000 euros (36.23% under 1500 euros, 21.01% between 1500 and 2000 euros, 21.01% between 2000 and 2500 euros, 13.04% between 2500 and 3000 euros, 2,17% between 3000 and 3500 and 6,25% more than 3500).

Our sample is therefore composed mainly of respondents under 30 years of age. More women than men are in the sample. The most represented professions are employees and students. The majority of respondents have a higher education diploma (university or not).

3.2.5 Reliability of the scale

Most variable-related constructs are composed of several items. These items may differ from each other and some constructs may not represent the variables we are trying to study. It is therefore necessary to check the reliability of the constructs and the consistency of the items between them.

In order to analyse the reliability of the constructs, the items need to follow 3 conditions: final commonalities need to be greater than 50%, the correlation between items and factors needs to be greater than 60% and the cross-loading needs to be less than 30%. Items that do not meet these conditions will be discarded.

To analyse the consistency of items within a construct, we will use Cronbach's alpha (Durant 2003). This is an indicator for determining the internal consistency of a scale and therefore its reliability. For the scale to be considered reliable, the indicator must be greater than 0.7. The indicator range is from 0 to 1 (Nunnally, 1978).

3.2.6 Summary table of analyses

Construct and Cronbach's Alpha	Items	Arithmetic mean	Standard deviation	Factor loading	Cumulative percentage variance
Perceived data-sensitivity (Sensitive data)	**SENS1:** Localisation	4,701	1,487		
	SENS2: Speed	3,688	1,575		
	SENS3: Travel time	3,442	1,509		
	SENS4: Age	4,156	1,377		
	SENS5: Residence				
Perceived data-sensitivity (Non-Sensitive data)	**SENS6:** Year of manufacture	3,279	1,781		
	SENS7: Car type	3,787	1,724		
	SENS8: Distance travelled	4,295	1,764		
Overall transparency in AI **α = 0,7661**	~~**TRA1**: The AI Product/Service allows me to track my activities.~~	4,304	1,417	0,6	59,4%
	TRA2: The AI Product/Service provides information about his decisions and actions.	3,239	1,483	0,76	
	TRA3: The AI Product/Service provides information on his rules and regulations.	3,355	1,429	0,829	
	TRA4: The AI Product/Service disseminates information on his own performance.	3,174	1,439	0,727	

	TRA5: Overall, AI Product/Service has an enhanced transparency on what it does.	2,4493	1,1012	0,764	
Privacy concerns **α = 0,7397**	**PCO1**: Compared with others, I am more sensitive about the way AI services/products handle my personal information.	4,08	1,566	0,739	66,2%
	PCO2: To me, it is the most important thing to keep my privacy intact from AI services/products.	4,855	1,422	0,845	
	PCO3: In general, I am very concerned about threats to my personal privacy.	4,406	1,597	0,852	
Overall trust in AI **α = 0,8845**	~~**TRU1**: AI Products/Services competently and effectively interact with me.~~	4,2246	1,0604	0,621	68,7%
	TRU2: AI Products/Services perform all their roles very well.	4,2899	1,1412	0,744	
	TRU3: Overall, AI Products/Services are capable and proficient.	4,4784	1,0754	0,708	
	TRU4: AI Products/Services are truthful to me.	2,986	1,184	0,89	

	TRU5: I would characterize AI Products/Services as being honest.	2,928	1,182	0,894	
	TRU6: AI Products/Services are sincere and genuine.	2,7464	1,153	0,886	
AI knowledge **α = 0,8429**	**AIK1:** I can explain how AI Products/Services operate.	3,906	1,593	0,873	68,2%
	~~**AIK2:** I can use AI Products/Services in different ways.~~	4,761	1,316	0,683	
	AIK3: I can do basic things regarding AI technology.	3,819	1,68	0,78	
	AIK4: I can explain general concepts related to AI technology.	3,877	1,736	0,903	
	AIK5: I can use AI Products/Services effectively.	4,217	1,464	0,736	
AI self-efficacy **α = 0,92**	**ASE1:** I have confidence in my ability to use AI effectively.	3,812	1,521	0,908	80,8%
	ASE2: I do not doubt my ability to use with AI effectively.	3,848	1,602	0,878	
	ASE3: I have excellent skills and ability in the field of AI.	2,826	1,479	0,907	
	ASE4: I am proud of my skills and ability in the field of AI.	2,833	1,478	0,902	

Perceived benefits **α = 0,8845**	**BEN1:** Providing my personal information to the AI service will entail benefits.	4,261	1,252	0,888	79,2%
	BEN2: Revealing my personal information to the AI service will help me obtain the services I want.	4,304	1,370	0,889	
	BEN3: I believe that as a result of my personal information disclosure, I will benefit from a better, more customized service.	4,203	1,389	0,893	
Perceived risks **α = 0,8967**	**RIS1:** It would be risky to give personal information to the AI service.	4,297	1,421	0,851	76,3%
	RIS2: There would be high potential for privacy loss associated with giving personal information to the AI service.	4,348	1,536	0,894	
	RIS3: Personal information could be inappropriately used by using the AI service.	4,71	1,51	0,875	
	RIS4: Providing the AI service with my personal information could involve many unexpected problems.	4,029	1,504	0,875	
	ITD1: Willing/unwilling	4,449		0,846	79,4%

Intention to disclose **α = 0,8687**	**ITD2:** Unlikely/likely	3,558		0,896	
	ITD3: Not probable/probable	3,659		0,928	

I did not conduct a factor analysis of the items in the Perceived data-sensitivity construct. This is due to the fact that each item individually analyses the sensitivity of individuals to a specific data. Only the average of the collected data allows me to determine the overall data-sensitivity of the respondents. I will analyse later the difference in respondents' perceived data-sensitivity depending on the survey they were confronted with (sensitive data survey/non-sensitive data survey).

4 RESULTS

In this chapter we will analyse the data obtained from the analysis of the data collected. To do this we will first look at the descriptive statistics of the data. Then we will analyse the covariances of the drivers. We will then analyse the relationships we have posed in our model: between drivers and overall trust in AI, between overall trust in AI and perceived risks, between perceived risks and perceived benefits and between perceived benefits/risks and intention to disclose data. Finally, I will analyse the impact of moderating variables on the relationship between drivers and overall trust in AI.

4.1 DESCRIPTIVE STATISTICS

The majority of the variables are measured by a 7-point Likert scale ranging from 1 (Strongly disagree) to 7 (Strongly agree). The only two exceptions are Perceived data-sensitivity and Intention to disclose which are calculated by a 7-point differential semantic scale. This other scale goes from 1 to 7 like the first one but makes the answer oscillate between 2 semantically opposed propositions like possible/impossible. This scale, for Perceived data-sensitivity, means: the higher the value, the more sensitive the respondent is to the data being asked. For Intention to disclose: the lower the number, the more the respondent intends to disclose his data.

Let us now focus on the drivers: Privacy concern, Overall transparency in AI and Perceived data-sensitivity. We can see that the Privacy concern and Perceived data-sensitivity constructs have relatively high average values (4.447 and 4.07). This indicates that the respondents on average perceived the data as sensitive and felt concerned about the use of their data. This is also in line with the average Overall transparency in AI of 3.0543. This means that the respondents do not perceive any positive or negative indication from the AIs in general regarding transparency in their functioning, use of data among others. These drivers influence Overall trust in AI in our model and the respondents feel rather indifferent to this variable with a mean of 3.4855 and the lowest standard deviation of all variables of 0.9492.

Let's look at the main elements of the privacy calculus: Perceived benefits, Perceived risks and Intention to disclose. The benefits and risks perceived by the respondents are relatively positive with an average of 4.256 for Perceived benefits and 4.346 for Perceived risks while the Intention to disclose is a bit negative with an average of 3.8888.

The moderator variables are relatively neutral. The mean of AI knowledge is 3.955 and AI Self-efficacy is 3.33. This means that the respondents' ability to interact with AIs is not high and that they do not consider themselves particularly capable of interacting effectively with AIs. An analysis of the socio-demographic elements of the moderator variables was carried out in the sample analysis section of the research design.

4.2 CORRELATION BETWEEN DRIVERS

The aim of this analysis is to check the independence of the explanatory variables in order to avoid multicollinearity problems.

We can see that all the coefficients are positive and very weak since they are lower than 0.4. If the Pearson coefficients are lower than 0.4, the correlation between the variables is said to be weak. There is therefore no link between them.

4.3 HYPOTHESIS VALIDATION

In order to properly analyse the assumptions, we made when building our model, I performed linear regressions between the dependent and independent variables. The aim is to determine whether the dependent variables are indeed explained by the independent variables.

4.3.1 Privacy paradox verification

Following the regression that tries to explain the variations of the **Intention to disclose** information by **Privacy concerns**, the Privacy concerns variable had to be discarded because its p-value is too large ($p = 0.102 > 0.05$). This confirms the privacy paradox, which states that there is no link between Privacy concern and Intention to disclose data.

4.3.2 Relation between Kind of Survey and Perceived data-sensitivity

The p-value of the independent categorical variable **Kind of Survey** is less than 0.05 ($p = 0.015 < 0.05$). Since the p-value of the constant is also less than 0.05, we can determine that the relationship holds and that Kind of Survey has an impact on the **Perceived data-sensitivity** variable. However, the R^2 of the relationship is very low 4.28%. This indicates that the Kind of survey can only explain very little of the variations in Perceived data-sensitivity.

4.3.3 Relation between Drivers and Overall Trust in AI

4.3.3.1 First regression

We have included all the second order terms in the linear regression (all the independent variables taken 2 by 2 and multiplied together) as well as the second order variables (the variables multiplied by themselves). We conclude that the two variables that are suitable to keep are **Perceived data-sensitivity**, **Perceived data-sensitivity*Overall transparency in AI** and **Perceived data-sensitivity*Privacy concerns** because their p-value < 0,1. We then try the simple linear regression by keeping only the variables we decided to keep.

4.3.3.2 Second regression

The two independent variables **Perceived data-sensitivity** and **Perceived data-sensitivity * Overall transparency in AI** both have p-values below 0.05. The same is true for the constant. The p-value of **Perceived data-sensitivity*Privacy concerns** is too large (p=0.597 > 0.05). We have to discard it.

4.3.3.3 Final regression

P-values of the 2 independent variables are both < 0.01. We can therefore trust these variables as influencing the value of the dependent variable. The p-value of the constant is also sufficiently low so that we can be confident in the relationship posed by the linear regression.

The R^2 of the regression is 36,82%. This means that the equation created and the independent variables used explain 36,82% of the variation in the dependent variable.

Finally, let's analyse the coefficients of the variables in the equation. The coefficient of **Perceived data-sensitivity** is negative which is logical in relation to **Overall trust in AI**. Individuals will be more suspicious of AIs if they ask them for data that they consider to be more sensitive. The coefficient of **Perceived data-sensitivity*Overall transparency in AI** is positive. It is lower than that of Perceived data-sensitivity but the values of Perceived data-sensitivity*Overall transparency in AI can be much higher than those of Perceived data-sensitivity because Perceived data-sensitivity*Overall transparency in AI is the multiplication of 2 factors which can only be positive. This is also logical because depending on the sensitivity of the data perceived, Overall transparency in AI will have more or less effect on Overall trust in AI as it will be perceived as more or less important for individuals.

4.3.4 Relation between Overall Trust in AI and perceived risk

The link between **Overall trust in AI** and **Perceived risk** must be rejected because the p-value for Overall trust in AI is too large (p = 0.615 > 0.05). We cannot therefore trust this variable to explain the variation in the Perceived risks and therefore, we cannot validate this relationship. There is no verified relationship between Overall trust in AI and Perceived risk in the data we have collected.

4.3.5 Relationship between Perceived risks/benefits and Intention to disclose

4.3.5.1 First regression

We can see from this linear regression that we have included all the second order terms (all the independent variables taken 2 by 2 and multiplied together) as well as the second order variables (the variables multiplied by themselves). We will have to exclude the variables **Perceived benefits** and **Perceived benefits*Perceived benefits** because their p-values are too large (> 0.05). The p-value of Perceived benefits is 0.26 and that of Perceived benefits*Perceived benefits is 0.398. We can also see that the p-value of the constant is too

high (0.527 > 0.05). We need to inspect whether, by removing some variables, we can bring this value down enough to make this linear regression valid.

4.3.5.2 Second regression

We can then see that the p-values of the independent variables have dropped to acceptable levels (p < 0,05). However, the constant still has a too large p-value (0.269). We therefore need to try another regression to find another version of this regression that we can accept.

The p-value of the constant is still too high which invalidates the equation because the constant must be rejected. I try again by rejecting **Perceived risks*Perceived risks** because it is the independent variable with the highest p-value (p = 0,009).

4.3.5.3 Final regression

We finally arrive at a linear regression in which we can be confident. The independent variables and the constant have a sufficiently low p-value (<0.05).

The R^2 is 45.97%. The independent variables explain via the linear regression equation 45.97% of the variation of the independent variable.

We can then take a look at the values of the constant and the coefficients in the linear regression equation. First of all, the constant is relatively small (2.199). The lower the value of **Intention to disclose**, the more respondents agreed to disclose their information. Next, we see that the coefficient of **Perceived risks** is relatively high (0.7326). This means that the perception of risk greatly reduces the intention to disclose. Finally, we can see that the coefficient of **Perceived risks*Perceived benefits** is negative (-0,0828). It is lower than Perceived risks but Perceived risks*Perceived benefits can take higher values because it is the multiplication of 2 positive variables. This means that the influence of Perceived benefits on Intention to disclose is moderated by the value of Perceived risk. The greater the Perceived risk is, the greater is the impact of the Perceived benefit.

4.3.6 Relationship between Perceived risks and Perceived benefits

The p-values of the constant and the independent variable **Perceived risks** are <0.05. The relationship is therefore valid and perceived risks have an influence on **Perceived benefits**. The R^2 is 8.74%. The value of the constant is 5.428 and the coefficient of Perceived risks is -0.2696. This indicates that even if the relationship between Perceived risks and Perceived benefits exists, it is very weak. Variations in Perceived risks only slightly explain variations in Perceived benefits (8.74%) and the impact of Perceived risks on Perceived benefits is very small (-0.2696). However, it can be noted that the influence of the relationship is negative and the constant has a particular high value (5.428).

4.3.7 Relationship between Perceived data-sensitivity and Perceived risks

The p-values of the constant and the independent variable **Perceived data-sensitivity** are <0.05. The relationship is therefore valid and Perceived data-sensitivity has an influence on the **Perceived risks**. The R^2 is 21,78%. The value of the constant is 2,315 and the coefficient of Perceived data-sensitivity is 0,4992. This indicates that the relationship between Perceived data-sensitivity and Perceived risks exists and is relatively strong. Variations in Perceived data-sensitivity explains a non-negligible part of the variations in Perceived risks (21,78%) and the impact of Perceived data-sensitivity on Perceived risks is important (0,4992). The positive relationship between the two variables can be noted too.

4.3.8 Relationship between Perceived data-sensitivity and Perceived benefits

The p-value of the independent variable **Perceived data-sensitivity** (0,763) is greater than 0.05. The independent variable Perceived data-sensitivity must therefore be rejected from the relationship between it and **Perceived benefits**. There is therefore no relationship between these two variables.

4.3.9 Relationship between Privacy concerns and Perceived risks

The p-values of the constant and the independent variable **Privacy concerns** (0.001) are <0.05. The relationship is therefore valid and privacy concerns has an influence on the **Perceived risks**. The R^2 is 8.44%. The value of the constant is 2.987 and the coefficient of Privacy concerns is 0.3. This indicates that even if the relationship between Privacy concerns and Perceived risks exists, it is very weak. The variations in Privacy concerns only slightly explain the variations in Perceived risks (8.44%) and the impact of Privacy concerns on Perceived risks is very low (0.3). However, the positive relationship between the two variables can be noted.

4.4 MODERATOR VARIABLES

In this section, we will examine whether the moderator variables influence the relationship between Drivers and Overall trust in AI. To do this, we will carry out new regressions by including the moderator variables individually in this relationship between Drivers and Overall trust in AI.

4.4.1 Kind of survey

The **Kind of survey** variable which is a categorical variable containing the kind of survey answered by the participants does not provide any additional information. Its p-value is too high ($p = 0.389 > 0.05$). We must therefore reject it. This can be explained quite easily because the information from the questionnaire that the participants answered is already present in the variables **Perceived data-sensitivity** and **Perceived data-sensitivity*Overall transparency in AI**.

For further analysis, we will leave the data analysis tables in the appendix and focus on the conclusions if we have to exclude the influence of the moderator variable.

4.4.2 AI knowledge

AI knowledge is indeed an interesting moderator variable. The P-values of all the variables are sufficiently low ($p < 0.05$) and an increase in the R^2 can be noted (36,82% => 42,48%). It can be seen that the coefficient value of AI knowledge is positive which indicates that the more knowledge respondents have about AI, the more overall trust they have in AI.

4.4.3 AI self-efficacy

AI self-efficacy is indeed an interesting moderator variable. The P-values of all the variables are sufficiently low ($p < 0.05$) and an increase in the R^2 can be noted (36,82% => 42,41%). It can be seen that the value of the coefficient of AI self-efficacy is positive which indicates that participants who feel able to interact effectively with AIs have more overall trust in them.

4.4.4 AI self-efficacy and AI knowledge

It is interesting to ask whether there is a correlation between **AI Knowledge** and **AI self-efficacy** in view of the results of the influence of the two variables on the relationship between the **Drivers** and the respondents' **Overall trust in AI**.

We can therefore see a strong correlation between these two variables ($r = 0,842 > 0.6$). This tells us that these two variables follow almost the same variations through the data collected.

4.4.5 Gender

In the analysis, **Gender** did not show to be a value we can trust to help explain variations in **Overall trust in AI** ($p = 0,084 > 0,05$).

4.4.6 Revenue

The p-values of the **Revenue** categories did not show us that this variable is relevant to explain the variations in **Overall trust in AI** (p values > 0.05).

4.4.7 Profession

The p-values of the **Profession** categories did not show us that this variable is relevant to explain the variations in **Overall trust in AI** (p values > 0.05).

4.4.8 Education level

The p-values of the **Education level** categories did not show us that this variable is relevant to explain the variations in **Overall trust in AI** (p values > 0.05).

4.4.9 Age

The p-values of the **Age** categories did not show us that this variable is relevant to explain the variations in **Overall trust in AI** (p values > 0.05).

4.5 ADDITIONAL ANALYSES

Following the analysis of the results, theoretical consequences took place and further analysis was provided. These analyses inspect the links between the Kind of survey, Privacy concerns and Perceived sensitivity to data. They also look at the relationship between Kind of survey, Privacy concerns, Perceived data sensitivity and Perceived risks.

4.5.1 Relation between Privacy concerns, Kind of survey and Perceived data-sensitivity

The constant as well as the p-values for **Privacy concerns** and **Kind of survey** are all < 0.05. The relationship is therefore verified and the independent variables are influential on the Perceived data-sensitivity variable. The R^2 is 11.05%. This indicates that the relationship exists but has little influence on the **Perceived data-sensitivity** result. On the other hand, the coefficients indicate that the Perceived data-sensitivity is influenced upwards by the variables. It is greatly influenced by Kind of survey (0.519) and to a lesser extent by Privacy concerns (0.2559).

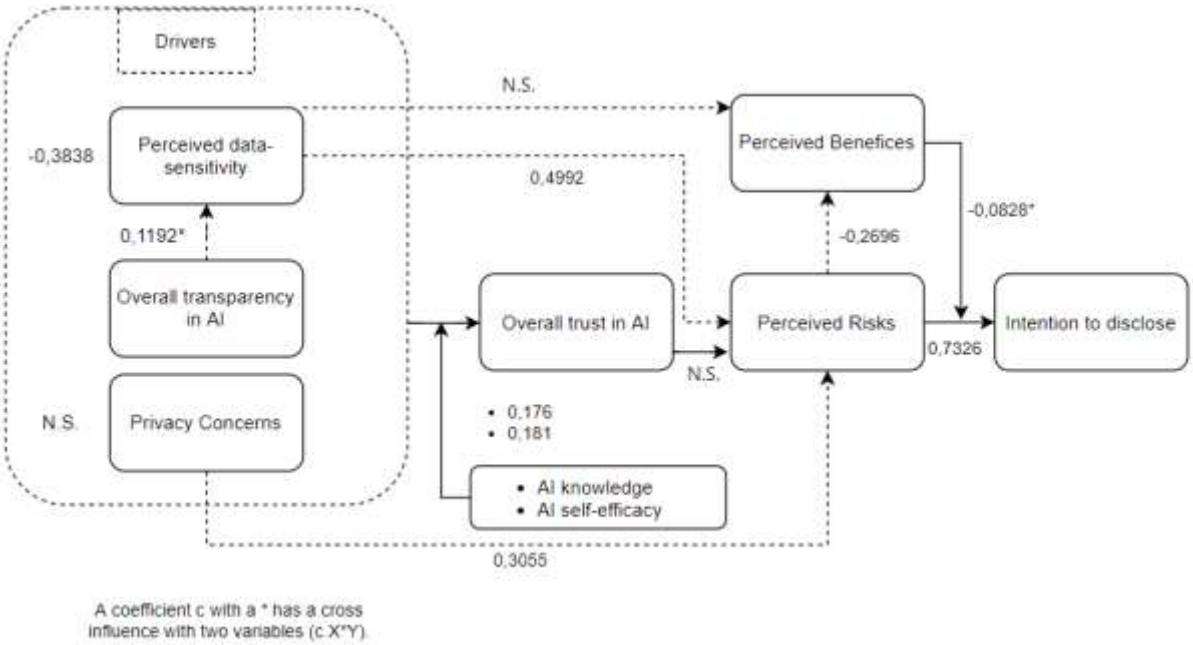
4.5.2 Relation between Privacy concerns, Kind of survey, Perceived data-sensitivity and Perceived risks

The constant and the independent variables all have p-values below 0.05. This indicates that the relationship is verified and that the independent variables (**Kind of survey**, **Privacy concerns**, **Perceived data-sensitivity**) influence the **Perceived risks**. The R^2 is 29.06%. This means that the established relationship explains a non-negligible part of the variation in Perceived risks (29.06%). The coefficients are all positive, which indicates that the independent variables positively influence the Perceived risks. The Kind of survey has a significant influence on the Perceived risks (0.546). The variable Perceived data-sensitivity has a relatively strong influence on Perceived risks (0.3984). The variable Perceived data-sensitivity has only a small influence on Perceived risks (0.2098).

4.5.3 Relation between Overall trust in AI and Perceived benefits

The p-value of the constant and the independent variable **Overall trust in AI** are less than 0.05. This means that the relationship is verified and that Overall trust in AI does have an influence on the **Perceived benefits**. The R^2 is 5.94%. This shows us that the relationship explains very little of the variation in Perceived benefits (5.94%). The coefficient on the independent variable is positive and not particularly high (0.306).

4.6 CORE MODEL WITH RESULTS



A coefficient c with a * has a cross influence with two variables (c X*Y).

5 DISCUSSION

5.1 SUMMARY OF HYPOTHESES RESULTS

Hypothesis	Result
H1: The overall transparency in AI positively influences the overall trust in AI.	Significant
H2: The perceived benefits positively influence the intention to disclose data.	Significant
H3: The perceived risks negatively influence the intention to disclose data.	Significant
H4: The perceived risks negatively influence the perceived benefits.	Significant
H5: A higher perceived data-sensitivity positively influences perceived risks.	Significant
H6: A higher perceived data-sensitivity negatively influences perceived benefits	Not-Significant
H7: A higher perceived data-sensitivity negatively influences overall trust in AI.	Significant
H8: The overall trust in AI negatively influences the perceived risks.	Not-Significant
H9: The privacy concerns negatively influence the overall trust in AI.	Not-Significant
H10: The privacy concerns positively influence the perceived risks.	Significant

5.2 DISCUSSION OF RESULTS

First of all, it is important to note that the conclusions drawn from the results cannot always be generalised. This is due to our sample. It is for example particularly young. The majority of respondents are under 30 years old. It is also of a particular socio-professional category. Most respondents are employees or students. It can also be noted that a large majority of them have a higher degree of education. Our sample therefore primarily represents young adults with a higher level of education. It will therefore be necessary to verify the results with a larger sample including more socio-demographic categories in order to be able to generalise the conclusions with confidence.

Secondly, one can develop a certain distrust of my construction of perceived sensitivity to data. This is due to the lack of due diligence on my part to check whether the data used was clearly sensitive or not for my participants. I relied in part on the data determined to be sensitive or not in the 2015 article by Kehr et al. In this article, the researchers determined sensitive or non-sensitive data based on a pre-questionnaire for a sample of Swiss and North American (USA) respondents. I felt that I could reuse the same data because the Swiss, North American and Belgian cultures are sufficiently similar.

One way to improve the quality of the sensitivity of the data submitted to the respondents would be to redo the survey using the same methodology as in the original article. This would allow the data to be adapted to the culture of the sample population.

This was partly seen in the descriptive analysis of the data. The average values of privacy concerns and perceived data-sensitivity are high. This shows a sensitivity to data and a high level of concern about their privacy. We can also see that participants also rated high values for perceived benefits and risks. This goes hand in hand with a slightly negative intention to disclose which shows that perceived risks have more influence than perceived benefits.

We then analysed the correlations between the drivers which showed an independence between them. This allowed us to analyse the first relationship in our model between the drivers and the respondents' overall trust in AI. This showed us that privacy concerns have no influence on overall trust in AI and that the effect of overall transparency in AI on overall trust in AI is through the filter of perceived sensitivity to data. This tells us that in order to improve the overall trust of individuals towards AI, it is more effective to act when the data requested is considered sensitive by the largest number of people.

According to the scientific literature, the perceived sensitivity of the data influences the perceived risks and benefits but also the overall trust in AI (Kehr and al., 2015). The only relationship that has not been verified in this literature is the relationship with perceived benefits. This can be explained by experimentation. Respondents faced an experiment representing a specific situation: a virtual driving coach. This situation could have been a hinder to the perception of benefits in view of my particularly young sample: they do not have a car, do not use a car, etc. A similar experiment with a more universal subject may improve the results regardless of the sample obtained.

The verification of the impact of transparency on trust is in line with the links developed in the literature between explanations (transparency) and trust (Dexe, J., Franke, U. & Rad, A., 2021). On the other hand, the impact of privacy concern on overall trust in AI has not been verified. This refer to the fact that the link between privacy concerns and overall trust of individuals is directed in different ways depending on the study. There is no fixed construction in the scientific literature between these two constructions (Wakefield, 2013, Bansal et al., 2010). Sometimes privacy concerns are posed as an antecedent to the overall trust. At other times it is placed as an outcome and at other times as two separate independent variables. It is therefore necessary to consider them as independent in view of

the results obtained. Privacy concerns also have an influence on the perceived risks, which is easily explained. Someone facing a data request will perceive more risk from the situation if he or she is generally concerned about privacy. This relation is verified in the data.

More generally, the elements influencing risk are Perceived data sensitivity, Privacy concerns and the Kind of survey. Perceived data sensitivity is itself influenced by the kind of survey and privacy concerns. This demonstrates the consistency of respondents' concerns about their privacy, the type of data they are asked to provide, their data sensitivity and their perceived risk of a situation.

For the relationship between drivers and overall trust in AI, we analysed the impact of moderating variables on it. Only two of them indicated a real impact on the relationship: AI Knowledge and AI self-efficacy. However, these variables were found to be highly correlated. This may be due to the fact that the two variables are very close in nature. Someone with knowledge about AIs will feel more able to interact effectively with it ("Dunning-Kruger effect" aside).

Next, we analysed the relationship between overall trust in AI and perceived risks. It turned out that this relationship does not appear in our data. There is no relationship between overall trust in AI and perceived risk in our data. This is in my view due to the type of variable that differs between them. Indeed, overall trust and transparency in AI were asked in a general way to the respondents during the questionnaire whereas risks follow the situation thanks to the experimentation. This changes the fact that we are moving from general opinions on AIs to an opinion on a specific situation that may have been "experienced" by the respondents. This is in line with the mistrust described in certain articles on the importance of impact of institutional trust (overall trust) on the privacy calculus (Malhotra and al., 2004, Bansal and al., 2010, Kehr and al. 2015). For these researchers, the impact of overall trust in AIs on privacy calculus is more likely to be found in the perceived benefits. This has been verified in the additional analyses but the influence is particularly weak in the data.

In my opinion, in order to be able to verify this relationship, which is posited in the scientific literature as existing (between trust and risk), it would be necessary to develop experimentation material that is closer to reality. A real application would be needed, offering users, after having provided their data, an AI result as well as feedback on how the data was used (explainable AI). This would allow the explanations to be varied, to see the impact on perceived transparency and to be able to ask for all the variables in a situational way. It would also require a larger sample size in order to have enough data in each sub-category (sensitive or non-sensitive data, levels of transparency). This would allow us to analyse the situational variables of transparency and trust. These would be much more interesting to analyse in the context of a process that is situation-based. Especially for the impact that situationally perceived trust can have on the privacy calculus (Dinev, Hart 2006, Dam and al. 2008).

The relationships that link perceived benefits and risks with intention to disclose was easy to demonstrate. All of the above variables are situational and form the core of the privacy calculus. To be more precise, the perceived risk does negatively influence the intention to disclose. Perceived benefit positively influences intention to disclose. The influence of perceived benefit is moderated by perceived risk. That is, if the perceived risk is high, the perceived benefit will have more influence on the intention to disclose. This is a good representation of the classical privacy calculus relationship with the relationship between risk and benefit and the relationship between risk, benefit and intention to disclose (Dinev, Hart 2006, Dam and al. 2008, Kehr and al. 2015).

6 CONCLUSION

The aim of my thesis was to highlight the link between the *explanation* of how personal data is used in an AI and the *readiness* of the user to disclose its data. To do so, I reviewed the literature to get an idea of the state of research regarding how the AI data use can be explained, to understand the known effects of explanation on trust and to understand the role of trust in the privacy calculus that results in the intention to disclose personal data or not.

After this step, I formulated a number of hypotheses and created a conceptual model respecting both the gathered theory and the assumptions made. I then created two surveys to collect data to test these hypotheses.

I then conducted a quantitative analysis of the data obtained in the 138 responses I received to 2 questionnaires (77 responses for the survey on sensitive data and 61 for the one on non-sensitive data).

Some hypotheses have been verified. The relationship between perceived data sensitivity, overall transparency in AI and overall trust in AI is confirmed. Amongst the drivers, only the privacy concerns did not influence the overall trust in AI. For privacy concerns, this echoes the fluctuating link between privacy concerns and overall trust (institutional trust) found in the literature. This means that, in our case, privacy concerns are not linked to overall trust in AI. This is in line with the part of the literature review detailing the link between transparency and trust. Explanations that improve the transparency of data use in the eyes of the customer will improve their trust in the predictions of the AI as well as in the AIs themself. This also follows the idea that transparency is even more important when handling user-sensitive data.

I also had the opportunity to check the links between the different constructs influencing perceived risks. Indeed, privacy concerns, perceived data sensitivity and the type of data respondents face all influence perceived risks. They are also linked because they influence perceived data sensitivity, apart from data sensitivity.

Another hypothesis that has been tested is the link between perceived risk, perceived benefits and intention to disclose information. Risk is obviously the most influential factor. The effect of perceived benefits on the intention to disclose is influenced by perceived risk. This is of course corroborated by the scientific literature, which assures us that the privacy calculus functions mainly around the perception of risk.

It is also interesting to note that AI self-efficacy and AI Knowledge play a role in the trust that users have in AI. This shows us that the ability, or perceived ability, to interact effectively with AIs has a positive impact on the overall trust that respondents have in AI.

All of this demonstrates what the literature has already shown us. The transparency of the operation of AIs when sensitive data is manipulated is all the more important to be

able to generate trust in AI among users. Risk is the main influence on the intention to transmit information. They are related to the sensitivity to data of people, the data they face and their privacy concerns. They also influence the effect of benefits on the intention to disclose information.

In essence, these are the two main concerns that practitioners need to anticipate when asking for sensitive data: “what is AI actually doing with this data?” and “what are the risks if I pass it on to you?”. The primary aim is to ensure trust and weaken risk by reducing the information gap created by this data request situation. To this end, XAIs can fill this information gap and help weaken user’s perception of risk by preventing them from filling the unknown with stereotypes.

For the researchers, this thesis corroborates the vision of privacy concerns and overall trust as two independent variables. It highlights aspects of the privacy calculus process that should not be overlooked: the knowledge of individuals on the subject, their self-efficacy on the subject and the sensitivity of the data they are dealing with. It also demonstrates the importance of individuals’ data sensitivity and transparency in the privacy calculus process.

6.1 LIMITATIONS

Unfortunately, I was not able to verify some assumptions. I was not able to establish a concrete link in my data between the explanations given about the data and the intention to disclose the data. This is due to the lack of verification of the relationship between overall trust in AIs and perceived risks following the experimentation. I think this is due to the difference in variable type (general >< situational). In my opinion, to be able to verify this relationship, the experiment would have to be repeated with more sophisticated experimentation equipment. A real application that uses AI with different XAIs. Different situations could be created: sensitivity of the data requested and XAI more or less advanced. This would allow to ask the users how much trust they have in the AI and how transparent they perceive this situation to be. This would help to confirm the model as a whole.

The basic sample is problematic if we wish to generalise our remarks. It is composed mainly of young adults who are mainly employed or still studying. This means that we need to repeat the experiment with people of more varied ages and occupations to ensure that this does not influence the final results. This will allow us to ensure that the results can be generalised.

7 BIBLIOGRAPHY

- Rai, A. Explainable AI: from black box to glass box. *J. of the Acad. Mark. Sci.* 48, 137–141 (2020).
- Chintagunta, P., Hanssens, D. M., & Hauser, J. R. (2016). Editorial—Marketing science and big data. Marketing Science, 35(3), 341–342.
- Jaap Wieringa, P.K. Kannan, Xiao Ma, Thomas Reutterer, Hans Risselada, Bernd Skiera, Data analytics in a privacy-concerned world, Journal of Business Research, Volume 122, 2021, Pages 915-925, ISSN 0148-2963.
- Wolfie, C. (2017). Corporate surveillance in everyday life. Vienna: Cracked Labs.
- Russell, Stuart, 2019, *Human Compatible: Artificial Intelligence and the Problem of Control*, New York: Viking.
- Hollebeek LD, Sprott DE, Brady MK. Rise of the Machines? Customer Engagement in Automated Service Interactions. *Journal of Service Research*. 2021;24(1):3-8.
- Bauer, K., Hinz, O., van der Aalst, W. *et al.* Expl(AI)n It to Me – Explainable AI and Information Systems Research. *Bus Inf Syst Eng* 63, 79–82 (2021).
- Federal Trade Commission (2014). Data brokers: A call for transparency and accountability.
- Farkhondeh Hassandoust, Saeed Akhlaghpour, Allen C Johnston, Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective, *Journal of the American Medical Informatics Association*, Volume 28, Issue 3, March 2021, Pages 463–471
- Huang M.; Rust R. (2020). *The Feeling Economy: How artificial intelligence is creating the era of empathy.* Switzerland: Palgrave Mcmillan.
- Shneider, Matthew J., Sharan Jagpal, Sachin Gupta, and Yan Yu (2017), "Protecting Customer Privacy when Marketing with Second-Party Data", *International Journal of Research in Marketing*, 34 (3), 593-603.
- Marca Tulio Ribeiro, Sameer Singh, and Carlos Guestrin, 2016. "Why Should I Trust You.": Explaining the Predictions of Any Classifier. *In Proceedings of the 22nd ACM SIGKDD International Conference on Kwowledge Discovery and Data Mining (KDD '16).* Association for Computiong Machinery, New York, USA, 1135-1144.
- Tamara Dinev, Paul Hart, 2006, An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research 17 (1)*, 61-80.
- Laufer, R. S., M. Wolfe. 1977. Privacy as a concept and a social issue:A multidimensional developmental theory. *J. Soc. Issues* 33(3), 22–42.
- Milne, G. R., M. J. Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *J. Interactive Marketing* 18(3) 15–29.

- McKnight, D. H., V. Choudhury, C. Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative topology. *Inform. Systems Res.* 13(3) 334–359.
- Mayer, R., J. H. Davis, F. D. Schoorman. 1995. An integrative model of organizational trust. *Acad. Management Rev.* 20(3) 709–734.
- Bunge, M., 1963. A General Black Box Theory. *Philosophy of Science*, Vol. 30, No. 4, pp. 346-358.
- Norman G. Vinson, Heather Molyneaux and Jean-Francois Lapointe., 2018, A review of the role of explanations for user acceptance in black box systems, *International Conferences Interfaces and Human Computer Interaction 2018,* National Research Council Canada, Ottawa, Ontario, Canada.
- Wolter Pieters, 2010, Explanation and trust: what to tell the user in security and AI?, *Ethics Inf Technol,* 13:53–64
- Molnar, C. (2020). Interpretable machine learning. Lulu. com.
- Kehr F., Kowatsch T., Wentzel D. and Fleisch E., 2015, Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus, *Information System Journal*, 25, 607-635.
- Hanoch, Y., 2002, "Neither an angel nor an ant": emotion as an aid to bounded rationality, *Journal of Economic Psychology*, 23, 1–25.
- Zajonc, R.B. (1980) Feeling and thinking - preferences need no inferences, *American Psychologist*, 35, 151–175.
- Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A., 2011, The effect of online privacy information on purchasing behavior: an experimental study, *Information Systems Research*, 22, 254–268.
- Brandimarte, L., Acquisti, A. & Loewenstein, G., 2012, Misplaced confidences: privacy and the control paradox, *Social Psychological and Personality Science*, 4, 340–347.
- Grimmelikhuijsen S., Herkes F., Leistikow I., Verkroost J., de Vries F., G. Zijlstra W., 2019, Can decision transparency increase citizen trust in regulatory agencies? Evidence from a representative survey experiment, *Regulation & Governance,* 17-31.
- Dexe, J., Franke, U. & Rad, A., 2021, Transparency and insurance professionals: a study of Swedish insurance practice attitudes and future development, *Geneva Pap Risk Insur Issues Pract*.
- Tang T., Tsai C., Wu W., 2005, The Relationships among Trust, E-Satisfaction, E-Loyalty, and Customer Online Behaviors, *Fifth International Conference on Electronic Business*, 788-794.
- Davis, F. D., 1989, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, Vol. 13:3, 319-339.
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government information quarterly*, *27*(3), 264-271.
- Naci Çoklar, A., & Ferhan Odabaşi, H. (2009). Educational Technology Standards Scale (ETSS) a study of reliability and validity for Turkish preservice teachers. *Journal of Computing in Teacher Education*, *25*(4), 135-142.
- Malhotra, N.K., Kim, S.S. & Agarwal, J. (2004) Internet users' information privacy concerns (IUIPC): tthe construct, the scale, and a causal model. Information Systems Research, 15, 336–355.

- Xie, E., Teo, H.-H. & Wan, W. (2006) Volunteering personal information on the Internet: effects of reputation, privacy notices, and rewards on online consumer behavior. Marketing Letters, 17, 61–74
- Dinev, T., Xu, H., Smith, J.H. & Hart, P. (2012) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22, 61–80.
- Anderson, C.L. & Agarwal, R. (2011) The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Information Systems Research, 22, 469–490.
- Lazić, Milica; Jovanović, Veljko; Gavrilov-Jerković, Vesna (2018). The general self-efficacy scale: New evidence of structural validity, measurement invariance, and predictive properties in relationship to subjective well-being in Serbian samples. Current Psychology, (), –.
- Sherer, Mark; Maddux, James E.; Mercandante, Blaise; Prentice-Dunn, Steven; Jacobs, Beth; Rogers, Ronald W. (1982). The Self-Efficacy Scale: Construction And Validation. , 51(2), 663–671.
- Yim, Chi Kin (Bennett); Chan, Kimmy Wa; Lam, Simon S.K (2012). *Do Customers and Employees Enjoy Service Participation? Synergistic Effects of Self- and Other-Efficacy. Journal of Marketing, 76(6), 121-140.*
- Naci Çoklar, A., & Ferhan Odabaşi, H. (2009). Educational Technology Standards Scale (ETSS) a study of reliability and validity for Turkish preservice teachers. *Journal of Computing in Teacher Education*, *25*(4), 135-142.
- Sailer, M., Stadler, M., Botes, E. *et al.* Science knowledge and trust in medicine affect individuals' behavior in pandemic crises. *Eur J Psychol Educ* (2021).
- van Esch, P., Cui, Y. (G.), & Jain, S. P. (2021). Self-efficacy and callousness in consumer judgments of AI-enabled checkouts. *Psychol Mark*, 38, 1081– 1100.
- Mothersbaugh, D. L.; Foxx, W. K.; Beatty, S. E.; Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research, 15(1), 76–98.
- Malhotra, Naresh K.; Kim, Sung S.; Agarwal, James (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355.
- Bansal, G., Zahedi, F.M. & Gefen, D. (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decision Support Systems, 49, 138–150.
- Wakefield, R. (2013) The influence of user affect in online information disclosure, Journal of Strategic Information Systems, 22, 157–174.
- Dan J. Kim; Donald L. Ferrin; H. Raghav Rao (2008). *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. , 44(2), 544–564.*

8 APPENDIX

8.1 SURVEYS

Etape 1 : Informations générales

Bonjour à toutes et à tous,

Dans le cadre de mon mémoire en ingénieur de gestion en finalité Data Science à l'université de Namur, je réalise une enquête sur la vie privée et les IA.

Dans notre monde connecté, les IA jouent un rôle de plus en plus important car elles sont intégrées dans notre manière de consommer. Pour fonctionner celles-ci nous demandent toujours de plus en plus d'informations. Coupler à une compréhension limitée de comment elle fonctionne, cela peut poser problème aux consommateurs. Lors de cette enquête, je souhaiterai en connaitre davantage l'impact que cette compréhension partielle à sur notre volonté de partager des informations personnelles.

Le questionnaire durera approximativement 10 min. L'anonymité vous est garanti. Les réponses que vous fournirez ne serons utilisé que dans le cadre de mon mémoire.

Un grand merci d'avance pour votre participation.

Pour toutes questions vous pouvez me contacter via l'adresse mail suivante : nicolas.wuyts@student.unamur.be

Etape 2 : Interaction avec les IA

Q1 : Avez-vous déjà interagit avec une IA (service ou produit en contenant) au cours du mois passé qui se trouve dans la liste ci-dessous ?

- Assistant de conduite, voiture autonome.
- Recommandations pour du shopping en ligne.
- Un assistant virtuel (Siri, Alexa …)
- Des assistants virtuels (Chats bots par exemple)
- Des recommandations Facebook (amis, fil d'actualité, etc.)
- Des recommandations de recherches de navigateur (Google, Firefox …)
- Des filtres de spam d'e-mail
- De la reconnaissance faciale
- D'autres types d'IA
- Aucune IA à ma connaissance.

Si un participant répond « Aucune IA à ma connaissance », le questionnaire se termine alors là pour ce participant.

Merci pour votre participation.

Si un participant répond toutes autres réponses, un message explicatif leur est transmis.

Pour que vous puissiez avoir une vision plus étendue des IA, il est important que vous ayez une vision de ce à quoi peut ressembler une IA. Tous les exemples que vous avez pu voir à l'exemple précédent possède une partie gérée par une IA. Ces IA effectuent des prédictions (recommandations, filtres, etc.) ou des décisions (reconnaissance faciale servant de mot de passe). Ces IA permettent à ces outils d'effectuer certaines actions de réflexions proches de l'homme (reconnaitre un visage, reconnaitre des sons, faire des recommandations, etc.) Il n'est donc pas impossible puisque ces IA ne sont pas visibles à première vue que vous interagissiez avec elles sans le savoir.

Q2 : À quelle fréquence pensez-vous interagir avec des IA contenu dans des produits/services ?

- Plus de 2 fois par jour
- Une fois par jour
- 2 à 3 fois par semaine
- Une fois par semaine
- Une fois tous les 2 mois
- Une fois par an
- Moins d'une fois par an
- Presque jamais

Etape 3 : Collecte de données sur des variables générales (AI knowledge, AI self-efficacy, Privacy concerns, Perceived transparency, AI perceived trust)

Q3 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord
Je peux expliquer le fonctionnement des produits/services d'IA.							
Je peux utiliser les produits/services d'IA de différentes manières.							
Je peux faire des choses de base concernant la technologie de l'IA.							
Je peux expliquer des concepts généraux liés à la technologie de l'IA.							
Je peux utiliser efficacement les produits/services d'IA.							

Q4 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord

J'ai confiance en ma capacité à utiliser l'IA efficacement.							
Je ne doute pas de ma capacité à utiliser l'IA de manière efficace.							
J'ai d'excellentes compétences et aptitudes dans le domaine de l'IA.							
Je suis fier de mes compétences et de mes capacités dans le domaine de l'IA.							

Q5 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord
Par rapport aux autres, je suis plus sensible à la manière dont les services/produits d'IA traitent mes informations personnelles.							
Pour moi, le plus important est de préserver ma vie privée face aux services/produits d'IA.							
En général, je suis très préoccupé par les menaces qui pèsent sur ma vie privée.							

Q6 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord
Le produit/service d'IA me permet de suivre mes activités.							
Le produit/service d'IA fournit des informations sur ses décisions et ses actions.							
Le produit/service d'IA fournit des informations sur ses règles et règlements.							
Le produit/service d'IA diffuse de l'information sur sa propre performance.							
Globalement, le produit/service IA a une transparence accrue sur ce qu'il fait.							

Q7 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du	2	3	4	5	6	7. Tout à

	tout d'accord						fait d'accord
Les produits/services d'IA interagissent avec moi de manière compétente et efficace.							
Les produits/services d'IA remplissent très bien tous leurs rôles.							
Dans l'ensemble, les produits/services d'IA sont capables et compétents.							
Les produits/services d'IA sont honnêtes avec moi.							
Je qualifierais les produits/services d'IA comme étant honnêtes.							
Les produits/services d'IA sont sincères et authentiques.							

Etape 4 : Expérimentation

Pour la suite des questions vous répondrez en fonction d'une situation précise représenté par l'image que vous retrouverez dessous.

L'application représenté est une application utilisant une IA qui a pour but de vous donner des conseils pour améliorer votre conduite. Pour ce faire, l'IA suit votre comportement de conduite afin de vous fournir un retour d'information personnalisé sur votre style de conduite.

Si la personne est face au questionnaire contenant les données sensibles, la fin de la* expérimentation *et la question 8 seront :

Q8 : Dans quelle mesure estimez-vous que les informations demandées par l'IA sont sensibles ?

	1. Pas du tout sensible	2	3	4	5	6	7. Très sensible.
Localisation							
Violation de vitesse potentielle							
Temps de trajet							

Si la personne est face au questionnaire contenant les données sensibles, la fin de la* expérimentation *et la question 8 seront :

Q8 : Dans quelle mesure estimez-vous que les informations demandées par l'IA sont sensibles ?

	1. Pas du tout sensible	2	3	4	5	6	7. Très sensible.
Année de construction de la voiture							
Le type de la voiture							
La distance parcourue							

Q9 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord
La communication de mes informations personnelles au service d'IA comporte des avantages.							
Révéler mes informations personnelles au service d'IA m'aidera à obtenir les services que je souhaite.							
Je crois qu'à la suite de la divulgation de mes informations personnelles, je bénéficierai d'un service meilleur et plus personnalisé.							

Q10 : Sur une échelle de 1 à 7, "1" étant pas du tout d'accord et "7 " tout à fait d'accord, veuillez indiquer dans quelle mesure vous êtes d'accord avec les propositions suivantes :

	1. Pas du tout d'accord	2	3	4	5	6	7. Tout à fait d'accord
Il serait risqué de donner des informations personnelles au service d'IA.							
Le risque d'atteinte à la vie privée lié à la communication d'informations personnelles au service d'IA est élevé.							
Les informations personnelles pourraient être utilisées de manière inappropriée en utilisant le service d'IA.							
Fournir au service d'IA mes informations personnelles pourrait entraîner de nombreux problèmes inattendus.							

Q 11: Veuillez préciser dans quelle mesure vous révèleriez vos informations personnelles pour utiliser le service AI

Volontiers	1	2	3	4	5	6	7	Réticent
Possible	1	2	3	4	5	6	7	Impossible
Probable	1	2	3	4	5	6	7	Improbable

Etape 5 : Positionnement socio-démographique

Q12 : Vous êtes un(e) :

- Homme
- Femme

Q13 : Dans quelle tranche d'âge vous situez-vous ?

- 18 ans ou moins
- 19-25
- 26-30
- 31-35
- 36-40
- 41-45
- 46-50
- 51-55
- 56-60
- Plus de 60 ans

Q14 : Quel est votre niveau d'éducation ?

- Primaire
- Secondaire inférieur
- Secondaire supérieur
- Supérieur non universitaire
- Universitaire
- Doctorat
- Autre

Q15 : Quelle est votre profession actuelle ?

- Etudiant(e)
- Indépendant(e)
- Cadre
- Employé(e)
- Ouvrier(ère)
- Profession libérale
- Pensionné(e)
- Chercheur d'emploi
- Personne au foyer
- Autre (précisez)

Q16 : Dans quelle tranche de revenu vous situez-vous ? (revenu mensuel)

- Moins de 1499 €
- Entre 1500 et 1999 €
- Entre 2000 et 2499 €
- Entre 2500 et 2999 €
- Entre 3000 et 3499 €
- Plus de 3500 €

Merci pour votre participation !

8.2 QUANTITATIVE ANALYSIS

8.2.1 Descriptive analysis

8.2.1.1 Items

Statistiques

Variable	Moyenne	ErT moyenne	EcTyp	Minimum	Maximum
AIK1	3,906	0,136	1,593	1,000	7,000
AIK2	4,761	0,112	1,316	1,000	7,000
AIK3	3,819	0,143	1,680	1,000	7,000
AIK4	3,877	0,148	1,736	1,000	7,000
AIK5	4,217	0,125	1,464	1,000	7,000
ASE1	3,812	0,130	1,521	1,000	7,000
ASE2	3,848	0,136	1,602	1,000	7,000
ASE3	2,826	0,126	1,479	1,000	7,000
ASE4	2,833	0,126	1,478	1,000	7,000
PCO1	4,080	0,133	1,566	1,000	7,000
PCO2	4,855	0,121	1,422	2,000	7,000
PCO3	4,406	0,136	1,597	2,000	7,000
TRA1	4,304	0,121	1,417	1,000	7,000
TRA2	3,239	0,127	1,487	1,000	7,000
TRA3	3,355	0,122	1,429	1,000	7,000
TRA4	3,174	0,123	1,439	1,000	7,000
TRA5	2,4493	0,0937	1,1012	1,0000	7,0000
TRU1	4,2246	0,0903	1,0604	1,0000	7,0000
TRU2	4,2899	0,0971	1,1412	2,0000	7,0000
TRU3	4,4783	0,0915	1,0754	2,0000	7,0000
TRU4	2,986	0,101	1,184	1,000	7,000
TRU5	2,928	0,101	1,182	1,000	7,000
TRU6	2,7464	0,0981	1,1530	1,0000	7,0000
SENS1	4,701	0,170	1,487	1,000	7,000
SENS2	3,688	0,179	1,575	1,000	7,000
SENS3	3,442	0,172	1,509	1,000	7,000
SENS4	4,156	0,157	1,377	1,000	7,000
SENS5	5,481	0,177	1,553	1,000	7,000
SENS6	3,279	0,228	1,781	1,000	7,000
SENS7	3,787	0,221	1,724	1,000	7,000
SENS8	4,295	0,226	1,764	1,000	7,000
BEN1	4,261	0,107	1,252	1,000	7,000
BEN2	4,304	0,117	1,370	1,000	7,000
BEN3	4,203	0,118	1,389	1,000	7,000
RIS1	4,297	0,121	1,421	1,000	7,000
RIS2	4,348	0,131	1,536	1,000	7,000
RIS3	4,710	0,129	1,510	1,000	7,000
RIS4	4,029	0,128	1,504	1,000	7,000
ITD1	4,449	0,114	1,335	1,000	7,000
ITD2	3,558	0,106	1,244	1,000	7,000
ITD3	3,659	0,114	1,343	1,000	7,000

8.2.1.1.1 Sensitive data (SEME = SENS 1-5) and Non-Sensitive data (SENSNS = SENS 6-8)

Statistiques

Variable	Moyenne	ErT moyenne	EcTyp	Minimum	Maximum
SEME	4,2935	0,0967	0,8489	2,2000	7,0000
SENSNS	3,787	0,196	1,530	1,000	7,000

8.2.1.2 Socio-demographics variables

8.2.1.2.1 Gender

Lignes : 41. Vous etes :

	Dénombrement	% de colonne
Un homme	52	37,68
Une femme	86	62,32
Total	138	100,00

8.2.1.2.2 Age

Lignes : AgeCat

	Dénombrement	% de colonne
18 ans ou moins	5	3,623
19-25	57	41,304
26-30	34	24,638
31-35	12	8,696
36-40	5	3,623
41-45	3	2,174
46-50	4	2,899
51-55	11	7,971
56-60	3	2,174
Plus de 60 ans	4	2,899
Total	138	100,000

8.2.1.2.3 Education

Lignes : Education Level

	Dénombrement	% de colonne
Autre	1	0,725
Doctorat	3	2,174
Secondaire inferieur	5	3,623
Secondaire superieur	11	7,971
Superieur non universitaire	38	27,536
Universitaire	80	57,971
Total	138	100,000

8.2.1.2.4 Profession

Lignes : Profession

	Dénombrement	% de colonne
Autre (precisez)	2	1,449
Cadre	8	5,797
Chercheur d'emploi	13	9,420
Employe(e)	62	44,928
Etudiant(e)	43	31,159
Independant(e)	2	1,449
Ouvrier(ere)	3	2,174
Pensionne(e)	3	2,174
Personne au foyer	1	0,725
Profession liberale	1	0,725
Total	138	100,000

8.2.1.2.5 Revenue

Lignes : RevenueCat

	Dénombrement	% de colonne
Entre 1500 et 1999	29	21,01
Entre 2000 et 2499	29	21,01
Entre 2500 et 2999	18	13,04
Entre 3000 et 3499	3	2,17
Moins de 1499	50	36,23
Plus de 3500	9	6,52
Total	138	100,00

8.2.1.3 Constructs

Statistiques

Variable	Moyenne	ErT moyenne	EcTyp	Minimum	Maximum
SEMEM	4,070	0,104	1,220	1,000	7,000
AIKM	3,955	0,114	1,337	1,000	7,000
ASEM	3,330	0,116	1,366	1,000	7,000
PCOM	4,447	0,106	1,241	2,000	7,000
TRAM	3,0543	0,0896	1,0523	1,0000	7,0000
TRUM	3,4855	0,0808	0,9492	1,4000	7,0000
BENM	4,256	0,101	1,190	1,000	7,000
RISM	4,346	0,111	1,305	1,000	7,000
ITDM	3,8888	0,0991	1,1644	1,0000	7,0000

8.2.2 Factorial analysis

8.2.2.1 Factors and communalities

8.2.2.1.1 Drivers

Saturations de facteurs et communalités avec rotations

Rotation varimax

Variable	Facteur1	Facteur2	Communalité
PCO1	0,096	0,734	0,548
PCO2	0,078	0,828	0,692
PCO3	-0,001	0,853	0,728
TRA1	0,600	0,155	0,384
TRA2	0,785	-0,039	0,618
TRA3	0,829	-0,078	0,694
TRA4	0,689	0,226	0,527
TRA5	0,702	0,032	0,494
Variance	2,6485	2,0370	4,6855
% variance	0,331	0,255	0,586

We have to remove TRA1.

Saturations de facteurs et communalités avec rotations

Rotation varimax

Variable	Facteur1	Facteur2	Communalité
PCO1	0,046	-0,730	0,534
PCO2	0,091	-0,835	0,705
PCO3	-0,007	-0,855	0,731
TRA2	0,769	0,027	0,593
TRA3	0,838	0,061	0,706
TRA4	0,704	-0,242	0,554
TRA5	0,760	-0,056	0,581
Variance	2,3783	2,0268	4,4050
% variance	0,340	0,290	0,629

8.2.2.2 Factors and Cronbach's alpha

8.2.2.2.1 Privacy concerns

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
PCO1	0,739	0,546
PCO2	0,845	0,713
PCO3	0,852	0,725
Variance	1,9847	1,9847
% variance	0,662	0,662

Alpha de Cronbach

Alpha
0,7397

8.2.2.2.2 Transparency

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
TRA2	0,760	0,578
TRA3	0,829	0,687
TRA4	0,727	0,528
TRA5	0,764	0,584
Variance	2,3777	2,3777
% variance	0,594	0,594

Alpha de Cronbach

Alpha
0,7661

8.2.2.2.3 Overall trust in AI

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
TRU1	0,621	0,386
TRU2	0,788	0,621
TRU3	0,740	0,547
TRU4	0,854	0,730
TRU5	0,858	0,736
TRU6	0,851	0,724
Variance	3,7432	3,7432
% variance	0,624	0,624

We have to remove TRU1.

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
TRU2	0,744	0,553
TRU3	0,708	0,501
TRU4	0,890	0,793
TRU5	0,894	0,800
TRU6	0,886	0,785
Variance	3,4325	3,4325
% variance	0,687	0,687

Alpha de Cronbach

Alpha
0,8845

8.2.2.2.4 Perceived benefits

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
BEN1	0,888	0,789
BEN2	0,889	0,790
BEN3	0,893	0,798
Variance	2,3766	2,3766
% variance	0,792	0,792

Alpha de Cronbach

Alpha
0,8845

8.2.2.2.5 Perceived risks

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
RIS1	0,851	0,723
RIS2	0,894	0,800
RIS3	0,875	0,766
RIS4	0,875	0,765
Variance	3,0539	3,0539
% variance	0,763	0,763

Alpha de Cronbach

Alpha
0,8967

8.2.2.2.6 Intention to disclose

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
ITD1	0,846	0,716
ITD2	0,896	0,804
ITD3	0,928	0,861
Variance	2,3813	2,3813
% variance	0,794	0,794

Alpha de Cronbach

Alpha
0,8687

8.2.2.2.7 AI self-efficacy

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
ASE1	0,908	0,824
ASE2	0,878	0,771
ASE3	0,907	0,822
ASE4	0,902	0,814
Variance	3,2318	3,2318
% variance	0,808	0,808

Alpha de Cronbach

Alpha
0,9200

8.2.2.2.8 AI knowledge

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
AIK1	0,836	0,699
AIK2	0,683	0,467
AIK3	0,772	0,596
AIK4	0,859	0,738
AIK5	0,772	0,596
Variance	3,0956	3,0956
% variance	0,619	0,619

We have to remove AIK2 because its communality is below 0,5.

Saturations de facteurs et communalités sans rotations

Variable	Facteur1	Communalité
AIK1	0,873	0,762
AIK3	0,780	0,608
AIK4	0,903	0,816
AIK5	0,736	0,542
Variance	2,7267	2,7267
% variance	0,682	0,682

Alpha de Cronbach

Alpha
0,8429

8.2.2.3 Correlation between Drivers (constructs)

Corrélation

	TRAM	PCOM
PCOM	0,117	
SEMEM	0,151	0,256

8.2.3 Verification of hypotheses

8.2.3.1 Privacy paradox verification

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,335	0,368	9,06	0,000	
PCOM	0,1245	0,0798	1,56	0,121	1,00

8.2.3.2 Relation between Kind of Survey and data-sensitivity

DONNÉES COMPILÉES (M).CSV

Analyse de régression : SEMEM en fonction de Questionnaire

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

SEMEM = 4,294 + 0,0 Questionnaire_1 - 0,506 Questionnaire_2

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	4,294	0,137	31,45	0,000	
Questionnaire					
2	-0,506	0,205	-2,47	0,015	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,19797	4,28%	3,58%	1,26%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	8,730	8,730	6,08	0,015
Questionnaire	1	8,730	8,730	6,08	0,015
Erreur	136	195,179	1,435		
Total	137	203,909			

Ajustements et diagnostics pour les observations aberrantes

Observation	SEMEM	Valeur ajustée	Résiduelle	Val. résid. norm.	
37	7,000	4,294	2,706	2,27	R
78	1,000	3,787	-2,787	-2,35	R
84	1,000	3,787	-2,787	-2,35	R
98	1,000	3,787	-2,787	-2,35	R
101	7,000	3,787	3,213	2,70	R
102	1,000	3,787	-2,787	-2,35	R
115	1,000	3,787	-2,787	-2,35	R
118	7,000	3,787	3,213	2,70	R
127	1,000	3,787	-2,787	-2,35	R
135	1,000	3,787	-2,787	-2,35	R

R : Valeur résiduelle élevée

8.2.3.3 Relation between Drivers and overall trust in AI

8.2.3.3.1 First regression

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	4,71	1,04	4,55	0,000	
SEMEM	-0,481	0,296	-1,62	0,107	30,65
TRAM	0,083	0,291	0,29	0,775	22,09
PCOM	-0,422	0,382	-1,10	0,272	52,88
SEMEM*SEMEM	-0,0276	0,0319	-0,87	0,388	21,86
TRAM*TRAM	0,0071	0,0474	0,15	0,881	28,05
PCOM*PCOM	0,0036	0,0436	0,08	0,935	55,90
SEMEM*TRAM	0,0926	0,0511	1,81	0,073	25,49
SEMEM*PCOM	0,0854	0,0444	1,92	0,057	35,11
TRAM*PCOM	-0,0037	0,0561	-0,07	0,948	34,97

8.2.3.3.2 Second regression

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,513	0,235	14,96	0,000	
SEMEM	-0,3495	0,0963	-3,63	0,000	3,26
SEMEM*TRAM	0,1203	0,0137	8,79	0,000	1,83
SEMEM*PCOM	-0,0067	0,0127	-0,53	0,597	2,87

8.2.3.3.3 Final regression

Equation de régression

TRUM = 3,543 - 0,3838 SEMEM + 0,1192 SEMEM*TRAM

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,760029	36,82%	35,89%	33,95%

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,543	0,227	15,60	0,000	
SEMEM	-0,3838	0,0711	-5,40	0,000	1,79
SEMEM*TRAM	0,1192	0,0135	8,85	0,000	1,79

8.2.3.4 Relation between overall trust in AI and perceived risks

Equation de régression

RISM = 4,553 - 0,059 TRUM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	4,553	0,425	10,70	0,000	
TRUM	-0,059	0,118	-0,50	0,615	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,30850	0,19%	0,00%	0,00%

8.2.3.5 Relationship between perceived Risk/Benefit and Intention to disclose

8.2.3.5.1 First regression

Equation de régression

ITDM = -0,94 + 1,713 RISM + 0,546 BENM - 0,0853 RISM*RISM - 0,0380 BENM*BENM
- 0,1351 RISM*BENM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	-0,94	1,49	-0,63	0,527	
RISM	1,713	0,383	4,48	0,000	47,75
BENM	0,546	0,483	1,13	0,260	63,35
RISM*RISM	-0,0853	0,0339	-2,52	0,013	31,00
BENM*BENM	-0,0380	0,0448	-0,85	0,398	38,96
RISM*BENM	-0,1351	0,0433	-3,12	0,002	16,01

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,845552	49,19%	47,27%	41,52%

8.2.3.5.2 Second regression

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	0,697	0,627	1,11	0,269	
RISM	1,504	0,301	5,00	0,000	29,61
RISM*RISM	-0,0844	0,0321	-2,63	0,009	27,86
RISM*BENM	-0,0892	0,0133	-6,70	0,000	1,52

8.2.3.5.3 Final regression

Equation de régression

ITDM = 2,199 + 0,7326 RISM - 0,0828 RISM*BENM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	2,199	0,267	8,25	0,000	
RISM	0,7326	0,0684	10,71	0,000	1,47
RISM*BENM	-0,0828	0,0134	-6,19	0,000	1,47

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,862266	45,97%	45,16%	42,58%

8.2.3.6 Relation between perceived risks and benefits

DONNÉES COMPILÉES (M).CSV

Analyse de régression : BENM en fonction de RISM

Equation de régression

BENM = 5,428 - 0,2696 RISM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	5,428	0,339	16,01	0,000	
RISM	-0,2696	0,0747	-3,61	0,000	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,14129	8,74%	8,07%	5,35%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	16,96	16,958	13,02	0,000
RISM	1	16,96	16,958	13,02	0,000
Erreur	136	177,14	1,303		
Inadéquation de l'ajustement	21	44,66	2,127	1,85	0,022
Erreur pure	115	132,48	1,152		
Total	137	194,10			

Ajustements et diagnostics pour les observations aberrantes

Observation	BENM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	1,000	3,541	-2,541	-2,27	R
37	7,000	3,541	3,459	3,09	R
38	6,670	4,215	2,455	2,16	R
84	4,000	5,158	-1,158	-1,04	X
97	2,000	4,889	-2,889	-2,57	R
101	7,000	4,484	2,516	2,22	R
102	7,000	5,091	1,909	1,71	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.3.7 Relation between perceived data-sensitivity and perceived risks

DONNÉES COMPILÉES (M).CSV

Analyse de régression : RISM en fonction de SEMEM

Equation de régression

RISM = 2,315 + 0,4992 SEMEM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	2,315	0,345	6,72	0,000	
SEMEM	0,4992	0,0811	6,15	0,000	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,15835	21,78%	21,20%	19,14%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	50,81	50,810	37,87	0,000
SEMEM	1	50,81	50,810	37,87	0,000
Erreur	136	182,48	1,342		
Inadéquation de l'ajustement	27	32,75	1,213	0,88	0,634
Erreur pure	109	149,73	1,374		
Total	137	233,29			

Ajustements et diagnostics pour les observations aberrantes

Observation	RISM	Valeur ajustée	Résiduelle	Val. résid. norm.	
37	7,000	5,809	1,191	1,05	X
45	2,500	4,810	-2,310	-2,01	R
60	7,000	4,211	2,789	2,42	R
78	2,750	2,814	-0,064	-0,06	X
84	1,000	2,814	-1,814	-1,61	X
98	3,500	2,814	0,686	0,61	X
101	3,500	5,809	-2,309	-2,04	R X
102	1,250	2,814	-1,564	-1,39	X
103	2,500	4,810	-2,310	-2,01	R
115	3,500	2,814	0,686	0,61	X
118	3,750	5,809	-2,059	-1,82	X
120	7,000	3,647	3,353	2,92	R
127	2,000	2,814	-0,814	-0,72	X
135	3,000	2,814	0,186	0,17	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.3.8 Relation between perceived data-sensitivity and perceived benefits

DONNÉES COMPILÉES (M).CSV

Analyse de régression : BENM en fonction de SEMEM

Equation de régression

BENM = 4,359 - 0,0253 SEMEM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	4,359	0,355	12,27	0,000	
SEMEM	-0,0253	0,0836	-0,30	0,763	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,19426	0,07%	0,00%	0,00%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	0,130	0,1302	0,09	0,763
SEMEM	1	0,130	0,1302	0,09	0,763
Erreur	136	193,972	1,4263		
Inadéquation de l'ajustement	27	42,088	1,5588	1,12	0,333
Erreur pure	109	151,884	1,3934		
Total	137	194,103			

Ajustements et diagnostics pour les observations aberrantes

Observation	BENM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	1,000	4,202	-3,202	-2,72	R
37	7,000	4,182	2,818	2,42	R X
38	6,670	4,253	2,417	2,03	R
78	4,000	4,334	-0,334	-0,29	X
84	4,000	4,334	-0,334	-0,29	X
98	6,000	4,334	1,666	1,43	X
101	7,000	4,182	2,818	2,42	R X
102	7,000	4,334	2,666	2,29	R X
115	4,000	4,334	-0,334	-0,29	X
118	2,670	4,182	-1,512	-1,30	X
127	3,330	4,334	-1,004	-0,86	X
135	4,000	4,334	-0,334	-0,29	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.3.9 Relation between privacy concerns and perceived risks

DONNÉES COMPILÉES (M).CSV

Analyse de régression : RISM en fonction de PCOM

Equation de régression

RISM = 2,987 + 0,3055 PCOM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	2,987	0,398	7,50	0,000	
PCOM	0,3055	0,0863	3,54	0,001	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,25324	8,44%	7,77%	5,08%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	19,69	19,686	12,53	0,001
PCOM	1	19,69	19,686	12,53	0,001
Erreur	136	213,60	1,571		
Inadéquation de l'ajustement	14	14,95	1,068	0,66	0,813
Erreur pure	122	198,66	1,628		
Total	137	233,29			

Ajustements et diagnostics pour les observations aberrantes

Observation	RISM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	7,000	4,109	2,891	2,32	R
53	7,000	4,109	2,891	2,32	R
57	6,500	4,005	2,495	2,00	R
82	7,000	3,598	3,402	2,76	R
84	1,000	3,598	-2,598	-2,11	R
97	2,000	4,616	-2,616	-2,10	R
102	1,250	5,025	-3,775	-3,06	R

R : Valeur résiduelle élevée

8.2.4 Additional analyses

8.2.4.1 Relation between Privacy concerns, Kind of survey and Perceived data-sensitivity

DONNÉES COMPILÉES (M).CSV

Analyse de régression : SEMEM en fonction de PCOM; Questionnaire

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

Questionnaire	
1	SEMEM = 3,161 + 0,2559 PCOM
2	SEMEM = 2,642 + 0,2559 PCOM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,161	0,377	8,38	0,000	
PCOM	0,2559	0,0798	3,20	0,002	1,00
Questionnaire					
2	-0,520	0,199	-2,61	0,010	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,15911	11,05%	9,73%	6,43%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	2	22,531	11,265	8,38	0,000
PCOM	1	13,801	13,801	10,27	0,002
Questionnaire	1	9,183	9,183	6,83	0,010
Erreur	135	181,378	1,344		
Inadéquation de l'ajustement	29	44,934	1,549	1,20	0,245
Erreur pure	106	136,444	1,287		
Total	137	203,909			

Ajustements et diagnostics pour les observations aberrantes

Observation	SEMEM	Valeur ajustée	Résiduelle	Val. résid. norm.	
78	1,000	3,581	-2,581	-2,25	R
98	1,000	3,410	-2,410	-2,11	R
101	7,000	4,177	2,823	2,47	R
102	1,000	4,349	-3,349	-2,95	R
115	1,000	3,665	-2,665	-2,32	R
118	7,000	4,433	2,567	2,27	R
127	1,000	3,837	-2,837	-2,47	R
135	1,000	4,006	-3,006	-2,62	R

R : Valeur résiduelle élevée

8.2.4.2 *Relation between Privacy concerns, Kind of survey, Perceived data-sensitivity and Perceived risks*

DONNÉES COMPILÉES (M).CSV

Analyse de régression : RISM en fonction de SEMEM; PCOM; Questionnaire

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

Questionnaire	
1	RISM = 2,033 + 0,3984 SEMEM + 0,2098 PCOM
2	RISM = 1,487 + 0,3984 SEMEM + 0,2098 PCOM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	2,033	0,446	4,56	0,000	
SEMEM	0,3984	0,0825	4,83	0,000	1,12
PCOM	0,2098	0,0794	2,64	0,009	1,08
Questionnaire					
2	-0,547	0,195	-2,80	0,006	1,05

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,11133	29,06%	27,47%	23,94%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	3	67,792	22,597	18,30	0,000
SEMEM	1	28,786	28,786	23,31	0,000
PCOM	1	8,623	8,623	6,98	0,009
Questionnaire	1	9,675	9,675	7,83	0,006
Erreur	134	165,498	1,235		
Inadéquation de l'ajustement	113	141,071	1,248	1,07	0,448
Erreur pure	21	24,427	1,163		
Total	137	233,290			

Ajustements et diagnostics pour les observations aberrantes

Observation	RISM	Valeur ajustée	Résiduelle	Val. résid. norm.	
53	7,000	4,795	2,205	2,00	R
60	7,000	4,666	2,334	2,12	R
82	7,000	4,030	2,970	2,77	R
102	1,250	3,285	-2,035	-1,93	X
120	7,000	3,600	3,400	3,10	R

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.4.3 Relation between Overall trust in AI and Perceived benefits

DONNÉES COMPILÉES (M).CSV

Analyse de régression : BENM en fonction de TRUM

Equation de régression

BENM = 3,191 + 0,306 TRUM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,191	0,377	8,47	0,000	
TRUM	0,306	0,104	2,93	0,004	1,00

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
1,15866	5,94%	5,25%	2,99%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	1	11,52	11,525	8,58	0,004
TRUM	1	11,52	11,525	8,58	0,004
Erreur	136	182,58	1,342		
Inadéquation de l'ajustement	21	21,24	1,011	0,72	0,804
Erreur pure	115	161,34	1,403		
Total	137	194,10			

Ajustements et diagnostics pour les observations aberrantes

Observation	BENM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	1,000	3,741	-2,741	-2,40	R
30	2,000	4,475	-2,475	-2,15	R
37	7,000	5,330	1,670	1,53	X
38	6,670	3,986	2,684	2,33	R
97	2,000	4,413	-2,413	-2,09	R
101	7,000	3,986	3,014	2,62	R
102	7,000	3,986	3,014	2,62	R

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5 Moderating variables

8.2.5.1 Drivers – Trust relation

8.2.5.1.1 Kind of survey

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,663	0,251	14,60	0,000	
SEMEM	-0,4010	0,0727	-5,52	0,000	1,87
Questionnaire					
2	-0,149	0,134	-1,12	0,266	1,05
SEMEM*TRAM	0,1205	0,0135	8,92	0,000	1,80

8.2.5.1.2 AI knowledge

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; AIKM

Equation de régression

TRUM = 2,921 - 0,3634 SEMEM + 0,1760 AIKM + 0,1067 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	2,921	0,277	10,54	0,000	
SEMEM	-0,3634	0,0683	-5,32	0,000	1,80
AIKM	0,1760	0,0485	3,63	0,000	1,09
SEMEM*TRAM	0,1067	0,0133	8,00	0,000	1,91

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,727882	42,48%	41,19%	38,80%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	3	52,436	17,4787	32,99	0,000
SEMEM	1	14,979	14,9795	28,27	0,000
AIKM	1	6,987	6,9871	13,19	0,000
SEMEM*TRAM	1	33,912	33,9124	64,01	0,000
Erreur	134	70,995	0,5298		
Inadéquation de l'ajustement	131	69,195	0,5282	0,88	0,663
Erreur pure	3	1,800	0,6000		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
19	1,600	3,150	-1,550	-2,18	R
23	1,800	1,506	0,294	0,43	X
37	7,000	6,840	0,160	0,26	X
58	5,200	3,627	1,573	2,19	R
76	5,200	3,283	1,917	2,66	R
78	3,800	3,808	-0,008	-0,01	X
79	1,400	3,605	-2,205	-3,06	R
98	5,400	3,670	1,730	2,45	R
111	2,400	2,610	-0,210	-0,31	X
115	2,400	4,216	-1,816	-2,64	R X
119	5,000	5,316	-0,316	-0,47	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.3 AI self-efficacy

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; ASEM

Equation de régression

TRUM = 3,058 - 0,3526 SEMEM + 0,1810 ASEM + 0,0998 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,058	0,256	11,95	0,000	
SEMEM	-0,3526	0,0687	-5,13	0,000	1,81
ASEM	0,1810	0,0502	3,61	0,000	1,21
SEMEM*TRAM	0,0998	0,0140	7,14	0,000	2,09

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,728320	42,41%	41,12%	38,24%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	3	52,351	17,4502	32,90	0,000
SEMEM	1	13,974	13,9744	26,34	0,000
ASEM	1	6,902	6,9016	13,01	0,000
SEMEM*TRAM	1	27,024	27,0238	50,95	0,000
Erreur	134	71,080	0,5304		
Inadéquation de l'ajustement	131	70,720	0,5398	4,50	0,119
Erreur pure	3	0,360	0,1200		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	1,800	1,672	0,128	0,19	X
37	7,000	6,746	0,254	0,41	X
58	5,200	3,551	1,649	2,30	R
76	5,200	3,244	1,956	2,71	R
78	3,800	3,846	-0,046	-0,07	X
79	1,400	3,503	-2,103	-2,92	R
98	5,400	3,729	1,671	2,37	R
111	2,400	2,439	-0,039	-0,06	X
115	2,400	4,372	-1,972	-2,91	R X
119	5,000	5,408	-0,408	-0,61	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.4 AI knowledge and AI self-efficacy

Corrélation

	AIKM
ASEM	0,842

8.2.5.1.5 Gender

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de TRAM; SEMEM; GENDERS

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

GENDERS	
0	TRUM = 3,683 - 0,3737 SEMEM + 0,1163 TRAM*SEMEM
1	TRUM = 3,451 - 0,3737 SEMEM + 0,1163 TRAM*SEMEM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,683	0,239	15,38	0,000	
SEMEM	-0,3737	0,0708	-5,28	0,000	1,80
GENDERS					
1	-0,232	0,134	-1,74	0,084	1,02
TRAM*SEMEM	0,1163	0,0135	8,63	0,000	1,81

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,754397	38,22%	36,83%	34,26%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	3	47,170	15,7232	27,63	0,000
SEMEM	1	15,843	15,8434	27,84	0,000
GENDERS	1	1,720	1,7205	3,02	0,084
TRAM*SEMEM	1	42,384	42,3843	74,47	0,000
Erreur	134	76,261	0,5691		
Inadéquation de l'ajustement	118	70,881	0,6007	1,79	0,092
Erreur pure	16	5,380	0,3363		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
23	1,800	1,855	-0,055	-0,08	X
37	7,000	6,764	0,236	0,36	X
52	5,600	3,989	1,611	2,16	R
59	2,800	4,433	-1,633	-2,20	R
76	5,200	3,213	1,987	2,67	R
79	1,400	3,761	-2,361	-3,18	R
98	5,400	3,426	1,974	2,70	R
111	2,400	2,224	0,176	0,24	X
119	5,000	5,569	-0,569	-0,81	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.6 Age

DONNÉES COMPLÉTÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; AgeCat

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

AgeCat	
18 ans ou moins	TRUM = 3,303 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
19-25	TRUM = 3,560 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
26-30	TRUM = 3,715 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
31-35	TRUM = 3,234 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
36-40	TRUM = 3,645 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
41-45	TRUM = 4,208 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
46-50	TRUM = 4,188 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
51-55	TRUM = 3,537 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
56-60	TRUM = 3,826 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM
Plus de 60 ans	TRUM = 2,910 - 0,4145 SEMEM + 0,1261 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,303	0,429	7,70	0,000	
SEMEM	-0,4145	0,0728	-5,69	0,000	1,92
AgeCat					
19-25	0,257	0,363	0,71	0,481	7,83
26-30	0,412	0,373	1,10	0,272	6,34
31-35	-0,069	0,402	-0,17	0,864	3,15
36-40	0,342	0,493	0,69	0,489	2,08
41-45	0,905	0,557	1,62	0,107	1,61
46-50	0,885	0,512	1,73	0,086	1,81
51-55	0,234	0,414	0,57	0,572	3,08
56-60	0,523	0,565	0,93	0,357	1,86
Plus de 60 ans	-0,393	0,522	-0,75	0,453	1,88
SEMEM*TRAM	0,1261	0,0142	8,89	0,000	2,03

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,750638	42,48%	37,46%	31,14%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	11	52,435	4,7669	8,46	0,000
SEMEM	1	18,254	18,2536	32,40	0,000
AgeCat	9	6,986	0,7763	1,38	0,205
SEMEM*TRAM	1	44,509	44,5089	78,99	0,000
Erreur	126	70,996	0,5635		
Inadéquation de l'ajustement	118	68,606	0,5814	1,95	0,156
Erreur pure	8	2,390	0,2988		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
11	5,000	4,243	1,357	2,03	R
22	3,400	3,303	0,097	0,16	X
30	4,200	3,632	0,568	0,93	X
37	7,000	6,510	0,490	0,79	X
43	3,200	3,171	0,029	0,05	X
44	3,800	3,808	-0,008	-0,01	X
52	5,600	4,088	1,512	2,12	R
59	2,800	4,490	-1,690	-2,31	R
66	5,600	3,991	1,609	2,17	R
72	2,000	2,571	-0,571	-0,88	X
76	5,200	3,010	2,190	2,95	R
79	1,400	3,622	-2,222	-3,01	R
87	4,600	5,197	-0,597	-1,00	X
98	5,400	4,152	1,248	1,96	X
100	4,000	4,367	-0,367	-0,57	X
101	2,600	2,690	-0,090	-0,15	X
102	2,600	2,968	-0,368	-0,58	X
118	3,800	3,934	-0,134	-0,22	X
119	5,000	5,544	-0,544	-0,84	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.7 Education level

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; Education Level

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

Education Level	
Autre	TRUM = 3,736 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM
Doctorat	TRUM = 3,497 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM
Secondaire inferieur	TRUM = 3,813 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM
Secondaire superieur	TRUM = 3,144 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM
Superieur non universitaire	TRUM = 3,524 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM
Universitaire	TRUM = 3,606 - 0,3940 SEMEM + 0,1217 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,736	0,810	4,61	0,000	
SEMEM	-0,3940	0,0729	-5,40	0,000	1,87
Education Level					
Doctorat	-0,239	0,884	-0,27	0,788	3,95
Secondaire inferieur	0,077	0,837	0,09	0,927	5,81
Secondaire superieur	-0,592	0,799	-0,74	0,460	11,12
Superieur non universitaire	-0,212	0,775	-0,27	0,785	28,48
Universitaire	-0,130	0,772	-0,17	0,867	34,45
SEMEM*TRAM	0,1217	0,0137	8,89	0,000	1,84

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,762202	38,81%	35,52%	*

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	7	47,907	6,8439	11,78	0,000
SEMEM	1	16,964	16,9645	29,20	0,000
Education Level	5	2,458	0,4916	0,85	0,519
SEMEM*TRAM	1	45,899	45,8994	79,01	0,000
Erreur	130	75,524	0,5810		
Inadéquation de l'ajustement	116	70,957	0,6117	1,88	0,091
Erreur pure	14	4,567	0,3262		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.		
11	5,600	4,744	0,856	1,27		X
37	7,000	6,730	0,270	0,42		X
49	2,600	3,507	-0,907	-1,47		X
52	5,600	4,366	1,234	1,82		X
59	2,800	4,297	-1,497	-2,01	R	
66	5,600	3,589	2,011	2,78	R	
70	3,400	3,248	0,152	0,24		X
76	5,200	3,101	2,099	2,78	R	
79	1,400	3,218	-1,818	-2,52	R	
98	5,400	3,577	1,823	2,46	R	
99	1,400	3,086	-1,686	-2,51	R	X
101	2,600	2,758	-0,158	-0,24		X
106	4,000	4,246	-0,246	-0,36		X
112	3,600	2,845	0,755	1,22		X
114	4,200	4,200	0,000	*		X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.8 Profession

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; Profession

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

Profession	
Autre (precisez)	TRUM = 4,066 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Cadre	TRUM = 3,472 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Chercheur d'emploi	TRUM = 3,713 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Employe(e)	TRUM = 3,620 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Etudiant(e)	TRUM = 3,542 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Independant(e)	TRUM = 3,589 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Ouvrier(ere)	TRUM = 3,366 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Pensionne(e)	TRUM = 3,487 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Personne au foyer	TRUM = 3,687 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM
Profession liberale	TRUM = 4,019 - 0,3878 SEMEM + 0,1162 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	4,066	0,605	6,72	0,000	
SEMEM	-0,3878	0,0782	-4,96	0,000	2,04
Profession					
Cadre	-0,594	0,618	-0,96	0,339	4,73
Chercheur d'emploi	-0,353	0,596	-0,59	0,555	6,87
Employe(e)	-0,446	0,563	-0,79	0,429	17,73
Etudiant(e)	-0,524	0,567	-0,92	0,357	15,62
Independant(e)	-0,477	0,798	-0,60	0,551	2,06
Ouvrier(ere)	-0,700	0,716	-0,98	0,331	2,47
Pensionne(e)	-0,579	0,717	-0,81	0,421	2,48
Personne au foyer	-0,379	0,975	-0,39	0,698	1,55
Profession liberale	-0,05	1,09	-0,04	0,966	1,94
SEMEM*TRAM	0,1162	0,0163	7,14	0,000	2,48

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,780536	37,81%	32,38%	*

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	11	46,667	4,2425	6,96	0,000
SEMEM	1	14,995	14,9948	24,61	0,000
Profession	9	1,218	0,1354	0,22	0,991
SEMEM*TRAM	1	31,019	31,0194	50,92	0,000
Erreur	126	76,764	0,6092		
Inadéquation de l'ajustement	115	74,514	0,6479	3,17	0,019
Erreur pure	11	2,250	0,2045		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
22	3,400	2,982	0,418	0,66	X
37	7,000	7,000	0,000	*	X
51	3,600	3,083	0,517	0,81	X
52	5,600	3,853	1,747	2,78	R X
55	3,600	3,807	-0,207	-0,38	X
66	5,600	3,990	1,610	2,09	R
76	5,200	3,183	2,017	2,70	R
79	1,400	3,757	-2,357	-3,18	R
98	5,400	3,580	1,820	2,42	R
99	1,400	2,641	-1,241	-1,96	X
101	2,600	2,600	0,000	*	X
102	2,600	3,535	-0,935	-1,49	X
112	3,600	3,393	0,207	0,38	X
114	4,200	3,974	0,226	0,41	X
120	2,600	3,106	-0,506	-0,80	X
136	4,000	4,226	-0,226	-0,41	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante

8.2.5.1.9 Revenue

DONNÉES COMPILÉES (M).CSV

Analyse de régression : TRUM en fonction de SEMEM; TRAM; RevenueCat

Méthode

Codage des prédicteurs de catégorie (1; 0)

Equation de régression

RevenueCat	
Entre 1500 et 1999	TRUM = 3,748 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM
Entre 2000 et 2499	TRUM = 3,572 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM
Entre 2500 et 2999	TRUM = 3,718 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM
Entre 3000 et 3499	TRUM = 3,861 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM
Moins de 1499	TRUM = 3,479 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM
Plus de 3500	TRUM = 3,686 - 0,4072 SEMEM + 0,1216 SEMEM*TRAM

Coefficients

Terme	Coeff	Coef ErT	Valeur de T	Valeur de p	FIV
Constante	3,748	0,287	13,06	0,000	
SEMEM	-0,4072	0,0758	-5,37	0,000	2,00
RevenueCat					
Entre 2000 et 2499	-0,177	0,201	-0,88	0,382	1,59
Entre 2500 et 2999	-0,030	0,230	-0,13	0,896	1,42
Entre 3000 et 3499	0,113	0,465	0,24	0,808	1,08
Moins de 1499	-0,270	0,184	-1,47	0,145	1,84
Plus de 3500	-0,063	0,303	-0,21	0,836	1,32
SEMEM*TRAM	0,1216	0,0140	8,71	0,000	1,89

Récapitulatif du modèle

S	R carré	R carré (ajust)	R carré (prév)
0,765280	38,32%	35,00%	29,88%

Analyse de la variance

Source	DL	SomCar ajust	CM ajust	Valeur F	Valeur de p
Régression	7	47,296	6,7566	11,54	0,000
SEMEM	1	16,904	16,9037	28,86	0,000
RevenueCat	5	1,847	0,3694	0,63	0,677
SEMEM*TRAM	1	44,470	44,4704	75,93	0,000
Erreur	130	76,135	0,5857		
Inadéquation de l'ajustement	120	73,085	0,6090	2,00	0,113
Erreur pure	10	3,050	0,3050		
Total	137	123,431			

Ajustements et diagnostics pour les observations aberrantes

Observation	TRUM	Valeur ajustée	Résiduelle	Val. résid. norm.	
26	4,900	3,924	0,976	1,41	X
37	7,000	6,793	0,207	0,33	X
69	2,800	3,641	-0,841	-1,35	X
76	5,200	2,917	2,283	3,02	R
79	1,400	3,521	-2,121	-2,82	R
98	5,400	3,643	1,757	2,48	R
99	1,400	2,986	-1,586	-2,13	R
109	3,600	3,635	-0,035	-0,06	X

R : Valeur résiduelle élevée
X : Valeur de X aberrante